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

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ
НДІ ТЕЛЕКОМУНІКАЦІЙ

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

14-18 квітня 2025 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

Nineteenth International Scientific Conference
"MODERN CHALLENGES IN TELECOMMUNICATIONS"

and

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

April 14-18, 2025

Conference proceedings

Kyiv

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

XIX Міжнародна науково-технічна конференція "Перспективи телекомунікацій" ПТ-2025: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2025. – с.417.

XIX International Scientific Conference "Modern Challenges in Telecommunications" MCT-2025. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2025 – p. .417.

XVII науково-технічна конференція студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» ПРІТС 2025: Збірник тез конференції. К.: КПІ ім. Ігоря Сікорського, 2025.

Збірник містить матеріали пленарних і секційних доповідей, представлених на Дев'ятнадцятій міжнародній науково-технічній конференції "Перспективи телекомунікацій" (ПТ 2025) та Сімнадцятій науково-технічній конференції студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» (ПРІТС 2025), дати проведення 14-18 квітня 2025 р. в м. Києві.

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

на https://journals.uran.ua/ за посиланням

https://conferenc-journal.its.kpi.ua/issue/archive (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*

Голова 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;

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, 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, Львів;
ЛЕМЕШКО О.В. - д.т.н., проф., ХНУРЕ, Харків;
ЛИСЕНКО О.І. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ЛУНТОВСЬКИЙ А.О. - Prof. at BA Dresden University, Дрезден, Німеччина;
МАКСИМОВ В.В. - к.т.н., доц. КПІ ім. Ігоря Сікорського, Київ;
МІНОЧКІН Д.А. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
МОШИНСЬКА А.В. - д.т.н., проф., 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., в.о. директора НН ІТС КПІ ім. І.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. - д.т.н., НЦ «МАН України», Київ;
ТЕНШИ Хара - Dr.-Eng. Technical University of Dresden, Дрезден, Німеччина;
ТОЛЮПА С.В. – д.т.н., проф., НУ ім. Т. Шевченка, Київ;
ТРУБІН О.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
УРИВСЬКИЙ Л.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ФЕЛЬДМАНН Маріус - Dr.-Eng. Technical University of Dresden, Дрезден, Німеччина;
ЧУМАЧЕНКО С.М. - д.т.н., с.н.с., НУХТ, Київ;
ШПІЛЬНЕР Йозеф - Dr. at ZHAW School of Engineering, Цюріх, Вінтертур, Швейцарія;
ЯВІСЯ В.С. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
ЯКОРНОВ Є.А. - к.т.н., проф., КПІ ім. Ігоря Сікорського, Київ.

Технічний комітет:

Дуля Ю.А. – головний бухгалтер НДІ ТК.
Березовська О.В. – реєстрація, забезпечення документообігу.
Мікляєв О.В. – технічне обслуговування.
Іванова Т.Л. – оформлення конференції на сайті НН ІТС.
Головай О.М. – технік І категорії.
Остапенко М.Ю. – реєстрація, забезпечення документообігу

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, Закриття конференції: м. Київ, пров. Індустріальний, 2, корпус 30, ауд. 602) та дистанційно (за допомогою on-line сервісів для відеоконференцій та вебінарів ZOOM та MEET).

ЗМІСТ

Пленарні доповіді

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:

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:

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:

Секція 4. Інформаційні технології в телекомунікаціях

Співголови:

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

Доповідачі:

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:

Сімнадцята 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:

Вітання

Виступ на відкритті
XIX Міжнародної науково-технічної конференції
«Перспективи телекомунікацій»

15 квітня 2025 р.

Сергій СТІРЕНКО
проректор з наукової роботи КПІ ім. Ігоря Сікорського,
д.т.н., професор

Шановні колеги, вітаю вас на відкритті XIX Міжнародної науково-технічної конференції «Перспективи телекомунікацій»!

Конференція «Перспективи телекомунікацій» вже дев'ятнадцятий рік поспіль проводиться на базі Навчально-наукового інституту телекомунікаційних систем. НН ІТС за змістом навчально-наукової діяльності був організований на засадах поєднання наукових досліджень і змісту навчання за новою для незалежної України спеціальністю в галузі телекомунікацій.

Результативність поєднання науки і навчання підтверджується фактом що в середовищі НН ІТС успішно працюють 15 лауреатів Державних премій в галузі науки і техніки України, в тому числі 5 стали лауреатами в 2004 році за виконання конкурсної роботи зі створення супутникової інформаційно-комунікаційної системи України з використанням мікрохвильових технологій і обчислювальних засобів. І сьогодні ця традиція має тенденцію до продовження оскільки 2025 році Ректорат і Вчена рада КПІ ім. Ігоря Сікорського подали на здобуття Національної премії ім. Бориса Патона ще одну роботу «Створення радіотехнічних систем з використанням тропосферних технологій та засобів електронних комунікацій». Учасниками цієї роботи є три науково-педагогічні працівники ІТС.

Нещодавно ректорат подав пропозицію до МОН України стосовно створення на базі НДІ Телекомунікацій науково-консультаційного центру «Зв'язок та навігація». Подібні центри будуть створені згідно рішення держави для приведення системи організації наукових досліджень у вищих навальних закладах до світових стандартів.

Фахівці НН ІТС і НДІ Телекомунікацій успішно виконують престижні наукові проекти Наукової ради НАТО «Наука заради миру та безпеки» “3D Метаматеріали для збирання енергії та електромагнітного зондування” і Національного Фонду Досліджень України «Мікрохвильові пристрої на основі резонансних структур з метаматеріальними властивостями для захисту життєдіяльності та інформаційної безпеки України».

12 квітня на черговий конкурс НФД України з виконання прикладних наукових досліджень і розробок, спрямованих на зміцнення обороноздатності та безпеки України подано проект, який стосується розвитку нового принципу побудови мікрохвильових частотно-вибіркових пристроїв наступного покоління та їх практичного застосування в ударних дронах.

Огляд напрямів виступів на конференції «Перспективи телекомунікацій-2025» вказує на те, що тематика конференції є дійсно сучасною оскільки відповідає світовим пріоритетам досліджень в галузі телекомунікацій. Серед них:

- технології 5G і 6G,
- системи Інтернету речей,
- застосування штучного інтелекту,
- дослідження метаматеріалів та їх застосування в телекомунікаціях.

Також важливою є представницька широка участь студентів НН ІТС як в конференції «Перспективи телекомунікацій-2025» так і у спеціально створеній для них сімнадцятій науково-технічній конференції студентів та аспірантів «Перспективи розвитку інформаційнотелекомунікаційних технологій та систем», яка проводиться як секція конференції «Перспективи телекомунікацій-2025».

Тож, вітаю з початком роботи XIX Міжнародної науково-технічної конференції «Перспективи телекомунікацій»!

СВІТОВІ ПРІОРИТЕТИ СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Виступ на відкритті
XIX Міжнародної науково-технічної конференції
«Перспективи телекомунікацій»

15 квітня 2025 р.

Михайло ІЛЬЧЕНКО
академік НАНУ, д.т.н., професор

Практичне використання інформаційно-комунікаційних технологій (ІКТ) впродовж останніх років стало науково-технічним базисом здійснення цифрової трансформації України і реалізації дистанційної діяльності суспільства. ІКТ є визначеними на державному рівні одним із пріоритетних напрямів розвитку науки і техніки, за яким здійснюються наукові дослідження в Україні. Стосовно світових пріоритетів зазначимо, що вони визначені першим в історії повністю віртуальним Всесвітнім Мікрохвильовим Конгресом, який спонсорувався IEEE MTT-S і відбувся в травні 2024 року. Рішеннями цього Конгресу до світових пріоритетів віднесені такі:

- Інтелектуальні 6G: пристрої, схеми і системи, а також їхні антени і матеріали;
- Штучний Інтелект в випробуваннях і вимірюваннях;
- Метаматеріальні поверхні та зондування ТГц;
- Квантові технології та інші.

Галузь ІКТ продовжує розвиватися винятково динамічно. І це необхідно враховувати при вдосконаленні змісту навчання наших студентів і організації наукових досліджень науково-педагогічними та іншими працівниками. Тому за моєї ініціативи в ІТС запроваджено інформаційний проект «Телеком-новини», завдяки якому упродовж календарного року викладачі, науковці, аспіранти та студенти мають можливість майже щоденно знайомитись з новинами, що розташовуються на сайтах інституту та деканату ІТС.

Всього за останній період ознайомлено з понад 2000 новинами, в тому числі майже 400 упродовж 2024 р. Як керівник проекту «Телеком-новини» дякую моїм колегам Ірині Кононовій, Ірині Кравчук, Вікторії Сєвєрєній за професійну участь у здійсненні проекту.

https://www.its.kpi.ua/uk/infotelecom_news

Зміст новин у нас диференційовано за такими напрямами:

- Електронні комунікації в Україні;
- Нові покоління мобільного зв'язку 5G і 6G;
- Супутникові телекомунікаційні технології;
- Системи Інтернету речей;
- Штучний інтелект в телекомунікаціях.

Наведемо окремі приклади сучасних новин і їхні першоджерела, інформацію про які організатори проекту отримали насамперед упродовж січня – березня 2025 року:

Глобальне впровадження 5G
https://iotbusinessnews.com/

- Світова індустрія бездротових телекомунікацій досягла історичної віхи у 2024 році - кількість підключень 5G у всьому світі досягла 2,25 мільярда.
- Глобальні підключення 5G: 1,5 бездротових з'єднань на людину в усьому світі до кінця 2024 року.
- Лідери – Північна та Латинська Америки, Китай.

Вплив 5G на розвиток IoT-пристроїв:
що очікувати в найближчі роки
https://expert.com.ua/

- У *2024* році було додано *438 мільйонів нових підключень* IoT, що збільшило загальну кількість у всьому світі до 3,6 мільярда.
- *5G* – це революційна технологія, здатна забезпечити швидкість передачі даних *до 20 Гбіт/с* і мінімальну затримку сигналу.
- 5G і IoT не просто змінюють окремі пристрої – вони трансформують цілі галузі та впливають на спосіб життя. І хоча шлях до повного розкриття цього потенціалу може зайняти кілька років, уже зараз видно, як ці технології роблять наше життя зручнішим, безпечнішим і цікавішим.

Samsung Electronics представила нову білу книгу 6G
https://www.rcrwireless.com/

- Нова технологія має покращити повсякденне життя споживача, зокрема, *XR-можливості* (розширену реальність) у розвагах, охороні здоров'я та науці.
- 6G покращить *масовий зв'язок*, забезпечуючи постійне з'єднання між безліччю пристроїв, датчиками, машинами та терміналами, а також зв'язок між наземними та супутниковими мережами і технологію Fixed Wireless Access.
- Це буде здійснено за допомогою використання *ШІ* у різних сегментах мережі *6G*.

6G вже близько: японські вчені встановили рекорд швидкості бездротового фотонного зв'язку

https://internetua.com/

- Науковці з Японії підняли планку швидкості бездротового зв'язку на безпрецедентний рівень. Їм вдалося домогтися швидкості передачі даних 240 Гбіт/с по одному цифровому каналу, що є революційним досягненням.
- Проблема полягала у зменшенні перешкод і фазового шуму, які можуть впливати на продуктивність багаторівневої модуляції сигналу на надвисоких швидкостях.
- Саме цю проблему вирішила команда з Університету Осаки. Вчені створили систему зв'язку на частоті 300 ГГц з генератором сигналу в приймачі і передавачі, що включає цифрову обробку сигналів для демодуляції сигналу і підвищення швидкості передачі даних. Цей інноваційний підхід значно зменшив фазовий шум, подолавши обмеження, які перешкоджали зв'язку на частоті 300 ГГц.

SpaceX готує нову антену Starlink, у 5 разів швидшу за нинішні моделі

https://itechua.com/

- SpaceX працює над створенням нової антени для Starlink, яка зможе передавати дані зі швидкістю до 1 Гбіт/с. Для досягнення таких результатів SpaceX планує оновити своє супутникове угруповання та розширити використання частотного діапазону для супутникового інтернету.
- Завдяки цим оновленням Starlink зможе стати серйозним конкурентом традиційним оптоволоконним мережам.
- SpaceX уже представила нову потужну плоску антену для бізнес-користувачів.

Революція WI-FI: коли в Україні з’явиться надшвидкий інтернет майбутнього

https://ysc.kiev.ua/

- З розвитком технологій зростає потреба у швидкому та стабільному бездротовому інтернеті. Wi-Fi 7 обіцяє вирішити цю проблему.
- Wi-Fi 7 (IEEE 802.11be) - це новий стандарт бездротового зв’язку, що забезпечує значно вищу швидкість, менші затримки та покращену стабільність підключення.
- Масове впровадження очікується уже в цьому році, коли нові маршрутизатори та гаджети почнуть широко підтримувати новий стандарт. Для повної реалізації переваг Wi-Fi 7 потрібні сумісний маршрутизатор і пристрої (смартфони, ноутбуки, телевізори).

Vodafone здійснив перший у світі відеодзвінок через супутниковий зв'язок

https://processer.media/

- Vodafone здійснив перший у світі відеодзвінок через супутниковий зв'язок зі стандартного смартфона та планує запустити цю технологію наприкінці 2025 – на початку 2026 року.
- Технологія дозволить користувачам у зонах без мобільного зв'язку здійснювати відеодзвінки, користуватися інтернетом і онлайн-сервісами без необхідності у спеціальному обладнанні.
- Смартфони з підтримкою 4G і 5G зможуть автоматично перемикатися між супутниковими та наземними мережами

«Київстар» і Starlink щодо впровадження послуги Direct to Cell в Україні

https://mediasat.info/

- Starlink планує спершу вивести на орбіту додаткові супутники для підтримки технології Direct to Cell. За планом компанії, кількість супутників необхідно подвоїти.
- Технологія надаватиме мобільний зв'язок через супутник будь-якому смартфону, що підтримує 4G.

Ajax Systems пропонує відеодзвінок Doorbell із вбудованим AI для розпізнання об'єктів

https://ko.com.ua/

- Пристрій легко інтегрується в екосистему Ajax та поєднує безперебійну роботу з передовими охоронними можливостями.
- Основна функція Ajax DoorBell – повідомляти користувача про гостей у реальному часі без затримок.
- Відеодзвінок має вбудований штучний інтелект, що розпізнає людей, тварин і транспортні засоби.

Україна займає п'яте місце у глобальному цифровому рейтингу ООН

https://www.ukrinform.ua/

- За п'ять років Україні вдалося піднятися за індексом онлайн-сервісів у глобальному рейтингу ООН зі 102-го на 5-те місце.

"Наш досвід побудови цифрової держави унікальний і важливий для всього світу. Працюємо далі та наближаємося до єдиного цифрового ринку ЄС" – заявили в Мінцифрі.

Впровадження штучного інтелекту (концептуально)

Ілон Маск стверджує, що ШІ вичерпав усі наявні людські знання

https://itechua.com/

На поточний момент існує брак реальних даних для навчання штучного інтелекту.

Рішення проблеми – використання синтетичних даних, що генеруються самими ШІ-моделями.

Ринок праці майбутнього: ШІ забезпечить 78 мільйонів нових вакансій.

https://itechua.com/

Прогноз Всесвітнього економічного форуму: до 2030 року впровадження штучного інтелекту призведе до створення 170 мільйонів робочих місць, але одночасно зникнуть 92 мільйони. У підсумку, очікується чистий приріст у 78 мільйонів робочих місць.

Штучний інтелект змінює фінансову галузь:
банки планують масові скорочення

https://itechua.com/

Світові банки планують скоротити близько 200 тисяч робочих місць у найближчі 3-5 років через активне впровадження штучного інтелекту.

Це дозволить банкам оптимізувати процеси й підвищити прибутковість, яка, за прогнозами, може зрости до 17% у 2027 році.

Велика Британія стане лідером у світі з розвитку ШІ

https://itechua.com/

План передбачає створення спеціальних зон для дата-центрів, прискорення їхнього будівництва та підтримку випускників, які обирають технологічні напрямки.

Повне впровадження ШІ може підвищити продуктивність на 1.5% на рік, що принесе економіці додатковий дохід у розмірі £47 млрд стерлінгів щороку впродовж 10 років.

США посилюють контроль над світовим ринком ШІ-чипів

https://itechua.com/

Запроваджуються жорсткіші обмеження на експорт чипів та технологій штучного інтелекту, прагнучи зберегти перевагу у передових розробках для власних потреб та союзників, водночас ускладнюючи доступ до цих технологій для Китаю.

Дослідження показало, наскільки люди готові довіряти штучному інтелекту.

https://itechua.com/

Дослідники з Університету Південної Австралії виявили, що довіра до ШІ залежить від рівня знань та значущості вибору. Опитавши 2 тис. респондентів із 20 країн, вони з'ясували, що люди зі знанням статистики частіше довіряють алгоритмам у простих ситуаціях, але сумніваються в них при прийнятті серйозних рішень.

Vodafone приєднався до ініціативи саморегулювання ШІ в Україні.

https://mediasat.info/

Телекомунікаційний оператор офіційно став учасником ініціативи саморегулювання у сфері ШІ, створеної українськими ІТ-компаніями.

Оператор має намір розвивати ШІ-технології з дотриманням етичних засад і стандартів безпеки.

Прорив у створенні та використанні дронів

- Українські оборонні сили активно застосовують високошвидкісні дрони, оснащені сучасними технологіями штучного інтелекту.
- У 2025 році на фронті очікується поява автономних "роботів-вбивць", здатних виконувати бойові завдання без прямого втручання людини.
- В Україні є вагомий досвід побудови саме української екосистеми дронобудівництва, зокрема перших у світі морських дронів.
- Для протидії радіоелектронному впливу українські інженери розробили навігаційні модулі, що працюють без GPS, та багаточастотні канали зв'язку, а також новітні FPV-дрони, що керуються через оптоволоконний кабель, розпочали розробку «Ловців -дронів».

Роль телекомунікацій в створенні дронів

Телекомунікації відіграють ключову роль у створенні різних конфігурацій дронів військового застосування.

Основні аспекти у розширенні функціоналу сфери використання дронів:

1. Управління та контроль:
2. Передача даних:
3. Системи зв'язку:
4. Автономність та інтеграція в бойові мережі:
5. Кібербезпека:
6. Моніторинг і контроль повітряного простору:

Дрони для розвитку телекомунікацій

Дрони все більше інтегруються в телекомунікації і ця тенденція сприяє розвитку нових технологій та підходів до передачі даних.

Основні напрямки розробок у цій сфері:

1. Мобільні базові станції на дронах (Cellular on Drone)
2. 5G на борту дронів
3. Інтернет речей (IoT) і дрони
4. Оптичний зв'язок (Free-Space Optics)
5. Штучний інтелект та автоматизація зв'язку
6. Технології позиціонування та безпека зв'язку
7. Розширення покриття мереж 5G і 6G

Світовий рівень дронобудування

https://terazus.com/

Китай розробив військову мобільну станцію 5G, яка змінить майбутнє воєн і реально здійснює технологічний прорив у військовому зв'язку:

Китайська система здатна одночасно керувати 10 000 дронів у радіусі 3 кілометрів, забезпечуючи швидкість передачі даних до 10 гігабіт на секунду. Затримка сигналу становить менше 15 мілісекунд, що критично важливо для координації військових дій у режимі реального часу.

Особливо вражає здатність системи працювати в найвимогливіших умовах. Мобільні станції можуть встановлюватися на військову техніку, а спеціальні дрони-ретранслятори забезпечують безперебійне покриття навіть у гірській місцевості та міській місцевості.

Важливою є амбітна ціль китайців – мати більше дронів, ніж живих солдатів. Система має надійний захист від електромагнітних перешкод і може автономно використовувати цивільну інфраструктуру 5G з більш ніж 4,2 мільйона базових станцій.

Експерти зазначають, що така технологія може суттєво змінити баланс сил у світі. Здатність керувати величезними роями дронів і роботизованих систем створює нові виклики для традиційних військових стратегій.

Відповідність наукових проектів ІТС і НДІ телекомунікацій світовим пріоритетам

На стадії виконання сьогодні такі міжнародні та вітчизняні проекти:

- Проєкт Наукової ради NATO за програмою «Наука заради миру та безпеки»

  “3D Metamaterials for Energy Harvesting and Electromagnetic Sensing**”** («3D метаматеріали для збору енергії на електромагнітних сенсорів», NATO MYP SPS G6002, 2024-2026рр.)

- ❖ Здійснено моделювання перспективних комірок метаматеріалів з використанням мікросмужкових і діелектричних резонаторів,
- ❖ Досліджено властивості створених комірок, як комбінованих структур для побудови ректен і електромагнітних сенсорів,
- ❖ Запроваджено принцип накопичення енергії протягом кількох періодів із її наступним детектуванням шляхом заміни узгоджувального кола на «помножувачі» енергії на базі резонаторів біжучої хвилі і спрямованих фільтрів на основі метаматеріальних структур, які встановлюються перед детектором.

- Проєкт Національного фонду досліджень України

  «Мікрохвильові пристрої на основі резонансних структур з метаматеріальними властивостями для захисту життєдіяльності та інформаційної безпекти України» (Договір №142/0030 від 03.03.2025)

- ❖ В рамках парадигми метаматеріальної мікрохвильової техніки науковою школою «З технологій електронних комунікацій» КПІ імені Ігоря Сікорського отримано нові наукові знання і створено низку пристроїв для практичного використання в радіотехнічних комплексах і системах електронних комунікацій. Конструювання структурних одиниць – комірок електромагнітних метаматеріалів ґрунтувалося на використанні резонансних явищ при взаємодії електромагнітного поля з діелектричними резонаторами, що збуджувалось різними типами коливань, а також зі смужковими резонаторами різних розмірів і топологій.
- ❖ Встановлено, що метаматеріальні властивості структур з’являються при збудженні одночасно, незалежно і паралельно як мінімум двох типів коливань, електричного та магнітного, або адекватних їм синфазних та

протифазних коливань.

- ❖ Серед властивостей і ефектів, які можна віднести до метаматеріальних, назвемо можливості здійснення:
  - аномально високого загасання режекторних структур;
  - аномально високого Q-фактора;
  - аномально високої часової затримки.

- ➢ Вагомі здобутки проекту НФДУ, а також розроблені портативні системи зв'язку в рамках роботи «**Створення радіотехнічних систем з використанням тропосферних технологій та засобів електронних комунікацій»** представлені на здобуття Національної премії України імені Бориса Патона 2025 року
- ❖ Науково-технічним результатом роботи є створення та впровадження мобільної цифрової тропосферно-радіорелейної станції, малогабаритної цифрової тропосферної станції, нових мікрохвильових елементів та приладів, в тому числі з використанням нових метаматеріалів, формування радіонавігаційного поля з визначеними параметрами шляхом використання тропосферних неоднорідностей.
- ❖ Розроблена портативна цифрова тропосферна станція з підвищеною завадостійкістю є станцією, яка відрізняється низьким енергоспоживанням, компактними габаритами та невеликою масою завдяки використанню новітньої елементної бази мікроелектроніки в НВЧ діапазоні, сучасних радіотехнологій формування та передачі радіосигналу через тропосферний канал.
- ❖ У роботі отримали подальший розвиток такі тропосферні технології: частотне рознесення сигналів; кутове рознесення сигналів; технологія підвищення завадостійкості тропосферних засобів електронних комунікацій за рахунок використання систем з розширенням спектра, як псевдовипадкова перебудова робочої частоти, так і широкосмугові сигнали; просторове рознесення сигналів на передачі.
- ❖ Пристрої з використанням метаматеріалів створені на рівні світових результатів є оригінальними і стосуються режекторних, смугових, спрямованих фільтрів, частотно-селективних поверхонь, антенних випромінювачів і частотно-стабілізованих генераторів. Ці прилади практично необхідні як для систем тропосферного зв'язку, так і для широкого кола радіотехнічних систем.

ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ
International Scientific Conference
«Modern Challenges in Telecommunications»
ISSN print 2663-502X ISSN online 2664-3057

МІЖНАРОДНА НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ "ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ"(МНТК "ПТ")/ INTERNATIONAL SCIENTIFIC AND TECHNICAL CONFERENCE "MODERN CHALLENGES IN TELECOMMUNICATIONS" (MCT)*

Іванова Т.Л., Новогрудська Р.Л.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: conf@its.kpi.ua

Міжнародна науково-технічна конференція «Перспективи телекомунікацій» *є важливим майданчиком для обміну знаннями та інноваціями у сфері телекомунікаційних технологій.* Вона проводиться щороку починаючи з 2007** в середині квітня, згідно Плану проведення наукових та науково-технічних заходів КПІ ім. Ігоря Сікорського, що підкреслює його значущість у академічному та професійному середовищі. Конференція проводиться на базі Навчально-наукового інституту телекомунікаційних систем та НДІ телекомунікацій КПІ ім. Ігоря Сікорського (за адресою провулок Індустріальний буд. 2, корпус КПІ № 30, м. Київ, Україна, 03056) та дистанційно (за допомогою on-line сервісів для відеоконференцій та вебінарів ZOOM та MEET), або у змішаному форматі.

** Назва МНТК до 2019 року "ПРОБЛЕМИ ТЕЛЕКОМУНІКАЦІЙ".*
*** Інформацію про всі минулі конференції дивитись за ПОСИЛАННЯМ.*

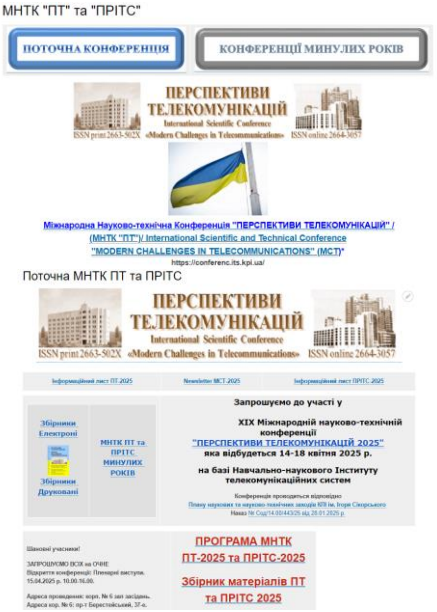
На базі Міжнародної Науково-технічної Конференції "Перспективи телекомунікацій" щороку починаючи з 2009, проводиться Науково-технічна конференція студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» (ПРІТС), як окрема секція.

Щорічно на базі Міжнародної Науково-технічної Конференції "Перспективи телекомунікацій" починаючи з 2018 року, проводиться постійно діюча науково-технічна он-лайн ВИСТАВКА: Інноваційні розробки в сфері телекомунікацій (https://conferenc.its.kpi.ua/*2025*/schedConf/presentations).

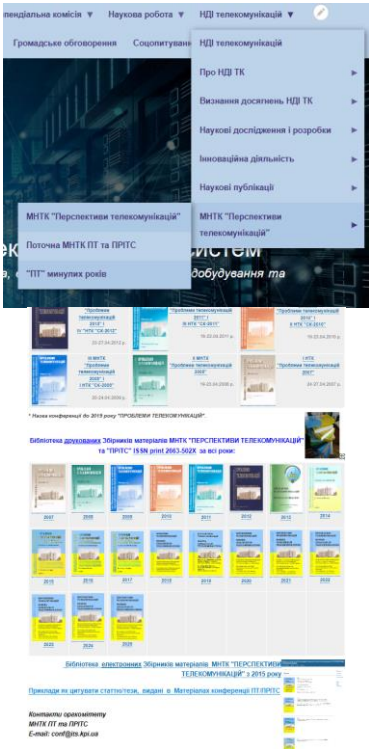
Метою конференції є сприяння розвитку телекомунікаційних технологій, обмін передовим досвідом та презентація новітніх досліджень. Вона об'єднує науковців, інженерів, викладачів і студентів з усього світу, створюючи платформу для діалогу та співпраці.

На теренах інтернету конференція має три локації, на яких розташовано інформаційно-демонстраційні ресурси та матеріали:

1. На сайті НН ІТС КПІ ім. Ігоря Сікорського https://conferenc.its.kpi.ua у вкладинці НАУКОВА РОБОТА – КОНФЕРЕНЦІЇ та у вкладинці НДІ Телекомунікацій – МНТК "ПТ" та "ПРІТС", де розголожується на сторінки загально-інформаційним, поточним та минулим контентом.



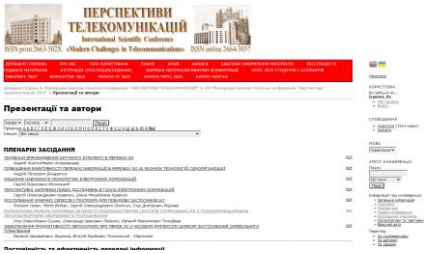
- Архів ВИСТАВКИ.
- ЗВІТИ по конференції з 2020 року (накази, рішення).



Бібліотека друкованих Збірників матеріалів МНТК ПТ та ПРІТ за всі роки

2. Одним із ключових активів конференції є її веб-сайт розташований на організаційній платформі Open Conference Systems (OCS) (https://conferences.uran.ua) - НАУКОВІ КОНФЕРЕНЦІЇ УКРАЇНИ, який з грудня 2017 року стабільно займає перші місця в рейтингу сайтів конференцій нашого університету.

Для участі в конференції необхідна електронна реєстрація як читача та автора, й подання матеріалів доповіді на організаційній платформі Open Conference Systems. Кожна подана стаття на МНТК ПТ та теза на НТК ПРІТС мають на платформі OCS своє індивідуальне посилання - URL-адресу.



3. Електронний збірник матеріалів МНТК «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ» (https://conferenc-journal.its.kpi.ua) - щорічне видання, що видається on-line на єдиній видавницько-технічній платформі Open Journal Systems (OJS) (http://journals.uran.ua) - НАУКОВА ПЕРІОДИКА УКРАЇНИ. Кожна стаття має на платформі OJS свою URL-адресу.

З 2019 році видання "Збірник матеріалів Міжнародної науково-технічної конференції "ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ" / ("MODERN CHALLENGES IN TELECOMMUNICATIONS") внесено у світову базу даних періодичних видань під постійними ISSN номерами:

Електронний збірник
ISSN online 2664-3057

Друкований збірник
ISSN print 2663-502X

Збірник включено до наступних баз даних: Наукова періодика України URAN (OJS), Електронного архіву наукових матеріалів ELA KPI. Видання індексується міжнародною наукометричною базою **Google Scholar**. Також повноцінно представляються у всесвітньому федеративному бібліотечному каталозі WorldCat, в каталогах наукових бібліотек, на пошукових платформах Google Scholar, Bielefeld Academic Search Engine (BASE), OpenAIRE та ін. Це підтверджує високий рівень організації та відповідність міжнародним стандартам наукових публікацій.

За результатами конференції на Вченій Раді НН ІТС КПІ ім. Ігоря Сікорського приймається РІШЕННЯ, в якому підводиться статистика і формуються висновки по конференції, та визначаються найкращі доповіді за наступними категоріями:

- доповідь, що викликала найбільший інтерес (обговорення-) нагороджуються сертифікатами;

- доповіді, які після певної доробки рекомендуються конференцією для підготовки до публікації в фаховому журналі ;

- доповіді (окремі або об’єднані), які після певної доробки можуть бути рекомендовані конференцією для підготовки до публікації в монографії «Springer»;

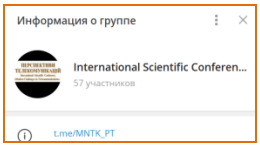
- доповіді, в яких представлені інноваційні розробки, що можуть рекомендуватися на конкурси/фестивалі Інноваційних проектів та стартапів (напр. Sikorsky Challenge);

- дотенційні нові наукові теми, що можуть бути запропоновані для участі в конкурсах на НДР, та доповіді, які ці теми визначають (обґрунтовують) та є новими науковими результатами.

4. Відео-записи МНТК "ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ" та ПРІТС розміщено з 2020 року на YouTube-каналі конференції МНТК "ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ" та ПРІТС.

З 2024 року відео засідань додатково розташовано на YouTube-playlist International Scientific and Technical Conference "MODERN CHALLENGES IN TELECOMMUNICATIONS".

5. Для експрес інформування учасників, з січня 2023 року створено телеграм-групу конференції t.me/MNTK_PT.



Завдяки активному супроводу сайт МНТК ПТ залишається лідером, забезпечуючи зручний доступ до інформації про конференцію, архів матеріалів та актуальні анонси.

Усі матеріали індексуються в Google Scholar, а анотації до робіт доступні для широкого загалу, що сприяє популяризації досліджень. Науковці можуть переглядати статистику своїх публікацій у персональних кабінетах, що підвищує прозорість і зручність роботи з матеріалами.

Запрошуємо науковців, аспірантів та студентів брати активну участь у Міжнародній Науково-технічній Конференції "Перспективи телекомунікацій" та Науково-технічній конференції студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем».

Оргкомітет МНТК «ПТ» та НТК «ПРІТС».

Джерела

1. Сторінка сайту НН ІТС КПІ ім. Ігоря Сікорського - МНТК "ПТ" та "ПРІТС" [https://its.kpi.ua/uk/conferences].
2. Сторінка сайту НН ІТС КПІ ім. Ігоря Сікорського - Поточна МНТК ПТ та ПРІТС[https://its.kpi.ua/uk/potochna%20MNTK%20PT].
3. Сторінка сайту НН ІТС КПІ ім. Ігоря Сікорського - "ПТ" минулих років[https://its.kpi.ua/uk/vsi%20MNTK%20PT].
4. АРХІВ МНТК "ПТ" та "ПРІТС" з 2016 року на організаційній платформі Open Conference Systems (OCS) (https://conferences.uran.ua) - НАУКОВІ КОНФЕРЕНЦІЇ УКРАЇНИ [https://conferenc.its.kpi.ua/index/schedConfs/archive].
5. Матеріали МНТК "ПТ" та "ПРІТС" 2025 року на організаційній платформі Open Conference Systems (OCS) (https://conferences.uran.ua) - НАУКОВІ КОНФЕРЕНЦІЇ УКРАЇНИ [https://conferenc.its.kpi.ua/2025/schedConf/presentations], із зміною цифри року посилання працюватиме для матеріалів починаючи з 2016 року.
6. АРХІВ Збірників матеріалів Міжнародної науково-технічної конференції «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ» з 2015 року [https://conferenc-journal.its.kpi.ua/issue/archive].
7. YouTube-канал конференції МНТК "ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ" та ПРІТС[https://www.youtube.com/channel/UC3FtHhQCTa8I252RSxXuYYg].
8. YouTube-playlist International Scientific and Technical Conference "MODERN CHALLENGES IN TELECOMMUNICATIONS" 2024 [https://www.youtube.com/playlist?list=PLurRYkN5hL0jf0QKFX41o82sY0U6cRuPd].
9. YouTube-playlist International Scientific and Technical Conference "MODERN CHALLENGES IN TELECOMMUNICATIONS" 2025 [https://www.youtube.com/playlist?list=PLurRYkN5hL0hr2Ts4KPOK-Sz-ooUBngPM].
10. Фотоальбом. Міжнародна науково-технічна конференція «Перспективи телекомунікацій - 2025»: результати [https://its.kpi.ua/uk/node/344].

ПЛЕНАРНІ ДОПОВІДІ

УДК 621.391

ТЕНДЕНЦІЇ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В МЕРЕЖАХ 6G

Астраханцев А.А.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: andrii.astrakhantsev@nure.ua

TRENDS OF IMPLEMENTING ARTIFICIAL INTELLIGENCE IN 6G NETWORKS

6G networks should be deployed by 2030. This paper describes the main vectors of 5G to 6G network development. The purpose of the paper is to analyze the main scenarios of 6G networks and to assess the capabilities of artificial intelligence to achieve the declared characteristics and scenarios in 6G networks.

Розквіт штучного інтелекту (ШІ) в таких сферах як охорона здоров’я, фінанси, промисловість вже призвів до істотних результатів [1,3]. Певні застосування ШІ вже набули поширення і в мобільних мережах 5G: він вдосконалює процес хендовера, оптимізує процедури планування мереж, зменшує енергоспоживання та передбачає аномалії в трафіку чи роботі мережі. Враховуючи, що системи мобільного зв'язку розвиваються від покоління до покоління приблизно кожні 10 років у напрямку підвищення продуктивності (наприклад, збільшення швидкості передачі даних і зменшення затримок) і кожне покоління пропонує нові інноваційні сервіси, то згідно [1] провідну роль в 6G мережах має зіграти саме штучний інтелект.

Дана робота ставить за мету аналіз сервісів, які мають привнести мережі 6G і оцінити тенденції застосування штучного інтелекту при застосуванні цих сервісів.

1. Основні сценарії застосування та атрибути мереж 6G.

Для оцінювання впливу ШІ розглянемо основні очікувані сценарії застосування мереж 6G. Згідно [2], мережі 6G передбачають продовження розвитку MIMO, надання можливостей повнодуплексного зв’язку без розподілу по частоті та часу, впровадження штучного інтелекту та машинного навчання для повітряного інтерфейсу та радіомереж наступного покоління. Основними сценаріями для 6G при цьому вважаються [3]:

Змішана реальність (XR) з повним зануренням (Truly Immersive XR) поєднує в собі сценарії віртуальної і доповненої реальності. На сьогодні застосування технології обмежують апаратні можливості пристроїв та вимоги до пропускної здатності мережі, але очікується капіталізація цієї послуги на рівні $87 млрд до 2030 р.

Мобільні голограми високої точності (High-Fidelity Mobile Hologram) є медіа-технологією наступного покоління, яка дозволяє реалізовувати голограми з ефектом присутності, передачею жестів і емоцій на спеціальних дисплеях. На сьогодні застосування технології обмежено екстремально високими вимогами до пропускної здатності, яка на порядок перевищує можливості 5G.

Третім сценарієм є *цифрова реплікація* (Digital Replication), яку ще називають технологією створення цифрових двійників (digital twin). Ця технологія дозволяє працювати віддалено з будь-якими об'єктами і є наступним кроком в моделюванні. Саме за допомогою штучного інтелекту та цифрової реплікації, виявлення та пом'якшення проблем можна ефективно здійснювати без присутності або навіть без детального нагляду з боку людини.

Наведені вище сценарії дозволяють виділити 4 ключові атрибути мереж 6G (рис.1):

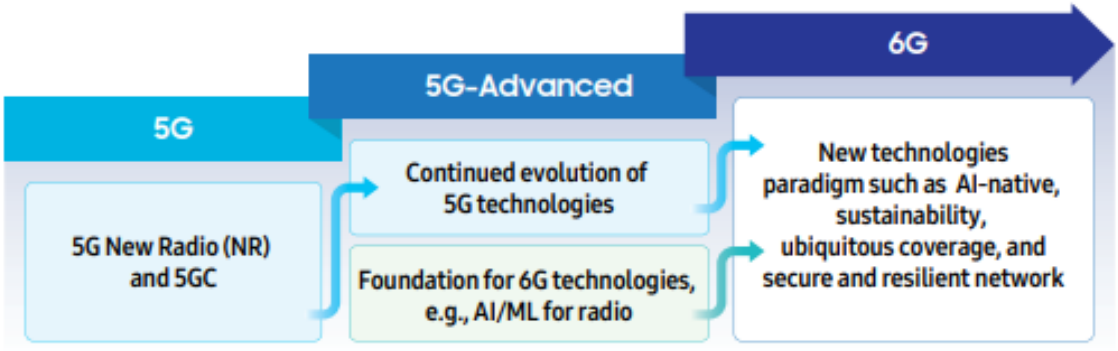


Рис.1. Еволюція мереж від 5G до 6G [1].

Нативний ШІ (AI-Native) передбачає використання та впровадження ШІ в комунікаційні функції (можливі приклади: стиснення та прогнозування інформації про стан каналу (CSI), алгоритми TX/ RX, а також експлуатація та обслуговування мережі) від початку проектування системи до розробки, управління та експлуатації систем, щоб досягти бажаного підвищення продуктивності.

Стала мережа (Sustainable Network) шляхом застосування ШІ має зменшити операційні витрати і вплинути на задоволеність користувачів за рахунок підвищення енергоефективності як мереж, так і терміналів.

Повсюдне покриття (Ubiquitous Coverage) застосовує ШІ для зменшення капітальних витрат на мережі та покращення якості послуг, що надаються користувачам, за рахунок розширення зони обслуговування зв'язку.

Безпечна та стійка мережа (Secure and Resilient Network) залежить від застосування ШІ, оскільки саме на ШІ покладаються задачі передбачення аномальної поведінки мережі, виявлення шкідоносного трафіка та застосування підходів до нейтралізації загроз.

2. Аналіз впливу ШІ на 6G мережі.

Базуючись на описаних вище атрибутах, розглянемо вплив ШІ (рис.2) і запропоновані методи, застосування яких дасть виграш в певних показниках (KPIs) під час побудови і експлуатації мережі [2]. Розглянемо їх більш детально.

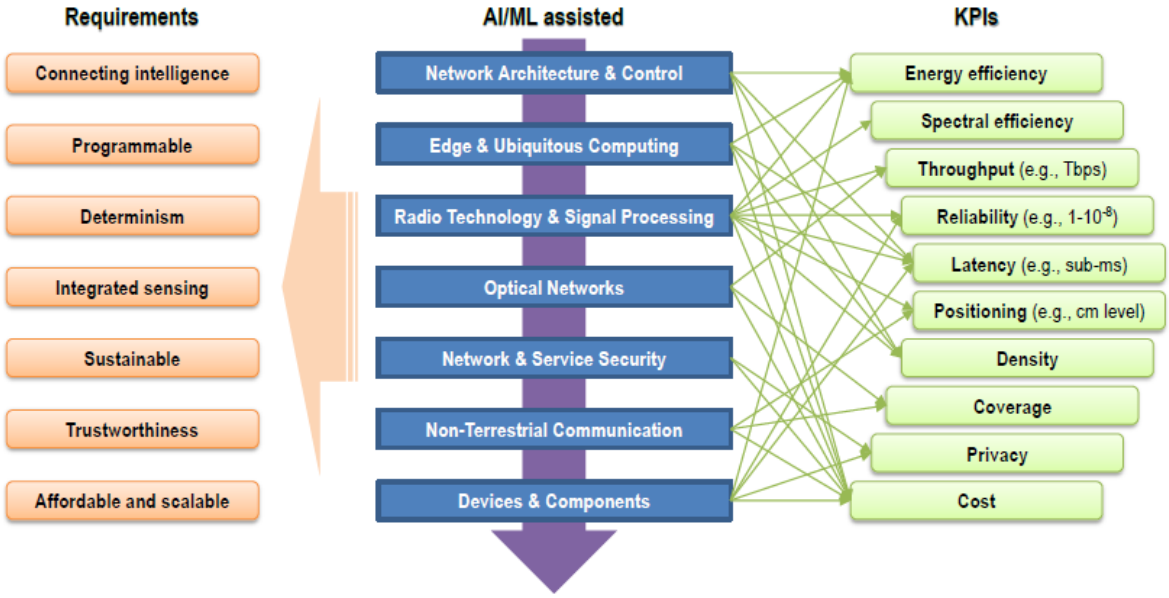


Рис.2. Вплив ШІ на різні технологічні процеси в 6G мережі [2].

2.1. ШІ в системній мережевій архітектурі та управління.

ШІ привертає багато уваги як інструмент для вирішення проблем, які раніше вважалися нерозв'язними через їхню величезну складність або відсутність необхідної моделі та алгоритму [3]. 6G передбачає комплексну систему штучного інтелекту для оптимізації загальної продуктивності системи та роботи мережі. Загалом, загальна архітектура мережі складається з чотирьох рівнів об'єктів: обладнання користувача (UE), базові станції (BS), ядро мережі та сервер додатків. Застосування ШІ можна розділити на 3 рівні (рис.3): 1) локальний ШІ, 2) спільний ШІ і 3) E2E ШІ.

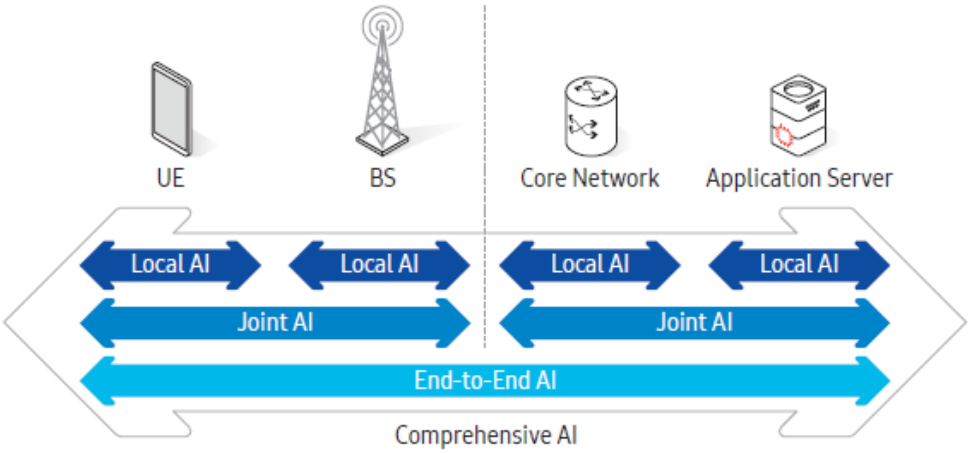


Рис.3. Колективний ШІ 6G мережі [3].

Локальний ШІ впроваджується в кожному елементі мережі. Прикладом є використання ШІ для оптимізації модуляції, кодування джерела та кодування каналу [3,5]. Спільний ШІ може оптимізувати спільну роботу UE і BS або спільну роботу магістральних мереж і серверів додатків. Прикладом можливості спільної оптимізації є оптимізація хендовера на основі прогнозування майбутніх мережевих умов у складних бездротових середовищах. E2E ШІ оптимізує всю систему зв'язку. За допомогою E2E AI стає можливим виявляти або прогнозувати аномалії в роботі мережі та пропонувати коригувальні дії.

Також ML буде необхідний для підтримки рентабельності експлуатації передбачуваних складних послуг 6G, таких як взаємодія у сферах «людина-цифровий світ-фізичний світ» та «Інтернет почуттів» [2]. Крім того, поширення численних технологій віртуалізації, включаючи віртуальні прилади, мікросервіси, контейнери, безсерверні функції та їхню інтероперабельність, збільшить складність мережевих операцій. Таким чином, механізми AI/ML стануть вирішальними для автоматизації процесів прийняття рішень. AI/ML також дозволить реалізувати предиктивну оркестровку в 6G, наприклад, для досягнення майже оптимальних рішень щодо розміщення базових станцій і конфігурації сервісів.

2.2. ШІ в граничних та повсюдних обчисленнях

Основними цілями периферійних і повсюдних обчислень є зменшення затримок і підвищення швидкості реагування, а також зменшення обсягу потоків даних між користувацькими IoT-пристроями і централізованими хмарними обчислювальними ресурсами. Впровадження методів ML/NN дозволяє оптимізувати потоки обчислень і забезпечити зменшення затримок. Прикладом таких процесів є динамічний розподіл спектру на основі ШІ (рис.4).

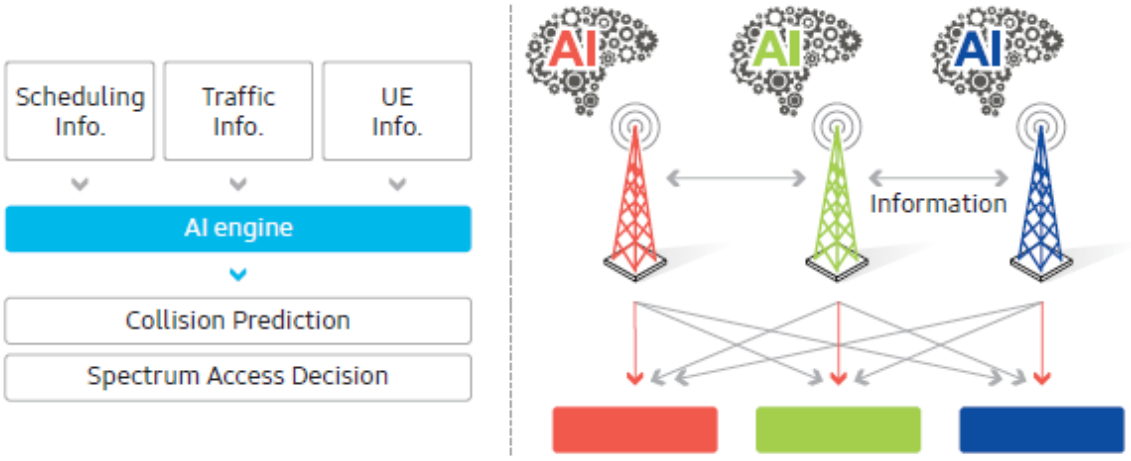


Рис.4. Розподіл спектру на основі ШІ [3].

Основним викликом динамічного розподілу спектру є уникнення (або мінімізації) колізій у використанні спектру між різними суб'єктами, при цьому надання їм доступу до спектру в динамічному режимі. Теоретично, щоб запобігти таким колізіям запобігти таким колізіям, мережеві оператори

могли б обмінюватися всією необхідною інформацією про доступ до спектру. На практиці, однак, це неможливо оскільки отримання всієї необхідної інформації для кожного суб'єкта в режимі реального часу призвело б до величезних накладних витрат на зв'язок. ШІ міг би уникнути колізій прогнозуючи використання спектру іншими суб'єктами обмінюючись обмеженим обсягом інформації.

2.3. ШІ для забезпечення безпеки мережі і сервісів.

Подання 6G як високорозподіленої архітектури обчислень і зв'язку, з віртуалізацією і автоматизацією критично важливих функцій управління призводить до створення набагато ширшої і складнішої поверхні атак, ніж в нинішньому домені 5G [4]. Система не лише вразлива до прямих кібератак, але й потребує виявлення збоїв у роботі автоматизованих функцій та мінімізації їхнього впливу. Гарантування надійності та достовірності системи буде одним з головних викликів. Такі рішення, як мікросегментація і нарізка без дотику, повинні бути гарантовані, а розподілені функції і моделі ШІ та ML повинні бути посилені, щоб уникнути збоїв і кібератак і гарантувати їх достовірність і безпеку (наприклад, щоб уникнути отруєння моделей і атак на виведення належності в розподілених архітектурах з федеративним навчанням).

2.4. ШІ для підвищення енергоефективності мережі

Енергозбереження в мережі є складною проблемою [5], що включає в себе кілька рівнів мережі та необхідність балансування з іншими ключовими показниками ефективності та вимогами до якості обслуговування (QoS). Традиційні механізми енергозбереження в мережі покладаються на конфігурацію на основі правил, наприклад, вмикання/вимикання осередків на основі різних порогових значень навантаження на осередок. Такі методи, засновані на правилах, є реактивними, негнучкими і складними для досягнення глобально оптимізованої продуктивності та енергоефективності системи. Алгоритми ШІ можуть використовувати дані RAN для оптимізації енергозбереження мережі, наприклад, прогнозування енергоефективності та навантаження в майбутніх станах, щоб уможливити проактивні, адаптивні дії з розвантаження трафіку, модифікації покриття та активації/деактивації стільників.

2.5. ШІ на MAC рівні.

Методи ML можуть ще більше вдосконалити нативний повітряний інтерфейс штучного інтелекту (AI-AI), передбачений для 6G [6]. Розглянемо декілька підходів.

Адаптивна модуляція та кодування є важливою функцією MAC рівня. Вона обирає найкращу схему модуляції та кодування (MCS), враховуючи часові характеристики каналу, розмір даних та системні обмеження. Базова евристика Inner Loop Link Adaptation (ILLA) використовує таблиці пошуку для вибору MCS, в той час як Outer Loop Link Adaptation (OLLA) коригує її, зміщуючи прогнози SINR для мінімізації BLER.

У мережах 4G і 5G управління потужністю передачі висхідної лінії зв'язку включає розімкнутий і замкнутий компоненти, які забезпечують

спектральну рівномірність, максимізацію SINR і мінімальний розряд акумулятора UE. Управління потужністю в розімкнутому контурі (OLPC) регулює потужність передачі за допомогою двох параметрів, специфічних для конкретної стільники: P0, який визначає очікувану потужність на PRB, і α, який позначає коефіцієнт компенсації втрат у тракті. Ці параметри зазвичай встановлюються оператором мобільного зв'язку методом проб і помилок. Хоча історично ці показники є надійними, вони часто неоптимальні. Дослідження нових значень (P0, α) несе ризики для зв'язку, а відсутність виразів у закритій формі для продуктивності мережі не дозволяє операторам відхилятися від встановлених значень. Для вирішення цих проблем останнім часом зусилля були зосереджені на методах оптимізації «чорної скриньки», таких як байєсівська оптимізація з гаусовими процесами (BOGP).

Згідно [6] впровадження ШІ на MAC-рівні дозволяє більше ніж на 15% підвищити медіанну швидкість передачі, на 65% зменшити використання CPU. Також застосування ШІ дозволяє зменшити рівень блокових помилок з 10^{-3} до 10^{-7} і зменшити кількість колізій.

Отже, в якості висновків можна зазначити, що фактично всі елементи мережі 6G мають застосовувати ті чи інші алгоритми ШІ. Більш того, штучний інтелект є об’єднуючим елементом для багатьох процесів і дозволяє підвищувати найрізноманітніші властивості мережі і забезпечувати очікувані від неї сервіси.

Література

1. Samsung’s 6G AI-Native & Sustainable Communication 2025. Available: https://research.samsung.com/next-generation-communications
2. Carlos J. Bernardos, Mikko Uusitalo, Carles Anton. European Vision for the 6G Network Ecosystem, June 2021, DOI:10.13140/RG.2.2.19993.95849.
3. Samsung, 6G The Next Hyper-Connected Experience for All., Jul. 2020. Available: https://cdn.codeground.org/nsr/downloads/researchareas/20201201_6G_Vision_web.pdf.
4. Y. Siriwardhana, P. Porambage, M. Liyanage and M. Ylianttila, "AI and 6G Security: Opportunities and Challenges," *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, Porto, Portugal, 2021, pp. 616-621, doi: 10.1109/EuCNC/6GSummit51104.2021.9482503.
5. X. Lin, L. Kundu, C. Dick and S. Velayutham, "Embracing AI in 5G-Advanced Toward 6G: A Joint 3GPP and O-RAN Perspective," in *IEEE Communications Standards* Magazine, vol. 7, no. 4, pp. 76-83, December 2023, doi: 10.1109/MCOMSTD.0005.2200070.
6. Alvaro Valcarce Rial, Petteri Kela. The Role of AI on 6G MAC, Nokia Bell Labs, Murray Hill, NJ, July 2023, DOI:10.36227/techrxiv.23708310.

УДК 621.391

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПЕРЕДАЧІ ІНФОРМАЦІЇ В МЕРЕЖАХ 5G ЗА РАХУНОК ТЕХНОЛОГІЙ САМООРГАНІЗАЦІЇ

Бондарчук А.П.
Державний університет інформаційно-комунікаційних технологій, Україна, Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна.
E-mail: dekan.it@ukr.net

INCREASING THE EFFICIENCY OF INFORMATION TRANSMISSION IN 5G NETWORKS THROUGH SELF-ORGANIZATION TECHNOLOGIES

The article examines the role of self-organizing technologies in 5G networks. It highlights key challenges and opportunities related to automated network management, including resource optimization, latency minimization, and data transfer efficiency improvement. It analyzes modern machine learning methods used for self-configuration and self-optimization of networks.

З розвитком мобільного зв’язку та впровадженням технологій 5G зростає потреба у високоефективних, гнучких і автономних мережних системах управління і забезпечення ефективності передачі інформації .

Самоорганізовані мережі (Self Organizing Network - SON) є перспективним рішенням, що забезпечує автоматичну конфігурацію, оптимізацію та відновлення мережевих ресурсів без ручного втручання. SON активно використовується в мережах LTE (4G). Для мереж 5G SON має використовувати нові підходи такі як машинне навчання (ML) і штучний інтелект (AI). Крім того, ми представляємо та коментуємо останні пропозиції щодо розгортання SON у мережах 5G. Типові приклади включають поєднання систем SON із такими методами, як віртуалізація мережевих функцій (NFV), Cloud RAN (C-RAN), наднадійні комунікації з низькою затримкою (URLLC), масовий зв’язок машинного типу (mMTC) для IoT.

Технологія SON усуває процеси, які займають багато часу, а саме, ручні процеси при експлуатації мереж, підвищує експлуатаційну ефективність і дозволяє операторам впроваджувати нові технології і розширювати мережі швидше, ніж до цього. Рішення SON підвищує ефективність експлуатації існуючих мереж за рахунок їх автоматичної установки для процесів хендовера, балансування навантаження мобільного трафіку і мінімізацію ручного тестуваннях та налаштування. Крім того, за рахунок компенсуючих функцій і самовідновлення мінімізується перерва в роботі мережі для кінцевих користувачів. Особливістю SON є підтримка конфігурації за принципом "plug & play", тобто "приєднав і працює", відсутня необхідність у виклику фахівців для установки програмного забезпечення і його налаштування для роботи в мережі. Автоматична конфігурація повністю позбавить від витрат на локальні настройки, а автоматичне розпізнавання сусіднього вузла значно знизить витрати на оптимізацію.

До основних можливостей SON можна віднести самоконфігурацію та

самооптимізацію. Процес самоконфігурації – це процес, при якому тільки що розгорнуті нові вузли автоматично, в процесі налаштування, конфігуруються шляхом отримання необхідної для роботи базовій конфігурації, тобто відбувається автоматичне введення в експлуатацію. Функція ANR (Automatic Neighbor Relations) – автоматизація відносин між сусідами, автоматичне виявлення та налаштування сусідніх базових станцій без ручного втручання. Ще одна функція Автоматична конфігурація радіомережі - початкове налаштування нових базових станцій, включаючи параметри частотного планування, потужності сигналу та ідентифікації. Дана функція дозволяє швидше адаптувати мережу до змін. Мобільні мережі 5G складаються з великої кількості базових станцій, які не можуть бути тільки під контролем оператора, тому функція самоконфігурації забезпечить мережу гнучкістю.

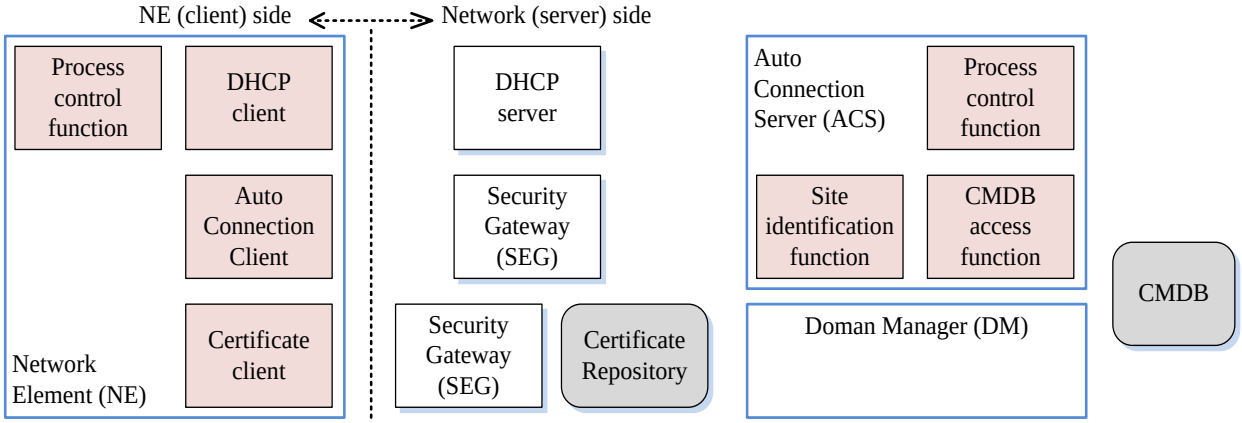


Рис. 1. Процес автоматизації взаємозв'язку між сусідніми сегментами мережі.

Процес самооптимізації визначено як процес, під час якого призначене для користувача устаткування і базова станція проводять вимірювання, результати яких використовуються для автонастройки мережі. Процес самооптимізації полягає в отриманні результатів вимірювань або контролю від обладнання користувача і мережного обладнання та за допомогою зовнішніх засобів оптимізації проводиться автоматичне підстроювання конфігураційних даних для оптимізації мережі. Ключовою функцією SON є оптимізація балансування навантаження мобільності. Mobility Load Balancing (MLB) – це функція SON, яка рівномірно розподіляє навантаження між базовими станціями, щоб уникнути перевантаження окремих комірок. Вона працює шляхом моніторингу навантаження, виявлення перевантажених сот і перенаправлення частини користувачів до менш завантажених сусідніх станцій. Це досягається коригуванням параметрів хендовера або зміною потужності передавачів. MLB покращує якість обслуговування, зменшує затримки та підвищує швидкість передачі даних. У мережах 5G ця функція використовує штучний інтелект для більш точного прогнозування і балансування трафіку.

Залежно від місця алгоритмів оптимізації SON можна розділити на три класи: централізовані, розподілені і гібридні. У централізованих SON алгоритми оптимізації виконуються в системі управління, в розподілених

SON виконуються в eNB. У гібридних SON частина алгоритмів оптимізації виконується в системі управління, а інша частина на базовій станції eNB.

Машинне навчання, як складова штучного інтелекту, відіграє ключову роль у системах SON, оскільки всі їхні функції базуються на інтелектуальних алгоритмах ML, що аналізують реальні мережеві дані для прийняття рішень щодо оптимізації та створення виконуваних сценаріїв. Вже зараз машинне навчання застосовується для самовідновлення та самооптимізації, наприклад, через самоорганізуючі карти (SoM), які здійснюють кластеризацію даних та групують стільники за схожими мережними параметрами для узгоджених змін. Навчання з підкріпленням (RL) ефективне для обслуговування автономних IoT-пристроїв, маршрутизації трафіку та самооптимізації, оскільки базується на взаємодії вузлів та використанні функції винагороди для оцінки ефективності. Глибоке навчання з підкріпленням є перспективним розвитком RL, що дозволяє покращити процеси прийняття рішень у 5G-мережах, підвищуючи їхню адаптивність та ефективність.

До подальших напрямків досліджень SON для 5G можна віднести:

• Розробку платформ Virtual SON (V-SON), а також прив’язування SON до C-RAN.

• Розробку нових алгоритмів ML і прив’язка SON до великих даних і технологій глибокого навчання.

• Поєднання SON із ключовими засобами підтримки 5G eMBB, такими як mmWave.

• Реалізацію SON в мережних інфраструктурах IoT і міжмашинною взаємодією (mMTC).

Висновок: Технології самоорганізації відіграють ключову роль в автоматизації мобільних мереж, забезпечуючи ефективне управління ресурсами та оптимізацію процесів за допомогою алгоритмів машинного навчання (ML). Вони дають змогу мережі автоматично налаштовуватися, адаптуватися та відновлюватися без ручного втручання, що підвищує її ефективність і надійність. Використання ML дозволяє аналізувати великі обсяги даних у реальному часі, приймати обґрунтовані рішення та динамічно коригувати параметри мережі. Це сприяє зменшенню затримок, зниженню експлуатаційних витрат і покращенню якості послуг для користувачів. Надалі розвиток алгоритмів самоорганізації стане визначальним фактором для підвищення автономності та продуктивності мобільних мереж.

Література

1. Papidas, A.G.; Polyzos, G.C. Self-Organizing Networks for 5G and Beyond: A View from the Top. Future Internet 2022, 14, 95. https:// doi.org/10.3390/fi14030095
2. Бондарчук А.П. Самозахист як пріоритетний напрям розвитку інфокомунікацій «Сучасний захист інформації». – Київ: ДУІКТ, 2013 – №1. – С.11-15.
3. 3GPP TR 28.861, V0.2.0 (2018–11). Study on the Self-Organizing Networks (SON) for 5G networks (Release 16). 3 February 2022.

УДК 004.8

МАШИННЕ НАВЧАННЯ В ТЕХНОЛОГІЯХ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

Могильний С.Б.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: isearch@ukr.net

MACHINE LEARNING IN ELECTRONIC COMMUNICATIONS TECHNOLOGIES

The implementation of ML technologies in various areas of our activity requires a broader study of their application in the telecommunications industry. Examples of ML applications are given with a brief analysis of the learning models used.

Серед задач телекомунікаційних технологій, які ефективно допомагає вирішити машинне навчання (ML – Machine Learning), наступні:

- Виявлення аномалій та вторгнень.
- Управління інтерференцією в стільникових мережах.
- Оптимізація мережі.
- Оптимізація параметрів радіосигналу.
- Управління живленням.
- Прогнозування обслуговування.
- Оцінка якості передачі.
- Класифікація трафіку та кластеризація потоків.

Важливо розуміти відмінності та зв’язки між штучним інтелектом (AI), машинним навчанням (ML), штучними нейронними мережами (ANN) та глибоким навчанням (DL). На рис.1 зображені ці відмінності та зв’язки.

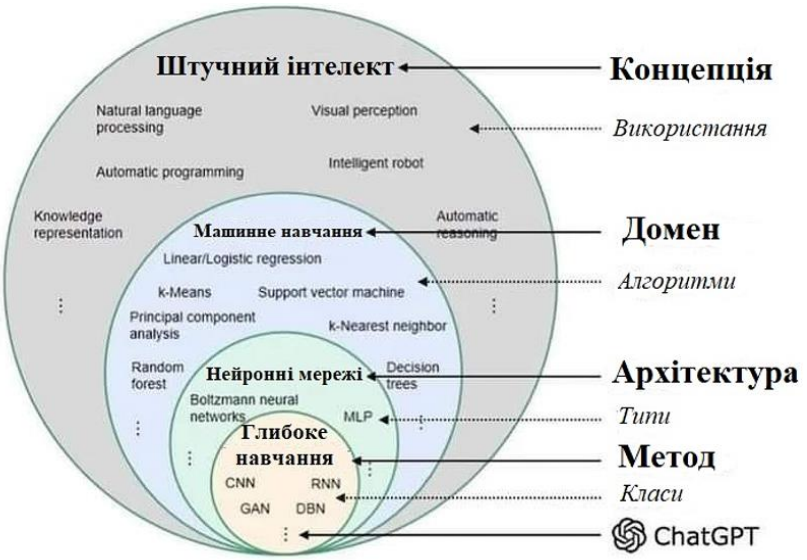


Рисунок 1. Розуміння штучного інтелекту, машинного навчання, штучних нейронних мереж і глибокого навчання.

Штучний інтелект: всеохоплююча концепція, яка включає все: від обробки природної мови до інтелектуальних роботів.

Машинне навчання: підмножина штучного інтелекту, зосереджена на розробці алгоритмів, які дозволяють комп’ютерам навчатися та робити прогнози на основі даних.

Штучні нейронні мережі: певний набір алгоритмів у системі машинного навчання, розроблений для розпізнавання шаблонів.

Глибоке навчання: найбільш спеціалізована форма нейронних мереж, яка працює з величезними обсягами даних і складними алгоритмами, такими як згорточні нейронні мережі (CNN), рекурентні нейронні мережі (RNN) і генеративні змагальні мережі (GAN).

В галузі електронних комунікацій важливі ті застосування ML, які дозволяють оптимізувати інженерні рішення, або отримати нові на основі оброблення великих масивів даних. Нижче наведені результати аналізу застосування ML в телекомунікаціях.

Таблиця. 1 Моделі категорії «ML з вчителем» з характеристиками та застосуванням [1].

Модель навчання	**Характеристики**	**Застосування**
Дерева рішень (Decision trees)	Прогнозує мітки даних шляхом ітерації вхідних даних через дерево навчання	Колекція шляху, рівень втрат, агрегація даних, аномалія [2]
Випадковий ліс (Random forest)	Колекція дерев, кожне з яких пропонує класифікацію	Покриття, розташування, протоколи MAC, дані категоризації [3]
Штучна нейронна мережа (Artificial neural network)	Блоки нейронів для ідеальної категоризації необроблених даних.	Виявлення вторгнення /аномалій /збоїв, локалізація, маршрутизація, контроль перевантаження [4]
К-найближчих сусідів (K-NN)	Більшість голосів сусідів	Агрегація даних, оцінка каналу, несправні вузли, система обробки запитів [5]
Метод опорних векторів (Support Vector Machine)	Роздільні входи, легке навчання	Розпізнавання спектру, виявлення аномалій [2]
Байєсова мережа (Bayesian network)	Статистичні моделі, незалежні результати, як в часових рядах Маркова	Оцінка каналу, спектру, покриття, помилок, відстеження пакетів [6]

Таблиця 2. Моделі категорії «ML без вчителя» з характеристиками та застосуванням.

Модель навчання	**Характеристики**	**Застосування**
К-середніх (K-means)	Відкриває найвигідніші параметри кластерів	Вилучення функцій, збір даних, прийняття рішень [7]
Нечітка кластеризація- с -середніх (Fuzzy-c-means)	Кластер на основі потужності, відстані, зв’язку	Локалізація, зв’язок, мобільність [3]
Опорний векторний вимір (Support Vector Dimension)	Зменшення розмірності для матричної факторизації	Класифікація, агрегація даних, маршрутизація [5]
Аналіз головних компонент (Principle component analysis)	Ортогональна вісь для максимізації дисперсії для зменшення розмірності	Усунення шумів, зменшення розмірності, вилучення ознак [8]
Незалежний компонентний аналіз (Independent component analysis)	Діаграма даних, багатовимірне спостереження в підкомпонентах	Зменшення даних, кластеризація даних, прийняття рішень [9]

Таблиця 3. Моделі DL з характеристиками та застосуванням [1].

Модель навчання	**Характеристики**	**Застосування**
Автокодер (Auto-encoder)	Зменшення вхідних даних до вихідних через специфікації	Визначення спектру, оцінка каналу, усунення шумів [3]
Рекурентна нейронна мережа (Recurrent neural network)	Введення/виведення складаються з автономних послідовностей	Час/подія, оцінка каналу [10]
Згорткова нейронна мережа (Convolution neural network)	Навчання багатошарових нейронів для зменшення обробки даних	Модульна класифікація, еволюція зв'язків, безпека, вилучення ознак [4]

Кількість задач, які вирішуються за допомогою ML, збільшується з впровадженням нових технологій. Так, в стандарті 6G виявлення сигналу користувача, визначення типу модуляції та напряму на джерело радіо випромінювання повністю виконується з допомогою ML [4, 5].

Література

1. Suganthi K., Karthik R., Rajesh G., Peter Ho Chiung Ching. Machine Learning and Deep Learning Techniques in Wireless and Mobile Networking Systems. CRC Press. 2022. 285 p.
2. Mohammad A. Matin, Sotirios K. Goudos, George K. Karagiannidis. Artificial Intelligence for Future Networks. IEEE Press. 2025. 592 p.
3. Garima Chopra, Suhaib Ahmed, Shalli Rani. Current and Future Cellular Systems. IEEE Press Wiley. 2025. 324 p.
4. Dragorad A. Milovanovic, Zoran S. Bojkovic, Tulsi Pawan Fowdur. Driving 5G Mobile Communications with Artificial Intelligence towards 6G. CRC Press. 2023. 503 p.
5. Radhika Ranjan Roy. Artificial Intelligence-Based 6G Networking. CRC Press. 2025. 381 p.
6. Mariyam Ouaissa, Mariya Ouaissa, Hanane Lamaazi, Khadija Slimani, Ihtiram Raza Khan, B. Sundaravadivazhagan. Machine Learning for Radio Resource Management and Optimization in 5G and Beyond. CRC Press. 2025. 249 p.
7. Payal Bansal, Rajeev Kumar, Ashwani Kumar, and Daniel D. Dasig, Jr. Artificial Intelligence and Communication Techniques in Industry 5.0. CRC Press. 2025. 421 p.
8. Daniel Minoli, Benedict Occhiogrosso. AI Applications to Communications and Information Technologies. John Wiley & Sons, Inc., Hoboken, New Jersey. 2024. 493 p.
9. Ramjee Prasad, Anand Raghawa Prasad, Albena Mihovska, Nidhi. 6G Enabling Technologies. New Dimensions to Wireless Communication. River Publishers. 2022. 382 p.
10. Samarendra Nath Sur, Agbotiname Lucky Imoize, Ankan Bhattacharya, Debdatta Kandar, Jyoti Sekhar Banerjee. Artificial Intelligence for Wireless Communication Systems: Technology and Applications. CRC Press. 2025. 319 p.

УДК 621.396.1

ПЕРСПЕКТИВНІ НАПРЯМКИ НОВИХ ДОСЛІДЖЕНЬ В ГАЛУЗІ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

Кравчук С.О., Кравчук І.М.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: sakravchuk@ukr.net

PROSPECTIVE DIRECTIONS OF NEW RESEARCH IN THE FIELD OF ELECTRONIC COMMUNICATIONS

This work aims to summarize and highlight key areas in the development of electronic communications that shape the present and future of the industry. It outlines scientific challenges and opportunities associated with the digitalization of society and the growing demand for fast, reliable, and secure data transmission. Additionally, this material serves as a reference for scientists, researchers, and telecommunications specialists, helping to identify relevant topics for further research and development.

У галузі електронних комунікацій продовжується стрімкий розвиток, що обумовлено постійним зростанням попиту на швидкість, надійність, безпеку передачі даних, а також інтеграцією нових технологій [1-7]. Особливо актуальним є визначення ключових напрямків подальших наукових досліджень, які сприятимуть розвитку електронних комунікацій у контексті цифровізації суспільства.

Дана робота має на меті узагальнити та висвітлити ключові напрямки розвитку електронних комунікацій, які визначають сучасний та майбутній стан галузі. Вона спрямована на окреслення наукових викликів і перспектив, що пов’язані з цифровізацією суспільства, зростанням попиту на швидку, надійну та безпечну передачу даних. Також матеріал слугує орієнтиром для науковців, дослідників та фахівців у сфері телекомунікацій, допомагаючи визначити актуальні теми для подальших досліджень та розробок.

Нижче наведено перелік найбільш актуальних напрямків для нових досліджень, які можуть визначити майбутнє цієї галузі (рис. 1).

1. 6G та майбутні покоління мереж (6G and the next generations of networks). Поки 5G впроваджується по всьому світу, науковці вже працюють над 6G, яка обіцяє ще вищі швидкості передачі даних (до 1 Тб/с), мінімальні затримки та підтримку нових сценаріїв використання, таких як голографічні комунікації, точний контроль роботів у реальному часі та інтеграція з квантовими технологіями.

2. Квантові комунікації (Quantum communications). Квантові технології забезпечують абсолютну безпеку передачі даних завдяки принципам квантової криптографії. Це стає особливо важливим у світі, де кіберзагрози стають все складнішими.

3. Інтернет речей (IoT) та його масштабування (Internet of Things (IoT) and its scaling). Кількість підключених пристроїв зростає експоненційно, що

вимагає нових підходів до управління мережами, енергоспоживання та обробки даних.

4. Штучний інтелект (AI) та машинне навчання (ML) у мережах (Artificial Intelligence (AI) and Machine Learning (ML) in Networks). AI та ML дозволяють оптимізувати роботу мереж, прогнозувати навантаження, виявляти аномалії та автоматизувати управління ресурсами.

5. Безпека та конфіденційність у електронних комунікаціях (Security and privacy in electronic communications). Зростання кількості кібератак, витоків даних та шпигунських програм вимагає нових підходів до захисту інформації.

Рис. 1. Напрямки для нових досліджень, які можуть визначити майбутнє електронних комунікацій.

6. Периферійні та туманні обчислення (Edge та Fog Computing). Зростання обсягів даних, що генеруються пристроями IoT, вимагає перенесення обробки ближче до джерела даних, щоб зменшити затримки та навантаження на централізовані хмарні сервери.

7. Віртуалізація мережних функцій (NFV) та програмно-визначені мережі (SDN) (Network Functions Virtualization (NFV) and Software-Defined Networking (SDN)). Ці технології дозволяють гнучко керувати мережевими ресурсами, що є ключовим для підтримки сучасних високонавантажених мереж.

8. Зелені комунікації (Green Communications). Енергоспоживання мереж зростає, що впливає на навколишнє середовище. Зелені технології

спрямовані на зменшення енерговитрат.

9. Голографічні та тактильні комунікації (Holographic and tactile communications). Ці технології відкривають нові можливості для освіти, медицини, розваг та промисловості, дозволяючи передавати не лише звук та відео, але й тактильні відчуття.

10. Мережі для критично важливих застосувань MCN (Mission-Critical Networks). Зростає потреба у надійних мережах для медицини, транспорту, енергетики та оборони, де навіть мінімальні затримки чи збої неприйнятні.

11. Глибокий космічний та міжпланетарний зв'язок (Deep Space and Interplanetary Connection). Ці дослідження відкривають нові горизонти для людства, роблячи космос більш доступним і зрозумілим.

Таким чином, перераховані напрями визначають майбутнє електронних комунікацій. Дослідження у цих сферах дозволять забезпечити стійкий розвиток галузі, враховуючи зростаючі потреби сучасного суспільства у швидких, безпечних та надійних технологіях передачі даних.

Література

1. Engheta N., Krishnaswamy H., Shroff N. Future Directions Workshop on Wireless Communications: XG and Beyond // Workshop sponsored by the Basic Research Office, Office of the Under Secretary of Defense for Research & Engineering June 8-9, 2022, https://basicresearch.defense.gov/Portals/61/Documents/future-directions/Future%20Directions%20-%20Wireless%20Communications%20-%20for%20public%20release.pdf?ver=LL4z9Lfey_VSpFp6Nnmwmw%3D%3D.
2. 10 telecommunications trends for 2025 // IOT Insider News, 19 November 2024, https://www.iotinsider.com/news/10-telecommunications-trends-for-2025/.
3. Magri T. 2025 Digital Communications Outlook: Top 5 Predictions // Industry Insight, January, 2025, https://www.smarsh.com/blog/thought-leadership/2025-digital-communications-outlook-top-5-predictions.
4. ICT Innovations Set to Dominate in 2025 // Telecom Review Europe, December 2024, https://www.telecomreview.com/articles/reports-and-coverage/8735-ict-innovations-set-to-dominate-in-2025.
5. Results of the exploratory consultation on the future of the electronic communications sector and its infrastructure // Directorate-General for Communications Networks, Content and Technology (European Commission), October 2023, https://digital-strategy.ec.europa.eu/en/library/results-exploratory-consultation-future-electronic-communications-sector-and-its-infrastructure.
6. Kravchuk S., Uryvsky L. Prospects for the spread of information technologies and artificial intelligence in the context of Academician Glushkov V.M. predictions // 2023 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), ISBN: 979-8-3503-4848-4, 13-18 November 2023, Kyiv, Ukraine. – p. 21-24, https://doi.org/10.1109/UkrMiCo61577.2023.10380386.
7. Ilchenko M., Kravchuk S., Uryvsky L. Continuation of academician VM Glushkov work on the development of modern information & communication technologies // Information and Telecommunication Sciences, No. 1, pp. 4-8 (2023) https://doi.org/10.20535/2411-2976.12023.4-8; http://infotelesc.kpi.ua/article/view/281956/276244.

ОГЛЯД ПЕРСПЕКТИВНИХ СУПУТНИКОВИХ СИСТЕМ НА ПОТРЕБУ УКРАЇНИ

[1]Капштик С.В., [2]Наритник Т.М., [1]Присяжний В.І.
[1] *Національний центр управління та випробувань космічних засобів*
[2] *Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського*
E-mail: s.kapshtyk@spacecenter.gov.ua, t.narytnyk@ukr.net, ncuvkz@spacecenter.gov.ua

REVIEW OF PROSPECTIVE SATELLITE SYSTEMS FOR UKRAINE'S NEEDS

There is presented an overview of promising satellite systems, the services of which are used and can be implemented in Ukraine in the near future. There are shown the possibilities of implementing the 5G architecture in satellite information systems and trends in the development of NTN (Non terrestrial networks) technology. Modern geostationary (GEO) High-Throughput Satellite systems (HTS), Very High-Throughput and Ultra High-throughput Satellite systems (VHTS and UHTS) are considered in terms of their ability to theirs interact with 5G networks on the example of the Viasat-3 (USA) and Ovzon-3 (Sweden, USA) satellites. The opportunity to establish the Regional System for Ukraine based on the technologies of HTS systems and a small GEO satellite of Astranis (USA) is noted. The tendency to combine the GEO component resource with the LEO and MEO components is identified on the example of the O3b/mPOWER systems of SES (Luxembourg) and the Eutelsat OneWeb system (France). It is shown that the manufacturers of user terminals All.Space and Kymeta offer appropriate solutions based on flat panels with phased array antennas for such services. The EU's project of secure satellite communication system IRIS² is developed as multi-orbit system based on such trends. The article shows innovations in the Starlink system regarding the using of laser communication for establish the Inter-Satellite-Links, the introduction of satellite access services as a cellular network base station in space, and intentions to apply the higher frequency bands and lower orbits. The tendency of satellite interaction with 4G, 5G networks to provide services by the AST Space Mobile system outside the service areas of terrestrial networks for traditional terminals such as smartphones and tablets is noted. The influence of the Cluster Launch Method of spacecraft on the Satellite Telecommunication Systems development is considered on the examples of satellite buses such as Starlink V0.9, Meridian Space (SpinLaunch), Flatellite (Rocket Lab), Enterprise, and SmallSat GEO™ (Terran Orbital). In conclusion, aspects of the development of satellite systems for Internet-of-Things services are considered.

1. Вступ

Події останніх років, що відбуваються на території України і пов'язані із відбиттям агресії рф, та розвиток технологій супутникових інформаційних систем призвели до формування нових поглядів та вимог до цих систем. Відомо, що на початковому етапі повномасштабної війни впровадження послуг низькоорбітальної супутникової системи широкосмугового доступу (ССШД) Starlink дозволило в стислі строки забезпечити скоординоване та контрольоване управління функціонуванням Сил оборони України. Разом із тим використання послуг тільки однієї супутникової системи призвело до критичної залежності систем зв'язку, управління та інформаційного забезпечення Сил оборони України від цієї системи, і створило передумови для загрози порушення функціонування цих інформаційних систем. Тому актуальним завданням став пошук альтернативних рішень, що можуть бути реалізовані шляхом залучення вже існуючих ССШД та систем, що знаходяться в стадії створення і формування орбітального угруповання та підготовки наземної інфраструктури.

Актуальність дослідження зумовлена зростаючим попитом на послуги супутникових телекомунікаційних систем, особливо на послуги широкосмугового доступу, який сформований на підставі більш ніж трирічного досвіду використання терміналів і послуг системи Starlink в Україні.

Метою доповіді є провести аналіз існуючих та перспективних супутникових телекомунікаційних систем, послуги яких можуть бути впроваджені в Україні, визначити тенденції в розвитку таких систем.

2. Основна частина

2.1. Впровадження архітектури 5G до супутникових інформаційних систем. Розвиток технології неназемних мереж NTN.

Архітектура мультиорбітальних супутникових систем, що передбачає безпосередню взаємодію між супутниками, що розташовані на різних орбітах

Розвиток технологій наземного мобільного широкосмугового доступу (НМШД) охоплює все більше технологій та сфер застосування технологій телекомунікацій. Це стосується і сегменту супутникових телекомунікаційних систем (СТС). Використання СТС рухається в напрямку від забезпечення підключення віддалених базових станцій (БС) мобільних операторів до магістральних каналів мережі радіодоступу і центрів мобільної комутації G2, або базової мережі EPC LTE. Важливий крок в подальшій інтеграції СТС до НМШД 5G зробила дослідницька група 3GPP в Релізі 17 [1]. В цьому документі введено поняття Неназемної мережі NTN (Non terrestrial networks), який визначає безліч сценаріїв зв'язку, починаючи від супутникового зв'язку і до зв'язку через повітряні станції, та враховує такі застосування, як керування польотом повітря-земля, або застосування в якості ретрансляторів безпілотних літальних апаратів. Особливе місце в технології NTN займає взаємодія із СТС, для яких передбачені різні сценарії зв'язку та використання супутників СТС на геостаціонарній орбіті (GEO), та на середній (MEO) і низькій навколоземній орбіті (LEO). Розглядаються різні зони покриття СТС та передбачено зв'язок між супутниками. Окремо потрібно виділити режим безпосереднього доступу чарунок стільникової мережі, де знаходяться термінали користувача (UE), до супутника D2C (Direct-to-Cell) [2].

Впровадження програмно-визначених мереж до мультиорбітальних систем

До особливостей систем 5G відноситься впровадження програмно-визначених мереж передачі даних SDN та віртуалізації мережевих функцій NFV. В ряді публікацій [3] розглядається це питання відносно архітектури NTN з D2S та з доступом через спеціалізовані термінали.

2.2. Створення геостаціонарних систем високої і надвисокої пропускної здатності, що забезпечують взаємодію з мережами та системами 5G.

Супутники Viasat-3

Архітектура сучасних СТС передбачає їх інтеграцію з архітектурою мереж 5G. Прикладом впровадження архітектури 5G в GEO системи є супутники серії Viasat-3 (США) [4]. Мережа супутників Viasat-3 має включати 3 супутники, що розташовані на GEO під взаємним кутом приблизно 120° для обслуговування практично всієї поверхні Землі. Корисне навантаження супутників побудовано за регенеративною схемою. Кожен супутник формує зону обслуговування із використанням майже тисячі надвузьких променів Ка-діапазону в таких регіонах: Америка; Європа, Близький Схід та Африка; Азіатсько-Тихоокеанський регіон [5]. Для формування надвузьких променів супутник обладнаний антеною діаметром 18 м. Загальна пропускна здатність кожного супутника становить понад 1 Тбіт/с та забезпечує динамічний перерозподіл пропускної здатності між променями. Швидкість передачі інформації до терміналу користувача становитиме до 100 Мбіт/с. Поява супутників серії Viasat-3 ознаменувала появу нового терміну: супутники з дуже великою пропускною здатністю VHTS (Very High-Throughput Satellite) та з ультра великою пропускною здатністю UHTS (Ultra-High Throughput Satellite). Україна, як й усі

Європа, входять до зони обслуговування другого супутника серії Viasat-3.

Шведсько-американська система Ovzon

В якості регіональної GEO системи супутникового зв'язку можна представити систему Ovzon (Швеція, США). Компанія Ovzon AB має власний GEO супутник і пропонує інтегровані послуги стаціонарного та рухомого супутникового зв'язку та передачі даних із використанням терміналів користувачів власної розробки [6]. Супутник Ovzon-3 обладнаний регенеративним корисним навантаженням на базі бортового процесора Ovzon (OBP) для створення mesh мережі в Ku-діапазоні з суверенним контролем. До відмінностей супутника також відноситься наявність керованих вузьких променів, орієнтація яких може змінюватись по командах з Землі. Для використанням послуг супутника Ovzon-3 спеціально розроблена лінійка терміналів користувачів, що включає малогабаритні термінали із параболічними антенами типу Ovzon Medium W/H, що забезпечують прийом інформації на швидкості 20-100 Мбіт/с та передачу на швидкості 1-70 Мбіт/с. Також лінійка терміналів включає плоскі термінали Ovzon T6 OTP (прийом на швидкості до 120 Мбіт/с та передача – до 70 Мбіт/с) та Ovzon T7 OTP (прийом на швидкості до 60 Мбіт/с, передача – до 10 Мбіт/с). Компанія Ovzon AB підтвердила ефективність використання запропонованих рішень в ході натурного експерименту по віддаленому керуванню безпілотним ровером UGV, що був обладнаний терміналом Ovzon F50 на дослідницькому центрі Кіруна з пункту управління в Стокгольмі. Відстань становила 950 км.

Повернення до ідеології використання малих геостаціонарних супутників на сучасній технологічній базі із використанням підходів до архітектури HTS

В якості цікавої тенденції щодо створення GEO систем із регіональним покриттям є проект компанії Astranis (США) із використанням малих GEO супутників. На відміну від традиційних підходів, супутники Astranis мають стартову масу порядку 600 кг [7], що більш ніж в десять разів менша за стартову масу порядку 6500 кг сучасних GEO супутників. Особливу увагу викликає платформа Omega, що побудована із використанням технології супутників VHTS щодо формування зони обслуговування надвузькими променямив Ка-діапазоні, та обладнана цифровим корисним навантаженням прозорого типу із загальною пропускною здатністю понад 50Гбіт/с. В конструкції супутника та його корисного навантаження використовуються сучасні технології програмно-визначеного радіо SDR, ефективної Холлівської рушійної системи та радіаційно стійкої електроніки. Мала стартова вага супутників дозволяє забезпечувати кластерний запуск одночасно 4 супутників на GEO. Привабливість такого рішення для України полягає в можливості створити отримати власну СТС із супутником на GEO, що покриває виключно територію України і надає пропускну здатність, що порівняна із пропускною здатністю LEO систем як то Starlink.

2.3. Формування мереж надвисокої пропускної здатності на середній навколоземній орбіті. Комплексне поєднання ресурсу систем на середній навколоземній та геостаціонарній орбітах.

Система O3b/mPOWER компанії SES – система надвисокої пропускної здатності на середній навколоземній орбіті

Компанія SES (Люксембург), яка є провідним оператором супутникових систем на GEO та MEO завершує оновлення власного угруповання O3b за рахунок запуску супутників O3b/mPOWER [8]. Супутники знаходяться на орбіті висотою 8200 км в площині екватора. Орбітальне угруповання системи складається з 11 супутників. Така конфігурація дозволить забезпечити надання послуг на всій території України в режимі 24/7. Супутники побудовані на базі платформи Boeing-702 і обладнані цифровим корисним навантаженням та фазованими антенними решітками. Кожен супутник здатен формувати до 5000 незалежних керованих променів в Ка діапазоні із пропускною здатністю від 40 Мбіт/с до 10 Гбіт /с (для окремого променю). Компанія декларує можливість встановлення станції спряження безпосередньо на території замовника, тобто

в Україні, що забезпечить підключення супутникового сегменту до національної магістральної мережі зв'язку та передачі даних. Система O3b/mPOWER призначена для надання послуг для урядових структур, включаючи Сили Оборони, та для цивільних корпоративних і приватних користувачів. Для користувачів розроблена та сертифікована лінійка різних терміналів. Особливу увагу с точки зору мобільних користувачів привертають термінали Hydra-2, Hydra-4, розроблені компанією AllSpace [9]. Термінали забезпечують одночасну роботу із супутниками на GEO та MEO в частотних діапазонах Ku та Ka, і використовують технологію формування керованих променів методом дійсної затримки випромінення випромінювачів (TTD, Thue Time Delay).

2.4. Тенденції розвитку низькоорбітальних систем широкосмугового доступу: цифрове регенеративне корисне навантаження, лазерні лінії зв'язку між супутниками, безпосередній доступ терміналів користувачів 4G, 5G до супутника.

Система Starlink впровадила оптичні ланаї зв'язку між супутниками та розпочала формувати угруповання для послуг D2C

Компанія SpaceX та Starlink залишаються лідерами з впровадження перспективних рішень в ССШД Starlink. По-перше, SpaceX продовжує нарощування складу орбітального угруповання Starlink, збільшивши кількість функціонуючих супутників до 7105 одиниць (на орбіті знаходяться 7135 супутників). Зараз для продовження формування орбітального угруповання запускаються супутники типу Starlink V2-mini, маса яких становить ~560-700кг. Супутники використовують Ku та Ka діапазони. Кожен супутник формує 16 керованих променів Ku-діапазону до користувачів (на відміну від 8 променів в супутниках першого покоління Starlink V0.9). Корисне навантаження супутників Starlink забезпечують маршрутизацію потоків на борту.

Компанія Starlink впровадила лазерні лінії зв'язку між супутниками. Кожен супутник Starlink обладнаний трьома оптичними трансіверами. Оптичні лазерні лінії забезпечують передачі інформації зі швидкістю до 200 Гбіт/с і утворюють глобальну mesh-мережу для забезпечення послуг споживачам в будь якій точці на поверхні Землі [12]. Проведені експерименти показали, що лазерна система Starlink змогла з'єднати два супутники, що знаходяться на відстані понад 5400 кілометрів один від одного. Зв'язок був настільки довгим, що він прорізав атмосферу аж до висоти 30 кілометрів над поверхнею Землі, перш ніж з'єднання розірвалося. Лазерні лінії використовуються для зв'язку супутника Starlink з двома сусідніми супутниками в своїй орбітальній площині і з одним супутником в орбітальній площині, що перетинається для вирішення проблеми «зшивання» орбітального угруповання.

Введення до складу системи лазерних ліній зв'язку між супутниками дозволили змінити структуру тракту надання послуг. Точка присутності PoP (Point-of-Present) забезпечує підключення до провайдерів послуг та є вхідних інтерфейсом для системи Sytarlink. Точка присутності підключена лінією оптико-волоконного зв'язку до станції спряження (GateWay), яка забезпечує підключення супутників Starlink до наземної мережі зв'язку через окремий промінь Ka-діапазону до станції спряження. В залежності від розташування кореспондента, супутник здійснює маршрутизацію інформаційного потоку в промінь до користувача, або в оптичну лінію зв'язку між супутниками. Ділянка між точкою присутності PoP та терміналом користувача має наскрізне AES-шифрування.

Ще одним напрямком розвитку послуг системи Starlink є впровадження послуг безпосереднього доступу пристроїв користувачів як то смартфон та планшет, до супутника, тобто послуга типу D2C (Direct-to-Cell) [10,11]. Мережа Direct-to-Cell забезпечує підключення та безперешкодний доступ до текстових повідомлень, голосу та даних для телефонів та пристроїв LTE по всьому світу в смузі частот 1800 МГц. Послуги текстових повідомлень розпочались в 2024 році, а у 2025 році — голосові, дані та послуги Інтернету речей (IoT). Для реалізації цього завдання супутники Starlink V.2mini-D2C обладнані фазованою антенною решіткою розміром 2,7 м × 2,3 м. Для надання послуг D2D компанія Starlink звернулась до Федеральної комісії зі зв'язку США (FCC) щодо

отримання ліцензій на використання орбіт висотою 340 км та нахиленням 53° та 360 км 96,9°, які отримали назву дуже низькі орбіти Very Low Earth Orbit (VLEO). Також до FCC подані заявки на отримання смуг частот в частотних діапазонах Q/V.

Нажаль до сьогодні якість послуг системи Starlink в Україні залишається такою, що не відповідає встановленим вимогам та корпоративним стандартам [15]. Основна причина полягає у відсутності на території України станції спряження. Користувачі в Україні обслуговуються станціями спряження Воля Кробовска (Польща) та Каунас (Литва).

Система Eutelsat OneWeb – інтеграція послуг низькоорбітальної та геостаціонарної складових.

Для диверсифікації послуг ССШД в Україні можливе використання послуг системи Eutelsat OneWeb [13]. За підсумками першого півріччя 2023 року Система OneWeb завершила формування повного орбітального угруповання у складі 648 супутників. Супутники розміщені у 18 орбітальних площинах на низькій навколоземній орбіті висотою 1200 км з нахиленням 87,9°. Система має спрощену архітектуру в порівнянні з Starlink. Кожен супутник OneWeb формує 16 некерованих променів Ku-діапазону до користувачів, які разом покривають територію 1100×1100 км. Формування трафіку для кожного променю здійснює станція спряження на підставі координат терміналів користувачів. Кожен супутник підтримує зв'язок із станцією спряження із використанням променю Ка-діапазону, в якому у окремих 8 смугах в двох поляризаціях передається трафік для 16 променів користувачів. На борту супутника здійснюється перенос смуги частот з КА-діапазону в Ku-діапазон та в зворотному напрямку. Термінал користувача змінює промінь кожні 18 сек., та змінює супутник кожні 2хв. 40сек. Регіональний трафік формується в точці присутності. Система Eutelsat OneWeb забезпечує 100% покриття території України із використанням станції спряження, що розташована в Болгарії.

Придбання компанією Eutelsat, яка є провідним оператором GEO супутників, компанії і LEO системи OneWeb створило умови для надання комплексних послуг LEO-GEO системи. Для реалізації цієї послуги можуть бути використані термінали Kymeta Hawk u8 [14]. Програмно-визначена та електронно керована антена u8 працює у всьому Ku-діапазоні. Плоскі панелі – термінали Kymeta Hawk u8 мають низькопрофільний аеродинамічний дизайн. На відміну від терміналів Starlink, в антенах типу Kymeta U8 застосована голографічна технологія формування променю із використанням жидкокристалічної технології LED та метаматеріалів. Антена Kymeta U8 оснащена модемною платою iQ 200 від ST Engineering iDirect, яка забезпечує ключові функції антени, зокрема: високу продуктивність та ефективність з прийнятим сигналом DVB-S2/DVBS2X та адаптивним зворотнім сигналом TDMA, безпечне 256-бітове AES-шифрування.

Система Amazon Kuiper розпочинає формування орбітального угруповання

В 2025 році розпочинається формування орбітального угруповання ССШД Amazon Kuiper [16]. Угруповання супутників складатиметься з 3 232 супутників, що розташовані в 98 орбітальних площинах на низькій навколоземній орбіті на висотах 590 км, 610 км та 630 км. Супутники будуть запущені в кілька етапів, причому на першому етапі буде розгорнуто 578 супутників на висоті 630 км з нахиленням орбіти 51,9°. Така конфігурація орбітального угруповання здатне забезпечити повне покриття території України та надання послуг в режимі 24/7. Система Amazon Kuiper використовує частоти, виділені фіксованій супутниковій службі FSS та рухомій супутниковій службі MSS в Ка-діапазоні в смугах частот: 27,5–27,8185 ГГц, 28,4545–28,8265 ГГц, 29,5–30 ГГц. В цих смугах частот здійснюється формування керованих променів до користувачів та до станцій спряження. В архітектурі орбітального угруповання використовуються лінії зв'язку між супутниками.

Структура тракту надання послуги включає: точку присутності PoP, до якої підключаються зовнішні інформаційні мережі; PoP через орендовані лінії волоконно-оптичного зв'язку підключені до станцій спряження GateWay, які підключені до супутників Kuiper через промені до станцій спряження. Користувачі отримають доступ до

супутника Kuiper через керовані промені до користувачів.

На супутниках Amazon Kuiper встановлене програмно конфігуроване корисне навантаження регенеративного типу, яке перепрограмовується для забезпечення пропускної здатності на основі потреб клієнтів у обслуговуваних районах. Підсистема мережевого та маршрутизаційного навантаження налаштовується наземними мережевими операціями системи Kuiper для попереднього програмування променів у відповідні віртуальні точки на землі. Весь висхідний та низхідний трафік повністю регенерується на супутнику, а між променями здійснюється маршрутизація/комутація/перепакування. Модеми підтримують широкий спектр варіантів модуляції та кодування, включаючи завадостійке кодування із пониженою щільністю перевірок на парність LDPC. Кожен модем підтримує адаптивне кодування та модуляцію для кожного каналу зв'язку та підтримує черги якості обслуговування для належної буферизації даних. Підсистема мережевого та маршрутизаційного навантаження підтримує кілька рівнів якості обслуговування, що дозволяє забезпечити виконання угод про рівень обслуговування.

Для надання послуг кінцевим споживачам система Amazon Kuiper пропонує кілька типів терміналів: надкомпактна модель, що забезпечує швидкість до 100 Мбіт/с; стандартна модель, що забезпечує швидкість до 400 Мбіт/с; найбільша модель, призначена для корпоративних, урядових та телекомунікаційних застосувань, забезпечує швидкість до 1 Гбіт/с. Усі моделі побудовані у вигляді плоских панелей та використовують технологію фазованих антенних решіток.

Заявлені характеристики системи Amazon Kuiper показують наміри компанії Amazon створити ССШД, що стане конкурентом системі Starlink.

Система AST-Space Mobile – впроваджує послуги 4G/5G в режимі D2S, що не передбачає модернізації терміналів користувачів

На сегмент ринку послуг у форматі D2S згідно архітектури 5G є проект створення системи AST Space Mobile [17]. Компанія AST SpaceMobile та її партнери по сьому світу будують першу і поки що єдину стільникову широкосмугову мережу космічного базування, яка забезпечуватиме доступ для стандартних смартфонів та планшетів (без будь-яких модернізацій). Ця стільникова мережа призначена для забезпечення підключень за стандартами та на швидкостях 4G/5G повсюди в межах зони обслуговування. 10 вересня 2022 року компанія AST SpaceMobile здійснила запуск супутника BlueWalker 3, який є попередником комерційних супутників під назвою BlueBirds. Супутник був побудований з апертурою ~64,5 м² для безпосереднього зв’язку з мобільними телефонами в смугах частот стандартів 3GPP. За допомогою цього супутника компанія AST SpaceMobile у партнерстві з Vodafone, AT&T та Nokia продемонструвала можливість надання послуг широкосмугового зв’язку 5G із використанням стільникової технології космічного базування, досягнувши швидкості передачі даних 14 Мбіт/с після успішних випробувань 4G. 12 вересня 2024 року були запущені п’ять комерційних супутників Блок 1 BlueBird на LEO.

Згідно із заявкою, до була подана в квітні 2020 року компанією AST & Science LLC до FCC (США), система передбачає використання орбітального угруповання у складі 243 супутників в 16 орбітальних площинах на орбітах між 725 та 740 км із нахиленням від 40° до 55°. Кожен супутник формуватиме 2800 променів до користувачів та 3 промені до станцій спряження.

Структура надання послуг включає станцію спряження, що забезпечує підключення до наземної магістральної мережі супутників із використанням фідерних ліній Q/V діапазонів. Термінали користувачів типу смартфон/планшет отримають безпосередній доступ до супутника в режимі D2S.

Європейська система захищеного зв’язку.

Зважаючи на результати використання в Україні системи Starlink в умовах повномасштабної війни, Європейський Союз прийняв рішення про створення власної багатоорбітальної системи захищеного зв’язку IRIS² (Infrastructure for Resilience,

Interconnectivity and Security by Satellite) [18]. Система, що буде надавати послуги на основі протоколів інтернет. Початок розгортання системи заплановано до 2027 року. Очікується, що початкові послуги державним користувачам будуть надаватись починаючи з 2030 року.

Система IRIS² складатиметься з 264 супутників на LEO на висоті 1200 км та 18 супутників на MEO на висоті 8000 км. Система призначена для забезпечення безпечного зв'язку, відстеження місцезнаходження та послуг спостереження за безпекою для урядових установ, що безпосередньо порівнюється з проектом Starshield американської компанії SpaceX.

Система також має на меті забезпечити широкосмуговий доступ для приватних компаній та громадян. На момент підписання контракту в грудні 2024 року оціночна вартість становила 10,5 мільярда євро, з яких 6,5 мільярда євро – державні кошти. IRIS² є частиною загальної космічної стратегії ЄС, включаючи Космічну стратегію ЄС щодо безпеки та оборони. Європейське космічне агентство (ЄКА) відповідає за розробку та розгортання системи, а Агентство Європейського Союзу з космічної програми (EUSPA) відповідає за надання державних послуг.

2.5. Вплив методу групового кластерного запуску на конструкцію космічних апаратів супутникових телекомунікаційних систем.

Платформи космічних апаратів для низькоорбітальних мультисупутникових систем.

Створення мультисупутникових систем, формування яких здійснюється із використанням запусків пакетів супутників в кілька десятків в одному запуску призвело до активізації розробки платформ LEO супутників, конструкція яких спеціально адаптована до умов групового запуску. Першими в цьому стали супутники Starlink V0.9. Подальші модернізації платформ супутників Starlink V2, V2mini також рухаються в цьому напрямку. Так супутники Starlink V2mini відрізняються від супутників Starlink V0.9 більшим розміром, кількістю фазованих антенних решіток, лазерними трансіверами і використанням двох панелей сонячних батарей замість однієї. Але плоска форма корпусу супутника збережена, що дозволяє формувати пакет з десятків супутників для групового запуску.

За прикладом Starlink американська компанія Rocket Lab оголосила про створення платформи Flatellite, що спеціально призначена для серійного виробництва супутників і адаптована для великий орбітальних угруповань [19]. При створенні платформи Flatellite компанія Rocket Lab інтегрувала традиційні компоненти та підсистеми, що мають досвід орбітального використанні, включаючи рушійну установку, програмне забезпечення для польоту, авіоніку, двигуни-маховики, зоряні датчики, систему розділення, сонячні батареї, радіостанції, композитні конструкції, паливні баки тощо.

На замовлення НАСА Аерокосмічна корпорація (Ел Сегундо, Каліфорнія) розробила демонстраційний макет супутника DiskSat товщиною 2,5 см та діаметром 1 м [20]. Аерокосмічна корпорація за підтримки Управління космічних технологій NASA (STMD) готує політ чотирьох DiskSat для запуску в 2026 році, щоб продемонструвати доцільність як диспенсера, так і платформи DiskSat.

Американська компанія SpinLaunch уклала контракт на суму 122,5 мільйона євро з компанією Kongsberg NanoAvionics на будівництво перших 282 супутників для комунікаційного угруповання Meridian Space компанії [21]. Meridian Space – це LEO угруповання телекомунікаційних супутників, розроблене SpinLaunch для надання глобальних високошвидкісних широкосмугових послуг корпоративним клієнтам. За даними SpinLaunch, супутники Meridian Space матимуть плоский форм-фактор, що дозволить розгорнути до 250 одиниць за один «традиційний ракетний запуск». 2 квітня NanoAvionics оголосила про укладення контракту на будівництво 282 супутників для угруповання SpinLaunch Meridian Space. Угода включає два орбітальні демонстратори та серійне виробництво перших 280 супутників у угрупованні, яке, як очікується, зросте щонайменше до 1190 космічних апаратів. Запуск першого демонстратора заплановано на

2026 рік, і він використовуватиме стандартну мікросупутникову шину MP42 NanoAvionics для перевірки корисного навантаження зв'язку SpinLaunch Meridian.

Компанія Terran Orbital оголосила про створення лінійки платформи Enterprise [22], що базується на довгій лінійці SmallSat, використовуючи ту саму авіоніку та алгоритми GNC, що й менші класи платформ супутників. Значні вдосконалення конструкції підтримують найбільші корисні навантаження та включають функцію оптичного міжсупутникового зв'язку (OISL). Для зменшення ваги та збільшення потужності, доступної для корисного навантаження, була розроблена нова система енергоживлення. Платформа Enterprise є однією з найбільших платформ, що пропонуються в стандартній лінійці продуктів, і є відправною точкою для вимог до плоского пакування, що дозволяє доставляти до 24 супутників за один запуск. Вона оптимальна для великих систем та доступна в трьох конфігураціях.

Платформа для малих геостаціонарних супутників.

Зважаючи на відновлення ринку малих GEO супутників компанія Terran Orbital розробила власне рішення – платформу SmallSat GEO™. Платформа дозволяє створити GEO супутник масою до 1250 кг, розмістити корисне навантаження до 300 кг, забезпечити постачання енергоживлення до 3 кВт та строк орбітальної експлуатації не менше 7 років.

2.6. Розвиток супутникових систем та послуг інтернету речей.

Дрейф операторів існуючих низькоорбітальних систем персонального зв'язку в напрямку послуг Інтернету речей.

Зважаючи на активне впровадження в СТС архітектури 5G, протягом останніх років на ринок почали активно виходити супутникові LEO системи інтернету речей IoT (Internet-of-Things). Першими в цьому сегменті ринку з'явились оператори LEO систем персонального супутникового зв'язку Iridium та Global Star [23,24]. Вихід на ринок ССШД призвів до дрейфу попиту в напрямку широкосмугових послуг і втрати цими компаніями їх звичайного ринку. Тому ці компанії звернули увагу на новий сегмент – IoT. Незважаючи на повний склад орбітального угруповання та багаторічний досвід експлуатації, до недоліків цих систем можна віднести використання пропрієтарних протоколів доступу.

Низькоорбітальні супутникові систем Інтернету речей на базі мікросупутників та кубсатів.

З іншого боку, розвиток технології мікро- та наносуптуників – CubSat в поєднанні із виходом на ринок візькосмугових протоколів IoT великого радіусу дії, як то NB-IoT та LoRaWAN, стали технологічною основою для появи спеціалізованих супутникових LEO систем IoT, що побудовані із використанням CubSat. Зважаючи на гетерогенний характер мереж радіодоступу в стандарті 5G, ці системи органічно вписуються в створювану екосистему NTN 5G.

Astrocast – це система швейцарської стартап-компані супутникового зв'язку з власною глобальною мережею наносупутників IoT для відстеження, моніторингу, управління та зв'язку з активами у віддалених регіонах світу [25]. Компанія базується поблизу Лозанни у Швейцарії. Маючи систему з 100 наносупутників, Astrocast надає повний комплексний сервіс прямого виведення на орбіту, що включає найсучасніші комунікаційні модулі та послуги корпоративного класу. Система побудована із використанням протоколу LoRaWAN. Для надання послуг компанія Astrocast розробила спеціальні чіпсети, що встановлюються в модуль Astronode S.

У 2018 році за ініціативою CNES (Франція) була створена компанія Kinéis [26]. Мета створення компанії - експлуатації системи Argos, що є результатом міжнародного наукового співробітництва між CNES (Франція), Національним управлінням океанічних і атмосферних досліджень (NOAA), Європейською організацією з експлуатації метеорологічних супутників (EUMETSAT) та Індійською організацією космічних досліджень (ISRO), для моніторингу дикої природи, рибальства та збору даних про клімат і навколишнє середовище Землі за допомогою CLS і призначена для ринку Інтернету

речей (IoT). Зараз система Kinéis має 25 наносупутників, що розташовані в п’яти орбітальних площинах на сонячно-синхронні орбіті. 18 березня 2025 року компанія Rocket Lab за допомогою ракети-носія Electron запустила фінальні 5 супутників, що завершило формування орбітального угруповання із 25 супутників. Нове орітальне угруповання Kinéis доповнить існуючу систему потужнішими наносупутниками класу 30 кг, які інтегрують технологію IoT та систему автоматичної ідентифікації (AIS) для відстеження суден. Після розгортання ця технологія дозволить Kinéis розширюватися охоплюючи різні галузі та масштабуватися з 20 000 підключених пристроїв до мільйонів.

Висновки.

Аналіз стану та напрямків розвитку супутникових телекомунікаційних систем свідчить про певні тенденції, а саме:

1. Протягом останнього часу відстежується тенденція щодо інтеграції супутникових систем та мобільних мереж 4G, 5G. Дослідницька група 3GPP визначила технологічні умови взаємодії мережі 5G та супутникових систем у форматі неназемних мереж NTN.

2. Інтеграція супутникових систем із мережами 5G створює передумови для конвергенції архітектури 5G до супутникових систем. Важливою відмінністю мереж 5G від попередніх генерацій є впровадження технологій програмно-визначених мереж та віртуалізації мережевих функцій. При розробці архітектури мультиорбітальних супутникових систем NTN окрема увага приділяється цим технологіям.

3. Сталою тенденцією в розвитку супутникових телекомунікаційних систем є освоєння більш високих діапазонів частот. Після Ка-діапазону оператори супутникових систем звернулись до частотних діапазонів Q та V. Відносно новим напрямком є вивільнення частотного діапазону С від наземних систем для використання супутниковими системами.

4. Геостаціонарні системи залишаються важливою складовою супутникових телекомунікаційних систем. За останнє десятиріччя в секторі геостаціонарних супутників відстежується тенденція до еволюційного переходу від супутників великої пропускної здатності HTS до супутників надвеликої пропускної здатності VHTS і супутників ультравеликої пропускної здатності UHTS. Усі знов створені системи здатні взаємодіяти з мережами 5G. До основних особливостей технологій HTS, VHTS та UHTS відносяться: формування зони обслуговування за рахунок великої кількісті (до тисячі) надвузьких променів Ка-діапазону до користувачів та використання цифрового регенеративного корисного навантаження. Для України особливу зацікавленість представляють проекти Viasat-3, Ovzon та Astranis. Наявність власної наземної інфраструктури значно поліпшить якість послуг та сприятиме підвищенню гнучкості, безпеки і надійності інформаційних мереж на їх основі.

5. Система O3b/mPOWER компанії SES, що використовує середню навколоземну орбіту MEO, є ефективним засобом широкосмугового зв’язку на швидкостях від 50 Мбіт/с до 1 Гбіт/с. Зважаючи на власний флот геостаціонарних GEO супутників компанія SES здатна запропонувати в Україні комплексу MEO-GEO послугу. Термінали Hydra 2, Hydra 4, що розроблені компанією all.space, призначені для одночасної роботи з супутниками на різних орбітах в широкому діапазоні частот. Компанія SES декларує можливість встановити станцію спряження на території замовника послуги, тобто в Україні, в разі бажання замовника.

6. Starlink залишається лідером у впровадженні нових рішень в низькоорбітальних системах широкосмугового доступу. Нове покоління супутників Starlink забезпечує лазерний зв’язок між супутниками та надання послуг в режимі «до чарунки стільникової мережі» (D2C). Система Starlink планує розширення доступної смуги частот за рахунок частотних діапазонів V та Q, і опанування наднизьких навколоземних орбіт VLEO.

7. Компанія Eutelsat після отримання системи OneWeb здатна надавати послуги широкосмугового доступу на території України, що певним чином диверсифікує постачання послуг широкосмугового супутникового доступу, та має можливість надавати комплексу послугу із використанням власного супутникового ресурсу на геостаціонарній

та низькій навколоземній орбіті GEO-LEO. Термінали Kymeta U8 є ефективним засобом для надання послуг GEO-LEO кінцевим користувачам.

8. Компанія Amazon Kuiper починає формування власного орбітального мультисупутникового угруповання. За своїми архітектурними особливостями та показниками послуг система близька до системи Starlink, але використовує більш високий Ка-діапазон в лінії до користувача. Послуги системи можуть бути доступні в Україні найближчим часом. Виходячи з досвіду використання послуг систем Starlink та Eutelsat OneWeb для поліпшення якості послуг створюваної системи Amazon Kuiper доцільно вирішити питання про будівництво в Україні станції спряження та точки присутності.

9. Система AST Space Mobile орієнтована на надання послуг користувачам мереж 4G/5G, що знаходяться поза межами зони обслуговування наземних мереж. До особливостей системи відноситься пропозиція послуги доступу терміналу користувача «безпосередньо до супутника» D2S, що не вимагає модернізації терміналів користувачів типу смартфон та планшет. Для впровадження послуг в Україні потрібна підготовка наземної інфраструктури – станції спряження.

10. Вимоги до перспективної європейської мільтиорбітальної системи захищеного зв'язку IRIS² сформовані із врахуванням досвіду використання супутникових систем широкосмугового доступу в Україні. Зважаючи на прагнення України щодо вступу до Європейського Союзу, в перспективі потрібно передбачати інтеграцію із інформаційними та телекомунікаційними мережами ЄС, до яких безперечно відноситься система IRIS².

11. Досвід формування мультисупутникових систем вплинув на конструктивні рішення щодо супутників. Сталою тенденцією в проектуванні супутників для таких систем стала плоска конфігурація, яка в найбільшій мірі адаптована до кластерного запуску пакету супутників однією ракетою-носієм.

12. Після виходу на ринок низькоорбітальних супутникових систем широкосмугового доступу та зважаючи на перспективи впровадження послуг систем, що сумісні з мережами 4G та 5G, оператори низькоорбітальних супутникових систем персонального зв'язку перенесли свою увагу на послуги Інтернету речей IoT на базі власних традиційних протоколів. Одночасно із цим почалось створення низькоорбітальних супутникових систем IoT із використанням малих супутників класу мікро- та наносупутник, або кубсат, що базуються на протоколах IoT великої дальності типу NB-IoT та LoRaWAN.

Література

1. NTN & Satellite in Rel-17 & 18. Електронний документ. Режим доступу: https://www.3gpp.org/news-events/partner-news/ntn-rel17
2. 5G NTN TAKES FLIGHT: TECHNICAL OVERVIEW OF 5G NON-TERRESTRIAL NETWORKS / Rohde & Schwarz White Paper | 5G NTN takes flight: Technical overview of 5G non-terrestrial networks / PD 3683.7383.52 | Version 01.00 | July 2022 (ch) | White Paper / © 2022 Rohde & Schwarz GmbH & Co. KG | 81671 Munich, Germany.
3. A Service Function Chain Deployment Scheme of the Software Defined Satellite Network / Wenxin Qiao, Xianglong Ni, Yu Lu, Xiongwei Li, Donghao Zhao, and Yicen Liu / Hindawi. Mobile Information Systems.Volume 2022, Article ID 6402481, 17 pages / https://doi.org/10.1155/2022/6402481
4. Interference-Limited Scenarios / Електронний документ. Режим доступу: https://www.viasat.com/about/what-we-do/satellite-fleet/viasat-3/
5. How 3D-Printing Is Changing RF Front-End Design for Space Applications / Oscar A. Peverini (Member, IEEE), Mauro Lumia (Member, IEEE), Giuseppe Addamo (Member, IEEE), Giuseppe Virone (Senior Member, IEEE), and Nelson J. G. Fonseca (Senior Member, IEEE) / IEEE Jornal of Microwaves / Digital Object Identifier 10.1109/JMW.2023.3250343
6. Celebrating One Year Since the launch of Ovzon 3 / Електронний документ. Режим доступу: https://www.ovzon.com/en/
7. Purpose-built for high orbits. Astranis satellites bring connectivity to remote areas, support the

US military, and provide critical capabilities like GPS / Електронний ресурс. Режим доступу: https://www.astranis.com/spacecraft
8. O3b mPOWER / Електронний ресурс. Режим доступу: https://www.ses.com/o3b-mpower
9. Hydra 2 (Dual-link) Ka Terminal / Електронний ресурс. Режим доступу: https://www.all.space/products-services/hydra-2
10. First Starlink Satellite Direct-To-Cell Phone Constellation Is Now Complete / Електронний документ. Режим доступу: https://insidetowers.com/first-starlink-satellite-direct-to-cell-phone-constellation-is-now-complete/
11. STARLINK DIRECT TO CELL. Engineered to eliminate mobile dead zones around the world. Service now available / Електронний ресурс. Режим доступу: https://www.starlink.com/business/direct-to-cell
12. Starlink's Laser System Is Beaming 42 Million GB of Data Per Day / Електронний документ. Режим доступу: https://www.pcmag.com/news/starlinks-laser-system-is-beaming-42-million-gb-of-data-per-day
13. Experience the Eutelsat OneWeb difference / Електронний ресурс. Режим доступу: https://oneweb.net/our-network/experience-oneweb
14. Hawk u8 / Електронний ресурс. Режим доступу: https://www.kymetacorp.com/products/hawk-u8
15. Електронний ресурс. Режим доступу: https://www.starlink.com/map?view=availability
16. Here's what to expect from Project Kuiper's first full-scale satellite launch. United Launch Alliance will send 27 Kuiper satellites into low Earth orbit as we begin a full-scale deployment of our satellite internet network / Електронний ресурс. Режим доступу: https://www.aboutamazon.com/news/innovation-at-amazon/project-kuiper-satellite-internet-first-launch
17. Space 5G Cellular Broadband / Електронний ресурс. Режим доступу: https://ast-science.com/
18. IRIS² / Електронний ресурс. Режим доступу: https://www.euspa.europa.eu/eu-space-programme/secure-satcom/iris2
19. Rocket Lab Announces Flatellite: A New Satellite Designed for Mass Manufacture and Tailored for Large Constellations / Електронний ресурс. Режим доступу: https://www.rocketlabusa.com/updates/rocket-lab-announces-flatellite-a-new-satellite-designed-for-mass-manufacture-and-tailored-for-large-constellations/
20. What is a DiskSat? Thinking Outside the CubeSat Box: DiskSat – A New Circular Small Spacecraft Designhttps / Електронний ресурс. Режим доступу: www.nasa.gov/smallspacecraft/disksat/
21. Meridian Space is a low-cost, highly differentiated LEO satellite communications constellation offering enterprises unmatched speed, reliability and flexibility / Електронний ресурс. Режим доступу: https://www.spinlaunch.com/meridianspace
22. CONNECTING THE WORLD / Електронний ресурс. Режим доступу: https://terranorbital.com/spacecraft-platforms/enterprise/
23. What is Satellite IoT and How is it Used? / Електронний ресурс. Режим доступу: https://www.iridium.com/blog/what-is-satellite-iot-and-how-is-it-used/
24. Industrial IoT Asset Tracking / Електронний ресурс. Режим доступу: https://www.globalstar.com/en-us/products/iot
25. A direct-to-satellite IoT connectivity service to scale-up your remote operations around the globe / Електронний ресурс. Режим доступу: https://www.astrocast.com/
26. Spatial IoT connectivity for humans, their activities, and their environment / Електронний ресурс. Режим доступу: https://www.kineis.com/en/spatial-iot-connectivity/

УДК 621.39

ДОСЛІДЖЕННЯ ХМАРНИХ СЕРВІСІВ І ПЛАТФОРМ ДЛЯ ПОБУДОВИ ЗАСТОСУНКІВ IoT

[1]Poonam Yadav, [1]Mohit Bidikar, [2]Осипчкук С.О., [2]Родічев І.Д.
[1] Department of Computer Science, University of York, England
[2]Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Київ, Україна
E-mail: poonam.yadav@york.ac.uk, mb2596@york.ac.uk, osypchuk.serhii@lll.kpi.ua, rodichev.igor@lll.kpi.ua

CLOUD SERVICES AND PLATFORMS RESEARCH FOR IOT APPLICATIONS DEPLOYMENT

The paper analyzes, considers selection criteria, and provides examples of choosing cloud services and platforms for building IoT applications.

В роботі проведено аналіз, розглянуто критерії вибору та наведено приклади вибору хмарних сервісів і платформ для побудови застосунків IoT.

Постановка завдання. У проектуванні і впровадженні сучасних IoT застосунків одним із ключових технічних рішень є вибір середовища для розгортання і впровадження функцій передавання, збереження і обробки інформації для функціонування IoT застосунку. Таке рішення приймається на основі специфіки застосунку IoT, його користувачів, кількості даних, необхідності масштабування застосунку, та бюджету для впровадження IoT застосунку. Отже, знання сучасних хмарних сервісів і платформ для побудови застосунків IoT є актуальним знянням сучасного інженера інфокомунікаційних систем.

Сучасні хмарні сервіси відіграють ключову роль у розвитку IoT-екосистем, забезпечуючи зручні інструменти для збору, обробки та аналізу даних. До найбільш популярних рішень належать AWS IoT, Azure IoT Hub, Google Cloud IoT, IBM Watson IoT та інші. Вони пропонують різні підходи до управління пристроями, забезпечення безпеки, масштабованості та інтеграції. Вибір конкретної платформи залежить від вимог до продуктивності, аналітичних можливостей та підтримки специфічних протоколів зв’язку.

Критерії вибору IoT-платформи. Вибір оптимальної IoT-платформи залежить від низки ключових критеріїв (Табл. 1), таких як аналітика, машинне навчання, зберігання даних, інтеграція з пристроями, вартість рішення, тощо.

Розширені аналітичні можливості та підтримка машинного навчання є критичними для побудови інтелектуальних IoT-систем. Наприклад, AWS IoT Greengrass дозволяє виконувати локальну обробку даних, тоді як Google Cloud IoT інтегрується з Google AI для складного аналізу даних. Наявність інструментів для аналітики та прогнозування допомагає оптимізувати роботу IoT-систем і зменшити витрати.

Обсяг, тип та швидкість доступу до даних є важливими факторами при виборі платформи. AWS надає такі сервіси, як S3 та DynamoDB для масштабованого зберігання, тоді як Azure IoT Hub інтегрується з Cosmos DB для роботи з великими масивами інформації. Важливо враховувати не лише можливості збереження, а й витрати на обробку та доступ до даних.

Таблиця 1. Критерії вибору хмарних IoT-платформ [1-3].

Критерій	**AWS IoT Core**	**Azure IoT Hub**	**Google Cloud IoT**	**IBM Watson IoT**	**ThingSpeak**
Підтримка протоколів	MQTT, HTTPS, WebSockets	MQTT, AMQP, HTTPS	MQTT, HTTP, CoAP	MQTT, HTTP	MQTT, HTTP, CoAP, WebSockets
Зберігання даних	S3, DynamoDB, Timestream	Cosmos DB, Blob Storage	Cloud Storage, Bigtable	Cloudant, Db2	PostgreSQL, InfluxDB (залежно від конфігурації)
Масштабованість	Висока, автоматичне масштабування	Висока, гнучкі сервіси	Висока, підтримка глобальних IoT-мереж	Висока, орієнтація на бізнес-рішення	Від середньої до високої, залежить від розгортання
Локальна обробка	AWS IoT Greengrass	Azure IoT Edge	Edge TPU, Cloud Functions	Edge Analytics	Можлива через сторонні рішення
Аналітика та машинне навчання	AWS IoT Analytics, Greengrass ML	Вбудована аналітика, інтеграція з Azure AI	BigQuery, AutoML, Google AI	IBM Cloud AI, Watson Analytics	Обмежена, залежить від інтеграцій
Вартість	Pay-as-you-go, безкоштовний рівень	Pay-as-you-go, безкоштовний рівень	Pay-as-you-go, є безкоштовний рівень	Дорого для корпоративних рішень	Безкоштовно і низька за хостинг та розширення

Підтримка широкого спектру протоколів зв’язку є необхідною умовою для IoT-платформи. Як показано у Табл. 1, у категорії "Зберігання даних" переміг AWS IoT Core, завдяки гнучкому та масштабованому зберіганню (S3, DynamoDB, Timestream). Найкращою платформою за "Підтримкою протоколів" став Azure IoT Hub, оскільки підтримує MQTT, AMQP та HTTP, що забезпечує універсальність підключення. За "Масштабованістю" лідерами є AWS IoT Core та Google Cloud IoT, оскільки обидві платформи надають автоматичне масштабування для великих IoT-мереж. У категорії "Вартість" переможцем стало open-source рішення ThingSpeak оскільки воно забезпечує найдешевший варіант для гнучких IoT-рішень.

У той же час, варто пам’ятати, що кожна платформа має свої переваги і недоліки для реалізації продукту, в залежності від специфічних вимог IoT застосунку.

Приклади вибору IoT-платформи. У табл. 2 наведені приклади IoT застосунків, IoT платформи для розгортання і хостингу IoT застосунків, та особливості реалізації IoT застосунку на вибраній платформі.

Таблиця 2. Приклади вибору IoT платформи для IoT застосунку.

IoT застосунок	**IoT платформа**	**Особливості реалізації IoT застосунку**
Розумне землеробство (точне землеробство)	Azure IoT Hub	Збирає дані в реальному часі з датчиків вологості ґрунту, температури та погоди. Інтегрується з машинним навчанням Azure для прогнозної аналітики. Автоматизує полив на основі прогнозів погоди та стану ґрунту.
Автоматизація розумного будинку	Blynk	Хмарна платформа для контролю домашньої безпеки, освітлення та побутової техніки. Підтримує такі пристрої IoT, як ESP8266, Raspberry Pi та Arduino.Надає інтуїтивно зрозумілий інтерфейс мобільного додатка з можливістю перетягування для моніторингу пристрою.
Промислове технічне обслуговування	AWS IoT Core	Відстежує продуктивність машин і прогнозує збої на заводах. Використовує AWS Lambda для обробки подій у реальному часі. Інтегрується з Amazon SageMaker для виявлення аномалій на основі штучного інтелекту.

Висновки. У ході проведеного аналізу хмарних IoT-платформ розглянуті ключові критерії, які визначають їх функціональність, масштабованість та здатність до інтеграції. Порівнявши популярні платформи, такі як AWS IoT Core, Azure IoT Hub, Google Cloud IoT, IBM Watson IoT та ThingSpeak, виявлено їх сильні сторони, що дозволяє зробити обґрунтований вибір для реалізації IoT застосунків. У результаті дослідження визначені оптимальні платформи для різних вимог, від масштабованості і безпеки до підтримки протоколів і інтеграційних можливостей. Це дозволяє кожному розробнику або підприємству вибрати найбільш підходящий інструмент для реалізації своїх IoT-ініціатив. Також, у роботі розглянуті приклади вибору IoT-платформи для реалізації IoT застосунків, і показано особливості їх реалізації.

Література

1. Gartner: Global Industrial IoT Platforms Reviews and Ratings. Access: https://www.gartner.com/reviews/market/global-industrial-iot-platforms.
2. In-Depth Comparison of 8 Leading IoT Cloud Platforms. Access: https://webbylab.com/blog/best-iot-cloud-platforms/.
3. 30 Best IoT Development Platforms in 2025. Access: https://www.intuz.com/blog/top-iot-development-platforms-and-tools.

УДК 621.382

МАТЕМАТИЧНА МОДЕЛЬ ПІДТРИМКИ ЗВ'ЯЗНОСТІ МОБІЛЬНОЇ МЕРЕЖІ СЕНСОРІВ СПРЯМОВАНОЇ ДІЇ З ТЕЛЕКОМУНІКАЦІЙНИМИ АЕРОПЛАТФОРМАМИ ДВОРІВНЕВОГО РОЗТАШУВАННЯ

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

MATHEMATICAL MODEL FOR MAINTAINING THE CONNECTIVITY OF A MOBILE DIRECTED-ACTION SENSOR NETWORK WITH TELECOMMUNICATION AERIAL PLATFORMS OF TWO-LEVEL ARRANGEMENT

The paper describes a mathematical model that, unlike existing mathematical models of MSNs with TA, includes mathematical models of the functioning of directed-action sensors and TA of two-level arrangement with different power supply. An algorithmically defined mathematical model is also presented, which allows calculating the criteria for assessing connectivity.

Існуюча на сьогодні система-прототип [1, 3] складається з наземних сенсорів всеспрямованої дії і ТА на базі БПЛА літакового та гелікоптерного типів, які виконують функцію збору та обміну інформації з іншими ТА і мережевими елементами (базовими станціями, супутниками тощо) використовуючи різні алгоритми та протоколи обміну даних. Місцерозташування даних систем являє собою зону надзвичайної ситуації, стихійного лиха природного або техногенного характеру в якій знищено інформаційно-телекомунікаційну інфраструктуру, а базові станції знаходяться на межі або поза даною зоною (рис.1).

В умовах сучасних та прогнозованих на майбутнє природних та техногенних надзвичайних ситуацій мобільним сенсорним мережам з телекомунікаційними аероплатформами (МСМ з ТА) для ефективного функціонування необхідно мати енергетичний запас майже на порядок більший ніж енергетичний запас, яким забезпечуються сучасні МСМ з ТА.

Сучасні МСМ з ТА мають недопустимо великий час затримки для передачі інформації, малу швидкість її передачі від вузла до кінцевого пункту, вимагають використання надзвичайно великої кількості телекомунікаційних аероплатформ для неперервної підтримки зв'язності.

Тому є об'єктивна необхідність апаратно (конструктивно-алгоритмічного) вдосконалення існуючих мобільних сенсорних мереж з телекомунікаційними аероплатформами для зменшення часу затримки передачі інформації та збільшення швидкості її передачі з кінця в кінець, а також зменшення кількості безпосередньо задіяних телекомунікаційних аероплатформ (ТА) із врахуванням потреби економнішого використання

наявного в вузлах мережі та на борту ТА енергетичного ресурсу.

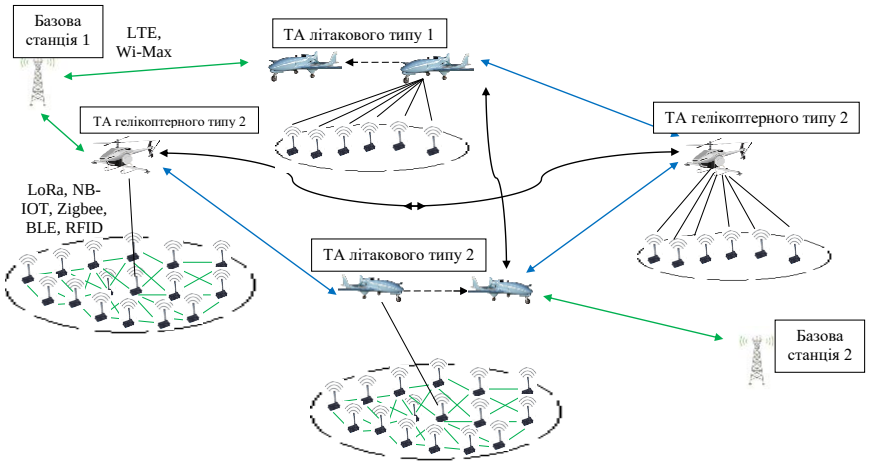


Рисунок 1. Структура мобільної сенсорної мережі з використанням телекомунікаційних аероплатформ на базі БПЛА літакового та гелікоптерного типів, яка поєднує різні алгоритми та протоколи обміну інформацією.

Було запропоновано вдосконалення існуючих МСМ з ТА, яке досягається завдяки застосуванню мобільної мережі сенсорів спрямованої дії з телекомунікаційними аероплатформами різнорівневого розташування [2, 4].

На нульовому рівні розташовані сенсори спрямованої дії, які розташовуються чи пересуваються по поверхні. ТА гелікоптерного типу (або в деяких випадках літакового) створюють 1-й рівень мережі (тактичний рівень), який забезпечує локальну зв'язність для збору та обміну інформації між технічними засобами рятування і пошуку та рятувальниками. Висота розташування від пів кілометра до одиниць кілометрів. Але щоб передати інформацію на далекі відстані до місць де приймаються загальні (оперативно-стратегічні) рішення необхідний ще один рівень ТА – 2-й (висота якого над земною поверхнею від декількох кілометрів до декількох десятків кілометрів). Він повинен взаємодіяти як з мережею ТА гелікоптерного типу (тактичний рівень) так із супутником на низькій навколоземній орбіті або із висотною телекомунікаційною платформою (псевдосупутником) для того, щоб з їх допомогою швидко передавати інформацію до головного центру прийняття рішень. Або передавати інформацію безпосередньо до цього центру (рис.2).

Для проведення імітаційного моделювання [5] була розроблена багатокритеріальна математична модель. Вона дозволяє моделювати як умови існування, так і відсутності зв'язності ММССД з ТА різнорівневого розташування та енергетичного забезпечення, а також обчислювати чисельні значення складових векторного критерію, за якими можна виконати кількісне оцінювання ефективності цієї зв'язності.

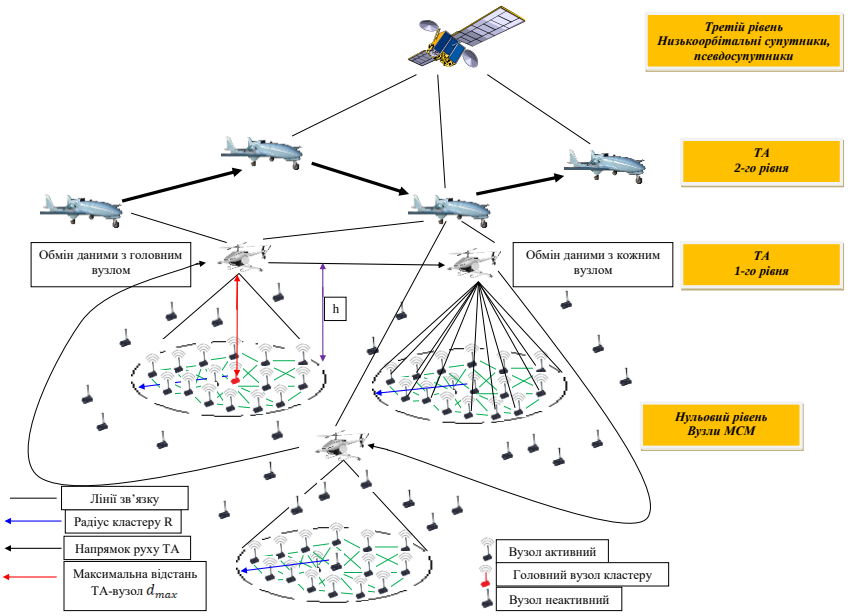


Рисунок 2. Структура мобільної мережі сенсорів спрямованої дії з використанням телекомунікаційних аероплатформ дворівневого розташування.

Кількісні значення скалярних критеріїв $W_i(X)$ $(i = \overline{1,11})$, що є складовими векторного критерію:

$$W(X) = \begin{bmatrix} W_1(X) \\ \vdots \\ W_{11}(X) \end{bmatrix},$$

де X – вектор керуючих параметрів, а його приналежність області допустимих значень G обчислюється за допомогою алгоритмічно заданої моделі функціонування ММССД з ТА різнорівневого розташування із різним енергетичним забезпеченням (рис. 3). Етапи її функціонування детально описано у статті [2].

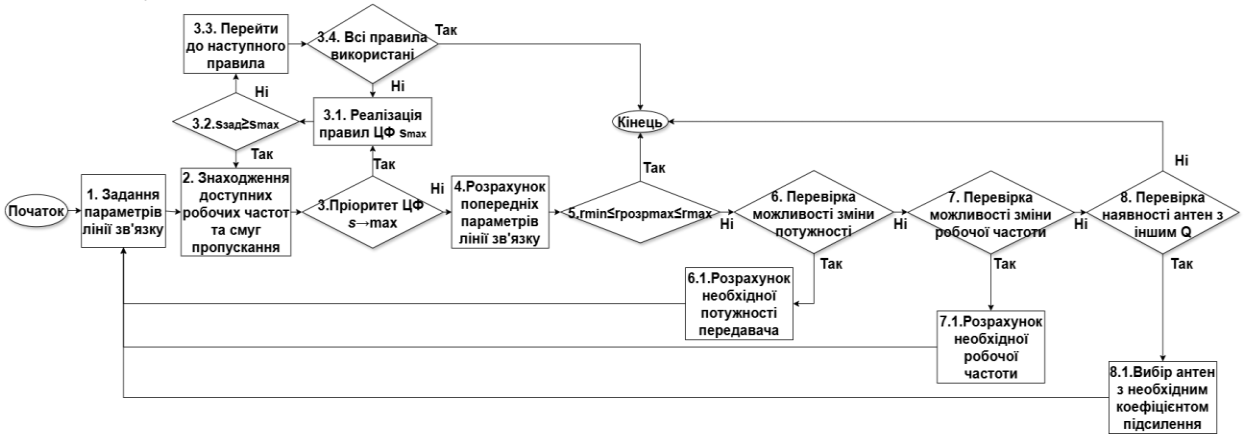


Рисунок 3. Алгоритмічно задана математична модель обчислення скалярних складових векторного критерію.

Складові вектору керуючих параметрів X: потужності передавачів вузлів, ТА першого та другого рівня; коефіцієнт підсилення антен вузлів та просторова орієнтація променю (азимут, кут місяця); робоча частота, смуга пропускання; кількість та розміри кластерів; час сну вузлів.

Для багатокритеріальної математичної моделі було сформовано набір

критеріїв $W_i(X)$ $(i = \overline{1,11})$ із переліку методичних рекомендацій МСЕ-Р та програмного комплексу Matlab:

$W_1(X)$ – час передачі інформації усереднений за кількістю сенсорів, с; $W_2(X)$ – швидкість передачі інформації усереднена за кількістю сенсорів, біт/с; $W_3(X)$ – кількість безпосередньо задіяних ТА усереднена за кількістю сенсорів, шт.; $W_4(X)$ – максимальна кількість ТА, шт.; $W_5(X)$ – медіана кількості ТА, шт.; $W_6(X)$ – мода кількості ТА, шт.; $W_7(X)$ – довжина маршруту усереднена за кількістю сенсорів, м; $W_8(X)$ – максимальна довжина маршруту, м; $W_9(X)$ – мінімальна довжина маршруту, м; $W_{10}(X)$ – медіана довжини маршруту, м; $W_{11}(X)$ – мода довжини маршруту, м.

Параметри математичної моделі, які вважаються незмінними:

1. Характеристики вузлів (кількість $N_{\text{вуз}}$, тип батареї, її ємність, формфактор);

2. Характеристики ТА (кількість ТА 1-го N_{TA1}та 2-го рівнів N_{TA2}, тип джерела живлення, швидкість, висота польоту або діапазон висот);

3. Площа на якій вони розташовуються та маршрути переміщення;

4. Координати вузлів і ТА в момент передачі інформації (при розгляді сценарію квазімобільності);

5. Об’єм даних (зокрема і службового) V_i i-го вузла, що необхідно передати, i=1…$N_{\text{вуз}}$;

6. Топологія та маршрути передачі даних з вузлів МСМ до супутника через ТА;

7. Можливості взаємодії між собою мережевих елементів кожного рівня.

Література

1. Romaniuk, V., Lysenko, O., Novikov, V., Sushyn, I. Development of methods of positioning, localization and data collection from nodes of a free mobile sensor network using intelligent adaptive telecommunication aeroplatforms. Information and Telecommunication Sciences, (2), 40–49, 2021. https://doi.org/10.20535/2411-2976.22021.40-49
2. Сушин, І., та Лисенко, О. Універсальна методика передачі даних із застосуванням сенсорів спрямованої дії. Вчені записки Таврійського Національного Університету імені В.І. Вернадського, Серія: Технічні науки, 35 (74)(2), 6–14, 2024. https://doi.org/10.32782/2663-5941/2024.2/02
3. Sushyn, I., Lysenko, O., Romaniuk, V., Yavisya, V., Kyselov, V., Novikov, V. UAV Connectivity Maintenance in Wireless Sensor Networks. In: Luntovskyy, A., Klymash, M., Melnyk, I., Beshley, M., Schill, A. (eds) Digital Ecosystems: Interconnecting Advanced Networks with AI Applications. TCSET 2024. Lecture Notes in Electrical Engineering, vol 1198. Springer, Cham. pp. 843-857. 2024. ISSN: 1876-1100. https://doi.org/10.1007/978-3-031-61221-3_41
4. Сушин, І., та Буткевич, Г. Методика оцінки зв’язності вузлів бездротової сенсорної мережі при умові використання багаторівневої мережі телекомунікаційних аероплатформ. Вчені записки Таврійського Національного Університету імені В.І. Вернадського, Серія: Технічні науки, 34 (73)(6), 39–46, 2023. https://doi.org/10.32782/2663-5941/2023.6/07
5. Sushyn, I., Ivashchev, D., Lysenko, O. Evaluating the functioning effectiveness of sensor ground-to-air network using multiple UAVs layers and directional antennas. Information and Telecommunication Sciences, (2), 32–38, 2024. https://doi.org/10.20535/2411-2976.22024.32-38

УДК 621.391

ЗАБЕЗПЕЧЕННЯ ПРОДУКТИВНОСТІ АВТОНОМНИХ NPN МЕРЕЖ 5G З ЧАСОВИМ ДУПЛЕКСОМ ШЛЯХОМ ЗАСТОСУВАННЯ СИМВОЛЬНОГО ПЛАНУВАННЯ

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

PROVIDING PERFORMANCE OF AUTONOMOUS NPN 5G NETWORKS WITH TIME DUPLEX BY USING SYMBOL PLANNING

A significant advantage of the autonomous NPN 5G network is the ability to slice the network operation for individual applications: eMBB, URLLC and mMTC. At the same time, different frequency-time parameters of equipment operating in a limited area are a source of mutual interference and reduce performance within the NPN network. To minimize the impact of interference, the symbol positions in the slot formats are defined in such a way as to ensure their compatibility.

Оцінка сумісності форматів слотів з модіфікованими гнучкими символами, яка проведена в [1], показала, що за критеріями мінімальних втрат у ємності (5%) і покритті (5%) реальний інтерес представляє лише обмежена кількість комбінацій слотових форматів (до 4-х), які відрізняються за рахунок модифікації гнучких символів, але, водночас, є сумісними, а тому можуть бути рекомендованими в завадових ситуаціях. Проведена оцінка не охоплює повний перелік ситуацій, в яких доцільно застосовувати символьне планування для покращення завдань планування мереж 5G, мінімізації дії завад і забезпечення сталої продуктивності мереж.

Тому у зв’язку із поширенням у світі малопотужних автономних (не загальних) мереж NPN (Non-Public-Network) в роботах [2-5] ставляться питання забезпечення сумісності обладнання 5G NR як всередені мережі, так і сумісності з сусідніми автономними мережами NPN, що спільно використовують той самий частотний ресурс. Причиною цього стали значні операційні і технічні обмеження, пов’язані із вторинною основою використання спектру мережами NPN поряд із первинною основою для загальних мереж 5G, накладанням обмежень на випромінювання (потужність і позасмугові випромінювання) і, чи не найважливіше, необхідністю забезпечення сумісної роботи обладнання для основних застосувань (швидкісна передача даних, низька затримка і міжмашинний зв'язок), що у NPN працюють на спільній обмеженій території в режимі розшарування (slicing) мережі.

З метою оцінки ефективності використання слотових форматів для забезпечення розшарування мережі NPN наразі проведено розрахунки сумісності типових слотових форматів (за номерами), що є характерними для використання в зазначених застосуваннях (рис. 1). Частина форматів (№№ 28; 34; 50; 10; 12; 14) обрані для розрахунків як характерні для застосувань розшарування і прийняті із технічних специфікацій [6] без змін в структурі. Решта форматів (№№ 52*; 52-1; 52-2; 52-3) отримана із формату слота № 52 шляхом модифікацій символу F в бік задоволення потреб застосувань розшарування.

eMBB (важкий і середній DL (з заміною F)):

28	D	D	D	D	D	D	D	D	D	D	D	D	F	U
52*	D	F	U	U	D	F	U	D	F	U	U	D	F	U

eMBB (важкий і середній UL):

34	D	F	U	U	U	U	U	U	U	U	U	U	U	U
50	D	D	D	F	U	U	U	D	D	D	F	U	U	U

URLLC (з заміною F):

52-1	D	F	U	D	F	U	D	D	F	U	D	F	U	D
52-2	D	F	D	F	D	F	D	D	F	U	D	F	U	D
52-3	D	F	U	D	F	U	D	D	F	D	F	D	F	D

mMTC

10	F	U	U	U	U	U	U	U	U	U	U	U	U	U
12	F	F	F	U	U	U	U	U	U	U	U	U	U	U
14	F	F	F	F	F	U	U	U	U	U	U	U	U	U

Рис 1. Обрані для розрахунків типові формати слотів для роботи з різними застосуваннями.
Умовні позначення: D - символи DL; U – символи UL;
F – гнучкі (flexible) символи або захисний інтервал GP.

Оцінка сумісності проводилась з використанням методу, наведеному в [1] шляхом перебору відповідних комбінацій форматів слотів для сценаріїв взаємодії: eMBB↔URLLC; eMBB↔mMTC; URLLC↔mMTC. На рис. 2 представлені результати розрахунків, отримані за допомогою програми Excel. Формати слотів для застосувань розшарування є критичними за своєю структурою і, тому, передбачувано є несумісними між собою. В жодному з сценаріїв взаємодії відсутні комбінації, що задовольняли би вимоги втрат ємності не більше за 5%. Проте існують наступні комбінації, що задовольняють вимоги не більше за 20 %, що в умовах завадової ситуації можна прийняти задовільними: 1) всі формати mMTC і №52 eMBB (середній DL); 2) формати №10, №12 mMTC і №52 eMBB (середній DL); 3) формат №12 mMTC і формат №50 (середній UL). З метою компенсації втрат у ємності необхідно вживати додаткові заходи, такі як: просторове рознесення БС, зміна сектору обслуговування і орієнтації пелюстків діаграми спрямованості антени.

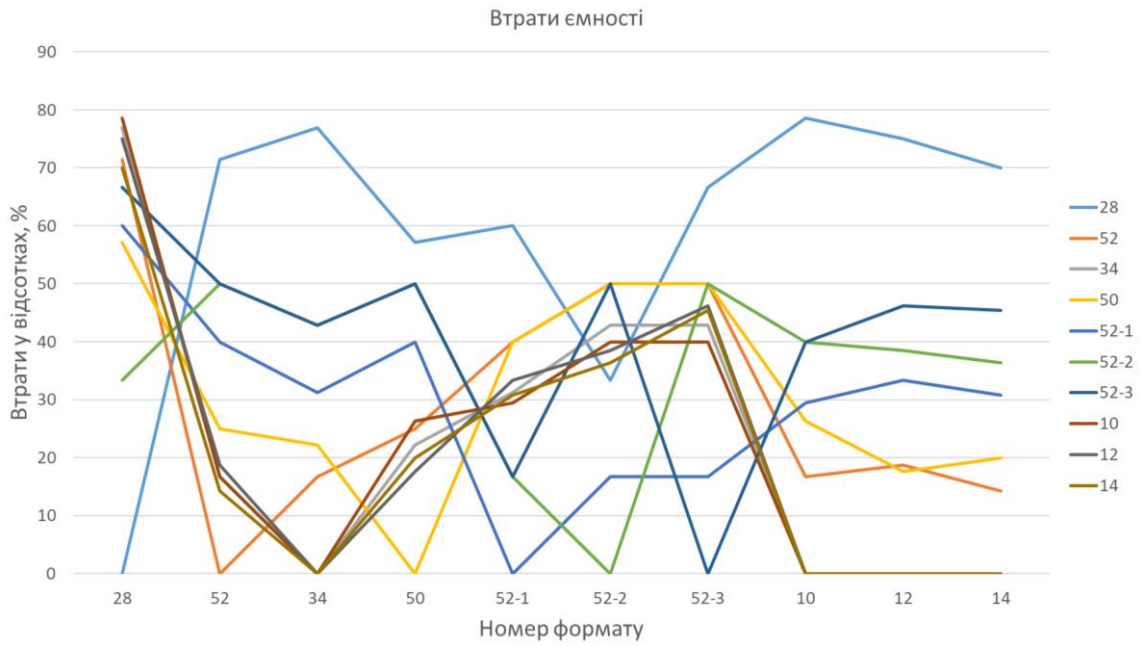


Рис.2. Результати розрахунків втрат ємності.

Отримані результати можуть бути рекомендовані для попереднього налаштування мереж NPN, де планується одночасна робота різних застосувань на обмеженій території (виробництво, фермерські хозяйства, медичні і навчальні заклади, кампуси тощо).

Література

1. Є.А. Якорнов, В.Ю. Тичинський-Мартинюк, Покращення ефективності символьного планування в мережах 5G шляхом застосування сумісних слотових форматів. 2024 , Матеріали XVIII Міжнародної науково-технічної конференції "Перспективи телекомунікацій - 2024" (ПТ24), https://conferenc-journal.its.kpi.ua/article/view/305629
2. 3GPP TS 22.261 V19.9.0 (2024-12) Service requirements for the 5G system; Stage 1 (Release 19)
3. 5G Stand Alone Core Network experience, commercial applications. Ericsson Presentation, Executive Training Program on Fifth Generation (5G) Implementation for Ukrainian officials, May 23 2024, https://drive.google.com/drive/folders/1z4hSkI0LIvt_dQ6hRP5TyuP6u8Jj2S4S?usp=sharing
4. ECC/DEC/(24)01 of 8 November 2024 on harmonised technical conditions for the shared use of the 3800-4200 MHz frequency band by low/medium power terrestrial wireless broadband systems (WBB LMP) providing local-area network connectivity, www.cept.org
5. ECC Report 358 In-band and adjacent bands sharing studies to assess the feasibility of the shared use of the 3.8-4.2 GHz frequency band by terrestrial wireless broadband low/medium power (WBB LMP) systems providing local-area network connectivity, approved 28 June 2024, www.cept.org
6. 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

УДК 621.391

ПОРІВНЯЛЬНИЙ АНАЛІЗ АКТУАЛЬНИХ МАТЕМАТИЧНИХ МОДЕЛЕЙ ОЦІНКИ ЗАВАДОСТІЙКОСТІ СИГНАЛІВ З ДИСКРЕТНОЮ МОДУЛЯЦІЄЮ

Уривський Л.О., Шмігель Б.О., Косогор А.В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: leonid_uic@ukr.net, bshmigel@gmail.com, kosogoranastasia@gmail.com

COMPARATIVE ANALYSIS OF CURRENT MATHEMATICAL MODELS FOR ASSESSING THE NOISE IMMUNITY OF SIGNALS WITH DISCRETE MODULATION

This paper presents a comparative analysis of current mathematical models used to assess the noise immunity of signals with discrete modulation.

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

Важливим інструментом вибору оптимальних варіантів СКК в каналах із різноманітними параметрами є оцінка ймовірності бітової помилки (BER), яка допомогає обрати спосіб маніпуляції та спосіб кодування для досягнення потрібних показників якості передавання інформації. Для поширених видів маніпуляції, зокрема, для квадратурної амплітудної модуляції (QAM) показник BER традиційно визначається шляхом розрахунку ймовірності помилки за допомогою відомих аналітичних залежностей [1-4].

Попри високу точність аналітичних виразів при високому відношенні сигнал-шум h^2, їх застосування при низьких значеннях h^2 може призводити до значних відхилень від точних значень BER. У зв'язку з цим постає необхідність порівняльного аналізу актуальних математичних моделей, щоб обрати найбільш достовірну оцінку завадостійкості сигналів із дискретною модуляцією.

У доповіді проведено огляд сучасних методів оцінки BER, визначено їхні переваги та недоліки, а також розглянуто можливі напрямки вдосконалення підходів до математичного моделювання завадостійкості цифрових сигналів.

Постановка задачі дослідження

Для оцінки завадостійкості широко використовують аналітичні та симуляційні підходи. Аналітичні методи забезпечують високу точність для високої енергетики та швидкість оцінювання характеристик завадостійкості

без великих обчислювальних витрат. Симуляційні методи (методи статистичного моделювання), наприклад. векторно-фазовий метод [5], дозволяють отримати емпіричні результати при різних умовах каналу, однак вони є затратними за часом та обчислювальними ресурсами.

У літературі наведено різні аналітичні співвідношення для визначення ймовірності помилки маніпульованого символу ($P_{\text{сим}}$) та інформаційного біта ($P_{\text{біт}}$) при використанні багатопозиційних сигналів.

Відомо кілька методів розрахунку символьних і бітових помилок, серед яких векторно-фазовий метод та підхід, запропонований Дж. Прокісом [1], Л. Фінком [2] , К. Чо та Д. Юном [3].

Для сигналів багатопозиційної маніпуляції Дж. Прокісом [1] запропоновані наступні аналітичні вирази:

- Ймовірність бітової помилки для QPSK

$$p_{b\ QPSK} = \frac{1}{2}\left[1 - F\left(\sqrt{2h^2}\cos\frac{\pi}{4}\right)\right]. \quad (1)$$

- мовірність бітової помилки для QAM-M

$$p_{b\ QAM} = \frac{4\left(1-\frac{1}{\sqrt{M}}\right)}{\sqrt{2\pi}} \int_{\sqrt{\frac{3}{M-1}h^2}}^{\infty} \exp\left(\frac{-u^2}{2}\right) du. \quad (2)$$

В своїй публікації [3] К. Чо і Д. Юн запропоновали альтернативні співвідношення:

- Ймовірність бітової помилки для QAM-M

$$p_{b\ M-QAM} \cong \frac{\sqrt{M}-1}{\sqrt{M}\ \log_2\sqrt{M}} \operatorname{erfc}\left(\sqrt{\frac{3\log_2 M \cdot h^2}{2(M-1)}}\right) + \frac{\sqrt{M}-2}{\sqrt{M}\ \log_2\sqrt{M}} \operatorname{erfc}\left(3\sqrt{\frac{3\log_2 M \cdot h^2}{2(M-1)}}\right). \quad (3)$$

В свою чергу, Л. Фінк [2] для m-багатопозиційних сигналів фазової маніпуляції запропонував аналітичні формули:

- Ймовірність бітової помилки для M-PSK

$$p_{b\ M-PSK} < 1 - F\left(\sqrt{2h^2}\sin\frac{\pi}{m}\right), \quad (4)$$

Для отримання точніших результатів необхідно провести розрахунки для аналітичних співвідношення, що дозволяють визначати ймовірності помилок для ширшого спектру видів маніпуляції сигналів.

У доповіді проведено аналіз для таких типів модуляції: QPSK та QAM-16, QAM-64. Аналітичні розрахунки та графічні залежності ймовірності бітових помилок від співвідношення сигнал/шум виконано за відомими формулами.

Порівняння результатів дослідження завадостійкості

Відомо, що завадостійкість сигналів QPSK, QAM-M істотно розрізняється при зміні позиційності M, тобто кількості біт в одному відліку модульованого сигналу.

Виходячи з виду QAM-M, кожному значенню h^2 можна поставити у відповідність значення P_b.

За допомогою виразів (1)…(4) проведено аналіз залежностей

ймовірності символьної помилки від співвідношення сигнал/шум для кожного типу модуляції побудовано за допомогою програмного середовища Matlab і наведено нижче.

На рисунку 1 наведено графіки залежностей завадостійкості сигналів бінарної BPSK та квадратурної QPSK маніпуляції, визначених за співвідношеннями (1), (3), (4). Криві для сигналів BPSK збіглися для всіх співвідношень, для сигналів QPSK найбільш достовірною є формула (4) [2].

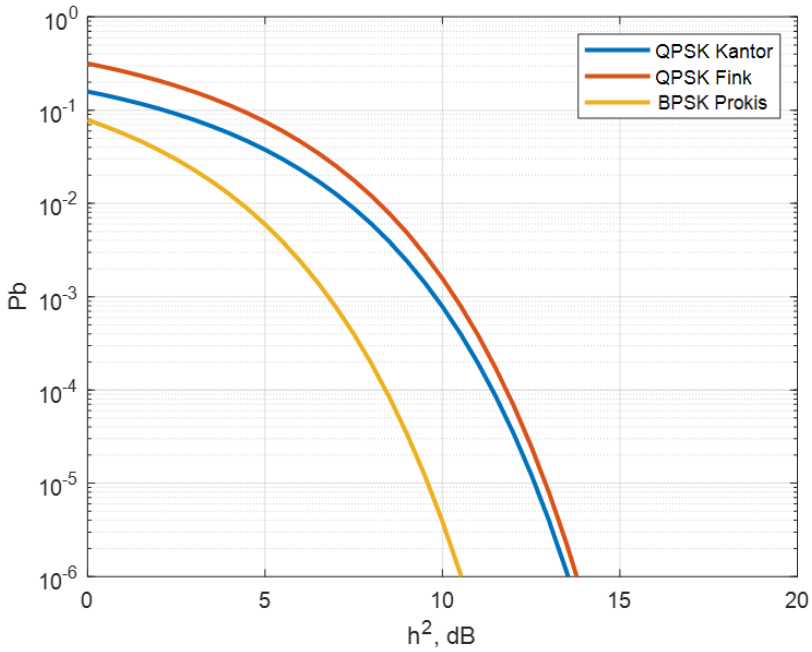


Рис. 1. Графік залежності ймовірності бітових помилок від h^2 для сигналів бінарної BPSK та квадратурної QPSK маніпуляції.

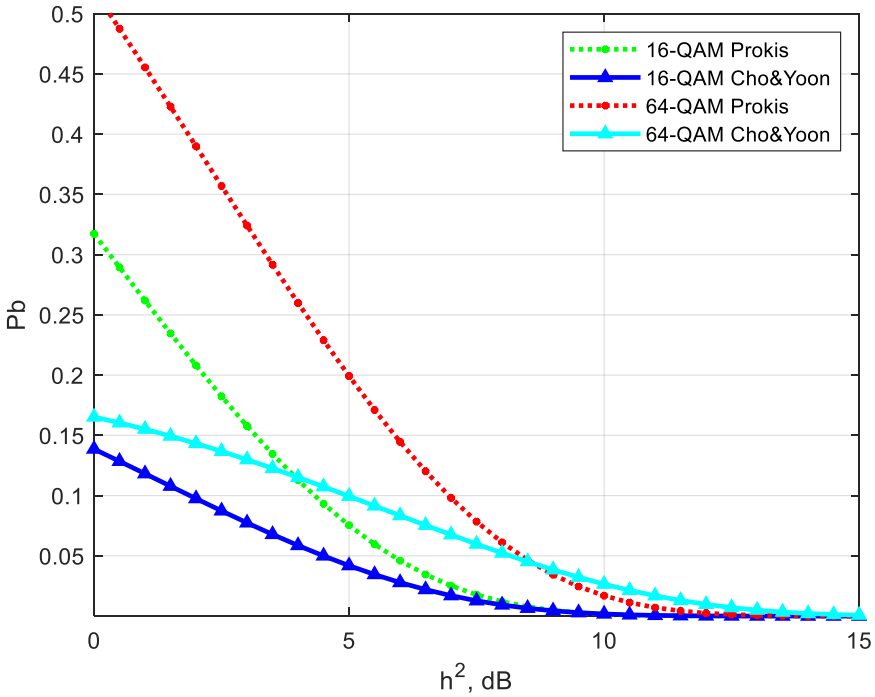


Рис. 2. Графік залежності ймовірності бітових помилок від h^2 для багатопозиційних сигналів 16-QAM та 64-QAM.

Залежності, які наведено на рис. 2 демонструють, що, за умов низької енергетики (h^2 < 8-10 дБ) формули Дж. Прокіса [1], використання яких дуже поширено в сучасних дослідження завадостійкості каналів з багатопозиційною маніпуляцією, не забезпечують достатньої точності.

При модуляції 16-QAM для h^2 > 8 дБ графічні залежності, отримані за виразами (2) і (3) майже ідентичні. Одночасно, при $h^2 \approx 0$ ймовірність помилки за методикою Прокіса становить близько 0.32, тоді як у К. Чо і Д. Юн вона близько 0.14.

Для випадку модуляції 64-QAM для h^2 > 9 дБ графічні залежності, отримані за виразами (2) і (3) майже ідентичні, але при менших значеннях h^2 результати суттєво різняться: ймовірність помилки за формулою (2) Дж. Прокіса при $h^2 \approx 0$ перевищує 0.5 (що не відповідає фізичному змісту цієї помилки), а метод Cho & Yoon надає результат, близький до 0.17.

Отже, модель К. Чо і Д. Юн [3] демонструє кращу точність при малих значеннях h^2 < 8-10 дБ. При високих значеннях h^2 > 8-9 дБ графіки завадостійкості сходяться, що означає, що для високої енергетики різниця між методами менш значуща.

Методика Дж. Прокіса (2) дає перевищену оцінку ймовірності помилки на низьких значеннях h^2, що означає знижену точність для низької енергетики. Натомість модель К. Чо і Д. Юн (3) є більш точною та стабільною в усьому діапазоні значень h^2.

Порівняння різниці в доповненнях показників завадостійкості результатами завадостійкого кодування (для досягнення потрібної достовірності) і змінах інформаційної ефективності

Оцінка завадостійкості прийнятого сигналу через показник BER є першим етапом обробки СКК. Наступним етапом є вибір способу кодування, який забезпечить прийом сигналу із заданою якістю. Сукупність способів обробки сигналу на першому і другому етапі визначають підсумкову ефективність використання наданих ресурсів (частоти і енергетики) каналу зв'язку. Фінальним показником є інформаційна ефективність каналу при наданих йому ресурсах. Для оцінки енергетичної, частотної та інформаційної ефективності використана відома методика [5, 6].

На прикладі сигналів з модуляцією QPSK (Рис. 3) показано, як варіюються вказані показники ефективності для досягнення необхідної бітової достовірності помилки 10^{-7}.

При вихідній бітовій ймовірності 10^{-3} в каналі (точка 1), можна використовувати завадостійкий блоковий код (127,99,4) для досягнення $P_b = 10^{-7}$ (точка 4), а при вихідній бітовій ймовірності 10^{-5} в каналі (точка 2), можна використовувати завадостійкий блоковий код (127,113,2) для досягнення $P_b = 10^{-7}$ (точка 5).

Як можна помітити з рис. 3, застосування ступені завадостійкого кодування завжди призводить до зниження частотної ефективності γ. Чим більше швидкість коду, тим меншу частотну ефективність воно забезпечує. Водночас, слід зауважити, що при застосуванні завадостійкого кодування

енергетична ефективність β покращується.

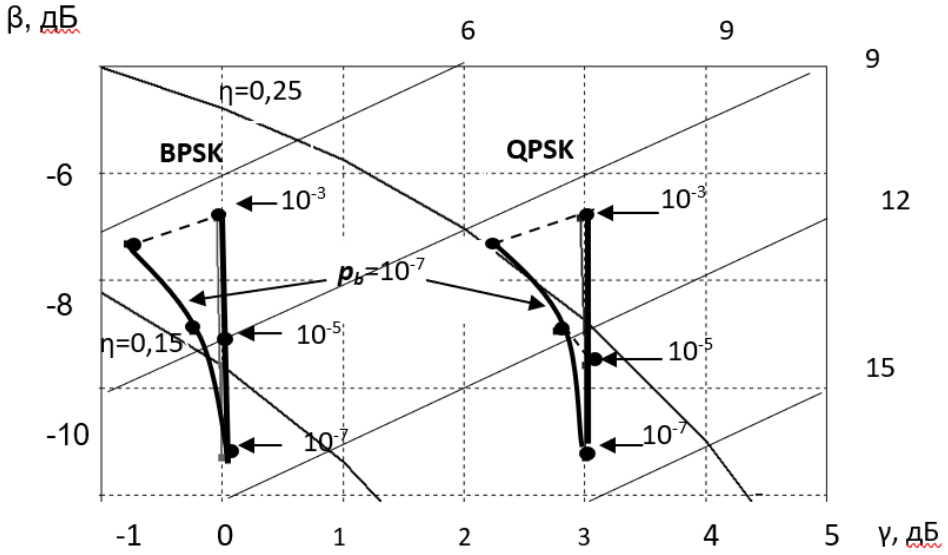


Рис. 3. Показники ефективності використання ресурсів при $P_b = 10^{-7}$.

Модифікована шкала ефективності дозволяє комплексно оцінити частотну γ, енергетичну β та інформаційну ефективності η використання багатопозиційної маніпуляції та завадостійкого кодування.

Такий спосіб оцінки розширює спектр пошуку оптимальних за відносним критеріям 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.

При цьому важливо виходити із достовірної оцінки якості прийому сигналів до кодування, щоб інструменти завадостійкого кодуванні чітко відповідали вимогам якості, оскільки надлишок ресурсів веде до зниження інформаційної ефективності, або нестача потужності коду не забезпечує вимого до достовірності прийму сигналів.

Висновки

1. У доповіді продемонстровано важливість використання сигнально-кодових конструкцій для підвищення ефективності цифрових систем зв’язку. Зокрема, розглянуто аналітичні підходи до оцінювання ймовірності бітової помилки для сигналів QPSK та QAM-M за формулами (1)…(4).

2. Порівняння результатів різних методів оцінки бітової помилки (Дж. Прокіс, К. Чо&Д. Юн, Л.Фінк) свідчить про переваги та обмеження кожного з підходів. Методи статистичного моделювання, такі як векторно-фазовий, дають змогу здобути більш універсальні результати за умов різних параметрів каналу, проте вимагають великих обчислювальних затрат. Аналітичні вирази є швидшими у реалізації і надійними для високих співвідношень сигнал/шум, але потребують корекції або розширення у разі низької енергетики чи нестандартних умов передачі. Усі ці методи доцільно враховувати при проєктуванні та оптимізації цифрових систем, особливо, коли на перший план виходять вимоги до точності, швидкодії та

ресурсоємності розрахунків.

3. Показано, що традиційні формули (4), (1) для сигналів BPSK і QPSK дозволяють точно оцінити ймовірність бітової помилки у випадку як за низького рівня енергії сигналу, так і для відносно високих співвідношень сигнал/шум, тоді можуть виникати помітні відхилення від емпіричних та більш точних аналітичних оцінок.

4. Для сигналів QAM-M формули (2), (3) дозволяють точно оцінити ймовірність бітової помилки у випадку відносно високих співвідношень сигнал/шум ($h2 > 10$ дБ), тоді як за низького рівня енергії ($h2 > 8$ дБ) можуть виникати помітні відхилення від емпіричних та більш точних аналітичних оцінок. За умов низької енергетики ($h2 < 8$-10 дБ) формули Дж. Прокіса [1], використання яких дуже поширено в сучасних дослідження завадостійкості каналів з багатопозиційною маніпуляцією, не забезпечують достатньої точності. Для оцінки завадостійкості сигналі QAM-M більш достовірною слід вважати методику К. Чо і Д. Юн [3].

5. Аналіз отриманих результатів демонструє, що застосування завадостійкого кодування впливає на частотну та енергетичну ефективність системи. Підвищення надійності шляхом кодування збільшує енергетичний виграш і знижує ймовірність помилки, але одночасно зменшує частотну ефективність. Отже, при виборі оптимальних параметрів модуляції та кодування доцільно враховувати як вимоги до якості зв'язку (BER, енергетична ефективність), так і обмеження щодо пропускної здатності каналу. Універсальний підхід, що поєднує аналітичне моделювання, емпіричні розрахунки й адаптивне налаштування системи, дозволить максимально ефективно використовувати ресурси сучасних цифрових систем передачі.

Література

1. Proakis, John G. Digital Communications. 4th ed. – New York: McGraw Hill, 2001.
2. Fink L. M. Discrete message transmission theory. – 1970. – 728 p.
3. Cho, K., and D. Yoon. "On the general BER expression of one- and two-dimensional amplitude modulations," IEEE Transactions on Communications, vol. 50, no. 7 (July 2002): 1074-1080. https://doi.org/10.1109/TCOMM.2002.800818.
4. Шмігель Б.О., & Уривський Л.О. (2021). ВИЗНАЧЕННЯ ЗАВАДОСТІЙКОСТІ СКК В УМОВАХ НИЗЬКОЇ ЕНЕРГЕТИКИ. Збірник матеріалів Міжнародної науково-технічної конференції «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ», с. 53–55. https://conferenc-journal.its.kpi.ua/article/view/230207
5. Уривський Л. О., Прокопенко К. А., Наталенко А. І. Векторно-фазовий метод для визначення показників завадостійкості багатопозиційних сигналів. – Зв'язок, № 12, 2012. – с. 58…63.
6. Uryvsky L., Moshynska A., Osypchuk S., Shmihel B. Comparison of methods for determining noise immunity indicators of a multiservice transmission system. / Advances in Information and Communication Technologies. Lecture Notes in Electrical Engineering, vol 560. / monograph. – Springer, Cham, p.p. 167…185. (2019). https://link.springer.com/chapter/10.1007/978-3-030-16770-7_8

УДК 621.39

МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОБРОБКИ RZ - СИГНАЛІВ НА ФОНІ НЕГАУСОВИХ ЗАВАД В ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМАХ (ІВС)

Зорін О.С.
Черкаський державний технологічний університет, Україна
E-mail: snjzrin@gmail.com

METHODS OF INCREASING THE EFFICIENCY OF PROCESSING RZ-SIGNALS AGAINST THE BACKGROUND OF NON-GAUSSIAN INTERFERENCE IN INFORMATION AND MEASUREMENT SYSTEMS

The paper considers the problem of increasing the efficiency of bipolar discrete RZ-signal detection systems in information and measuring systems operating under non-Gaussian interference. It is proposed to use the moment-cumulative description of random processes to develop momentary quality criteria for testing statistical hypotheses and polynomial decision-making rules. The proposed approach allows taking into account non-Gaussian interference parameters, which significantly increases the accuracy of signal processing. It is established that the use of moment-cumulative representation of signals and synthesized algorithms allows reducing the probability of errors in systems against the background of non-Gaussian interference, which is confirmed by the results of modeling, using ROC curves.

Системи передачі та прийому даних є невід'ємною складовою сучасних ІВС. Розвиток таких систем супроводжується зростанням вимог до якості обробки прийнятих даних. При проєктуванні подібних систем широко використовується лінійне кодування повідомлень, зокрема RZ-кодування [1].

На функціонування сучасних ІВС, як правило, впливають різноманітні дестабілізуючі завади, що в свою чергу позначається на якості та ефективності їхньої роботи. Один із дієвих підходів до вдосконалення процесів обробки інформації в ІВС — це розробка методів і засобів математичного та комп'ютерного моделювання, що дозволяє підвищити точність обробки сигналів і знизити ймовірність помилок в умовах дії завад.

Проблеми, що виникають при вдосконаленні ІВС, пов'язані зі створенням ефективних методів обробки сигналів на фоні негаусових завад, які є випадковими процесами. Традиційний підхід до дослідження та розробки систем обробки суміші дискретних сигналів і негаусових завад має значні обмеження, зумовлені складністю алгоритмічної реалізації та високими обчислювальними витратами. Це ускладнює розробку якісних програмно-алгоритмічних і апаратних засобів для обробки сигналів. Зазначені особливості можуть значно ускладнювати застосування традиційних методів обробки сигналів, заснованих на ймовірнісних критеріях якості, таких як критерій Байєса, максимальної правдоподібності або Неймана-Пірсона. У цих методах випадкові величини описуються за допомогою щільностей розподілу ймовірностей, що створює додаткові труднощі при роботі з негаусовими завадами [2].

Отже, альтернативним підходом до розв'язання задачі може стати використання моментно-кумулянтного опису випадкових процесів та

моментних критеріїв якості перевірки статистичних гіпотез, для розробки правил виявлення сигналів на фоні негаусових завад.

Метою роботи є підвищення ефективності систем прийому даних для виявлення RZ - сигналів на фоні негаусових завад шляхом застосування моментно-кумулянтного представлення випадкових величин. Це включає розробку моментного критерію якості для перевірки статистичної гіпотези та поліноміальних правил прийняття рішень.

Постановка задачі: Нехай на інтервалі спостереження $(0-T)$ спостерігаються випадкові сигнали $\xi_i(t)$, $i=0,1,2$ які являють собою адитивну суміш постійних корисних сигналів a_1, $-a_2$ та з $\eta(t)$ – асиметрично-ексцесної негаусової завади з нульовим математичним сподіванням та дисперсією χ_2: $\xi_0(t)=\eta(t)$, $\xi_1(t)=a_1+\eta(t)$, $\xi_2(t)=-a_2+\eta(t)$.. З випадкової суміші сигналів $\xi_i(t)$, $i=0,1,2$ отримуємо вектор вибіркових значень $X=\{x_1,x_2,...x_n\}$, за результатами обробки якого необхідно прийняти рішення про реалізацію гіпотези H_1 або H_2, що відповідає прийому постійного корисного сигналу a_1 або $-a_2$ відповідно, або рішення про реалізацію гіпотези H_0, що характеризує наявність адитивної негаусової завади. Кожному сигналу, який приймається, відповідає моментно-кумулянтний опис, представлений у вигляді кінцевої послідовності моментів $m_i[\{0,\chi_{i2},\gamma_{i3},...\gamma_{ij}\}]$, де $\gamma_{i3},...\gamma_{ij}-$ кумулянтні коефіцієнти, які описують ознаки негаусової завади $\eta(t)$.

Для обробки вектору вибіркових значень $X=\{x_1,x_2,\cdots,x_n\}$ пропонується використовувати нелінійні розв'язувальні правила (РП), які представлено у вигляді стохастичних поліномів. Синтезовані РП при степені полінома $S=1$, являють собою систему рівнянь перевірки гіпотез H_{10},H_{20},H_{21}, які не враховують негаусівський розподіл досліджуваних випадкових процесів. При збільшенні степені полінома до $S=2$ використовуються початкові моменти 3-го та 4-го порядків, що дає можливість врахувати негаусові параметри досліджуваних випадкових процесів, зокрема для даної постановки задачі у вигляді коефіцієнту асиметрії та ексцесу γ_3,γ_4 відповідно [3].

Аналіз отриманих результатів: Для оцінки ефективності отриманих результатів проведено побудову ROC (receiver operating characteristic) кривої, яка застосовується для оцінки якості моделей (в даному випадку вона характеризує помилки першого та другого роду при степені поліному $S=1,S=2$). На рис.1. показано результати моделювання ROC кривої детектора поліноміальної обробки сигналу на фоні негаусових завад.

Показано, що для моделі негаусової завади, коли коефіцієнти асиметрії (γ_3) і ексцесу γ_4) дорівнюють нулю, характеристики лінійного РП ($S=1$) і нелінійного РП ($S=2$) однакові (рис. 1а). Важливо відзначити, що лінійне РП збігається з класичним РП, яке виведене із ймовірності передбачуваної моделі негаусової завади. Із збільшенням коефіцієнта асиметрії (значення γ_3 = 0.5, 1.0, 1.2 для кількості вибіркових значень n=100, на рис. 1в і 1г значення γ3 однакові

і дорівнюють 1.0 (на рис. 1в gam 3=1, на рис. 1г gam 3=1.0), наведені на рис.1. б, в, г) крива відхиляється у верхній лівий кут. Це свідчить про збільшення ефективності роботи нелінійного РП в порівнянні з лінійним. Врахування негаусової характеристики досліджуваних процесів у вигляді коефіцієнтів асиметрії та ексцесу ($\gamma_3 \neq 0, \gamma_4 \neq 0$) дозволяє збільшити ефективність роботи РТ при нелінійній обробці вибіркових значень $S = 2,$ у порівнянні з добре відомими результатами для негаусових моделей $S = 1.$

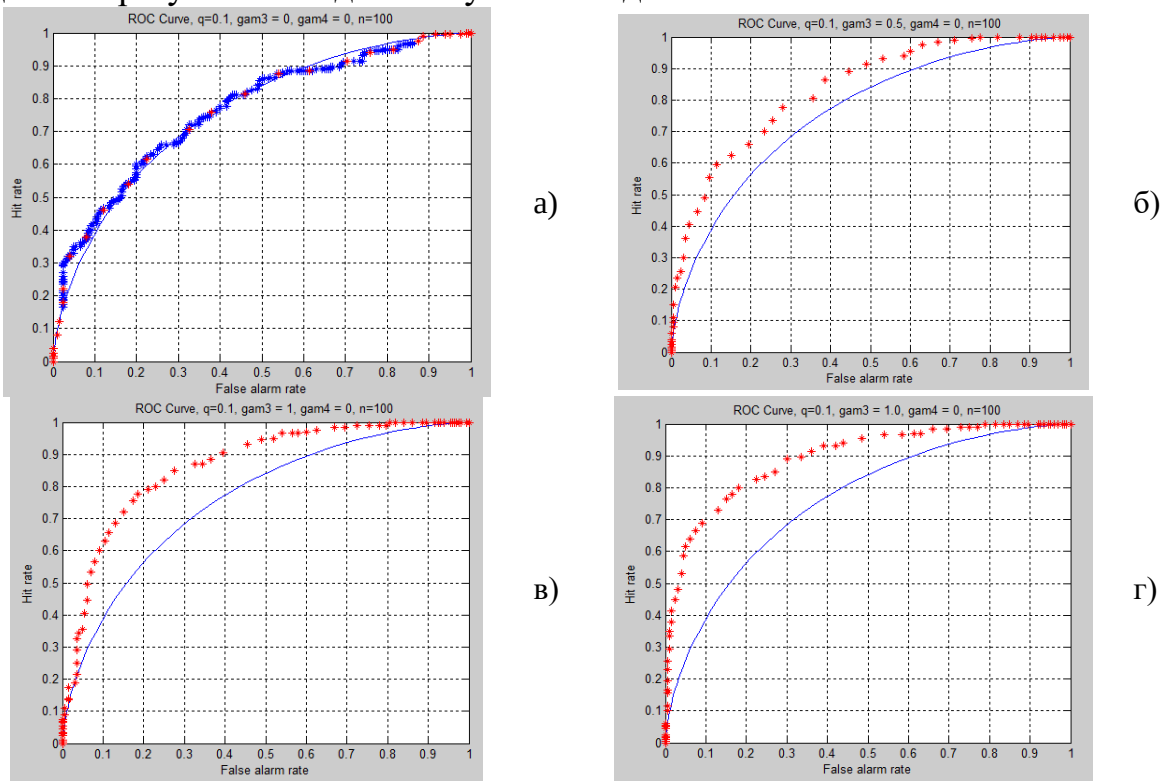


Рис.1. Моделювання кривої ROC детектора поліноміального сигналу на фоні негаусових завад.

Висновки. У роботі запропоновано альтернативний підхід до опису випадкових процесів. Цей підхід заснований на використанні моментів і кумулянтів, нескінченна послідовність яких дозволить точно наблизити запропонований опис випадкових величин до повного імовірнісного процесу. Дослідження показали, що новий підхід до опису випадкових величин і синтезу РП може підвищити точність обробки сигналів порівняно з добре відомими результатами. Використання запропонованого методу та синтезованих алгоритмів підвищує завадостійкість системи прийому біполярних дискретних сигналів в ІВС, що підтверджено результатами моделювання.

Література

1. Mahmoud M. A., Ahmed Nabih Zaki Rashed. Hybrid NRZ/RZ line coding scheme based hybrid FSO/FO dual, Indonesian Journal of Electrical Engineering and Computer Vol. 22, No. 2, May 2021 p. 866-873.
2. Y.Kunchenko: Polynomial Parameter Estimations of Close to Gaussian Random Variables, Aachen: Shaker Verlag, 2002.
3. V. Palahin, O. Zorin., Models and methods for RZ-signals distinction in non-Gaussian noise for information-measurement systems, Journal of Electrical Engineering, Vol. 75, No. 5, 2024, pp. 372-382.

УДК 621.382

СЦЕНАРІЇ ТА СТРАТЕГІЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ В СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

Мошинська А. В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: avmoshinskaya@gmail.com

SCENARIOS AND STRATEGIES FOR INFORMATION TRANSMISSION IN INTERNET OF THINGS SYSTEMS

The concepts of Scenario and Strategy of information transmission in Internet of Things systems are considered. A solution to the conflict between the capabilities provided by the available resource and the capabilities that the required telecommunication resource could provide is presented.

Протиріччя між безперервно зростаючими інформаційними потребами суспільства і відставання фізичних можливостей телекомунікацій з переміщення інформації від джерел до одержувачів становить тривалу в часі проблему з позиції сучасної парадигми телекомунікаційних знань [1].

Системи Інтернету речей відображають можливий шлях вирішення даного протиріччя завдяки поєднанню різноманітних сценаріїв передачі інформацій та способів їх реалізації. Сукупність використовуваних послуг одного користувача, групи користувачів, спільноти або суспільства визначає інформаційний сценарій передачі інформації.

Сценарій містить в собі весь набір послуг, який необхідно реалізувати для користувача відповідно до його побажань (від розумного будинку до промислових автоматизованих процесів та оборонних систем).

Так, наприклад, підхід до реагування на кризові ситуації на основі Інтернету речей пропонує низку вагомих переваг порівняно з традиційними методами. Використовуючи дані та аналітику в режимі реального часу, рішення, засновані на Інтернеті речей, дозволяють швидко та ефективно виявляти, відстежувати та реагувати на катастрофи. Додатково, системи, побудовані на базі Інтернету речей, можуть бути використані для інформування про плани евакуації або сигнали про небезпеку [3].

Кожен елемент сценарію має тривимірну структуру:

$$X_i\{Q_i;\Delta T_i;Sp_i\}, \tag{1.1}$$

де X_i – *i*-й елемент сценарія, Q_{Si} – характеристика об’єму інформації, пов’язаний з *i*-м елементом, T_{Si} – часове обмеження, пов'язане з наданням послуг і-го елемента, Sp_{Si}– просторова характеристика *i*-го елемента.

При об'єднанні елементів у сценарій утворюється вектор

$$X_j = \{X_{1j}, X_{2j}, X_{ij}, ..., X_{nj}\} \tag{1.2}$$

де X_j – *j*-я версія сценарія, характеризується набором елементів X_{ij}.

При виборі способу реалізації кожного (X_j – го) сценарію важливу роль відіграє точна відповідність між необхідними обсягами передачі інформації (інформаційна компонента), часом обробки і доставки інформації (часова компонента) і місцем реалізації сценарію (просторова компонента).

Таким чином, сценарій, як сукупність елементів, характеризується також трьома координатами:

$$X_j \left\{ Q_j, T_j, Sp_j \right\}. \tag{1.3}$$

де X_j – *j*-я версія сценарія, Q_j – характеристика об'єму інформації, пов'язаного з *j*-м сценарієм, T_j – часове обмеження, пов'язане з наданням послуг в рамках *j*-го сценарія, Sp_j– просторова характеристика, пов'язана з наданням послуг в рамках *j*-го сценарія.

У найпростішому випадку характеристики обсягу інформації підсумовуються:

$$Q_j = \sum_{(i)} Q_{ij}\ , \tag{1.4}$$

часова компонента:

$$T_j = \min_{(i)} \left\{ T_{ij} \right\}, \tag{1.5}$$

просторова компонента:

$$Sp_j = \max \left\{ Sp_{ij} \right\} \tag{1.6}$$

приймають екстремальні значення (1.5-1.6).

У загальному випадку характеристики вектора (1.3) можна представити у вигляді тривимірної матриці-вектора, де кожної компоненті обсягу інформації відповідає своє значення часової і просторової компоненти. [1]

Системи Інтернету речей мають як інформаційну (сервісну) компоненту, реалізовану апаратно-програмними засобами, так і компоненту доставки послуги користувачеві (телекомунікаційну компоненту), завдяки чому поєднують в собі всі необхідні умови імплементації сценаріїв, що надалі визначається, як стратегії передачі інформації. [2]

Наочний приклад стратегій для телекомунікаційної ланки систем Інтернету речей можна побачити на малюнку 1.

Під Стратегією слід розуміти сукупність способів передачі інформації, що використовує обґрунтоване поєднання протоколів передачі та засобів перенесення електричних сигналів.

$$Y_i = \Phi \left\{ X_J \right\} \left| \Delta F, E_S \right. \tag{1.7}$$

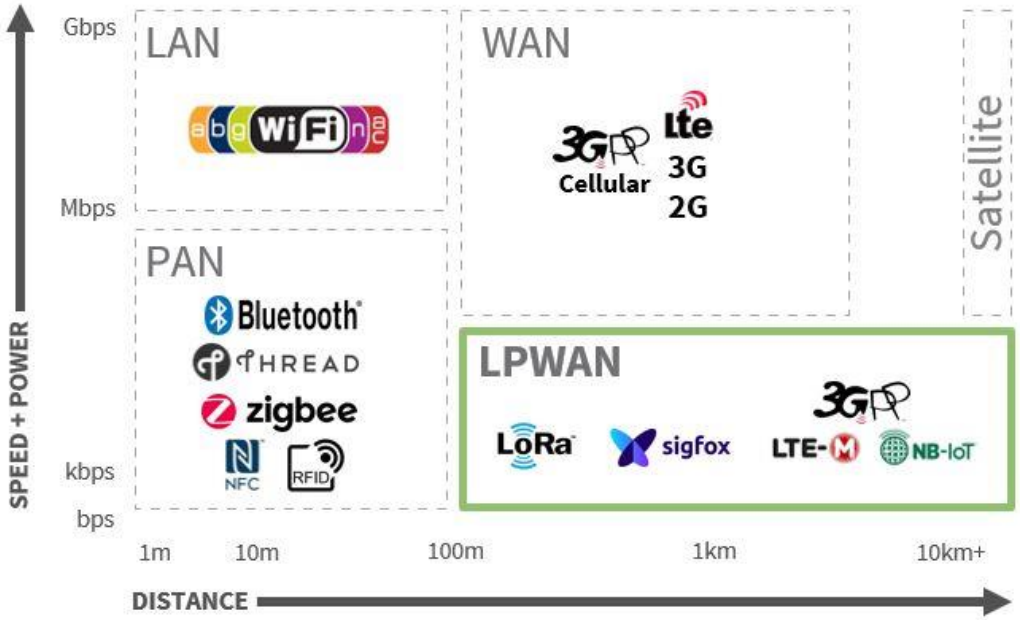


Рис. 1. Телекомунікаційні протоколи та технології систем Інтернету речей.

$$Y_i = \Phi\left\{ V_{Si} = \frac{Q_j}{\Delta T_j} \le \Delta F; E_S(V_{Ci}, Sp_J); p_b(E_S, \frac{V_{Si}}{V_{Ci}}) \le p_{b0} \right\} \Big| \Delta F, E_S \qquad (1.8)$$

Можливість реалізації Сценарію засобами обраної Стратегії для забезпечення надання відповідних послуг залежить від наявного телекомунікаційного ресурсу, а саме: енергетики в каналі в точці передачі і пунктах прийому інформації (E); смуги (або діапазону) частот (F), наданих для передачі; часу, необхідного для передачі інформації (T).

Таким чином, інструментом реалізації Сценаріїв передачі інформації в системах Інтернету речей є реальні ресурси телекомунікаційної системи. Кожна ТКС надає певний протокол передачі інформації, спосіб передачі інформації, енергетику в каналі в залежності від виду зв'язку, заданої якості та обсягу інформації, що передається.

Література

1. Ilchenko M. Developing of Telecommunication Strategies based on the Scenarios of the Information Community / M. Ilchenko, L. Uryvsky, A. Moshynska // Springer Science + Business Media, New York, 2017. – New York, 2017. – P. 905–913.
2. IoT solutions research and development for wide range applications / L. Uryvsky, A. Moshynska, S. Osypchuk, V. Kyrashchuk // Sciences of Europe, Praha, Czech Republic. – Praha, 2019. – Vol. 1, N 36. – P. 40–54.
3. Голяткін А.О, МошинськаА.В. Розширення функціоналу пристроїв IoT в умовах надзвичайних ситуацій / А.В. Мошинська, А.О. Голяткін // Information Technology and Security. К: 2023. – vol. 11, iss. 2 (21). – pp. 126-136.

УДК 621.391

ПОРІВНЯЛЬНИЙ АНАЛІЗ РАДІОТЕХНОЛОГІЙ МЕРЕЖ ІОТ

Кузьмінський А.Р., Носков В.І.
Навчально-науковий інститут телекомунікаційних систем
НТУУ «КПІ» ім. Ігоря Сікорського, Україна
E-mail: artemschoolacc1@gmail.com; nvi2010@ukr.net

COMPARATIVE ANALYSIS OF RADIO TECHNOLOGIES FOR INTERNET OF THINGS NETWORKS

The modern development of the Internet of Things (IoT) creates a need for efficient radio technologies for data transmission in networks of various scales and application specifics. IoT radio technologies are becoming particularly relevant in the context of smart city development, industrial Internet of Things, agricultural systems, and conventional household solutions. The primary objective of this study is to compare various radio technologies based on their technical specifications, such as energy consumption, communication range, bandwidth, and deployment costs, which allows for the identification of optimal solutions for different application scenarios.

Сучасний розвиток Інтернету речей (IoT) створює потребу у використанні ефективних радіотехнологій для передачі даних у мережах різного масштабу та специфіки застосування. Радіотехнології IoT набувають особливої актуальності в умовах розвитку смарт-міст, промислового Інтернету речей, аграрних систем та і у звичайних побутових рішеннях. Основна мета дослідження полягає у порівнянні різноманітних радіотехнологій з огляду на їх технічні характеристики, такі як енергоспоживання, дальність зв'язку, пропускну здатність та вартість розгортання, що дозволяє визначити оптимальні рішення для різних сценаріїв їх застосування.

Інтернет речей докорінно змінив концепцію підключення, розширивши її від взаємодії між людьми до інтеграції майже всіх пристроїв, здатних до зв'язку. Головною метою такої масштабної мережі взаємопов'язаних об'єктів є підвищення якості життя та стимулювання економічного розвитку шляхом упровадження IoT-рішень у різні сфери, зокрема: автомобільну промисловість, моніторинг довкілля, медицину, промислову автоматизацію, носимі пристрої, автоматизоване сільське господарство, інтелектуальні енергомережі тощо.

Проте для повноцінного функціонування IoT необхідно вирішити низку важливих технічних питань, серед яких: ідентифікація пристроїв, сенсорика, комунікація, обчислювальні потужності, надання сервісів та інтерпретація даних. У цьому контексті важливу роль відіграють комунікаційні технології, які забезпечують взаємозв'язок між різними гетерогенними пристроями для реалізації очікуваних послуг.

Інтернет речей (IoT) використовує різноманітні радіотехнології для

з’єднання пристроїв. Для енергоефективного зв’язку на малих дистанціях Інститут інженерів з електротехніки та електроніки (IEEE) запропонував два ключові стандарти: IEEE 802.15.4 та IEEE 802.11 (WiFi). Провідні організації, такі як Bluetooth, SIG та ZigBee Alliance, адаптували ці стандарти, що дозволило створити економічно ефективні рішення для бездротового зв’язку на короткі відстані. Водночас поширені радіотехнології SigFox та LoRa, які забезпечують велику дальність передачі з низьким енергоспоживанням. Порівняння поширених радіотехнологій IoT наведено в табл. 1.

Таблиця 1. Порівняння радіотехнологій IoT.

Технологія	**Частота**	**Дальність**	**Швидкість**	**Енерго-споживання**	**Переваги**	**Недоліки**
Wi-Fi	2,4 ГГц / 5 ГГц	До 100 м	11–9600 Мбіт/с	Високе	Висока швидкість, велика кількість пристроїв	Високе споживання енергії, мала дальність
Bluetooth (BLE)	2,4 ГГц	До 100 м (BLE)	До 2 Мбіт/с	Низьке	Енергоефективність, сумісність зі смартфонами	Мала дальність, обмежена кількість пристроїв
Zigbee	2,4 ГГц	До 100 м	До 250 Кбіт/с	Низьке	Мережева топологія, низьке споживання	Низька швидкість, обмежена дальність
Z-Wave	868 МГц (ЄС) / 908 МГц (США)	До 100 м	До 100 кбіт/с	Низьке	Енергоефективність, хороша прохідність через стіни	Менша підтримка пристроїв, обмежена пропускна здатність
LoRa (LoRaWAN)	868 МГц (ЄС) / 915 МГц (США)	2–15 км	До 50 кбіт/с	Дуже низьке	Велика дальність, робота в складних умовах	Низька швидкість, ліцензування частот у деяких країнах
NB-IoT	Ліцензовані діапазони (700-2100 МГц)	1–15 км	До 250 кбіт/с	Низьке	Інтеграція з мобільними мережами, висока надійність	Залежність від операторів, плата за підключення
Sigfox	868 МГц (ЄС) / 902 МГц (США)	10–50 км	До 100 біт/с	Дуже низьке	Велика дальність, енергоефективність	Дуже низька швидкість, обмежена підтримка

Вибір технології залежить від вимог щодо дальності зв’язку, енергоспоживання, швидкості передачі даних та вартості.

Аналіз наведених радіотехнологій дозволяє надати наступні рекомендації щодо їх використання:

- Wi-Fi – підходить для високошвидкісного IoT (розумні будинки, камери, потокове відео);
- Bluetooth (BLE) – ідеальний для переносних пристроїв (фітнес-браслети, розумні годинники);
- Zigbee, Z-Wave – добре працюють у розумних будинках та автоматизації;
- LoRa, Sigfox – ефективні для розподілених датчиків (розумне місто, аграрні рішення);
- NB-IoT – підходить для IoT у сфері індустрії, транспорту та інфраструктури.

Література

1. Elkhodr, M., Shahrestani, S., & Cheung, H. (2016). "Emerging Wireless Technologies in the Internet of Things: A Comparative Study." International Journal of Wireless & Mobile Networks (IJWMN). DOI: 10.5121/ijwmn.2016.8505
2. Науковий журнал «Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки». Том 31 (70), № 6, 2020, Частина 1.
3. Морін, Е., Маман, М., Гвізетті, Р., & Дуда, А. (2017). "Порівняння тривалості роботи пристроїв у бездротових мережах для Інтернету речей." DOI: 10.1109/ACCESS.2017.2688279.
4. Al-Sarawi, S., Anbar, M., Alieyan, K., & Alzubaidi, M. (2017). "Internet of Things (IoT) Communication Protocols: Review." 2017 8th International Conference on Information Technology (ICIT). DOI: 10.1109/ICITECH.2017.8079928.
5. Bhoyar, P., Sahare, P., Dhok, S. B., & Deshmukh, R. B. (2018). "Communication Technologies and Security Challenges for Internet of Things: A Comprehensive Review." DOI: 10.1016/j.aeue.2018.11.031.
6. Badihi, B. (2021). Analysis and characterization of short-range and low-power radio technologies for Internet of Things: Protocol and Application. [Doctoral Thesis, Aalto University]. ISBN:978-952-64-0240-6

УДК 621.391

ПРОБЛЕМИ ТА НАПРЯМКИ ДОСЛІДЖЕННЯ ПРОТОКОЛУ RPL МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ

Страшко П.В., Носков В.І.
Навчально-науковий інститут телекомунікаційних систем
НТУУ «КПІ» ім. Ігоря Сікорського, Україна
E-mail: straz0507@gmail.com; nvi2010@ukr.net

PROBLEMS AND DIRECTIONS OF THE RPL PROTOCOL RESEARCH IN THE INTERNET OF THINGS NETWORKS

In IoT networks, the RPL (Routing Protocol for Low-Power and Lossy Networks) protocol is used as a routing protocol specially designed for networks with power constraints and high channel error rates. Despite its widespread use, RPL has certain problems such as the lack of effective load balancing mechanisms, limited mobility support, and vulnerability to attacks such as black hole attacks or selective packet drop. In this regard, research into RPL is necessary to develop advanced routing algorithms that will improve the performance and reliability of IoT networks.

В мережах Інтернету речей у якості протоколу маршрутизації використовується протокол RPL (Routing Protocol for Low-Power and Lossy Networks), спеціально розроблений для мереж з обмеженнями в енергоспоживанні та високим рівнем помилок в каналах. Незважаючи на широке використання, RPL має певні проблеми такі як відсутність ефективних механізмів балансування навантаження, обмежена підтримка мобільності, вразливості до атак, таких як атака «чорна діра» або селективне відкидання пакетів. У зв’язку з цим дослідження RPL є необхідним для розробки вдосконалених алгоритмів маршрутизації, які сприятимуть покращенню продуктивності та надійності IoT-мереж.

Інтернет речей (IoT) забезпечує інтеграцію численних сенсорних пристроїв у різних галузях, зокрема в промисловості, медицині, транспорті та розумних містах. Одним із головних викликів таких мереж є забезпечення ефективної маршрутизації даних при обмежених енергетичних та обчислювальних ресурсах. Дистанційно-векторний протокол маршрутизації RPL є стандартизованим (RFC 6550) і розроблений спеціально для енергоефективних бездротових мереж із високим рівнем втрат. Його ключовою особливістю є побудова спрямованого ациклічного графа (DODAG) (рис.1), що дозволяє ефективно організовувати маршрути передачі даних та мінімізувати енергоспоживання.

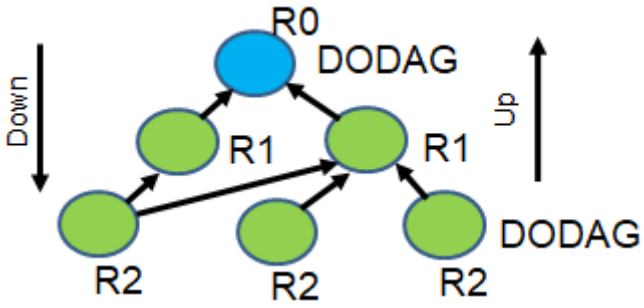


Рисунок 1. Структура DODAG (спрямований ациклічний граф).

Незважаючи на широке використання, RPL має певні обмеження. Відсутність ефективних механізмів балансування навантаження призводить до перевантаження окремих вузлів, що знижує продуктивність мережі. Обмежена підтримка мобільності ускладнює роботу в динамічних середовищах, де структура мережі постійно змінюється. Крім того, вразливості до атак, таких як атака «чорна діра» або селективне відкидання пакетів, створюють загрози для безпеки переданих даних. У зв'язку з цим дослідження RPL є необхідними для розробки вдосконалених алгоритмів маршрутизації, які сприятимуть покращенню продуктивності та надійності IoT-мереж. Оптимізація RPL можлива шляхом покращення механізмів балансування навантаження, підвищення адаптивності до мобільних пристроїв, зменшення затримок у передачі даних та впровадження вдосконалених заходів безпеки. Важливим напрямком дослідження є розробка нових алгоритмів вибору оптимальних маршрутів, що враховують як енергоспоживання, так і пропускну здатність вузлів мережі. Аналіз існуючих підходів (табл. 1) показує, що RPL поступається деяким альтернативним протоколам у певних аспектах. Зокрема, AODV (Ad hoc On-Demand Distance Vector Routing) забезпечує кращу підтримку мобільності за рахунок швидкої адаптації до змін топології, тоді як OLSR (Optimized Link State Routing Protocol) демонструє високу пропускну здатність, хоча і за рахунок збільшеного службового трафіку.

Таблиця 1. Порівняння протоколів маршрутизації.

Параметр	**RPL**	**AODV**	**OLSR**
Енергоспоживання (мВт)	15	35	50
Затримка передачі (мс)	50 – 100	80 – 120	30 – 70
Пропускна здатність (кбіт/с)	40 – 60	40 – 80	100 – 200
Час конвергенції (с)	0,5 – 2	0,1 – 1	2 – 5
Частота оновлення (Гц)	0,2 – 1	1 – 5	2 – 10
Втрата пакетів під час мобільності (%)	10 – 20	5 – 15	20 – 40
Handover Delay (мс)	100 – 300	50 – 200	200 – 500
Безпека (шифрування)	AES-128	Обмежена	Обмежена

Параметр	RPL	AODV	OLSR
Обсяг коду (КБ)	40 – 100	50 – 120	80 – 150
Використання CPU (%)	5 – 15	10 – 25	15 – 35
Обсяг RAM (КБ)	20 – 50	30 – 70	40 – 100
Службовий трафік (пакетів/сек)	0,2 – 1	1 – 5	2 – 10
Складність конфігурації (1-5)	3	4	5

Основними перевагами RPL є **низьке енергоспоживання, ефективне управління маршрутами та мінімізація службового трафіку**, що дозволяє масштабувати мережу до тисяч вузлів. Проте, він має обмежену підтримку мобільності, що може стати критичним фактором у високомобільних мережах, де AODV або інші протоколи можуть працювати ефективніше. Також зі збільшенням трафіку можливе перенавантаження вузлів. Певні проблеми з безпекою вимагають пошук ефективних методів її підвищення. Все це і визначає напрямки подальших досліджень з метою вдосконалення протоколу RIP.

Література

1. RFC 6550 - "Routing Protocol for Low-Power and Lossy Networks". [Інтернет-стандарт]. Доступ: https://tools.ietf.org/html/rfc6550.
2. Kharrufa, H., Al-Dubai, A., Ekonomou, E., & Wadhaj, I. (2019). RPL-Based Routing Protocols in IoT Applications: A Review. IEEE Sensors Journal, 19(15), 5982-5998. DOI: 10.1109/JSEN.2019.2916014.
3. Taghizadeh, S., Rahmani, A. M., & Othman, M. (2018). CLRPL: Context-Aware and Load Balancing RPL for IoT Networks Under Heavy and Highly Dynamic Load. IEEE Access, 6, 23277-23291. DOI: 10.1109/ACCESS.2018.2827360.
4. Матвієнко С. (2023). 6LoWPAN протокол – аналіз та впровадження у IoT. Журнал сучасних телекомунікацій, 28(2), 45-56.
5. Enhancing IoT Routing Security and Efficiency: Towards AI-Enabled RPL Protocol (2022). Journal of Internet of Things Research, 7(3), 112-130.
6. A Comprehensive Survey on Node Metrics of RPL Protocol for IoT (2021). International Journal of Communication Networks and Distributed Systems, 14(1), 56-79.
7. Kim, J., Lee, S., Park, H., & Jung, Y. (2021). Energy-Efficient RPL Enhancements for Large-Scale IoT Deployments. Sensors Journal, 21(12), 3421-3435. DOI: 10.3390/s21103421.

УДК 621.382

ПОКАЗНИКИ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ТА ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ РОЗУМНИХ МІСТ

Максимов В. В., Скиба В.В.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: maksimov46@ukr.net, skyba.viktor@lll.kpi.ua

EFFECTIVENESS INDICATORS OF THE APPLICATION OF CLOUD TECHNOLOGIES AND THE INTERNET OF THINGS FOR SMART CITIES

This paper analyzes the key performance indicators for smart sustainable cities, which are designed to assess the role and effectiveness of information and communication technologies in the economic dimension of the city.

Стрімке зростання урбанізації та концентрація населення в містах вимагають нових підходів до міського планування та управління. Ключову роль у вирішенні цих викликів відіграють цифрові технології, зокрема концепція "розумних міст", забезпечуючи сталий розвиток та покращення якості життя мешканців.

Розумні міста використовують дані з IoT-пристроїв для оптимізації ресурсів, зниження витрат та підвищення якості послуг. Для обробки великих обсягів даних, що генеруються в розумних містах, критично важливими є хмарні технології, забезпечуючи масштабованість, надійність та централізоване керування. Ефективність застосування хмарних технологій та IoT в розумних містах визначається як ступінь досягнення цілей з мінімальними ресурсами та максимальним позитивним впливом на якість життя, враховуючи економічні, соціальні та екологічні аспекти. Аналіз ефективності впровадження хмарних технологій в IoT в розумних містах є важливим для обґрунтування інвестицій, оптимізації ресурсів та покращення якості життя громадян.

Рекомендація ITU-T Y.4903 [1] містить ключові показники продуктивності (key performance indicators (KPIs)) для розумних сталих міст, які призначені для оцінки ролі та ефективності інформаційно-комунікаційних технологій (ІКТ) у трьох вимірах міста: економіка, навколишнє середовище, суспільство та культура. Серед життєво важних економічних категорій розумних міст слід виділити водопостачання (KPIs: розумні лічильники води, моніторинг водопостачання), електропостачання (KPIs: розумні лічильники електроенергії, ІКТ моніторинг електропостачання), транспорт (KPIs: динамічна інформація про громадський транспорт, моніторинг дорожнього руху, контроль перехресть) і державний сектор (KPIs: відкриті дані).

Показник «Розумні лічильники води» дозволяє у режимі реального часу контролювати обсяги споживання, виявляти несанкціоноване використання або витоки, а також оптимізувати розподіл водних ресурсів. Розраховується як відсоток встановлених розумних лічильників води від загальної кількості

встановлених лічильників води.

Показник «ІКТ моніторинг водопостачання» дозволяє у режимі реального часу швидко реагувати на аварійні ситуації, своєчасно проводити технічне обслуговування та мінімізувати втрати води. Розраховується як відсоток довжини системи диспетчерського контролю та збору даних (SCADA Supervisory Control and Data Acquisition) водопостачання, яка контролюється ІКТ (км) від загальної довжини системи водопостачання (км).

Використання цих показників надає можливість розумним містам досягти цілі сталого розвитку в категорії водопостачання, а саме: до 2030 року суттєво підвищити ефективність використання води в усіх секторах і забезпечити сталий забір і постачання прісної води для вирішення проблеми дефіциту води та суттєвого зменшення кількості людей, які страждають від нестачі води. Слід також відзначити, що впровадження хмарних IoT-технологій в сфері «розумного» водопостачання вже довело свою ефективність на прикладі Барселони, дозволивши зекономити 58 мільйонів євро на рік [2].

Показник «Розумні лічильники електроенергії» дозволяє в режимі реального часу вимірювати навантаження на електромережу, що забезпечує точний облік споживання, виявлення аномалій та оперативне реагування на збої чи аварійні ситуації. Розраховується як відсоток встановлених розумних лічильників електроенергії від загальної кількості встановлених лічильників електроенергії.

Показник «ІКТ моніторинг електропостачання» визначає рівень використання систем моніторингу SCADA, IoT та хмарних технологій для централізованого збору, аналізу та обробки даних з електромереж в режимі реального часу. Такий моніторинг дає змогу отримати детальну інформацію про кількість енергії, необхідної для різних служб (громадське освітлення, транспорт, світлофори та камери відеоспостереження), прогнозувати потенційні аварійні ситуації та забезпечувати своєчасне технічне обслуговування. Розраховується як відсоток довжини системи диспетчерського контролю та збору даних (SCADA) електропостачання, яка контролюється ІКТ (км) від загальної довжини системи електропостачання (км).

Використання цих показників надає можливість розумним містам досягти цілі сталого розвитку в категорії електропостачання, а саме: до 2030 року подвоїти глобальні темпи підвищення енергоефективності. Слід також відзначити, що застосування розумних датчиків освітлення не тільки надає нову світлодіодну технологію для зменшення споживання, але й виявляти відсутність пішоходів, щоб зменшити інтенсивність світла. Для Барселони таке впровадження призвело до 30% економії електроенергії, або близько 37 мільйонів євро щороку [9]. На прикладі Единбургу це дозволило скоротити річні витрати на електроенергію на 1,6 мільйона фунтів стерлінгів або 50% на рік [3]. Проект Smartcity Malaga в перші 5 років досягнув 25% економії загального споживання електроенергії та скоротив викид CO2 на 4500 тон на рік, що становило 20% скорочення викидів, завдяки впровадженню концепту

«Smart Grid» розумних IoT-систем моніторингу електроспоживання [4].

Показник «Динамічна інформація про громадський транспорт» визначає здатність міста надавати пасажирам актуальну інформацію про стан та рух громадського транспорту у режимі реального часу. Завдяки інтеграції IoT пристроїв, GPS трекінгу та хмарних технологій, динамічна інформація про стан системи, а також час прибуття та час у дорозі дозволяє не лише покращити досвід користувачів, але й допомагає операторам коригувати розклади, оптимізувати маршрути та управляти ресурсами більш ефективно. Розраховується як відсоток кількості зупинок і станцій з доступною динамічною інформацією від загальної кількості зупинок і станцій.

Показник «Моніторинг дорожнього руху» визначає здатність системи в режимі реального часу збирати та аналізувати дані про рух транспортних засобів на головних (основних) вулицях, які включатимуть лише магістралі та шосе (житлові вулиці не включаються). Цей показник охоплює вимірювання швидкості руху, інтенсивності трафіку, виявлення заторів та різних аварійних ситуацій. Завдяки інтеграції IoT-пристроїв, відеокамер, GPS-трекінгу та хмарних технологій, система дозволяє оперативно коригувати налаштування світлофорів, перенаправляти потоки транспорту та інформувати громадян про поточну ситуацію на дорогах. Розраховується як відсоток кількості довжини основних вулиць, які контролюються ІКТ (км) від загальної протяжність основних вулиць (км).

Показник «Контроль перехресть» вимірює ефективність адаптивного управління дорожнім рухом або визначення пріоритетів на перехрестях за допомогою світлофорів у розумних містах. За допомогою інтеграції IoT датчиків, камер відеоспостереження, GPS систем та хмарних технологій, система збирає дані в режимі реального часу про інтенсивність трафіку, середній час затримки, довжину автомобільних потоків та інші параметри роботи перехрестя. На основі цих даних адаптивні системи, такі як SCATS, SCOOT або ATSAC автоматично коригують тривалість зеленого, жовтого та червоного сигналів, оптимізують розподіл потоку транспортних засобів, що сприяє зниженню заторів, скороченню часу перебування автомобілів на перехрестях та підвищенню рівня безпеки. Розраховується як відсоток кількості перехресть з адаптивним регулюванням руху від загальної кількості регульованих перехресть.

Використання цих показників надає можливість розумним містам досягти цілі сталого розвитку в категорії транспорту, а саме: до 2030 року забезпечити доступ до безпечних, недорогих, доступних і стійких транспортних систем для всіх, покращуючи безпеку дорожнього руху, зокрема шляхом розширення громадського транспорту, приділяючи особливу увагу потребам тих, хто перебуває в уразливих ситуаціях, жінок, дітей, людей з обмеженими можливостями та людей похилого віку. Слід відзначити, що впровадження технологій надання динамічної інформації про громадський транспорт в Гаазі дозволило скоротити час очікування на 20% та підвищити ефективність використання транспортної мережі [5]. Впровадження системи автоматичного контролю трафіку на перехрестях (ATSAC) в Лос-Анджелесі

дозволило скоротити затримки трафіку на 32%, а також зменшити викиди шкідливих газів від транспортних засобів на 3% [6, 7].

Показник «Відкриті дані» вимірює рівень доступності, якості та використання даних, що публікуються міською владою, в тому числі отриманих за допомогою IoT-пристроїв і оброблених хмарними технологіями. Високий рівень відкритих даних сприяє підвищенню прозорості роботи державних органів, залученню громадськості до аналізу та контролю за діяльністю влади, а також стимулює розвиток інноваційних додатків і послуг у громадському секторі. Розраховується як відсоток загальної кількості опублікованих наборів відкритих даних від загальної кількості наборів даних.

Використання цього показника надає можливість розумним містам досягти цілі сталого розвитку в категорії державний сектор, а саме: розвивати ефективні, підзвітні та прозорі установи на всіх рівнях та забезпечити репрезентативне, оперативне прийняття рішень на всіх рівнях. Лідером у використанні відкритих даних є місто Нью-Йорк завдяки порталу NYC Open Data, що налічує близько 2,6 тисяч наборів даних, та 6 мільярдів рядків даних. Завдяки цьому проекту розробники та громадські організації можуть створювати безліч інноваційних рішень, зокрема додатки для аналізу трафіку, оптимізації використання ресурсів та моніторингу ефективності міських послуг [8].

Висновок. Інтеграція хмарних технологій та IoT-пристроїв є основою розвитку розумних міст, забезпечуючи централізоване управління та підвищення ефективності послуг.

Література

1. International Telecommunication Union. (03/2022). Key performance indicators for smart sustainable cities to assess the achievement of sustainable development goals. ITU-T Recommendation Y.4903 https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14173.
2. Cisco. Розумне місто Барселона. (2014) https://www.cisco.com/c/dam/m/es_la/ioe/public_sector/pdfs/Jurisdictions/Barcelona_Jurisdiction_Profile_final.pdf.
3. Dizon, E., & Pranggono, B. (2022). Smart streetlights in Smart City: a case study of Sheffield. https://www.researchgate.net/publication/263962649_Performance_Measures_for_Traffic_Signal_Systems_An_Outcome-Oriented_Approach#pf7f.
4. Felipe A. C., Susana C. G., Josep B., & F., Enrique A. (2009). Malaga Smart-City: A Smart Grid Project Demonstration. https://www.researchgate.net/publication/332471607_Title_Malaga_Smart-City_A_Smart_ Grid_Project_Demonstration_2009.
5. Dziekan, K., & Kottenhoff, K. (2007). Dynamic at-stop real-time information displays for public transport: effects on customers. https://www.sciencedirect.com/science/article/abs/pii/S0965856406001431.
6. Day, C. M., Bullock, D. M., Li, H., Remias, S. M., Hainen, A. M., Freije, R., Stevens, A., Sturdevant, J. R., & Brennan, T. M. (2014). Performance Measures for Traffic Signal Systems: An Outcome-Oriented Approach. https://www.researchgate.net/publication/263962649_Performance_Measures_for_Traffic_Signal_Systems_An_Outcome-Oriented_Approach#pf7f.
7. LADOT. ATSAC. (2020) https://ladot.lacity.gov/projects/transportation-technology/atsac.
8. NYC Open Data. (2025) https://opendata.cityofnewyork.us/dashboard/.
9. Maria G. Smart Cities in Action. Barcelona. https://blog.bismart.com/en/why-barcelona-is-a-smart-city.

УДК 621.9

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ СИСТЕМ ТА МЕРЕЖ ІОТ ДЛЯ ІНТЕЛЕКТУАЛЬНИХ ТРАНСПОРТНИХ СИСТЕМ

Григоренко О.Г., Петренко В.О.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: olenagri@ukr.net, petrenko.vladislava@lll.kpi.ua

APPLICATION FEATURES OF IoT SYSTEMS AND NETWORKS FOR INTELLIGENT TRANSPORT SYSTEMS

The application features of the Internet of Things for intelligent transport systems are analyzed, which contributes to increasing the efficiency of vehicle and logistics management.

Проаналізовані особливості застосування Інтернету речей для інтелектуальних транспортних систем, що сприяє підвищенню ефективності управління транспортними засобами і логістикою.

Системи та мережі Інтернету речей все глибше проникають у наше повсякденне життя, зокрема при користуванні автомобілями, тому актуальність застосування IoT в транспортних системах є актуальною. Автомобільні IoT-системи розвиваються швидкими темпами, і разом із цим з'являються нові виклики та загрози. Щороку з'являються нові IoT-рішення, більш потужні датчики, швидші мережі зв'язку (5G, 6G), удосконалені алгоритми штучного інтелекту для автономного водіння. Це означає, що сьогоднішні стандарти та підходи можуть стати застарілими вже через кілька років. Дослідження особливостей застосування систем та мереж IoT дозволяє передбачити ці зміни та адаптуватися до них.

Інтелектуальна транспортна система (ІТС) - це система, що інтегрує сучасні технології управління з телематикою, призначена для автоматизованого пошуку та прийняття найбільш ефективних сценаріїв керування транспортного засобу і його елементів з метою забезпечення мобільності. У світовій практиці ІТС визнані як спосіб інтеграції досягнень сучасних методів управління і телематики в усі види транспортної діяльності для вирішення проблем економічного і соціального характеру: підвищення ефективності функціонування пасажирського та вантажного транспорту, зниження транспортних витрат, забезпечення транспортної безпеки і поліпшення екологічних показників [1].

У Директиві 2010/40/ЄС Європейського Парламенту та Ради від 7 липня 2010 року «Про фреймворк для розгортання інтелектуальних транспортних систем у сфері автомобільного транспорту та для інтерфейсу з іншими видами транспорту» визначено, що ІТС означають системи, в яких інформаційні та комунікаційні технології застосовуються у сфері автомобільного транспорту [2], включаючи інфраструктуру, транспортні засоби та користувачів, а також в управлінні рухом і мобільністю, та для інтерфейсу з іншими видами транспорту.

Міжнародний стандарт ISO 21217:2020 (Інтелектуальні транспортні системи - станційна та телекомунікаційна архітектура) надає приклади комунікацій в ITC, щоб підтримати велику різноманітність послуг з різними вимогами, а також ефективний обмін інформацією, яку зберігають окремі сервісні програми [2].

Однією з особливостей застосування систем та мереж IoT для ITC є необхідність поєднувати технології безпроводового доступу та протоколи зв'язку з відмінними характеристиками продуктивності (дальність зв'язку, доступна смуга пропускання, затримка наскрізної передачі, якість обслуговування, безпека тощо) [2].

Машинно-орієнтований зв'язок (МОЗ) - це форма передавання даних між двома або більше об'єктами, під час використання якої щонайменше одному об'єкту не потрібне обов'язкове втручання людини в процес зв'язку [2]. Домен пристроїв машинно-орієнтованого зв'язку містить пристрої та шлюзи МОЗ. Пристрої можуть бути різних типів, як видно з рисунка 1 [2].

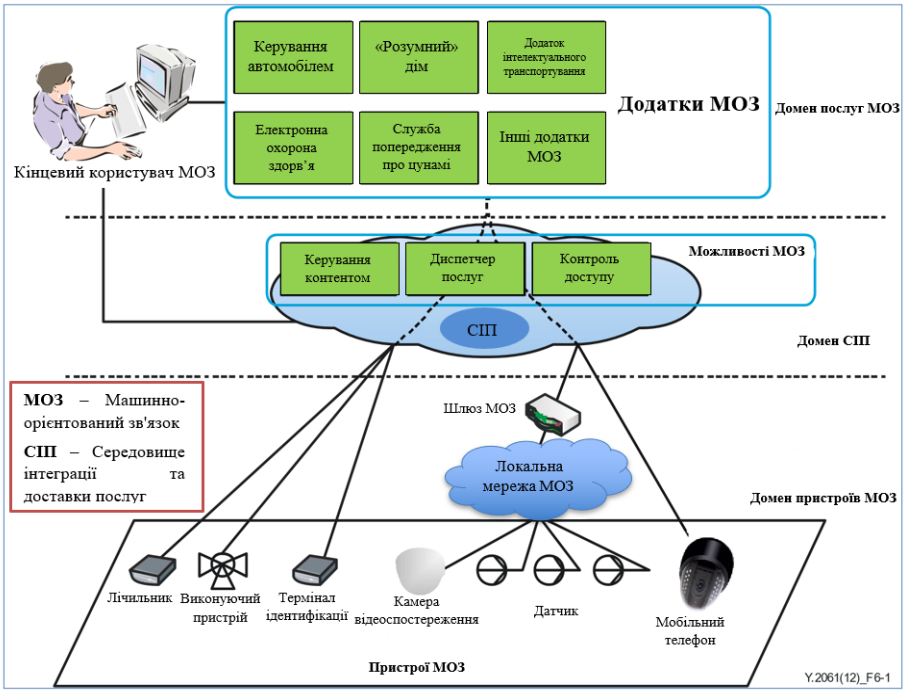


Рис.1. Огляд мереж, що забезпечують підтримку додатків машинно-орієнтованого зв'язку (МОЗ) у середовищі мереж наступних поколінь NGN [2].

Ефективність та результативність управління транспортною логістикою залежить від складу та стану парку, продуктивності водіїв, комунікації водіїв та диспетчерів. Автоматизувати ці процеси допомагають системи управління парком (FMS), які не тільки дозволяють ефективно контролювати рух транспорту, планувати оптимальні та найефективніші маршрути для доставки товарів та уникати затримок, але й використовувати моніторинг та аналіз поведінки водіїв, його стиль водіння, використання гальм та ін., що дозволяє покращити безпеку на дорозі, знизити ризик нещасних випадків та зменшити знос транспортних засобів [3].

Наприклад, системи FMS TomTom Telematics, забезпечують збір даних про рух автопарку, включаючи швидкість, пробіг, використання

палива, здійснює аналітику та повідомляє про необхідність технічного обслуговування транспортних засобів, включаючи перевірку мастила та заміну деталей. Щодо покращення управління транспортною логістикою TomTom Telematics надає можливість зручними засобами здійснювати комунікацію між диспетчерами та водіями, сприяти співпраці всередині команди, дозволяє ефективно координувати рух транспорту, надсилати повідомлення про зміни в маршруті або інструкції для водіїв, а також отримувати зворотний зв'язок [3].

Кожен підключений автомобіль обладнаний датчиками, GPS, камерою та шлюзом служби управління підключеним автомобілем. Центр управління збирає дані про місцезнаходження, швидкість і конкретну ситуацію від датчиків, GPS-приймача і відеокамер в автомобілі. Дані, зібрані через розташований в автомобілі шлюз, передаються в мережі наступних поколінь бездротовим каналом зв'язку (LTE, 4G, 5G тощо). Коли датчик в автомобілі виявляє аномальну ситуацію, наприклад запах бензину, в центр управління надсилається відповідне сповіщення. Коли автомобіль виїжджає за межі заданого маршруту, повинна слідувати реакція з боку додатка, наприклад дзвінок водієві або сповіщення адміністратору автомобіля [2].

В інтернеті з'являється безліч привабливих нових служб, наприклад служби соціальних мереж. Додатки МОЗ повинні мати можливість взаємодії з цими інтернет-службами, щоб клієнти могли з ними працювати, використовуючи ці додатки. Застосунки МОЗ, інтегровані з інтернет-службами, характеризуються довшими ланцюжками створення доданої вартості та залучають більше клієнтів [2].

Підсумовуючи, зазначимо, що впровадження IoT-рішень сприяє підвищенню ефективності управління транспортною логістикою завдяки інтеграції даних у реальному часі, автоматизації процесів та оптимізації маршрутів. Успішне впровадження IoT-рішень у транспортній галузі вимагає міжгалузевої співпраці та державної підтримки. Також IoT має значний потенціал для трансформації транспортних систем, забезпечуючи їхню ефективність, безпеку та екологічність. Подальші дослідження у цьому напрямку сприятимуть створенню нових інноваційних рішень та розширенню сфер застосування IoT в автомобільній промисловості.

Література

1. ІНТЕЛЕКТУАЛЬНІ ТРАНСПОРТНІ СИСТЕМИ / [Електронний ресурс] – Режим доступу: https://stud.com.ua/120718/informatika/intelektualni_transportni_sistemi
2. ITU-T Y.2061, Requirements for support of machine-oriented communication applications in the NGN environment / [Електронний ресурс] – Режим доступу: https://1f8a81b9b0707b63-19211.webchannel-proxy.scarabresearch.com/rec/T-REC-Y.2061-201206-I/en
3. Головіна О. Сучасні технології в управлінні транспортною логістикою. International Science Journal of Management, Economics & Finance. Vol. 2, No. 3, 2023, pp. 35-42. / [Електронний ресурс] – Режим доступу: https://isg-journal.com/isjmef/

УДК 621.9

ЗАГРОЗИ ТА ВРАЗЛИВОСТІ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ У КІБЕРПРОСТОРІ

Григоренко О.Г., Сачек Р.В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: olenagri@ukr.net, srv300333@gmail.com

THREATS AND VULNERABILITIES OF INTERNET OF THINGS SYSTEMS IN CYBERSPACE

The main threats, vulnerabilities, and attacks in Internet of Things networks have been analyzed, which allows for timely application of countermeasures and safe use of IoT in cyberspace.

Проаналізовані основні загрози, вразливості, атаки в мережах Інтернету речей, що дозволяє вчасно застосувати заходи протидії і безпечно використовувати IoT у кіберпросторі.

Інтернет речей безсумнівно є сьогодні одним з головних компонентів науково-технічного прогресу. Кількість пристроїв невпинно зростає (рис.1) і ця тенденція зберігатиметься і надалі [1,3]. За визначенням компанії Gartner: “Інтернет речей (IoT) — це мережа фізичних об’єктів, які містять вбудовану технологію для спілкування та сприйняття або взаємодії з їхнім внутрішнім станом або зовнішнім середовищем” [4]. Тобто, це екосистема пристроїв і технологій, підключених через Інтернет, які постійно збирають і передають дані. Часто такі пристрої називають «смарт» або «розумний».

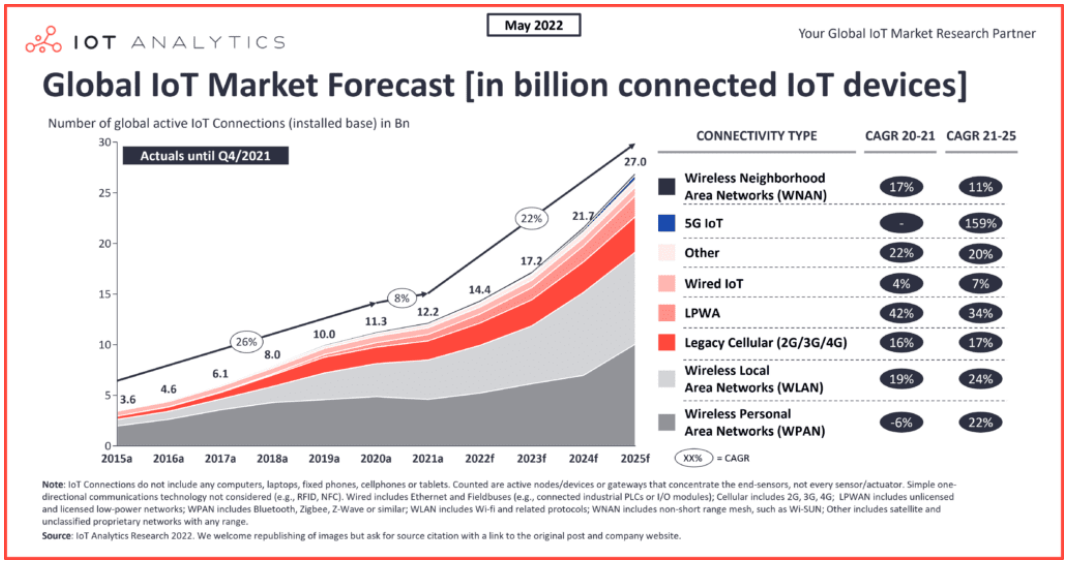


Рис.1. Тенденція розвитку IoT(в мільярдах підключених пристроїв IoT) [1].

IoT є дуже зручним та корисним набором технологій, що значно спрощує як повсякденне життя людини, так і роботу організацій. Проте, пристрої і мережі IoT мають вразливості, які важко вчасно визначати. Також IoT мережі – це екосистема речей, де нікому відслідковувати нетипову ситуацію і віруси. Кожен пристрій IoT є потенційно вразливою точкою входу в мережу та

бізнес-процеси. Тому такі мережі можуть стати (і стають) першим етапом більших зламів, особливо якщо атака таргетована саме на конкретну організацію. Зважаючи на це, кібербезпека пристроїв Інтернету речей стає все більш критичним питанням, оскільки кількість пристроїв, які можуть отримувати та надсилати конфіденційні дані, щоденно росте. Тож впровадження й оновлення заходів безпеки пристроїв має стати пріоритетом на найближчі роки для технології IoT [1].

Найпоширенішими атаками на пристрої Інтернету речей (IoT) є [1,2,5]:

DDoS-атаки (Distributed Denial of Service) – Хакери використовують зламані IoT-пристрої для створення ботнетів (наприклад, Mirai) і перевантажують сервери жертви трафіком.

Brute-force атаки на паролі – Багато IoT-пристроїв мають слабкі або стандартні паролі (типу "admin/admin"), які зловмисники легко підбирають.

Атаки через незахищені API – Якщо IoT-пристрій взаємодіє з сервером через API без належної автентифікації або шифрування, хакери можуть отримати контроль над ним.

MITM-атака (Man-in-the-Middle) – Перехоплення незашифрованих даних між IoT-пристроєм і сервером, що дозволяє змінювати або викрадати інформацію.

Фізичний злам пристрою – Якщо хакер отримує фізичний доступ до пристрою, він може витягнути дані з пам’яті, підключитися до управляючих портів (наприклад, JTAG, UART) або змінити мікропрограму (firmware).

Атака на оновлення прошивки – Якщо пристрій оновлюється без перевірки цифрового підпису, зловмисники можуть підсунути шкідливе програмне забезпечення (ПЗ).

Перехоплення та підміна радіосигналів – Наприклад, атаки на Wi-Fi, Zigbee, Bluetooth, RFID, LoRaWAN, коли хакери перехоплюють або модифікують передані дані.

Експлуатація вразливостей у ПЗ – Використання дефектів у прошивці або операційній системі IoT-пристрою для виконання шкідливого коду або отримання доступу до системи.

Зловживання стандартними сервісами (MQTT, CoAP, UPnP) – Деякі IoT-протоколи не мають шифрування за замовчуванням, що дає змогу хакерам шпигувати або підробляти команди.

Атаки на блокчейн у IoT – Якщо IoT-пристрій використовує блокчейн для збереження даних, можливі атаки на смарт-контракти або мережу (наприклад, 51% атака).

Захист пристроїв Інтернету речей є життєво важливим компонентом безпеки сучасної мережі в організаціях. Одним із засобів захисту від різного роду атак є процес аутентифікації в мережі.

Ризики IoT легко не помітити, якщо не використовувати призначені для цього інструменти. Іноді співробітники з інформаційної безпеки нехтують інвентаризацією кінцевих точок, через це легко можна пропустити потенційно вразливий до атак пристрій. Сьогодні існують програмні продукти для проведення інвентаризації та моніторингу всіх підключених IoT пристроїв. Такий тип рішень з безпеки значно знижує ризики, аналізуючи потенційні атаки.

Різноманітність пристроїв IoT у поєднанні з їх широким розгортанням у

критичних секторах, потребує багатогранного підходу до безпеки, який виходить за рамки традиційних заходів. Удосконалення методів шифрування, алгоритмів збереження конфіденційності, виявлення аномалій за допомогою штучного інтелекту представляють важливі кроки в забезпеченні безпеки середовищ IoT [5,6].

Також необхідно застосовувати цілісні наскрізні структури кібербезпеки, які можна легко інтегрувати в життєвий цикл IoT — від проєктування мережі, виробництва та розгортання пристроїв до поточної експлуатації та виведення з неї. Відсутність стандартизованих протоколів безпеки та інфраструктури в різних екосистемах Інтернету речей є значною перешкодою для досягнення надійної безпеки, що призводить до непослідовних положень безпеки на різних пристроях і мережах, створюючи вразливості, які можуть бути використані зловмисниками. Майбутні дослідження мають надавати пріоритет розробці сумісних і масштабованих інфраструктур безпеки, які можна адаптувати до різноманітних пристроїв IoT [5].

Однією з перспектив є інтеграція штучного інтелекту та машинного навчання в кібербезпеку [5,6]. Тому важливим є розробка стійких моделей ШІ, які можуть протистояти різним атакам, а також необхідність постійного моніторингу та оновлення цих моделей, щоб не відставати від нових загроз.

З вищезазначених векторів атак на IoT можна зробити висновок, що основні компоненти систем Інтернету речей є досить вразливими до атак зловмисників, тому безпека IoT повинна розглядатися ще на етапі проектування, щоб покращити її інтегрування.

Література

1. Д.Діденко. Поширені атаки на IoT та захист від них. / [Електронний ресурс] – Режим доступу: https://corewin.ua/blog/attacks-on-iot-how-protect/
2. Kupershtein L., Malinovskyi V., Kaplun V. CYBER SECURITY OF MOBILE DEVICES AND INTERNET OF THINGS / КІБЕРБЕЗПЕКА МОБІЛЬНИХ ПРИСТРОЇВ ТА ІНТЕРНЕТУ РЕЧЕЙ.-2024/ [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/379257182_CYBER_SECURITY_OF_MOBILE_DEVICES_AND_INTERNET_OF_THINGS_KIBERBEZPEKA_MOBILNIH_PRISTROIV_TA_INTERNETU_RECEJ
3. IoT-analytics/ [Електронний ресурс] – Режим доступу:https://iot-analytics.com/
4. Gartner:/ [Електронний ресурс] – Режим доступу:https://www.gartner.com/en/information-technology/glossary/internet-of-things
5. E.Dritsas, M.Trigka. A Survey on Cybersecurity in IoT. – Future Internet 2025, 17(1), 30 / [Електронний ресурс] – Режим доступу: https://www.mdpi.com/1999-5903/17/1/30
6. M.Aziz Al Kabira, W.Elmedanya, M.Saeed Sharif. Securing IoT Devices Against Emerging Security Threats:Challenges and Mitigation Techniques. – JOURNAL OF CYBER SECURITY TECHNOLOGY. – 2023, VOL. 7, NO. 4, 199–223 / [Електронний ресурс] – Режим доступу: https://www.tandfonline.com/doi/epdf/10.1080/23742917.2023.2228053?needAccess=true

УДК 621.39

АНАЛІЗ МЕТОДІВ ПІДВИЩЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ В МЕРЕЖАХ 5G

Григоренко О.Г., Колесник Я.В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: olenagri@ukr.net, kolesnik.y2004@gmail.com

ANALYSIS OF ENERGY EFFICIENCY ENHANCEMENT METHODS IN 5G NETWORKS

The main methods of increasing energy efficiency in 5G networks are analyzed, allowing to reduce energy consumption without losing productivity and communication quality. Modern technological solutions that contribute to the optimal use of energy resources are considered.

Проаналізовано основні методи підвищення енергоефективності в мережах 5G, що дозволяють зменшити споживання енергії без втрати продуктивності та якості зв'язку. Розглянуто сучасні технологічні рішення, які сприяють оптимальному використанню енергетичних ресурсів.

Мережі п'ятого покоління (5G) стали ключовим елементом цифрової трансформації, забезпечуючи високу швидкість передачі даних, низьку затримку та підтримку масового підключення пристроїв. За прогнозами Ericsson до кінця 2025 року 2,6 мільярдів пристроїв буде підключено до 5G, а споживання трафіку зросте до 24 Гігабайт [3], що суттєво підвищить вимоги до інфраструктури. У звіті Ericsson Mobility Report за листопад 2024 року прогнозується, що до 2030 року мобільні підключення 5G становитимуть 60% від загальної кількості підключень, досягнувши 500 мільйонів на Близькому Сході та в Північній Африці [1]. Однак разом із технологічними перевагами 5G приносить проблему високого енергоспоживання. Базові станції 5G, оснащені технологією Massive MIMO та малими сотами (small cells), споживають у 2-3 рази більше енергії порівняно з мережами 4G. Це створює виклики як для операторів, які прагнуть знизити операційні витрати, так і для суспільства, що орієнтується на сталий розвиток.

Питання енергоефективності в телекомунікаціях набуває особливої актуальності в контексті глобальних екологічних ініціатив, таких як Паризька угода [2]. Тому є актуальним проаналізувати сучасні методи підвищення енергоефективності в мережах 5G, оцінити їх ефективність та визначити перспективи розвитку.

Для підвищення енергоефективності в мережах 5G застосовуються різноманітні технології, які можна поділити на апаратні, програмні, мережеві архітектурні рішення тощо.[4-6]

Технології апаратного рівня. Одним із ключових підходів є використання енергоефективних чипів, виготовлених за 7-нм технологією. Такі процесори зменшують споживання енергії на 20-30% порівняно з попередніми поколіннями. Іншим важливим рішенням є технологія Massive MIMO, яка завдяки адаптивному керуванню антенами дозволяє оптимізувати

передачу сигналу, знижуючи енергоспоживання на одиницю переданих даних. Проте висока щільність антен потребує складного налаштування, що може обмежувати її масове впровадження.

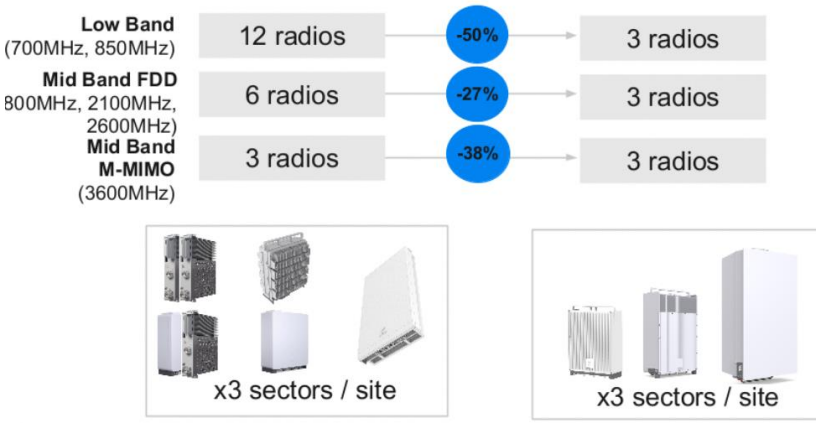


Рис.1. Приклад впровадження рішень з енергоефективності в Telstra у 2023р. Економія енергії 50, 27 та 38 % [4].

Програмні рішення. Алгоритми "сплячого режиму" (Sleep Mode) для базових станцій дають змогу вимикати окремі компоненти під час низького мережевого навантаження. За оцінками, це знижує енергоспоживання до 40% у нічні години. Динамічне управління ресурсами (Dynamic Resource Allocation) також відіграє важливу роль, дозволяючи адаптувати потужність передачі до поточного трафіку. Такі методи прості у впровадженні, але їхня ефективність залежить від стабільності навантаження.

Інтеграція з відновлюваними джерелами енергії. Усе більше операторів експериментують із живленням базових станцій від сонячних панелей і вітрових турбін. Наприклад, у сільських регіонах Індії вже реалізовано проєкти, де до 60% енергії для 5G-станцій надходить із зелених джерел. Це не лише знижує вуглецевий слід, а й зменшує залежність від традиційних енергоносіїв [6].

Мережева архітектура. Технологія Cloud RAN (Centralized Radio Access Network) переносить обчислення з периферійних вузлів до централізованих дата-центрів, що скорочує енергоспоживання малих сот. Водночас впровадження штучного інтелекту (AI) для управління мережею дозволяє прогнозувати пікові навантаження та автоматично оптимізувати ресурси.

Для оцінки ефективності розглянутих методів [4-6] використано такі критерії як енергоефективність (Вт/біт), вартість впровадження, складність інтеграції та вплив на якість сервісу (QoS).

Massive MIMO демонструє високу енергоефективність (до 10 Мбіт/Вт у порівнянні з 5 Мбіт/Вт у 4G), але потребує значних інвестицій у модернізацію обладнання та складного калібрування. Вплив на QoS позитивний завдяки кращій пропускній здатності, але затримки можуть зростати при неправильному налаштуванні.

Sleep Mode є економічно вигідним рішенням із низькою вартістю впровадження. Енергоефективність зростає на 30-40% у періоди низького

трафіку, однак у пікові години метод втрачає актуальність, а перемикання режимів може тимчасово погіршувати QoS.

Відновлювані джерела енергії знижують операційні витрати в довгостроковій перспективі, але потребують значних початкових інвестицій і залежать від кліматичних умов. Їхній вплив на QoS нейтральний, якщо мережа має резервне живлення.

Cloud RAN забезпечує енергоефективність на рівні 15 Мбіт/Вт у великих мережах, але висока складність інтеграції та потреба в потужних оптичних каналах роблять його дорогим. AI-оптимізація додатково підвищує ефективність на 10-15%, зберігаючи стабільний QoS.

Аналіз показав, що найбільш перспективними є комбіновані підходи, які поєднують апаратні інновації (Massive MIMO, енергоефективні чипи) з програмними рішеннями (Sleep Mode, AI-управління). Такі стратегії дозволяють досягти балансу між енергоефективністю, вартістю та якістю сервісу. Інтеграція з відновлюваними джерелами енергії є важливим кроком до екологічної стійкості, особливо в регіонах із високим сонячним або вітровим потенціалом.

Рекомендується зосередити подальші дослідження на розвитку AI-технологій для автоматичної оптимізації енергоспоживання та на стандартизації гібридних енергетичних систем. У 2025 році енергоефективність може стати конкурентною перевагою для операторів, які прагнуть відповідати екологічним стандартам і знижувати витрати. Таким чином, мережі 5G не лише забезпечать технологічний прогрес, а й сприятимуть сталому розвитку телекомунікаційної галузі.

Література

1. Ericsson Mobility Report: 5G will outpace 4G in 2027/ [Електронний ресурс] – Режим доступу:https://www.ericsson.com/en/press-releases/5/2024/ericsson-mobility-report-5g-will-outpace-4g-in-2027
2. Паризька угода/ [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_l61#Text
3. 2025 рік/ [Електронний ресурс] – Режим доступу: https://epravda.com.ua/news/2019/11/25/654105/
4. S.Kinney. A three-step approach to 5G sustainability/ [Електронний ресурс] – Режим доступу:https://www.rcrwireless.com/20231208/5g/a-three-step-approach-to-5g-sustainability
5. A.Ichimescu, N.Popescu, E.C.Popovici, A.Toma. Energy Efficiency for 5G and Beyond 5G: Potential, Limitations, and Future Direction. – Sensors 2024, 24(22), 7402/ [Електронний ресурс] – Режим доступу:https://www.mdpi.com/1424-8220/24/22/7402
6. GSMA. (2023). The Mobile Economy 2023. London: GSMA Intelligence/ [Електронний ресурс] – Режим доступу:https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2023/03/270223-The-Mobile-Economy-2023.pdf

УДК 621.391

ДОСЛІДЖЕННЯ ДИНАМІЧНИХ ВЛАСТИВОСТЕЙ АДАПТИВНИХ ПРОГРАМНО-КЕРОВАНИХ РАДІОЗАСОБІВ У ПРОСТОРІ СТАНУ

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

INVESTIGATION OF DYNAMIC PROPERTIES OF ADAPTIVE SOFTWARE-CONTROLLED RADIO DEVICES IN STATE SPACE

The problems of analyzing the dynamics of the processes of restructuring software-controlled radio devices (SRD) are analyzed. The considered mathematical apparatus of the state space allows us to obtain algorithms for statistical analysis, optimal and quasi-optimal control of SRD, which in some cases lead to significant gains in efficiency compared to known algorithms

Незважаючи на досить велику кількість публікацій з проблем проектування адаптивних систем, динаміку процесів перебудови програмно-керованих радіозасобів (ПРС) вивчено недостатньо. Залишаються невирішеними такі завдання:

- оцінка впливу виду та параметрів закону перебудови ПРС на величину динамічної похибки при заданих параметрах адаптивних систем;
- аналізу впливу виду, порядку та параметрів апроксимуючої функції на динамічну похибку різних класів таких адаптивних систем при заданому законі перебудови;
- синтезу адаптивних систем, що перебудовуються за заданим законом та забезпечують необхідну динамічну точність;
- оптимізації закону перебудови з урахуванням вимог до динамічної точності, а також низку інших практично важливих завдань.

Розглянемо адаптивні системи довільного класу та порядку, перебудова яких забезпечується шляхом зміни періоду дискретизації. Такі адаптивні системи описуються нестаціонарними різницевими рівняннями динаміки виду

$$\begin{cases} \mathbf{x}(n+1) = \mathbf{A}_d \mathbf{x}(n) + \mathbf{B}_d e(n) \\ y(n) = \mathbf{C}\mathbf{x}(n) + de(n) \\ T(n) = T / \Psi(n) \end{cases}, \qquad (1)$$

де $e(n)$, $y(n)$, $\mathbf{x}(n)$ – вхідна, вихідна змінні та вектор змінних стану; $\mathbf{A}_d$, B_d, C та d – параметри адаптивної системи; $T(n)$ – керована тривалість часового інтервалу між сусідніми відліками; $\Psi(n)$ – закон перебудови ($\Psi(n) \geq 0$).

Дискретна передатна функція адаптивної системи при постійному

впливі, що управляє $\Psi(n) = const = \Psi$ має вигляд

$$K_d(z,\psi) = \mathbf{C}(z^{1/\psi}\mathbf{I} - \mathbf{A}_d)^{-1}\mathbf{B}_d + d = K_d(z^{1/\psi},1), \qquad (2)$$

де $H_d(z,1)$ – вираз цієї функції при $\psi = 1$, $z = e^{pT}$.

Величина ψ визначає масштаб частотних характеристик по осі частот (частоту налаштування адаптивної системи) $\omega_c(\psi) = \psi\omega_c(1)$.

Так як система рівнянь (1) не може бути вирішена методами теорії дискретних систем, то перейдемо від ґратчастих функцій до безперервних

$$e(n) \to e(t), y(n) \to y(t), \psi(n) \to \psi(t),$$
$$\mathbf{x}(n) \to \mathbf{x}(t), \mathbf{x}(n+1) \to \mathbf{x}(t) + T\mathbf{x}(t)/\psi(t)$$

і перейдемо до еквівалентної безперервної системи, що описується диференціальними рівняннями

$$\begin{cases} \dot{\mathbf{x}}(t) = \psi(t)\left[\mathbf{A}\mathbf{x}(t) + \mathbf{B}e(t)\right] \\ y(t) = \mathbf{C}\mathbf{x}(t) + de(t) \end{cases}, \qquad (3)$$

де $\mathbf{A} = T^{-1}\mathbf{A}_d - \mathbf{I}$, $\mathbf{B} = T^{-1}\mathbf{B}_d$.

Слід зазначити, що адекватним інструментом дослідження процесів перебудови може бути динамічна частотна характеристика (ДЧХ). За фізичним змістом ДЧХ близька до комплексного коефіцієнта передачі стаціонарної системи, оскільки служить коефіцієнтом пропорційності між гармонійним вхідним впливом та вимушеною складовою реакції системи.

Динамічна АЧХ відображає процес зміни в часі модуля коефіцієнта передачі на частоті впливу, а динамічна ФЧХ – фазового зсуву, що вноситься.

Як вихідні дані використовується закон перебудови та математична модель еквівалентної безперервної стаціонарної адаптивної системи (ПРС) у формі імпульсної функції $h(t)$ або передавальної функції $K(p)$.

Вважаючи, що законом перебудови є невід'ємна інтегрована функція $\psi(t)$, визначимо загальний вираз ДЧХ методом τ-перетворень. Ідея цього методу полягає в переході до нової (приведеної) шкали часу, пов'язаної з абсолютними співвідношеннями $\tau = \varphi(t) = \int_0^t \psi(t)dt$, $t = \phi(\tau)$, в якій рівняння (3), що розглядаються щодо τ-зображень змінних $\left(e_r(\tau), y_r(\tau), \mathbf{x}_r(\tau), \dot{\mathbf{x}}_r(\tau)\right)$, перетворюються на стаціонарний і набувають вигляду

$$\begin{cases} \dot{\mathbf{x}}_r(\tau) = \mathbf{A}\mathbf{x}_r(\tau) + \mathbf{B}e_r(\tau) \\ y_r(\tau) = \mathbf{C}\mathbf{x}_r(\tau) + de_r(\tau) \end{cases}. \qquad (4)$$

За допомогою τ-перетворень представимо τ-зображення вхідного впливу $e(t) = \exp(pt), (p = j\omega)$ у вигляді $e_r(\tau) = \exp[p\phi(\tau)]$ та отримаємо ДЧХ

$$K_r(p,\tau) = \int_0^\infty h(x) e^{p[\varphi(\tau - x) - \varphi(\tau)]} dx. \quad (5)$$

Після зворотного τ-перетворення виходить шуканий вираз ДЧХ

$$K(p,t) = \int_0^\infty h(x) e^{-pR(t,x)} dx, \quad (6)$$

де $R(t,x) = t - \phi[\varphi(t) - x]$.

У практично важливому випадку закон перебудови є ступінчастою функцією

$$\psi(t) = \begin{cases} 1 & \text{при } t < 0 \\ \beta & \text{при } t \geq 0 \end{cases},$$

а закони τ-перетворень визначаються виразами

$$\varphi(t) = \begin{cases} t & \text{при } t < 0 \\ \beta & \text{при } t \geq 0 \end{cases}, \quad \phi(t) = \begin{cases} \tau & \text{при } \tau < 0 \\ \tau/\beta & \text{при } \tau \geq 0 \end{cases}.$$

Тоді вираз ДЧХ для даного випадку має вигляд

$$K(p,t) = \begin{cases} K(p) & \text{при } t < 0 \\ K(p/\beta) + \Delta K(p,t) & \text{при } t \geq 0 \end{cases}, \quad (7)$$

де $\Delta K(p,t)$ – динамічна похибка.

$$\Delta K(p,t) = \frac{p(1-\beta)}{\exp(-pt)} \sum_{i=1}^{N} \frac{A(p_i)\exp(\beta p_i t)}{B(p_i)(p - p_i)(p - \beta p_i)};$$

N – порядок фільтра, p_i – полюси передавальної функції $K(p) = A(p)/B(p)$.

З аналізу (7) випливає:

1) ДЧХ адаптивних систем, що дискретно перебудовуються, є функцією трьох змінних – частоти ω, часу t та глибини перебудови β;

2) асимптотами цієї характеристики служать початкові та кінцеві вирази статичної передавальної функції

$$K(p,t) = \begin{cases} K(p) & \text{при } t < 0 \\ K(p/\beta) & \text{при } t \to \infty \end{cases};$$

3) ДЧХ є безперервною функцією часу – у момент перемикання вона змінює своє значення

$$K(p,0^{(+)}) = K(p,0^{(-)}) = K(p);$$

4) динаміка процесу перебудови повністю визначається динамічною похибкою $\Delta K(p,t)$;

5) початкове значення динамічної похибки дорівнює збільшенню статичної передавальної функції $\Delta K(p,0) = K(p) - K(p/\beta)$;

6) при малій величині кроку перебудови $\Delta\beta = 1-\beta << 1$ амплітуда похибки пропорційна величині цього кроку.

Висновки.

1. Розглянутий математичний апарат простору станів дозволяє отримати алгоритми статистичного аналізу оптимального та квазіоптимального управління ПРС, що призводять у ряді випадків до суттєвих виграшів у ефективності порівняно з відомими алгоритмами.

2. Дослідження динамічних властивостей адаптивних програмно-керованих радіозасобів у просторі стану показало, що ДЧХ ПРС є безперервною функцією часу – у момент перемикання вона не змінює свого значення, а динаміка процесу перебудови повністю визначається динамічною похибкою $\Delta K(p,t)$.

Література

1. J. Mitola et al., “Cognitive radio: Making software radios more personal,” IEEE Personal Communication, vol. 6, no. 4, pp. 13–18, Aug. 1999.
2. S. Haykin, “Cognitive radio: Brain-empowered wireless communications,” IEEE J. Sel. Areas Comm. vol. 23 no 2, pp. 201–220, 2005.
3. R. Venkatesha Prasad, “Cognitive Functionality in Next Generation Wireless Networks: Standardization Efforts,” IEEE Communication magazine, vol 64, issue: 4, pp.72-78, April 2008.
4. Amir Ghasemi and Elvino S. Sousa, “Spectrum Sensing in Cognitive Radio Networks: Requirements, Challenges and Design Trade-offs,” IEEE Communication Magazine, volume:46, issue:4, pp. 32-39, April 2008.

УДК 004.7

АНАЛІЗ ВЗАЄМОДІЇ ПРОТОКОЛІВ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ NGN

Руденко А. А., Гаттуров В. К.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: anastasiarudenko078@gmail.com

ANALYSIS OF PROTOCOL INTERACTION IN NGN TELECOMMUNICATION NETWORKS

This article examines the interplay of Softswitch-based NGN and IMS NGN protocols in the world of active IMS migration.

Ця стаття розглядає взаємодію протоколів мереж NGN на базі Softswitch та NGN IMS у світлі активного переходу на мережі IMS.

Наразі в Україні відбувається активний перехід операторів до архітектури IMS, що надає абонентам мереж такі переваги як, наприклад, дзвінки за технологією VoLTE (дзвінки через мережу LTE) та VoWiFi (дзвінки через мережу Wi-Fi), що покращує якість звуку, зменшує час з'єднання з абонентом (через відсутність процедури Circuit Switching Fallback – перехід в мережу 2/3G), та надає можливість користування Інтернетом під час виклику. Але на даний час залишається велика кількість людей, мобільні термінали чи SIM-карти яких не підтримують дану технологію, тому використання старих технологій та мереж на базі Softwitch ще досі залишається актуальним. Як відомо, при використанні архітектури мережі нового покоління, обмін повідомленням між елементами мережі відбувається за протоколами H.323 та Session Initiation Protocol (надалі - SIP), в той час як в IMS використовується тільки SIP. Так як самим протоколом SIP передбачено використання різними пристроями та додаванням нових заголовків постає питання: яким чином сторони зможуть "порозумітися", якщо вони по різному можуть реалізовувати SIP в своїх повідомленнях, або взагалі використовувати різні протоколи?

Одним із рішень даної проблеми можна вважати таке поняття як нормалізація повідомлень. Нормалізація повідомлень - це додавання, видалення та заміни рядків, що призводить до узгоджених форматів, що виконує такий елемент як **S**ession **B**order **C**ontroller (надалі SBC). Під час нормалізації видаляються невідомі або нестандартні елементи повідомлень перед їхнім пересиланням. Ці елементи можуть включати заголовки, параметри заголовків і поля тіла Session Description Protocol (при використанні мережею на базі Softswitch протоколу SIP). Наприклад, SBC

надходить ненормалізоване повідомлення в якому зазначений номери абонентів в національному форматі, SBC може виконати переформатування в інтернаціональний формат або, за потреби, навпаки та взагалі приховати номер, підставивши значення Anonymous у поле From або To. При чому, не дивлячись на рекомендацію E.164 може використовуватись, як і національний, так і інтернаціональний формат номеру, залежно від призначення та налаштувань Softswitch.

Також, мережа IMS використовує динамічну маршрутизацію та інший формат адресу, і, під час виклику, для забезпечення коректної маршрутизації між мережами IMS та мережі на базі Softswitch також відбувається підміна адреси, що характерна для мережі IMS на адресу, що використовується в мережі NGN на базі Softswitch, як вказано на рис. 1:

Рис. 1. Конвертація адреси формату IMS у адресу, характерну для NGN на базі Softswitch, де NDC – код оператора, SN - номер абонента, mnc00x – ідентифікатор оператора, mcc255 – код України.

У випадку використання стеку протоколів H.323 SBC виконує конвертацію повідомлень з SIP у H.323 та навпаки. На рисунку нижче показано яким чином відбувається обмін повідомленнями між пристроями, які “розуміють” тільки або протокол SIP, або H.323 (рис.2).

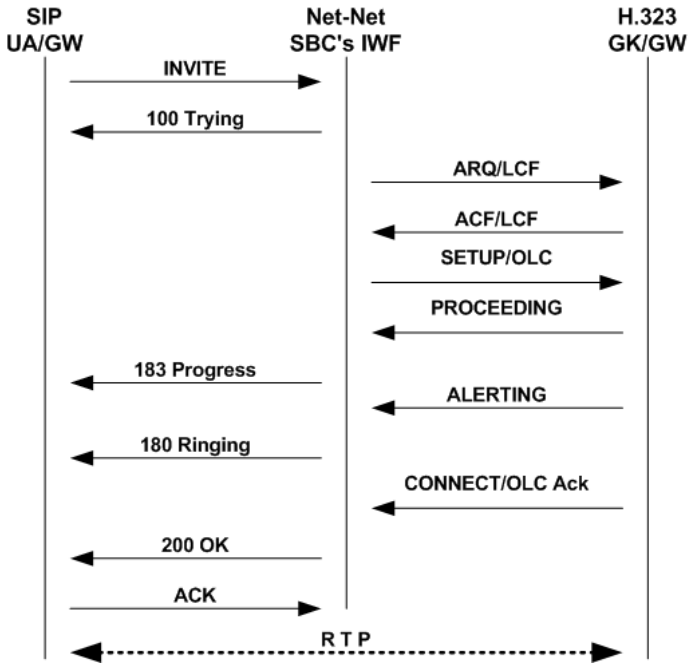


Рис.2. Обмін повідомленнями між пристроями, що використовують SIP протокол та пристроєм, що використовує стек протоколів H.323 через SBC[3].

Із рисунку видно, що відбувається конвертація повідомлень Invite в Setup, Proceeding в183 Progress, Alerting в 180 Ringing, Connect в 200 OK. Цікаво, що повідомлення 100 Trying відправляє SBC як знак, що він буде встановлювати з'єднання з іншою стороною та на даний момент не означає, що від SBC були якісь звернення до іншої сторони. Також останнє повідомлення ACK означає, що сеанс встановлено, але в стеку протоколів H.323 немає відповідника даного повідомлення, тому SBC не конвертує його. Після цього, як бачимо, сесія встановлена.

SBC також може виконувати мапінг (відповідність сигналів) для SIP та H.323, до прикладу:

Unreachable Destination (H.323) ↔ 404 Not Found (SIP)

No Permission (H.323) ↔ 401 Unauthorized (SIP)

Мапінг можливо налаштувати та модифікувати конвертацію коду причини. Це стосується не тільки протоколу H.323, а і ISUP, стеку протоколів SS7.

Висновки. Не дивлячи на стрімкий розвиток в Україні мереж нового покоління IMS, ще багато пристроїв потребують обслуговування мережею нового покоління на базі Softswitch, в цих мережах є багато відмінностей, які потрібно враховувати задля безперебійного надання послуг операторського зв'язку. Більшість з цих проблем, такі як проблеми з маршрутизацією чи повним нерозумінням пристроєм повідомлення можна вирішити нормалізацією повідомлень або повною їх конвертацією в інший протокол таким елементом мережі як SBC. Також варто зазначити, що частина нормалізації може виконуватися не тільки SBC, а і MGC, MGCF чи S-CSCF.

Література

1. С.О. Кравчук, Теорія систем мобільних інфокомунікацій. Системна архітектура: навчальний посібник для студ. спеціальності 172 «Телекомунікації та радіотехніка» – Київ : КПІ ім. Ігоря Сікорського, 2023. – 682 с.: Іл.
2. [Електронний ресурс] /«Configuring SIP Message Manipulation»– 2024. – Режим доступу: URL: <https://techdocs.audiocodes.com/session-border-controller-sbc/mp-1288/user-manual/version-740/Content/UM/Configuring%20SIP%20Message%20Manipulation.htm>.
3. [Електронний ресурс] / «SIP and H.323»– 2024. – Режим доступу: URL:<https://docs.oracle.com/en/industries/communications/session-border-controller/9.3.0/configuration/sip-and-h-323.html#GUID-6E3AC13A-400D-4ECE-A33A-405E16D81CF1>
4. [Електронний ресурс] / «SIP Number Normalization»– 2024. – Режим доступу: URL:<https://docs.oracle.com/en/industries/communications/session-border-controller/9.1.0/configuration/sip-number-normalization.html#GUID-D4FCC2E5-EA8C-40E2-9B88-05B0A795948F>

UDC 621.396.946

SCATTERING PARAMETERS OF OPTICAL FILTERS ON WHISPERING GALLERY MODE MICRORESONATORS FOR INTERLEAVERS BUILDING

Trubin A. A.
National Technical University of Ukraine "Kyiv Polytechnic Institute"
E-mail: atrubin9@gmail.com

ПАРАМЕТРИ РОЗСІЮВАННЯ ОПТИЧНИХ ФІЛЬТРІВ НА МІКРОРЕЗОНАТОРАХ З КОЛИВАННЯМИ ШЕПОЧУЧЕЙ ГАЛЕРЕЇ ДЛЯ ПОБУДОВИ ІНТЕРЛІВЕРІВ

Вперше розглядуються характеристики розсіювання відомих оптичних фільтрів, побудованих на Діелектричних Резонаторах (ДР) з коливаннями шепочучей галереї з урахуванням вищих та нижчих смуг частот, обумовлених іншими коливаннями резонаторів.

Досліджуються вплив різних коливань резонаторів на параметри розсіювання фільтрів з багато смуговими характеристиками. Отримані закономірності добре узгоджуються з результатами інших публікацій, отриманих на основі застосування чисельних методів та експериментальних досліджень. Представлені методики є основою для моделювання і побудови широкого класу інтерліверів сучасних систем оптичного зв'язку.

Dielectric microresonators with whispering gallery modes (WGM) have a quasi-periodic frequency spectrum, which makes them convenient for use in interleavers optical wavelength ranges. [1 - 15].

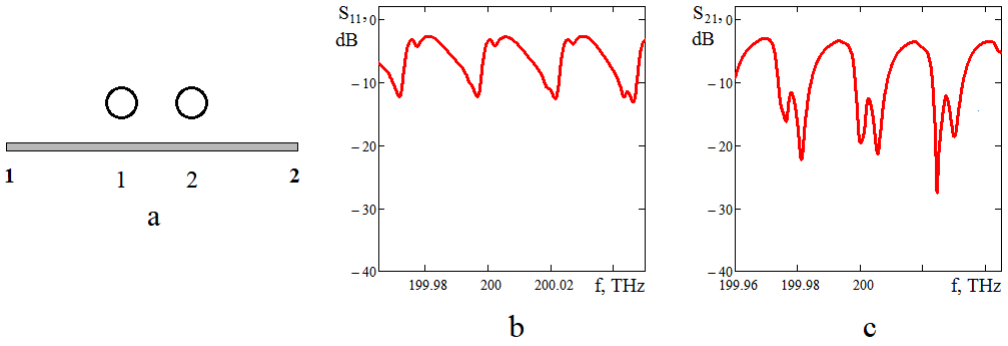


Fig. 1. Scattering characteristics (b - e) of two DR in a transmission line (a) calculated for seven oscillations of degenerate WGM: $f_0 = 200\,\text{THz}$; $FSR = 25\,\text{GHz}$; DR coupling coefficients with a transmission line: for even mode: $\tilde{k}_s^e = 3\cdot10^{-5}$; for odd mode: $\tilde{k}_s^o = 5\cdot10^{-6}$; coupling coefficients of the DRs with open space: $\tilde{k} = 10^{-7}$; mutual coupling coefficients between DRs: for even mode: $k_{12}^e = -6{,}5\cdot10^{-5}$; for odd mode: $k_{12}^o = 2\cdot10^{-5}$; dielectric loss Q-factor $\text{Q}^{\text{D}} = 10^5$.

Relative distance between resonators $\Gamma\Delta z_{1,2} = 31\pi/2$ (Γ is a waveguide wave number).

This paper presents new results of modeling the scattering characteristics of transmission line waves on DRs with WGM built on the basis of previously conducted theoretical studies [16 - 17]. For the first time, S-matrices of notch (Fig. 1) and different Add/Drop (Fig. 2, 3) filters are investigated taking into account several types of oscillations.

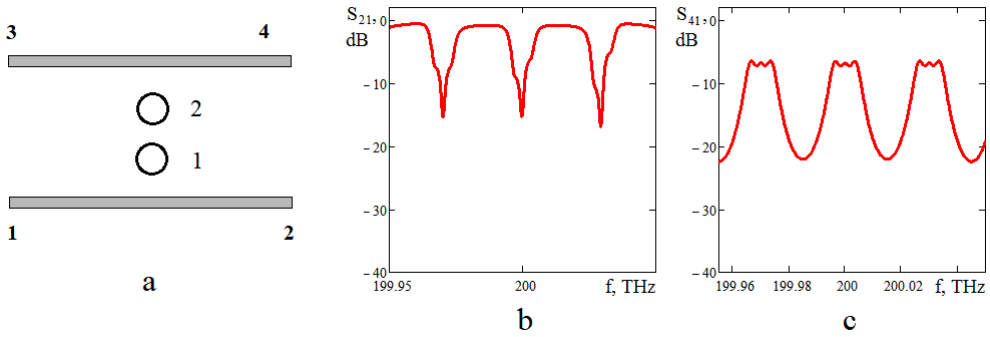


Fig. 2. Scattering characteristics (b - f) of two DR Add/Drop Filter (a) calculated for seven oscillations of degenerate WGM: $f_0 = 200\,\text{THz}$; $FSR = 25\,\text{GHz}$; DR coupling coefficients with a transmission line: for even mode: $\tilde{k}_s^e = 2\cdot10^{-5}$; for odd mode: $\tilde{k}_s^o = 2\cdot10^{-5}$; with open space: $\tilde{k} = 10^{-7}$; coupling coefficients between DRs: for even mode: $k_{12}^e = 4\cdot10^{-5}$; for odd mode: $k_{12}^o = -2\cdot10^{-6}$; dielectric loss Q-factor $\text{Q}^\text{D} = 10^6$.

For the ferst time showed the possibility of constructing electrodynamics models of filters with periodic scattering characteristics.

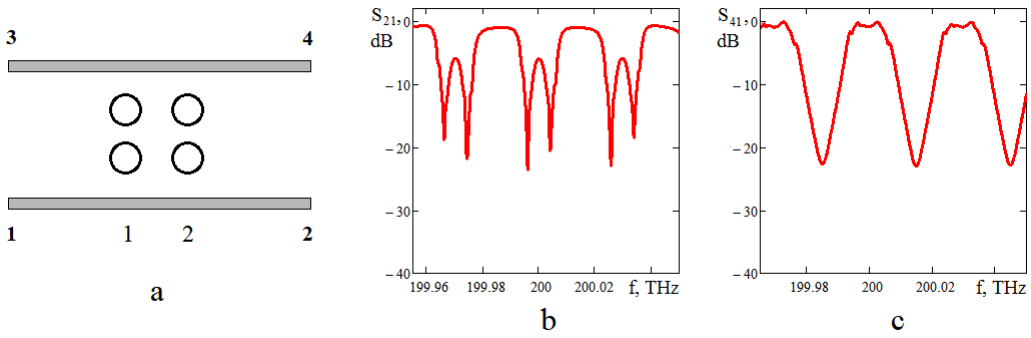


Fig. 3. Scattering characteristics (b - e) of 4 DR Twisted double-channel SCISSOR (a) calculated for seven oscillations of degenerate WGM: $f_0 = 200\,\text{THz}$; $FSR = 30\,\text{GHz}$; DR coupling coefficients with a transmission line: for even mode: $\tilde{k}_s^e = 1,2\cdot10^{-5}$; for odd mode: $\tilde{k}_s^o = 1,2\cdot10^{-5}$; coupling coefficients of the DRs with open space: $\tilde{k} = 10^{-8}$; coupling coefficients between DRs: for even mode: $k_{12}^e = 1\cdot10^{-6}$; for odd mode: $k_{12}^o = -1\cdot10^{-6}$; coupling coefficients between "vertically-coupled" DRs: for even mode: $k_{12}^{eV} = 6\cdot10^{-5}$; for odd mode: $k_{12}^{oV} = -3,5\cdot10^{-5}$; dielectric loss Q-factor $\text{Q}^\text{D} = 10^6$.

Presented electrodynamics' model allows to significantly accelerate the design

and optimization of scattering characteristics of modern optical communication systems using interleavers in technology WDM.

References

1. S. A. Alboon, J. M. H. Barakat, A. S. Karar. Angle-tuned optical interleaver based on Fabry–Perot cavities with reconfigurable angle range // Results in Optics. 2024. 16. 100722. pp. 1 – 6.
2. N. Saha, G. Brunetti, A. di Toma, M. N. Armenise, C. Ciminelli. Silicon Photonic Filters: A Pathway from Basics to Applications // Review. Adv. Photonics Res. 2024, 2300343. PP. 1 – 44.
3. D. R. Arrieta et al., "Proof-of-Concept Real-Time Implementation of Interleavers for Optical Satellite Links," in Journal of Lightwave Technology, 2023, Vol. 41, No. 12, pp. 3932-3942.
4. Q. Li, H. Zhu, H. Zhang, H. Hu. Electro-optical tunable interleaver in hybrid silicon and lithium niobate thin films // Optics Express. Vol. 31, No. 15 / 17 Jul, 2023, pp. 24203 – 24212.
5. W. Qin, J. Liu, H.-L. Zhang, W.-W. Yang, J.-X. Chen. Bandpass Filter and Diplexer Based on Dual-Mode Dielectric Filled Waveguide Resonators // IEEE Access. V. 10, 2022. PP. 29333 – 29340.
6. A. Wldaa, M. Hoft. Miniaturized Dual-Band Dual-Mode TM-Mode // Dielectric Filter in Planar Configuration // IEEE Jornal of Microwaves. Vol. 2, No. 2, April 2022. PP. 326 – 336.
7. H. Gevorgyan, K. A. Qubaisi, M. S. Dahlem, A. Khilo. Silicon photonic time-wavelength pulse interleaver for photonic analog-to-digital converters // Optics Express. 2016 . Vol. 24, No. 12,. pp. 13489 – 13499.
8. C. Chen, X. Niu, C. Han, Z. Shi, X. Wang, X. Sun, F. Wang, Z. Cui, D. Zhang. Reconfigurable optical interleaver modules with tunable wavelength transfer matrix function using polymer photonics lightwave circuits // Optics Express. 2014. Vol. 22, No. 17, pp. 19895 – 19911.
9. D. Dai, J. E. Bowers. Silicon-based on-chip multiplexing technologies and devices for Peta-bit optical interconnects (Review article) // De Gruyter. Nanophotonics 2014; No. 3(4-5), pp. 283–311.
10. L. Zhuang, W. Beeker, A. Leinse, R. Heideman, P. van Dijk, C. Roeloffzen 1. Novel wideband microwave polarization network using a fully-reconfigurable photonic waveguide interleaver with a two-ring resonatorassisted asymmetric Mach-Zehnder structure // Optics Express. Vol. 21, No. 3, 2013, pp. 3114 – 3124.
11. L.W. Luo, S. Ibrahim, A. Nitkowski, Z. Ding, C. B. Poitras, S. J. Ben Yoo, M. Lipson. High bandwidth on-chip silicon photonic interleaver // Optics Express. 2010. Vol. 18, No. 22, pp. 23079 – 23087.
12. S. A. Alboon, A. S. Abu-Abed, R. G. Lindquist, H. R. Al-Zoubi H. R. Al-Zoubi. Novel Liquid Crystal Tunable Flat-Top Optical Interleaver // Progress In Electromagnetics Research B, Vol. 19, 2010, pp. 263 – 283.
13. J. Song, H. Zhao, Q. Fang, S. H. Tao, T. Y. Liow, M. B. Yu1, G. Q. Lo1, D. L. Kwong. Effective thermo-optical enhanced cross-ring resonator MZI interleavers on SOI // Optics Express. Vol. 16, No. 26. 2008, pp. 21476 – 21482.
14. J. Song, Q. Fang, S. H. Tao, M. B. Yu, G. Q. Lo, D. L. Kwong. Proposed silicon wire interleaver structure // Optics Express. 2008. Vol. 16, No. 11. PP. 7849 – 7859.
15. R.M. de Ridder, C.G.H. Roeloffzen, “Interleavers”, in Wavelength Filters for Fibre Optics, ed. by H. Venghaus, Springer Series in Optical Sciences, 2006. Vol. 123, pp. 381- 432.
16. A.A. Trubin. Electrodynamic modeling of Add-drop filters on optical microresonators // Information and Telecommunication Sciences, V.1, N1, 2019, pp. 30 - 36.
17. A.A. Trubin. Scattering of electromagnetic waves by frequency-detuned systems of dielectric resonators // Visnyk NTUU KPI Seriia - Radiotekhnika Radioaparatobuduvannia. 2024. Iss.96. PP. 5 – 13.

UDC 621.396.946

OPTICAL ANTENNAS-FILTERS ON DIFFERENT SPHERICAL MICRORESONATORS FOR USE IN ACCESS POINTS

Trubin A. A.
National Technical University of Ukraine "Kyiv Polytechnic Institute"
E-mail: atrubin9@gmail.com

ОПТИЧНІ АНТЕНИ-ФІЛЬТРИ НА РІЗНИХ ТИПАХ СФЕРИЧНИХ МІКРОРЕЗОНАТОРІВ ДЛЯ ВИКОРИСТАННЯ В ТОЧКАХ ДОСТУПУ

Пропонується новий тип оптичних антен, побудованих на декількох підрешітках Діелектричних Резонаторів (ДР) різних видів. Показано, що запропоновані антени дозволяють вирішити актуальні завдання розширювання частотних смуг.

Встановлено, що антени на різних підрешітках ДР можуть робити в декількох режимах, кожний із яких характеризується збудженням заданої підсистеми резонаторів. Це додатково дозволяє керувати діаграмою спрямованості. Показано також, що вибір параметрів - типів коливань, а також числа резонаторів, дозволяє ефективно розширяти смугу пропускання антени.

Вперше розглядуються характеристики розсіювання та діаграми спрямованості антен-фільтрів, одночасно побудованих на Діелектричних Резонаторах з коливаннями шепочучей галереї, та на резонаторах з основними типами власних коливань.

Представлені результати є основою для подальшого моделювання і оптимізації широкого класу антен для побудови точок доступу сучасних систем оптичного зв'язку та Інтернету речей.

In works [1 - 3] a new class of microwave antennas was investigated for simultaneously performing the functions of spatial distribution of the radiation field and at the same time frequency filtering. The obtained results and design principles cannot be transferred to shorter-wave – infrared, optical frequency ranges due to the known shortcomings of physical materials. In this paper a new principle of the antenna-filters design in the optical range, based on usage of coupled sublattices of different types microresonators is proposed. A new kind of the antenna, containing several different lattices of dielectric resonators is proposed. In this case one of the sublattices consists of microresonators with whispering gallery oscillations (WGM), this sub lattice forms frequency band of the antenna. The second sub lattice consists of microresonators with lower modes and forms the spatial distribution of the radiation field in the wave zone.

The main difficulty in calculating such antennas lies in the very high degree of degeneration of the higher types of natural oscillations of the DRs. As an example, the results of modeling a new linear optical antenna [3 – 6] built on two types of spherical microresonators are given. (Fig. 1, a).

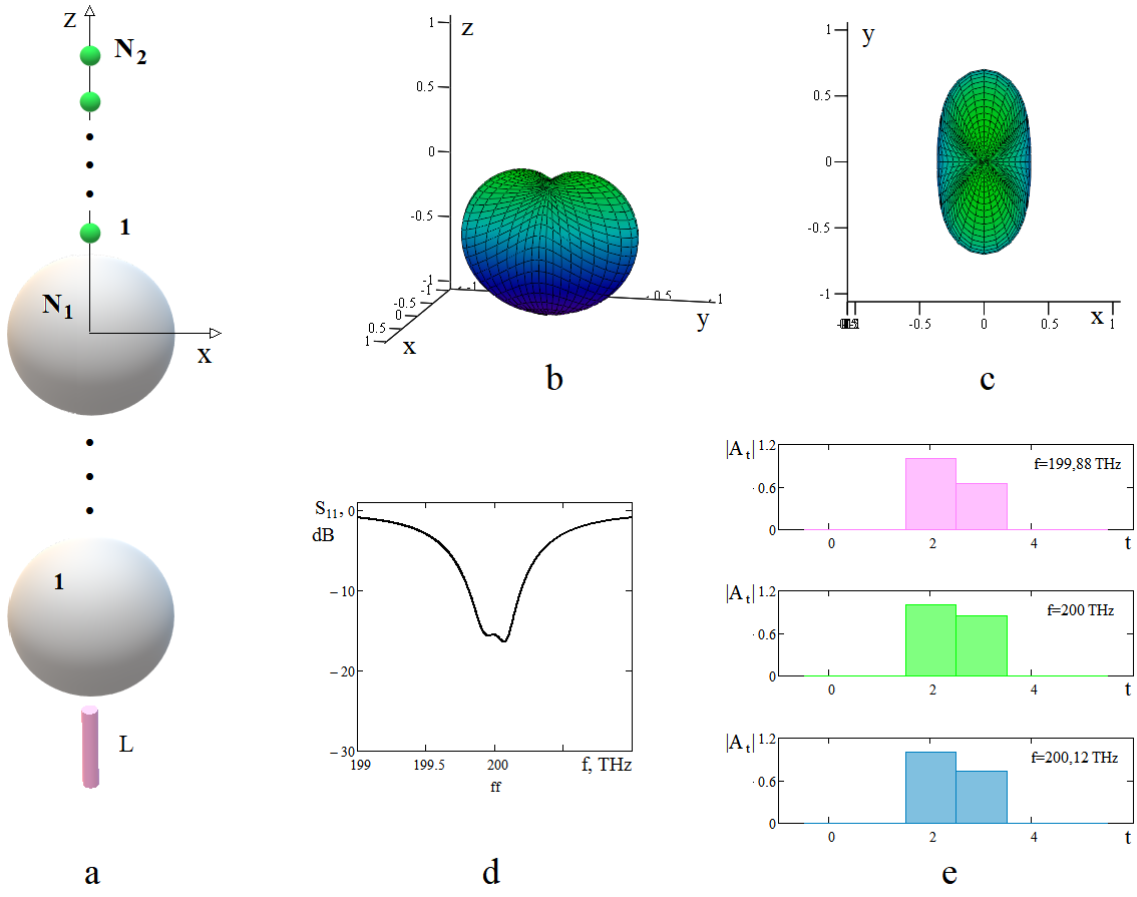


Fig. 1. One-dimensional dielectric antenna (b - e) made on two sublattices of spherical DR: with WGM oscillations $H_{25,1,1}$ $(1,2,...,N_1)$; and DR with $H_{1,1,1}$ oscillations $(1,2,...,N_2)$. Radiation characteristics of a 6-cavity antenna ($N_1 = 2$; $N_2 = 4$) $f_0 = 200$ THz; 1 DR coupling coefficients with a transmission line L: $\tilde{k}_L = 4,5 \cdot 10^{-3}$; permittivity of resonators $\varepsilon_{1r} = 2,25$; dielectric loss Q-factor of 1 sublattices resonators: $Q_1^D = 10^7$; dielectric loss Q-factor of 2 sublattices resonators: $\varepsilon_{2r} = 25$; dielectric loss Q-factor $Q_2^D = 10^3$. Relative distance between 2 sublattices resonators $k_0 \Delta z_{1,2} = \pi / 2$; Antenna Directivity Diagram (b, c); input reflection coefficient frequency response (d); amplitude modules of forced oscillations of the DR lattice at different frequencies of the operating band (e) ($t = 0,1,..., N_1 + N_2 - 1$).

The conducted studies have shown that in the sublattices of various DRs, conditions can be created under which the coupling element of the antenna with the transmission line effectively excites only the oscillations of the low-Q microresonators of the sublattice (Fig. 1, e; Fig. 2, d). At that, the lattice consisting from high-Q DRs, forms the antenna bandwidth (Fig. 1, d; Fig. 2, c).

At the same time, it has also been shown that changing one or several of the antenna parameters, for example frequency, in some cases can lead to a significant restructuring of its radiation pattern. (Fig. 2, a, b). The restructuring of the antenna's directional pattern is caused by a partial redistribution of the amplitudes of the field of the coupled oscillations of the "radiating" sublattice (Fig. 2, d).

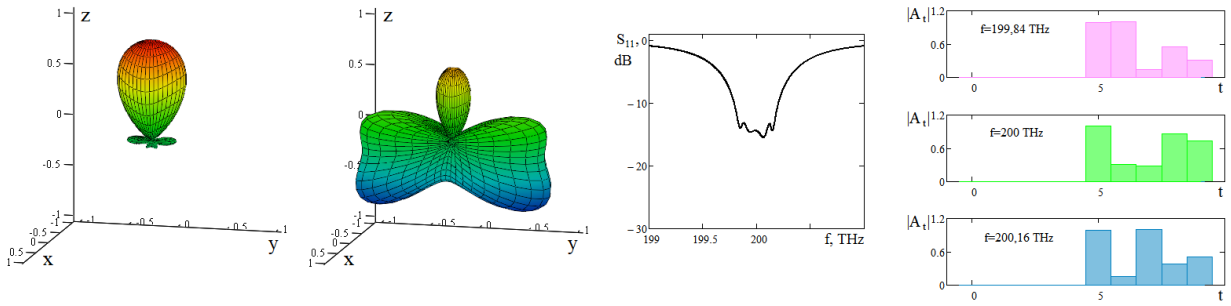


Fig. 2. Radiation characteristics of a one-dimensional 10-resonator dielectric antenna (Fig. 1, a: $N_1 = 5; N_2 = 5$) (the parameters of the resonators and antenna are the same as on Fig.1) Antenna Directivity Diagram (a, b); input reflection coefficient frequency response (c); amplitude modules of forced oscillations of the DR lattice at different frequencies (d) ($t = 0,1,..., N_1 + N_2 - 1$).

The obtained research results demonstrate the possibility of constructing a new class of dielectric antenna-filters in the optical wavelength range, performed on the basis of application of sublattices build on different microresonators, characterized by a controlled frequency band and directional characteristics. Presented results are the basis for further modeling and optimization of a wide class of antennas for building access points of modern optical communication systems, as well as IOT.

References

1. R. H. Mahmud, I. H. Salih, X. Shang, T. Skaik, Y. Wang. A filtering waveguide aperture antenna based on all-resonator structures // Microw. Opt. Technol. Lett. 2023; 65. PP. 2378–2383. doi:10.1002/mop.33706doi:10.1002/mop.33706
2. A.A. Trubin. Study of integrated antennas-filters on dielectric resonators // Bulletin of NTUU "KPI" ser. Radiotechnique, Radioaparatus Building. 2019. No 77, pp. 36-41.
3. Lim E.H., Leung K.W. Use of the Dielectric Resonator Antenna as a Filter Element // IEEE Trans. on Antennas and Propagation. – 2008. - Vol. 56. -No. 1. – PP. 5 – 10.
4. A.A. Trubin. Mutual coupling coefficients basic and higher modes of spherical dielectric resonators // Modern Challenges in Telecommunications. 18 Int. Sci. Techn. Conf. 2024". PP. 97-99.
5. A.A. Trubin. Coupling coefficients of the Spherical dielectric microresonators with whispering gallery modes // Visnyk NTUU KPI Seriia - Radiotekhnika Radioaparatobuduvannia. 2015. Iss. 26. PP. 49 – 61.
6. A.A. Trubin. Coupling coefficients of different Spherical Dielectric Microresonators // Information and Telecommunication Sciences, 2018, V. 9, No 1, pp. 49-56.

УДК 621.395

МЕТОДИ TRAFFIC ENGINEERING В SDN МЕРЕЖАХ ДАТА-ЦЕНТРІВ ДЛЯ ОПТИМІЗАЦІЇ ВИКОРИСТАННЯ МЕРЕЖЕВИХ РЕСУРСІВ

Романов О.І, Нестеренко М.М, Марінов А. І.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: a_i_romanov@ukr.net, nikolaiy.nesterenko@gmail.com, marinov.anton99@gmail.com.

METHODS FOR OPTIMIZING NETWORK RESOURCE UTILIZATION IN DATA CENTER SDN NETWORKS BY TRAFFIC ENGINEERING

The study provides a comparative analysis of modern Traffic Engineering (TE) methods in Software-Defined Networks (SDN). Analyzed key approaches, such as ECMP with hashing, Min-Max Fairness, the Epstein algorithm, and load-balancing methods focused on managing elephant and mice flows. Also has been reviewed efficiency of SDN in dynamically managing traffic and adapting to real-time changes. By the results of analysis claimed that the combination of TE and SDN significantly improves network performance, reduces latency, and optimizes resource utilization.

Сучасний розвиток мереж та додатків, особливо в мережах дата-центрів, вимагає гнучкості у їх розгортанні для забезпечення належної якості обслуговування (QoS) та ефективної обробки трафіку. Дата-центри оперують великими обсягами даних та високошвидкісними потоками, що потребує динамічного управління трафіком та оптимального використання ресурсів. Традиційні методи маршрутизації часто є статичними та не забезпечують ефективної адаптації до змін у навантаженні, що особливо критично для масштабованих інфраструктур. Інженерія трафіку (Traffic Engineering, TE) допомагає вирішити ці проблеми шляхом аналізу мережевого стану, балансування навантаження та адаптивної маршрутизації. Впровадження SDN-моделі стало ключовим кроком у розвитку TE, оскільки дозволяє централізовано керувати мережею дата-центрів, автоматизувати адаптацію до змін у трафіку та застосовувати політики маршрутизації для підвищення продуктивності та зниження експлуатаційних витрат.

Наразі найбільш ефективні та популярні методи TE у SDN базуються на задіянні технології SDN, та її поєднання або з механізмом маршрутизації Equal Cost Multi-Path (ECMP routing), або з алгоритмом Min-Max Fairness [1], або з алгоритмом оптимізації розподілу мережевих ресурсів Еппштейна [3].

Рішення, яке використовує у своїй реалізації підхід з залученням Min-Max Fairness та ECMP є B4 від Google [4], де розгорнуто приватну SDN для з'єднання своїх центрів обробки даних по всьому світу. Увесь обчислювальний процес мережі знаходиться у централізованому сервері керування трафіком і виконується за допомогою програмно-релізованих додатків. Розгортання SDN технології тут дозволило швидко розгортати нові або стандартні протоколів, та функцій управління ресурсами. Однією з таких впроваджених функцій є ECMP з хешуванням, яке дозволяє мережі адаптувати пропускну здатність на користь ефективного використання усіх доступних шляхів між вузлами без перевантаження одного з них, що в рази

зменшує ймовірність перевантаження каналів зв’язку і призводить до зменшення затримок при передачі трафіку.

Хеш-функція у ECMP відповідає за передачу усіх пакетів одного потоку через однаковий маршрут, що запобігає проблемам зі змішуванням пакетів. Алгоритм Min-Max Fairness використовується для балансування ресурсів, враховуючи поточне завантаження мережі, що дозволяє вирішити проблему з несправедливим виділенням ресурсів тому чи іншому сервісу. За алгоритмом, спочатку виділяється мінімальна пропускна здатність для кожного потоку (гарантований рівень кожного сервісу, Min), після чого система оцінює залишкові ресурси та розподіляє їх між найбільш навантаженими потоками, щоб максимально використовувати доступну ємність мережі (Max). У разі виходу з ладу частини мережі чи її компонентів, застосовується класифікація трафіку та пріоритезація, де трафік ділиться на критичний (наприклад, запити до Google Search) та некритичний (резервне копіювання даних між дата-центрами), тоді система автоматично знижує пропускну здатність для некритичного трафіку, щоб забезпечити безвідмовну роботу важливих сервісів, але в цей же час глобальний SDN-контролер, який моніторить стан мережі, в режимі реального часу обчислює і перенаправляє більш пріоритетний трафіку через доступні маршрути (некритичні задачі будуть затримані, але не припинятимуть роботу).

MSDN-TE (Multipath Software-Defined Networking Traffic Engineering) [2], який використовує багатошляхову маршрутизацію для оптимізації використання мережевих ресурсів та підвищення продуктивності мережі, в свою чергу, використовує підхід SDN з використанням алгоритму Еппштейну. Підхід базується на використанні декількох шляхів для пересилання потоків з урахуванням фактичного навантаження на них при прийнятті рішень про пересилання, та ґрунтується на обчисленні k-шляхів, доступних для пересилання потоків між будь-якою парою Source-Destination (S-D), і виборі найменш завантаженого шляху для обробки вхідного потоку. На меті у MSDN-TE стоїть запобігання створення перевантажених точок в мережі.

Алгоритм Еппштейна дозволяє створити метод оптимізації розподілу ресурсів, який балансуватиме навантаження між каналами у мережі. Алгоритм функціонує по принципу: збору мережевих метрик, де визначаються всі можливі шляхи передачі між джерелом і призначенням (S-D), і збираються дані про мережеві параметри: затримки, поточне завантаження каналів зв’язку; обчисленню ваги кожного шляху за допомогою функції:

$$W(P) = \alpha \times delay + \beta \times loss + \gamma \times utilization, \qquad (1)$$

де: *delay* – затримка; *loss* – втрата пакетів; *utilization* – завантаження каналу; коефіцієнти α, β, γ визначають вагу (weigh) кожної метрики.

Наступним кроком йде вибір найоптимальнішого шляху, по якому далі потоку присвоюється шлях передачі з найменшим значенням *W(P)*. Останнім кроком йде процес динамічного коригування, де при зміні мережевого стану (збільшення завантаженості, відмова каналів зв’язку) алгоритм перераховує параметр ваги шляху (*W(P)*) та адаптує маршрутизацію під стан мережі.

Якщо розглядати принцип роботи MSDN-TE, то матимемо такі кроки: коли до мережі надходить новий потік, він перевіряється на існування присвоєного шляху передачі для даного потоку (якщо *k*-шляху між S-D не існує – створюється і прописується такий маршрут/шлях); обчислюється вартість (вага) усіх шляхів (*W(P)*) за певними метриками у *k*-шляхах, передача потоку призначається шляху з найнижчою вартістю (з найменшим *W(P)*); зчитується загальна статистика мережі (навантаження, затримки) та порівнюється з попередньо розрахованими значеннями; фіксується споживання ресурсів користувачами (агрегована пропускна здатність користувачів); всі метрики каналів оновлюються (бітрейт, відсоток втрат, вартість); відбувається перехід до етапу 3 (або ж до етапу 1, якщо виявлено новий вхідний потік).

Також існують методи (DevoFlow, Hedera, MiceTrap), що мають за основу розподіл трафіка на великі (elephant-flows) та малі потоки (mice-flows), а також спеціальну їх обробку. Перші фокусуються на виявленні великих потоків (які можуть без обробки суттєва навантажувати мережу), з подальшою їх маршрутизацією оптимальними шляхами. Тоді як другі зосереджені на малих потоках, що становлять до 90% усього трафіку, використовуючи алгоритми зваженої маршрутизації для рівномірного розподілу навантаження у мережі.

Досліджено поєднання ECMP та Min-Max Fairness у технології B4, що забезпечує збалансоване навантаження між маршрутами мережі різних дата-центрів. Особливу увагу варто зосередити на застосуванні методів TE як при обслуговуванні “elephant”, так і “mice” потоків з метою оптимізації використання мережевих ресурсів і зменшення ймовірності появи перевантажень в мережі. Визначено, що гібридні підходи, які поєднують SDN та сучасні методи TE, забезпечують високу якість обслуговування (QoS), масштабованість та гнучкість сучасних мереж дата-центрів.

Література

1. Abbasi, M., Guleria, A., Devi, M.: Traffic engineering in software defined networks:A survey. Journal of Telecommunications and Information Technology 4, 3–14(2016), DOI:10.26636/jtit.2016.4.757.
2. K. T. Dinh, S. Kukli´nski, W. Kujawa, and M. Ulaski, “MSDN-TE:Multipath Based Traffic Engineering for SDN,” in Asian Conferenceon Intelligent Information and Database Systems. Springer, 2016, pp.630–639. DOI:10.1007/978-3-662-49390-8_61.
3. D. Eppstein, “Finding the k-shortest paths”, SIAM J. Comput., vol. 28, pp. 652–673. 1999. DOI:10.1109/SFCS.1994.365697.
4. S. Jain et al., “B4: Experience with a globally-deployed software defined WAN”, ACM SIGCOMM Comp. Commun. Rev., vol. 43, no. 4, pp. 3–14, 2013. DOI:10.1145/2534169.2486019.
5. Romanov, O., Siemens, E., Nesterenko, M., Mankivskyi, V. Mathematical description of control problems in SDN networks/Proceedings of International Conference on Applied Innovation in IT, 2021, 9(1), pp. 33–39, http://dx.doi.org/10.25673/36582
6. Romanov, O., Nesterenko, M., Boggia, G., Striccoli, D. Construction and Methods for Solving Problems at the SDN Control Level // Lecture Notes in Electrical Engineering,t2023, 965 LNEE, pp. 85–101, https://link.springer.com/chapter/10.1007/978-3-031-24963-1_6

УДК 621.395

ПРОГНОЗУВАННЯ СПОТВОРЕНИХ СИГНАЛІВ ВІД LED ЛАМП В СИСТЕМАХ ПОЗИЦІОНУВАННЯ ВСЕРЕДИНІ ПРИМІЩЕНЬ

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

FORECASTING DISTORTED SIGNALS FROM LED LAMPS IN INDOOR POSITIONING SYSTEMS.

The paper analyses the possibility of forecasting distorted signals from LED transmitting lamps used as signal transmitters in indoor positioning systems. It is shown that using the 'fingerprint' method, it is possible to determine which lamps in a Li-Fi network are distorted.

Сьогодні позиціонування всередині приміщень широко використовується у різних галузях сучасних досліджень. Внутрішнє позиціонування зараз все більше і більше використовують для взаємодії між роботами та різними автоматизованими об'єктами. Ці проблеми особливо актуальні в Інтернеті речей (IoT), враховуючи швидке зростання IoT у «розумних» містах, «розумних» мережах та «розумних» медичних закладах.

На даний час для вирішення такої задачі в основному використовуються радіотехнології, такі як Wi-Fi, Bluetooth, ZigBee, або навіть GPS, який призначений, в основному, для зовнішнього використання. Основними недоліками цих методів є те, що вони мають малу точність, не можуть використовуватися там, де є обмеження на застосування радіохвиль (наприклад в лікарнях) і , крім того, вже відчувається нестача в радіочастотному (РЧ) спектрі.

Тому зараз почали використовувати видиме світло (VLC), як інноваційне рішення для бездротової передачі даних. На базі VLC зараз будують мережі Li-Fi, які мають ряд переваг у порівнянні з радіотехнологіями тим, що видиме світло має в 10 000 разів більший діапазон частот[1], може використовувати для передавання даних світлодіодні LED лампи, які є частиною готової інфраструктури освітлення, і одночасно на цій базі можливе здійснити рішення задач визначення місцеположення об'єктів усередині приміщення [2,3].

Розглянемо структуру системи на базі VLC, яка дозволяє вирішити задачу позиціонування. Зазвичай в приміщеннях розташовано декілька LED ламп, і всі ці лампи можна використовувати для передавання інформації і визначення місцеположення об'єкта (рис 1) [4,5].

Дослідження полягає в розробці алгоритму для визначення LED ламп, від яких приймач користувача отримує спотворені сигнали. Вирішення цієї задачі дозволяє значно підвищити точність визначення координат користувача, коли система позиціонування працює в умовах наявності

завад.[6]

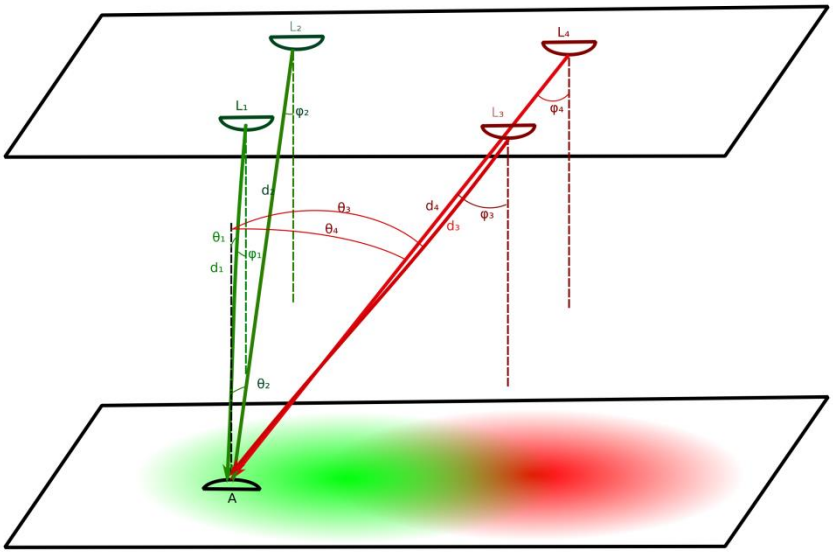


Рис.1. модель системи позиціонування на базі мережі Li-Fi.

На рис.1 представлено модель системи позиціонування на базі мережі Li-Fi та її основні елементи. Передавачі в системі представлені у вигляді світлодіодних LED ламп { L_1, L_2, L_3,L_4}. Причому лампи, від яких користувач отримує неспотворені сигнали, мають зелені кольори { L_1, L_2}, а лампи, від яких користувач отримує спотворені сигнали, мають червоні кольори { L_3,L_4}. Крім того, на рис.1 показані кути передавання і приймання світлових сигналів в мережі Li-Fi. Вони дозволяють розрахувати загасання світлових сигналів в процесі його переміщення від передавача до приймача.[7]

Для рішення задачі позиціонування в даній роботі використовується метод «відбитки пальців». Запропоновано наступний алгоритм визначення LED ламп, від яких приймаються неспотворені сигнали:

Шаг 1. Оператор A1-розрахунок різниці прийнятого сигналу об'єктом та еталонним сигналом в базі даних для кожної точки. Позначення на рис.2: $M_{fingerprint}$ –матриця відбитків пальців, в якій міститься інформація о потужності сигналів в опорних точках; M_{user} – прийняті значення потужності сигналів від різних ламп, M_{diff} - різниця між потужністю прийнятих сигналів користувачем та в опорних точках.

Шаг 2. Оператор A2-фільтрація різниці прийнятої потужності та потужності в базі даних; filter – функція яка визначає де може знаходитись об'єкт.

Шаг 3. Оператор A3-групування ламп, де group ($M_{filtred}$) by (x,y) означає що після фільтрації всі лампи групуються за спільними координатами.

Шаг 4. Оператор A4-обрахунок середньоквадратичного значення потужності для кожної пари LED ламп.

Шаг 5. Оператор A5-визначення найменшого середньоквадратичного значення помилки $\min(M_{RSM})$.

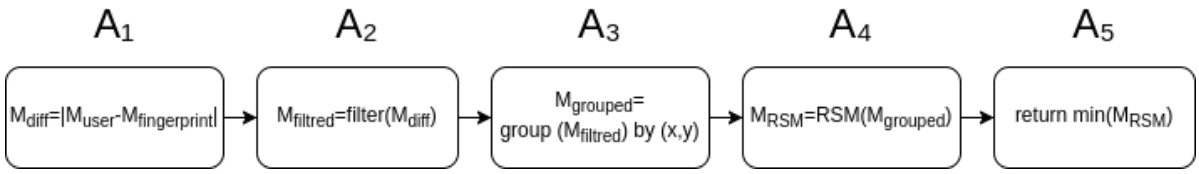


Рис.2. Алгоритм визначення LED ламп, від яких приймаються неспотворені сигнал.

Для перевірки алгоритму було проведено моделювання, яке показало що правильне визначення ламп, від яких сигнал є неспотвореним складає 97%.

Висновки. У роботі розглянуто систему позиціонування всередині приміщення, яка працює в умовах завад. Запропоновано алгоритм, який дає змогу з високим ступенем імовірності визначати LED лампи, сигнали від яких приймається без завад. Це дає можливість підвищити точність розв'язання задач позиціонування всередині приміщень в умовах завад.

Література

1. IEEE, “IEEE Approved Draft Standard for Information Technology– Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks–Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 7: Light Communications,” IEEE P802.11bb/D7.0, March 2023, pp. 1–29, 2023.
2. Petrosino A., Striccoli, D., Romanov, O., Boggia, G., Grieco, L.A. Fidelity for Internet of Things: A survey/ Optical Switching and Networking, Volume 48, March 2023, 100732, https://doi.org/10.1016/j.osn.2023.100732
3. V. P. Rekkas et al., "Artificial Intelligence in Visible Light Positioning for Indoor IoT: A Methodological Review," in IEEE Open Journal of the Communications Society, vol. 4, pp. 2838-2869, 2023, doi: 10.1109/OJCOMS.2023.3327211.
4. Романов О., Бурлака Г., Берестовенко О., Підпалий 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.
5. Romanov, O., Dong, T.T., Nesterenko, M. The possibilities for deployment eco-friendly indoor wireless networks based on LiFi technology/Proceedings of International Conference on Applied Innovation in IT, 2020, 8(1), стр. 41–48
6. Romanov, O.I., Fediushyna, D.M., Dong, T.T. Model and method of Li-Fi network calculation with multipath light signals/2018 International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2018 - Proceeding, 2018, 9047550
7. 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 - Proceedings, 2017, 8095404

УДК 520.6

СИНТЕЗ ЗОБРАЖЕННЯ ЗОРЯНОГО НЕБА ДЛЯ НАЛАШТУВАННЯ ДЕТЕКТОРА ЗІРОК

Іванов С.В., Олійник П.Б.
Навчально-науковий інститут телекомунікацій
Державний університет інформаційно-комунікаційних технологій, Україна
E-mail: ivanov.sergiyvik@gmail.com

STARRY SKY IMAGE SYNTHESIS FOR STAR DETECTOR SETUP

An algorithm for image synthesis for a starry sky simulator suitable for use in debugging and simulation tests of J, H and K-band IR star detector is considered. In the algorithm proposed, image is synthesized while taking temperature, radiation spectrum and magnitude of stars, light dispersion, and image blurring into account. Algorithm also allows one to take star detector resolution and spectral sensitivity into account. Modeling of the algorithm operation is done and starry sky images are formed using MATLAB.

Важливим елементом сучасних навігаційних систем є астровізор, який стабілізується системою на основі волоконно-оптичних гіроскопів. Для налагодження та випробування астровізорів, телескопів та ін. використовують імітатори зоряного неба – пристрої, які створюють зображення неба з урахуванням фізичних законів випромінювання, поглинання та розсіювання світла. З точки зору всепогодної навігації важливим є створення імітаторів для інфрачервоного (ІЧ) діапазону, оскільки атмосфера прозора для ІЧ випромінювання в певних діапазонах частот (J, H, K -band).

Класичний підхід до формування імітатора зоряного неба – створення моделей зірок на сфері за допомогою світлодіодів, і встановлення астровізора всередині сфери на механічному поворотному столі [1]. Такий імітатор не дозволяє імітувати шуми в зображенні та вплив атмосфери, тому в сучасних імітаторах зоряного неба застосовують комп'ютерний синтез зображень на основі використання зоряних каталогів, наприклад 2MASS (Two Micron All-Sky Survey) [2] та Gaia (Global Astrometric Interferometer for Astrophysics) [3].

В роботі [4] проведено симуляцію зображення зоряного неба, оцінено відношення сигнал-шум та вплив на зображення руху та вібрації об'єкту. Недоліком дослідження [4] є те, що в ньому використано лише діапазон J-band.

Автори [5] використали при моделюванні зображення зоряного неба індекс кольору зірки і теорію випромінювання чорного тіла; згідно [5] точність моделювання інтенсивності випромінювання підвищилася на 5..15%, однак модель не враховує вплив руху платформи астровізора і вібрації.

У роботі [6] представлено симулятор зоряного неба та платформу для верифікації астровізорів, які дозволяють моделювати зоряне небо; недолік – вплив вібрації та температурні ефекти в [6] не проаналізовано.

В [7] запропоновано алгоритм симуляції зоряного неба, котрий враховує моделі деградації точок, що представляють зірки, модель шуму зображення, і модель нерівномірного освітлення та збурень положення астровізора. Моделювання показало подібність з реальними зображеннями, однак модель не враховує накладання зображень зірок; також необхідно провести детальний аналіз шумів зображення.

В роботі [8] проведено аналіз впливу на зображення зоряного неба високотемпературних та високошвидкісних полів при гіперзвуковому польоті (швидкості від 6 до 16 Махів). Похибка проведеної симуляції порівняно з експериментом склала 30%, що є недостатнім для практичного використання.

Таким чином, завдання створення імітатора зоряного неба актуальною задачею; ключовим елементом такого імітатора є алгоритм синтезу зображення.

Метою дослідження є створення алгоритму синтезу зображень для імітатора зоряного неба в ІЧ діапазоні, а також перевірка можливості застосування синтезованого зображення для налаштування астровізора.

Для синтезу зображення зоряного неба, придатного для налаштування астровізора, запропоновано алгоритм, що складається з таких кроків:

- визначення ділянки неба, покритого полем зору астровізора, на основі координат місця спостереження (широти і довготи), висоти над рівнем моря, часу спостереження (UTC), азимуту і куту піднесення (що визначають орієнтацію астровізора), а також куту зору астровізора;
- виділення з каталогу даних зірок, що попадають в поле зору (при цьому для забезпечення коректної ідентифікації та калібрування треба не менше 5 зірок);
- формування зображень зірок, з урахуванням їх температури та спектру випромінювання, а також зоряної величини (визначають діапазон випромінювання та яскравість зірки);
- формування засвітки зоряного неба та фонових шумів;
- врахування атмосферних ефектів – в першу чергу, послаблення світла і розмивання зображення – для підвищення реалістичності зображень;
- врахування роздільної здатності астровізора (визначає деталізацію зображень) і його спектральної чутливості кожному діапазоні.

Запропонований алгоритм дасть змогу перевірити роботу приладу в умовах, максимально наближених до реальних. Сформоване зображення ділянки зоряного неба буде реалізоване в проекторі, який може бути оптичним, інфрачервоним або комбінованим пристроєм.

Як приклад, розглянемо формування зображення зоряного неба, яке буде відображено на датчику з матрицею 512 × 512 пікселів і розміром пікселя 10мкм. Алгоритм формування зображення створено в MATLAB, і він полягає у виборі з каталогу зірок із зоряною величиною $m \leq 2$, врахування фонового шуму та впливу атмосфери. Вплив атмосфери змодельовано шляхом застосування гаусівського розмиття з $\sigma = 2$. Змодельоване зображення зоряного неба показано на рис. 1. Як видно з рис. 1, зорі на зображенні через

застосування розмиття представлено не як яскраві точки, а в формі розмитих кругів. Відповідно, для ідентифікації зірок і визначення їх координат доведеться застосовувати визначення центрів характерних (найбільш яскравих) зірок.

На рис. 2 показано результати обробки в MATLAB зображення зоряного неба, і ідентифіковані за методом найближчого сусіда характерні зірки.

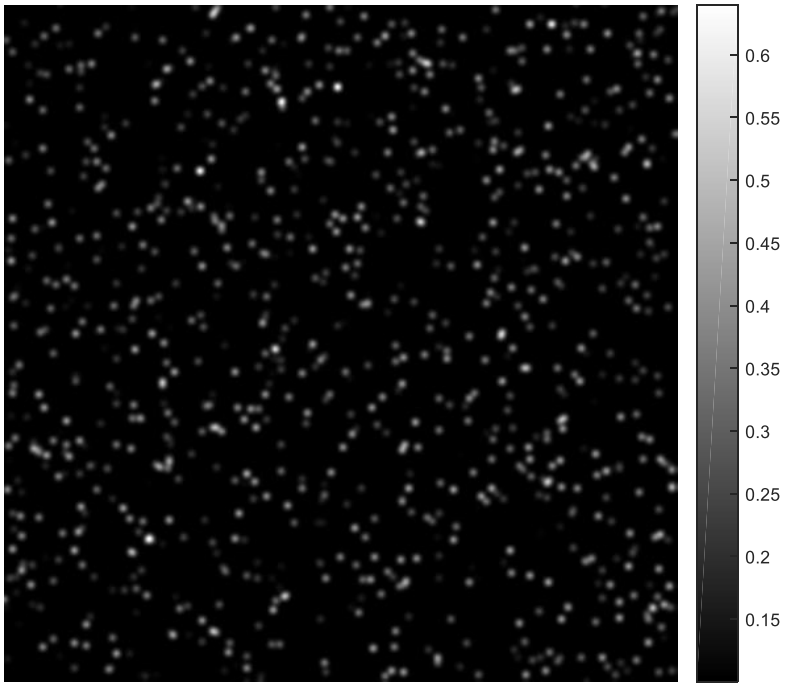


Рис.1. Змодельоване зображення зоряного неба з атмосферними ефектами (розмиття і послаблення). Праворуч шкала інтенсивності.

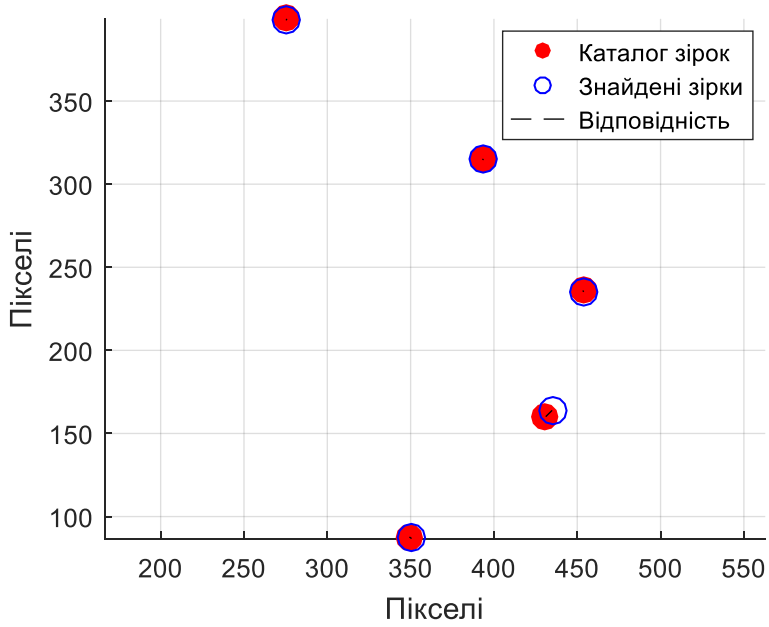


Рис.2. Оброблене зображення неба з виділенням характерних зірок, оброблене за методом найближчого сусіда.

З рис. 2 видно, що отримане за описаним вище алгоритмом зображення дає змогу ідентифікувати характерні зірки і отримати їх координати з точністю до 3-5 пікселів, тобто синтезоване зображення придатне для налаштування астровізора.

Для врахування руху астровізора необхідно забезпечити генерацію зображень неба з частотою мінімум в два рази більшою, ніж швидкість оновлення зображень з ПЗЗ-матриці астровізора (це випливає з теореми Найквіста). Якщо синтез зображення зоряного неба з заданою якістю в реальному масштабі часу неможливий, то можна провести синтез зображень, а потім в процесі налаштування відтворювати відео.

Якщо налаштовується астровізор, що має стабілізацію поля зору, за допомогою запропонованого алгоритму можливе моделювання залишкового дрейфу приладу. У випадку присутності вібрацій в кожному кадрі можна додати мікрозміщення зірок. Крім того, для того, щоб зменшити час створення кадру, можна інтерполювати проміжні положення зірок в проміжних кадрах.

Висновки. Результати моделювання показали, що запропонований алгоритм можна використовувати для моделювання зоряного неба в імітаторі зоряного неба інфрачервоного діапазону і синтезоване зображення придатне для налаштування астровізора. Подальші дослідження можуть бути присвячені вдосконаленню алгоритму з метою поліпшення моделювання зоряного неба.

Література

1. Boone B. G. Optical simulator and testbed for spacecraft star tracker development / B. G. Boone, J. R. Bruzzi, W. F. Dellinger, B. E. Kluga, K. M. Strobehn // Proceedings Volume 5867, Optical Modeling and Performance Predictions II. – 2005. – Vol. 5867. – pp. 586711-1 – 586711-14. – https://doi.org/10.1117/12.619133
2. IRSA Viewer – Title form screen. – Accesible at: https://irsa.ipac.caltech.edu/irsaviewer/?__action=layout.showDropDown&view=IrsaCatalog
3. Gaia archive – Title form screen. – Accesible at: https://gea.esac.esa.int/archive//
4. Zheng, Xunjiang Star map simulation and platform influence of airborne star sensor based on J-band data of 2MASS catalog / Xunjiang Zheng, Jie Shen, Zheng Wei, Hongyuan Wang // Infrared Physics & Technology. – 2020. – Vol. 111, Issue 12. – 10 p. - https://doi.org/10.1016/j.infrared.2020.103541
5. Wang, Hongyuan A new high-precision star map simulation model and experimental verification/ Hongyuan Wang, Zhiqiang Yan, Xiaonan Mao, Bingwen Wang, Xiang Liu & Wen Kang // Journal of Modern Opticsю – 2021. – Vol. 68, Issue 16. – pp. 856 – 867. – DOI: 10.1080/09500340.2021.1955165.
6. Schulz, V.H. Universal Verification Platform and Star Simulator for Fast Star Tracker Design / Schulz, V.H.; Marcelino, G.M.; Seman, L.O.; Santos Barros, J.; Kim, S.; Cho, M.; Villarrubia González, G.; Leithardt, V.R.Q.; Bezerra, E.A. // Sensors. – 2021. – Vol. 21, Issue 3. – pp. 907 – 930. – https://doi.org/10.3390/s21030907
7. Yang, H. Image Degradation Model for Dynamic Star Maps in Multiple Scenarios / Yang, H.; Jin, Y.; Hu, Y.; Zhang, D.; Yu, Y.; Liu, J.; Li, J.; Jiang, X.; Yu, X. // Photonics. – 2022. – Vol. 9, Issue 10. – pp. 673 – 686. - https://doi.org/10.3390/photonics9100673
8. Liu, Hao-Nan Development and validation of full-field simulation imaging technology for star / Hao-Nan Liu, Ting Sun, Si-Yao Wu, Kang Yang, Bao-Sen Yang, Guo-Teng Ren, Jia-Hui Song, and Guan-Wen Li // Optics Express. – 2025. – Vol. 33, Issue 3. – pp. 6526-6542. - https://doi.org/10.1364/OE.550772

УДК 621.395

ЗАХИСТ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ BLOCKCHAIN

Підпалий О.І.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
Email: sashapispalyi@gmail.com

SECURING SOFTWARE-CONFIGURABLE NETWORKS WITH BLOCKCHAIN TECHNOLOGY

The study analyzes the integration of Software-Defined Networking (SDN) and Blockchain to improve network security. It has been established that the combination of SDN and Blockchain provides decentralized management, cryptographic protection, and immutability of network transactions. The key security mechanisms are identified: policy automation through smart contracts, decentralized event log management, and dynamic access control. The architectural solutions are effective for IoT, telecommunications and corporate networks. The scientific novelty is the substantiation of the concept of integrating SDN and Blockchain, which is superior to traditional approaches to cybersecurity.

Дослідження аналізує інтеграцію Software-Defined Networking (SDN) та Blockchain для підвищення мережевої безпеки. Встановлено, що поєднання SDN і Blockchain забезпечує децентралізацію управління, криптографічний захист та незмінність мережевих транзакцій. Визначено ключові механізми безпеки: автоматизація політик через смарт-контракти, децентралізоване управління журналами подій та динамічний контроль доступу. Архітектурні рішення ефективні для IoT, телекомунікаційних та корпоративних мереж. Наукова новизна – обґрунтування концепції інтеграції SDN і Blockchain, що перевершує традиційні підходи до кіберзахисту.

Сучасний розвиток інформаційно-комунікаційних технологій характеризується безперервним ускладненням мережевих архітектур та механізмів забезпечення кібербезпеки. Фундаментальні трансформації в галузі мережевих технологій, зокрема впровадження Software-Defined Networking (SDN) та блокчейн-технологій, зумовлені критичною необхідністю вирішення системних проблем інформаційної безпеки в умовах постійно еволюціонуючих кіберзагроз [1,2,3].

Дослідження інтеграції Software-Defined Networking (SDN) та блокчейн-технологій проводилося комплексно з використанням широкого спектру інформаційних джерел та методологічних підходів. Основним напрямком дослідження є безпека мережі [4,5,6].

Аналіз безпекових викликів SDN-архітектури виявляє три критичні вектори потенційних атак:

- уразливість контролера,
- DDoS-атаки на площину керування
- Атаки на площину даних

Дана робота розглядається на основі таких елементів мережі: користувачі, SDN комутатори, Контролер SDN, блокчейн додаток

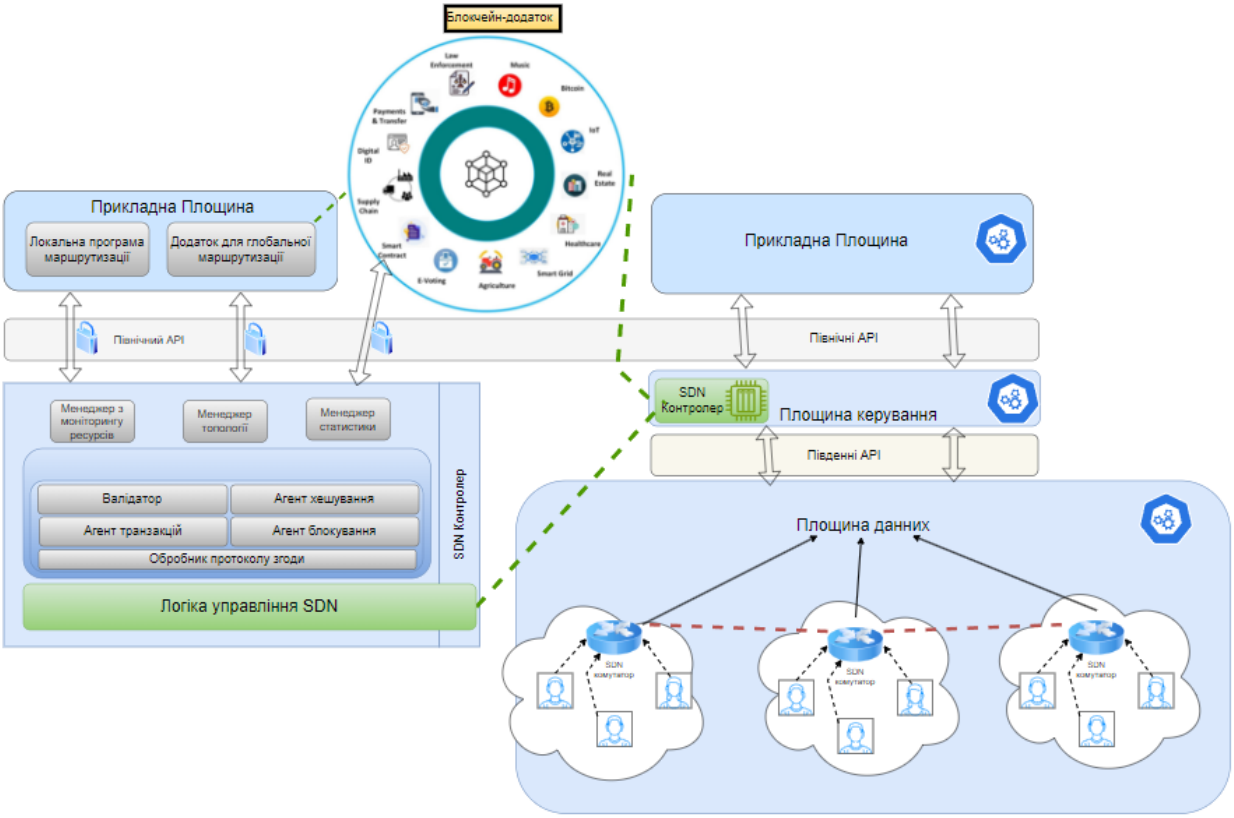


Рис.1. Схематична модель мережі з інтеграцією Blockchain у SDN.

У рамках дослідження було проведено тестування кількох типів атак, щоб оцінити ефективність Blockchain технологій у програмно-конфігурованих мережах (SDN) [7,8].

Результати тестування показали, що інтеграція Blockchain технології значно підвищила рівень безпеки програмно-конфігурованих мереж.

Таблиця 1. Результати тестування інтеграції Zero Trust і Blockchain

Тип атаки	Вплив до впровадження	Вплив після впровадження	Заблоковано атак (%)	Час відповіді контролера (мс)
DDoS-атаки	Повна втрата доступності контролера	Стабільна робота мережі	95%	10
Атаки на площину керування	Зміна правил маршрутизації	Неможливість зміни маршрутизації	98%	12
Атаки на площину даних	Перехоплення трафіку	Автентифікація та шифрування даних	97%	8

Під час тестування використовувалися такі основні метрики:

1. Час відповіді контролера (T_{resp})

Визначався як середній час (у мілісекундах) між надсиланням запиту від мережевого пристрою та отриманням відповіді від SDN-контролера:

$$T_{resp} = \frac{\sum T_i}{N} \quad (1)$$

де: T_i – час відповіді для і-го запиту; N – загальна кількість запитів.

2. Кількість успішно заблокованих атак (P_{block})

Оцінювалася як відсоток атак, які були виявлені та заблоковані системою безпеки, від загальної кількості атак:

$$P_{block} = \left(\frac{A_{blocked}}{A_{total}}\right) \times 100\% \quad (2)$$

де: $A_{blocked}$ – кількість успішно заблокованих атак; A_{total} – загальна кількість атак.

Висновки: Результати тестування показують, що інтеграція Blockchain з SDN не лише підвищила рівень безпеки мережі, але й значно покращила її продуктивність і стійкість до атак. Скорочення часу відповіді контролера забезпечило швидке реагування на загрози, що є критично важливим для запобігання їх негативному впливу. Високий рівень блокування атак свідчить про надійність впроваджених механізмів захисту, а продуктивність блокчейну підтвердила його придатність для використання у масштабованих системах.

Література

1. Romanov, O., Siemens, E., Nesterenko, M., Mankivskyi, V. Mathematical description of control problems in SDN networks/Proceedings of International Conference on Applied Innovation in IT, 2021, 9(1), стр. 33–39, http://dx.doi.org/10.25673/36582
2. 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 https://link.springer.com/chapter/10.1007/978-3-030-58359-0_13
3. Romanov O., Korniienko N., Obod I., Svyd I. Construction of the SDN Control Level Based on ONOS./ 2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odesa, Ukraine, 2021, pp. 127-132, doi: 10.1109/UkrMiCo52950.2021.9716691.
4. Romanov, O., Nesterenko, M., Boggia, G., Striccoli, D. Construction and Methods for Solving Problems at the SDN Control Level // Lecture Notes in Electrical Engineering,t2023, 965 LNEE, p. 85–101https://link.springer.com/chapter/10.1007/978-3-031-24963-1_6
5. Al-Emari, S., Anbar, M., Sanjalawe, Y. K., Manickam, S., & Hasbullah, I. H. 2022. Intrusion detection systems using blockchain technology: a review, issues and challenges. Computer Systems Science and Engineering, 40(1), 87-112. https://doi.org/10.32604/csse.2022.017941
6.Algarni, S., Eassa, F., Almarhabi, K. A., Algarni, A., & Albeshri, A. 2022. Bcnbi: a blockchain-based security framework for northbound interface in software-defined networking. Electronics, 11(7), 996. https://doi.org/10.3390/electronics11070996
7. Alharbi, T. 2020. Deployment of blockchain technology in software defined networks: a survey. IEEE Access, 8, 9146-9156. https://doi.org/10.1109/access.2020.2964751
8. Ali, G. M. and Chen, H. 2023. Power of fuzzing and machine learning in smart contract security validation. Fuzzy Systems and Data Mining IX. https://doi.org/10.3233/faia231090

УДК 621.382

ПОРІВНЯЛЬНИЙ АНАЛІЗ ШВИДКОСТІ ПОШУКУ В KNOWLEDGE GRAPHS

Маньківський В.Б., Зозуля В.С.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: v.b.mankivskiy@gmail.com , zozulya.vladyslav@lll.kpi.ua

BENCHMARKING SEARCH SPEED IN KNOWLEDGE GRAPHS

Knowledge Graphs (KG) play a key role in storing and retrieving structured knowledge, but traditional database methods such as SQL and NoSQL often introduce delays in query execution. This paper proposes methods to optimize search speed by using graph indexes, vector node representations, and modern similarity search algorithms such as HNSW (Hierarchical Navigable Small World) and FAISS (Facebook AI Similarity Search). The research results demonstrate improved search performance, which contributes to a more effective use of Retrieval-Augmented Generation (RAG) in large knowledge graphs.

Knowledge Graphs є важливим компонентом сучасних систем штучного інтелекту, що дозволяють моделювати зв'язки між об'єктами та ефективно використовувати їх для пошуку інформації. Проте традиційні підходи до зберігання та обробки KG засновані на SQL або NoSQL базах даних, що не завжди забезпечують достатню швидкість для роботи у реальному часі. Оптимізація швидкості пошуку в KG є критичною задачею, особливо для застосувань, що використовують Retrieval-Augmented Generation (RAG).

Основними проблемами, які досліджуються у цій роботі, є порівняння методів оптимізації через застосування:

- HNSW та FAISS для швидкого пошуку релевантних фактів.
- Кластеризація вузлів для швидшого доступу до схожих фактів.
- Адаптація Graph Transformer Networks (GTN) для семантичного пошуку.

HNSW є ефективним алгоритмом для побудови графів найближчих сусідів, що значно пришвидшує пошук подібностей у великих наборах даних. FAISS, у свою чергу, використовується для векторного пошуку, що дозволяє знаходити найбільш релевантні вузли у KG. HNSW забезпечує ефективну навігацію у високорозмірних просторах за допомогою ієрархічної структури графа. FAISS дозволяє виконувати швидкий пошук схожих векторів за допомогою компресії та попередньої індексації.

Кластеризація вузлів KG дозволяє групувати схожі об'єкти, що сприяє швидкому виявленню релевантної інформації. Методи кластеризації: K-Means, DBSCAN, Spectral Clustering. Переваги даного підходу - це зменшення кількості порівнянь між вузлами, що покращує продуктивність пошуку.

GTN використовують трансформерні архітектури для аналізу зв'язків між вузлами, що підвищує точність семантичного пошуку у KG. Graph

Attention Networks (GAT): покращує розуміння важливих зв'язків між вузлами. Transformer-based Search допомагає ідентифікувати найрелевантніші вузли для конкретного контексту запиту.

Оптимізація швидкості пошуку у Knowledge Graphs є критичним завданням для підвищення ефективності роботи сучасних AI-систем. Використання HNSW, FAISS, кластеризації вузлів та Graph Transformer Networks значно покращує продуктивність RAG, роблячи систему більш швидкою та точною. Подальші дослідження можуть бути спрямовані на адаптацію цих методів до динамічних KG та розподілених обчислювальних систем.

Для порівняння ефективності пошуку в Knowledge Graphs із використанням різних методів індексації та пошуку (SQL/NoSQL, HNSW, FAISS, GTN) можна запропонувати такі практичні метрики та експерименти:

Метрики ефективності:

- Час виконання пошуку (Query Latency, ms) – середній час обробки запиту у різних методах.
- Пропускна здатність (Queries per Second, QPS) – кількість запитів, які система може обробити за секунду.
- Точність пошуку (Precision@K, Recall@K, MRR) – оцінка релевантності результатів у порівнянні з еталонною відповіддю.
- Використання пам'яті (Memory Consumption, MB) – обсяг оперативної пам'яті, необхідний для підтримки індексу.
- Ємність збереження (Storage Size, GB) – обсяг дискового простору, необхідний для індексованого графа.

В результаті було отримане наступні дані, яке використовувалось для побудови залежності, показаної на рис. 1:

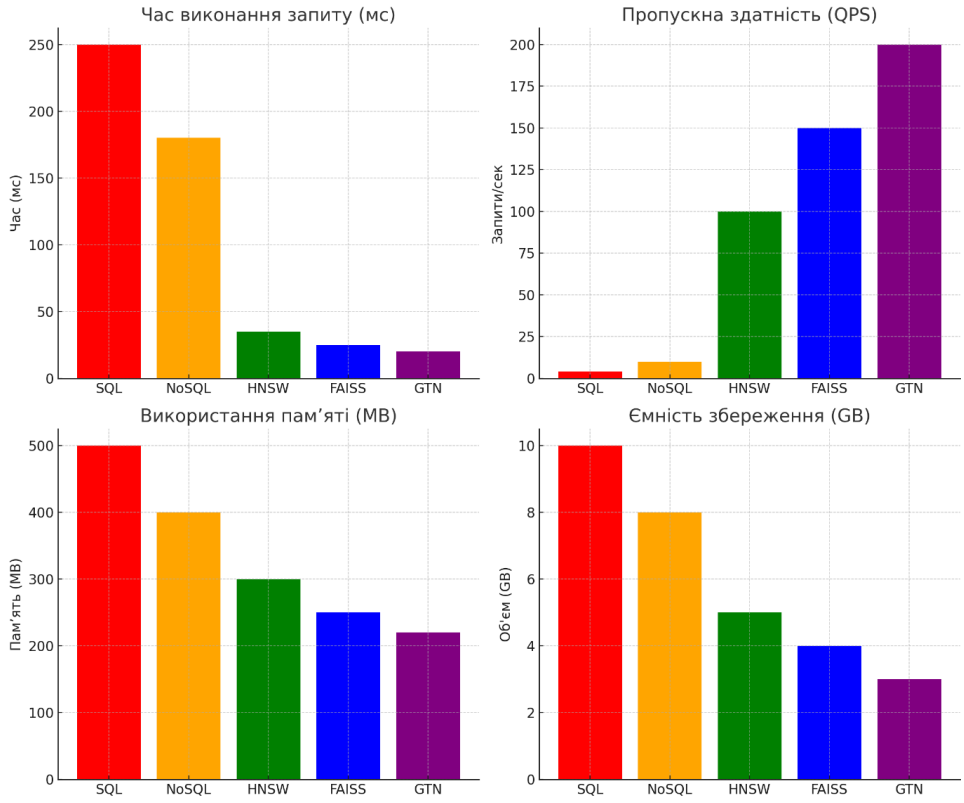


Рис.1. Порівняння ефективності методів пошуку в Knowledge Graphs.

Для оцінки ефективності різних методів пошуку в Knowledge Graphs (Рис.1) було проведено серію експериментів, спрямованих на аналіз швидкості пошуку, точності результатів і ресурсоспоживання.

Традиційні підходи (SQL, NoSQL) демонструють значні затримки (~180-250 мс). Векторні методи (HNSW, FAISS) значно швидші (~25-35 мс). GTN забезпечує найнижчу затримку (~20 мс) завдяки глибокому аналізу зв'язків.

При оцінці пропускної здатності необхідно було визначити, скільки запитів у секунду може обробляти кожна система. SQL і NoSQL обробляють лише 4-10 запитів/сек через обмеження індексування. HNSW і FAISS досягають 100-150 QPS завдяки ефективному векторному пошуку. GTN демонструє найкращий результат (~200 QPS), використовуючи оптимізовані графові структури.

При аналіз ресурсоспоживання було виконано оцінку, скільки оперативної пам'яті та місця на диску займає кожен метод. SQL і NoSQL мають найбільші вимоги до пам'яті (~400-500 MB) та зберігання (~8-10 GB). HNSW і FAISS більш оптимізовані (~250-300 MB пам'яті, 4-5 GB сховища). GTN споживає найменше ресурсів (~220 MB, 3 GB), забезпечуючи при цьому високу продуктивність.

Використання графових індексів (HNSW, FAISS) суттєво прискорює пошук у Knowledge Graphs. Graph Transformer Networks (GTN) забезпечують найкращий баланс між швидкістю, точністю та ресурсоспоживанням. Запропонований підхід дозволяє оптимізувати продуктивність RAG у великих графах знань.

Література

1. Gao, Y., Liu, Y., Zhang, H., Li, Z., Zhu, Y. Estimating GPU Memory Consumption of Deep Learning Models. In Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, Virtual, 8–13 November 2020.
2. Xu, Y.; Xie, L.; Gu, X.; Chen, X.; Chang, H.; Zhang, H.; Chen, Z.; Zhang, X.; Tian, Q. QA-LoRA: Quantization-Aware Low-Rank Adaptation of Large Language Models. arXiv 2023, arXiv:2309.14717.
3. Romanov, O., Nesterenko, M., Mankivskyi, V., Zhuk, O. Principles of Building Modular Control Plane in Software-Defined Network//Lecture Notes in Networks and Systems, 2023, 548, страницы 333–355. https://link.springer.com/chapter/10.1007/978-3-031-16368-5_17
4. Christophe, C.; Kanithi, P.K.; Munjal, P.; Raha, T.; Hayat, N.; Rajan, R.; Al-Mahrooqi, A.; Gupta, A.; Salman, M.U.; Gosal, G.; et al. Med42—Evaluating Fine-Tuning Strategies for Medical LLMs: Full-Parameter vs. Parameter-Efficient Approaches. arXiv 2024, arXiv:2404.14779v1.
5. Han, T.; Adams, L.C.; Papaioannou, J.-M.; Grundmann, P.; Oberhauser, T.; Löser, A.; Truhn, D.; Bressem, K.K. MedAlpaca—An Open-Source Collection of Medical Conversational AI Models and Training Data. arXiv 2023, arXiv:2304.08247
6. O. Romanov, M. Nesterenko, and V. Mankivskyi, "The usage of regress model coefficient utilization of channels for creating the load distribution plan in network" in visnyk ntuu kpi seriia-radiotekhnika radioaparatobuduvannia, 2016, pp. 34-42.

УДК 621.382

МОДЕЛЬ ЧЕРГ KAFKA ОБРОБКИ ПОДІЙ У РЕАЛЬНОМУ ЧАСІ

Маньківський В.Б., Гриценко Д.Г.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: v.b.mankivskiy@gmail.com, grytsenko.danyl@lll.kpi.ua

KAFKA QUEUES MODEL FOR REAL TIME EVENT PROCESSING

This paper considers the problem of efficient message queue management in the Apache Kafka system, which is used for processing streaming data in distributed environments. A mathematical model based on the theory of M/M/c/K queues is proposed, which allows estimating the probability of message loss (℘_loss) depending on the size of the Kafka buffer (B). The impact of this parameter on system performance is analyzed. The simulation results demonstrate that increasing the buffer size leads to an exponential decrease in the probability of loss, but after a certain threshold, a saturation effect is observed.

Apache Kafka широко використовується для обробки подій у реальному часі в таких галузях, як фінансові технології, IoT та телекомунікації. Однак продуктивність системи значною мірою залежить від правильної конфігурації параметрів черг. У даній роботі ми дослідили вплив розміру буфера B на ймовірність втрат повідомлень та запропонували оптимізаційні підходи.

Проблематика дослідження. У багатьох реальних сценаріях використання Kafka (наприклад, фінансові транзакції, моніторинг IoT-пристроїв, обробка потоків даних у реальному часі) надходження повідомлень є нерівномірним і може значно перевищувати можливості їх обробки. Це може призводити до переповнення черг, втрати критично важливих даних та зниження продуктивності системи.

Основними проблемами, які досліджуються у цій роботі, є:

• Визначення оптимального розміру буфера (B), який мінімізує втрати повідомлень, не перевантажуючи пам’ять системи.

• Дослідження впливу різних параметрів Kafka (кількість консьюмерів, швидкість обробки) на ефективність обробки повідомлень в черзі.

• Аналіз впливу ефекту насичення на продуктивність Kafka.

Для аналізу вище зазначених проблем, перше за все, необхідно визначитися з моделлю, яка би змогла описати поставлені проблеми і підштовхнула до їх вирішення.

Математична модель черги у Kafka. Система чергування у Kafka може бути змодельована як система масового обслуговування M/M/c/K, де:

• λ - інтенсивність надходження повідомлень (подій за секунду).

• μ - швидкість обробки повідомлень одним консьюмером.

• c - кількість консьюмерів у Consumer Group.

• B - розмір буфера Kafka (у кількості повідомлень).

• Ploss - ймовірність втрати повідомлення через переповнення черги.

Модель M/M/c/K є класичною в теорії масового обслуговування і найкраще підходить для опису черг у Kafka через такі особливості:

1. Poisson-розподіл надходження повідомлень: Потоки даних у Kafka часто мають випадковий характер, тому припущення про випадкові часові інтервали між подіями відповідає реальним сценаріям використання.

2. Експоненційний розподіл часу обробки: Консюмери можуть обробляти події з випадковою затримкою, що характерно для багатьох потокових сервісів.

3. Обмежена довжина черги (B): Kafka має обмежений розмір буфера, після чого нові повідомлення втрачаються. Ймовірність втрат розраховується за формулою Ерланга (1):

$$P_{loss} = \frac{\left(\frac{\lambda}{\mu}\right)^{B} / B!}{\sum_{n=0}^{B} \left(\frac{\lambda}{\mu}\right)^{n} / n!} \quad (1)$$

Умова неперервності полів на границі резонатор – вакуум при означає рівність тангенційних складових відповідних поперечних компонент магнітного та електричного полів. В результаті було отримане наступне характеристичне рівняння, яке використовувалось для побудови залежності, показаної на рис. 2:

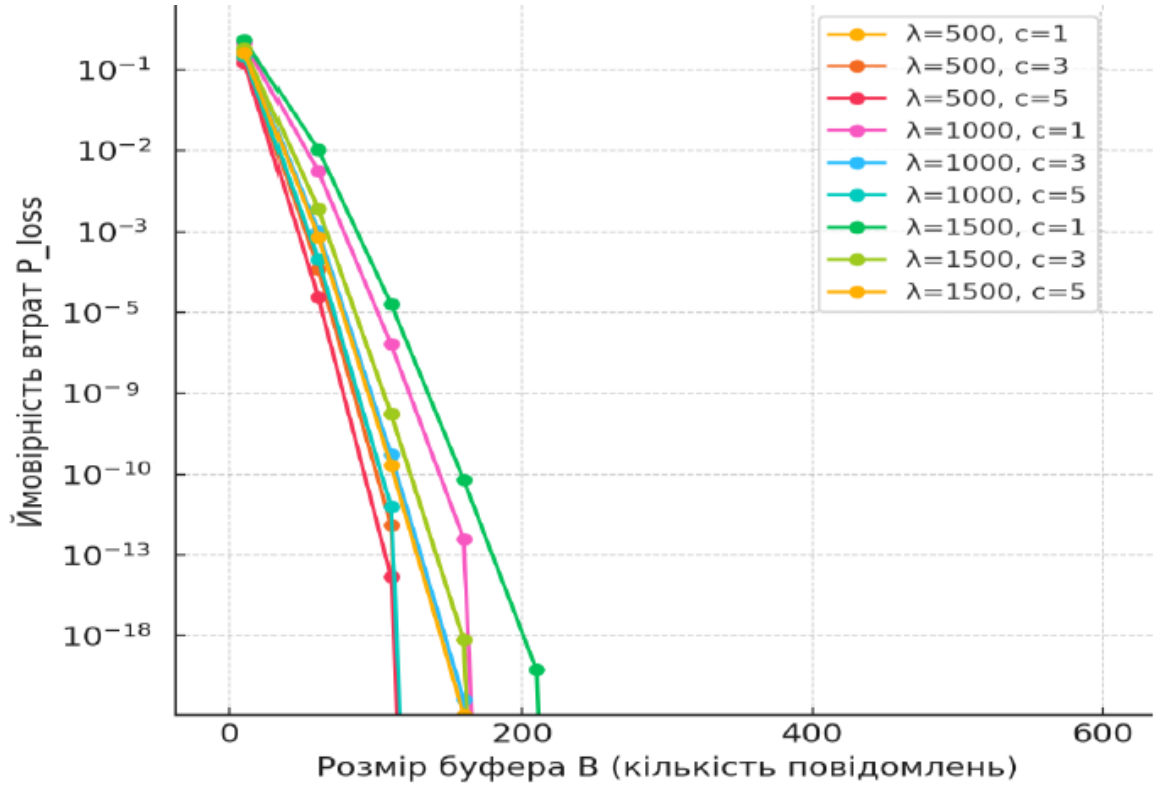


Рис.1. Залежність ймовірності втрат повідомлень (P_loss) від розміру буферу Kafka (B).

Рисунок 1 демонструє залежність ймовірності втрат повідомлень Ploss від розміру буфера Kafka B для різних значень інтенсивності надходження

повідомлень (λ) та кількості консьюмерів (c). Як видно, збільшення BBB суттєво знижує втрати, проте після певного рівня ефект насичення стає помітним.

Графіки показали наступні тенденції:

• При малих значеннях B (10-50) втрати повідомлень перевищують 15%, особливо при високих значеннях λ.

• Збільшення B до 200 суттєво зменшує втрати, досягаючи значень <1%.

• Подальше збільшення B понад 500 майже не впливає на втрати, але може підвищувати середній час затримки.

• Зі збільшенням кількості консьюмерів (c) затримка зменшується, але при c > 5 ефект покращення продуктивності стає незначним.

Окреслені перспективні напрямки досліджень Kafka черг через математичну модель. Розраховані параметри дають змогу зробити висновок, що збільшення буфера (B) суттєво знижує ймовірність втрат повідомлень, однак надмірне його збільшення не дає значного покращення після певного порогу. Оптимізація розміру буфера повинна враховувати інтенсивність надходження подій (λ) і продуктивність консьюмерів (μ). Використання математичної моделі M/M/c/K дає змогу більш точно прогнозувати продуктивність Kafka та уникати надмірних втрат повідомлень у реальному часі. Отримані результати можуть бути використані для розробки ефективних алгоритмів керування чергами у реальних розподілених системах.

Література

1. Jun Rao Jay Kreps, Neha Narkhede. Kafka: A distributed messaging system for log processing. In Proceedings of 6th International Workshop on Networking Meets Databases (NetDB), Athens, Greece, pages 1–7, 2011.
2. Kafka Inside Keystone Pipeline. https://medium.com/netflix-techblog/kafka-inside-keystone-pipeline-dd5aeabaf6bb/. [Online; accessed 25-Jun-2018].
3. Romanov, O., Nesterenko, M., Mankivskyi, V., Zhuk, O. Principles of Building Modular Control Plane in Software-Defined Network//Lecture Notes in Networks and Systems, 2023, 548, страницы 333–355. https://link.springer.com/chapter/10.1007/978-3-031-16368-5_17
4. G. Wang, J. Koshy, S. Subramanian, K. Paramasivam, M. Zadeh, N. Narkhede, et al., "Building a replicated logging system with apache kafka", Proc. VLDB Endow., vol. 8, no. 12, pp. 1654-1655, Aug. 2015, [online] Available: http: //dx.doi.org/10.14778/2824032.2824063.
5. P. Helland, "Immutability changes everything", Queue, vol. 13, no. 9, pp. 40:101-40:125, Nov. 2015, [online] Available: http://doi.acm.org/10.1145/2857274.2884038.
6. O. Romanov, M. Nesterenko, and V. Mankivskyi, “The usage of regress model coefficient utilization of channels for creating the load distribution plan in network” in visnyk ntuu kpi seriia-radiotekhnika radioaparatobuduvannia, 2016, pp. 34-42.

УДК 621.395

ДОСЛІДЖЕННЯ ШВИДКОСТІ НАВЧАННЯ НЕЙРОННИХ МЕРЕЖ В ЗАЛЕЖНОСТІ ВІД ФУНКЦІЇ АКТИВАЦІЇ

Кравченко А. В., Романов А.О.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна;
Національний Авіаційний Університет, Україна
E-mail: kravchenko.andriy@lll.kpi.ua, anton3329@gmail.com

STUDY OF THE LEARNING SPEED OF NEURAL NETWORKS DEPENDING ON THE ACTIVATION FUNCTION

The paper studies the learning speed of a neural network depending on the activation function used. Three types of activation functions were considered: the Heaviside function, the Sigmoid activation function, and the Hyperbolic Tangent activation function. It was determined that the activation function has a significant impact on the quality of learning. In addition, the coupling coefficients of the neural network and the range of input data values have a great impact on the speed and quality of solving the problem.

В роботі проведено дослідження швидкості навчання нейронної мережі в залежності від функції активації, що використовується. Було розглянуто три види функцій активації: функція Хевісайду, функція активації Сигмоїда та функція активації Гіперболічний тангенс. Було визначено, що функція активація має значний вплив якість навчання. Крім того, на швидкість та якість розв'язання задачі мають великий вплив коефіцієнти зв'язку нейронної мережі та діапазон вхідних значень даних.

Метою дослідження є аналіз впливу різних функцій активації на швидкість навчання нейронної мережі. Дослідити залежність швидкості навчання від типу функції активації, коефіцієнтів зв’язку.

Сучасні телекомунікаційні мережі постійно розширюються. Це в свою чергу вимагає ефективного аналізу трафіку, стану телекомунікацій. Нейронні мережі дозволяють оптимізувати цей процес. Шляхом визначення оптимальної функції активації можна покращити швидкість навчання та краще адаптуватися до нових умов [1,2].

В дослідженні використовувався одношаровий перцептрон (рис.1). Він працюють по принципу:

- на входи мережі подаються значення, які перемножуються на коефіцієнти
- далі значення підсумовуються та до них застосовується функція активації.

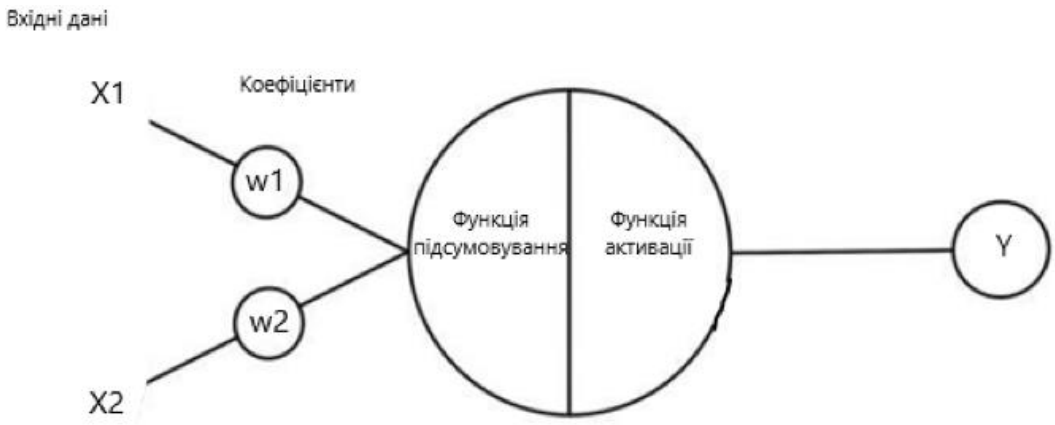


Рис. 1. Схематична модель одношарового перцептрону.

На рис. 1 позначено: X1, X2 – вхідні параметри; Y – вихідний результат; w1, w2 – коефіцієнти нейронної мережі.

Даними, на яких начався перцептрон слугували значення, які приймає логічна функція імплікації:

$$y = (x_1 \longrightarrow x_2) \quad (1)$$

де: x_1, x_2 – використовуються як вхідні значення в нейронну мережу; y – вихідні значення; ⟶ - оператор логічної імплікації.

Мережа навчалась за алгоритмом градієнтного спуску. Метрикою, за допомогою якої визначалась швидкість навчання має наступний вид: N_{epoch} – кількість епох навчання. Епоха – один повний цикл навчання мережі на наборі даних, який використовується для тренування моделі. Початкові коефіцієнти w_1 w_2 встановлювались рівними одному значенню w [3, 4, 5].

Результати експериментів показали, що при навчанні з кожною функцією активації є значення коефіцієнтів при яких швидкість навчання є найбільшою.

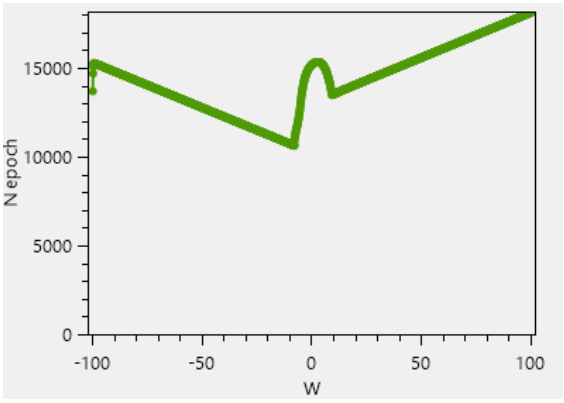


Рис 2. Результати навчання одношарового перцептрону з функцією активації Сигмоїда.

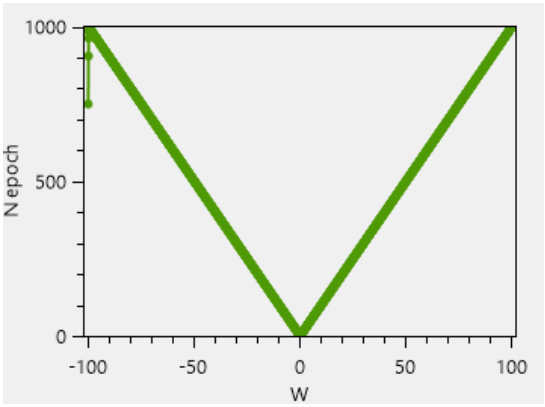


Рис. 3. Результати навчання одношарового перцептрону з функцією активації Хевісайда.

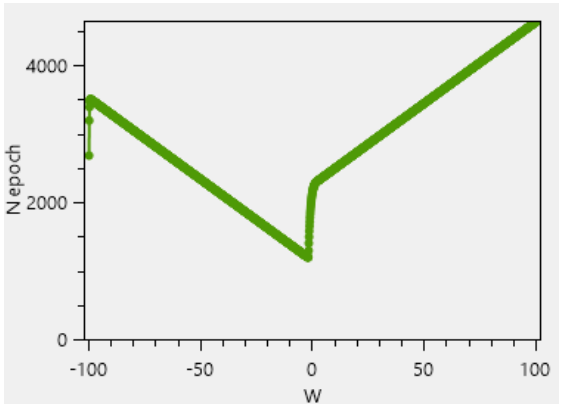


Рис. 4. Результати навчання одношарового перцептрону з функцією активації Гіперболічний тангенс.

На рис. 2, 3, 4 позначено: N_{epoch} – кількість епох навчання; W – значення, які набувають коефіцієнти перцептрону w1, w2.

Висновки: Результати експериментів показують, що перцептрон з різними функціями активації має різний час навчання при однакових коефіцієнтах. Було встановлено, що при використанні функції Хевісайда і діапазоні вхідних значень x_1, $x_2 \in [0;1]$ швидкість навчання мережі є найбільшою. Перцептрон з даною функцією найшвидше навчається при величині коефіцієнтів, рівних нулю, що свідчить про те, що при ініціалізації коефіцієнтів випадковими числами краще брати значення, близькі до нуля.

Література

1. Mahmoud Abbasi, Amin Shahraki, Amir Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Survey / Taherkordi 2021 https://www.sciencedirect.com/science/article/pii/S0140366421000426
2. Abbasi, M., Shahraki, A., & Taherkordi, A. (2021). Deep learning for Network Traffic Monitoring and Analysis (NTMA): A survey. Computer Communications, 170, 19–41. https://doi.org/10.1016/j.comcom.2021.01.021
3. Annette Lopez Davila, Professor Chi-Kwong Li Neural Networks: The Backpropagation Algorithm / 2020 https://cklixx.people.wm.edu/teaching/math400/Annette-paper.pdf.
4. Gal Vardi, Gilad Yehudai 2021 Learning a Single Neuron with Bias Using Gradient Descenthttps://papers.neurips.cc/paper_files/paper/2021/file/f0f6cc51dacebe556699ccb45e2d43a8-Paper.pdf.
5. 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

УДК 621.382

ПРОБЛЕМИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ Li-Fi В МЕРЕЖІ IOT

Бушинський Д.А., Романов А.О
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: dbushynskyi2002@gmail.com, anton3329@gmail.com

CHALLENGES OF IMPLEMENTING LI-FI TECHNOLOGY IN THE IOT NETWORK

Suggestions for improving the quality of information transmission in networks of interaction between the Internet of Things and Li-Fi technologies by using different types of modulation.

Сучасні тенденції розвитку телекомунікації характеризуються швидким зростанням кількості підключених пристроїв. Це спричиняє появу нових проблем, які можуть бути вирішені шляхом збільшення ємності, підвищення енергоефективності, оптимізації використання спектра та зниження вартості. Цього можна досягти шляхом інтеграції Інтернету речей (IoT) та технології Light Fidelity (LiFi), яка спрямована на покращення ефективності системи за допомогою комунікацій у видимому світлі (VLC) та [1]. LiFi є перспективним рішенням для різних застосувань IoT, зокрема для роботи в приміщеннях і на відкритому повітрі.

Розглядаючи питання інтеграції з’являються вагомі переваги використання цих двох технології разом, серед яких [2]:

- Захищеність. Видиме світло не проходить крізь стіни, що ускладнює перехоплення даних. Це робить технологію потенційно безпечнішою, ніж традиційний Wi-Fi. На відміну від радіочастотних технологій, Li-Fi дозволяє повністю покрити закриту цільову кімнату сигналом.
- Високошвидкісна передача даних. Комунікація через видиме світло дозволяє передавати дані в мережу зі швидкістю значно вищою за традиційні методи, що надзвичайно необхідно для пристроїв з використанням великих обсягів інформації.
- Відсутність перешкод. Оптичний канал зв’язку не створює радіочастотних перешкод, що робить його придатним для використання у чутливих до радіохвиль середовищах.
- Енергоефективність. Світлодіоди можуть виконувати функції як передавача, так і засобу освітлення приміщення.
- Безпека. Радіо хвилі можуть негативно впливати на здоров’я людини, в той час як світло від LED лампи не проникає крізь тіло. Мерехтіння

світлодіода під час передачі не помітне людському оку, тому це не викличе дискомфорту у користувачів.

Однак варто зазначити, що для правильної роботи пристрої IoT повинні мати можливість розпізнавати інформацію, обробляти її та зв'язуватися з іншими девайсами [3]. Ці потреби часто стають перешкодою для повноцінного впровадження технології, оскільки вони спричиняють різні складнощі, які ускладнюють виконання цих вимог. Деякі з цих проблем полягають у забезпеченні надійної та двонаправленої сигналізації, яка є важливою для забезпечення передачі інформації. Це необхідно вирішити за допомогою надійного двостороннього каналу зв'язку, який дозволить як надсилати, так і отримувати дані [4]. Зважаючи на те що пристрої інтернету речей можуть бути не завжди в прямій видимості, а отримувати сигнал шляхом відбиття світла від різних об'єктів чи перебувати в русі або бути в зоні опромінення іншими джерелами світла це створює одну з основних проблем впровадження технології Li-Fi в системи інтернету речей.

Множина різних видів модуляції сигналу, може ефективно застосовуватись для вирішення подібних складнощів, оскільки використання різних алгоритмів за певних сценаріїв допоможе зберегти ефективність передачі даних. Як правило, типові методи модуляції, що використовуються для радіочастотного зв'язку, можна використовувати для систем LiFi, оскільки і світлові, і радіочастотні хвилі є електромагнітними хвилями. Однак, особливості світлового сигналу дають змогу використовувати деякі унікальні методи. Загалом можна розділити види модуляції, з однією несучою (SCM) та декількома несучими (MCM) [5], як це показано на рисунку 1:

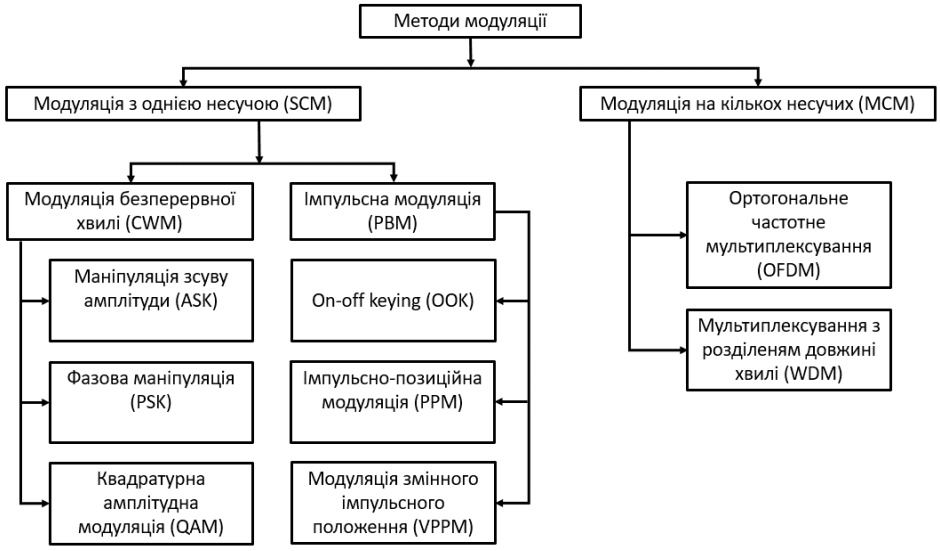


Рис. 1 Види модуляції LiFi.

Для зв’язку у видимому світлі в приміщенні проведено аналіз співвідношення продуктивності між методами модуляції. Результати показують, що продуктивність методів з однією несучою погіршується зі збільшенням швидкості передачі даних через міжсимвольну інтерференцію. Модуляція з декількома несучими є більш енергозатратним, але більш ефективним щодо пропускної здатності порівняно з SCM. OFDM є однією з найпоширеніших схем, що застосовуються в MCM. Незважаючи на складність в реалізації цей метод дає змогу коригувати частотні зміщення якщо пристрій рухається або знаходиться не у зоні прямої видимості. Приклади схем з однією несучою також включають маніпуляцію (OOK) і імпульсну позиційну модуляцію (PPM), які були вивчені та порівняні в системах бездротового інфрачервоного зв’язку [6]. Перший тип є простим у реалізації та підходить для пристроїв IoT, проте він чутливий до шуму. PPM має більшу енергоефективність. VPPM за рахунок чіткішої часової організації імпульсів може уникнути впливу світлових перешкод. PSK добре підходить для девайсів з середньою складністю обчислень, має непогану стійкість до шумів, проте вимагає фазової синхронізації [7]. Використання QAM дозволяє досягти максимальної швидкості користуючись ефективним використанням спектру, однак такий вид модуляції потребує значних ресурсів.

Проведений аналіз проблем впровадження Li-Fi в мережі IoT, викликані особливістю девайсів інтернету речей. Досліджено способи забезпечення ефективності роботи Light Fidelity шляхом використання різних типів модуляції при певних сценаріях, таких як вплив зовнішнього світла, відсутність прямої видимості та рухомі девайси.

Література

1. Rozin B., Shamala S. Integration of the Internet of Things With Light Fidelity: Potential Challenges a Review. Researchgate. URL: https://www.researchgate.net/publication/367465305_Integration_of_the_Internet_of_Things_With_Light_Fidelity_Potential_Challenges_a_Review.
2. Safwan A. Review of LiFi Technology and Its Future Applications. Researchgate. URL: https://www.researchgate.net/publication/326075664_Review_of_LiFi_Technology_and_Its_Future_Applications.
3. Swarnkar M., Bhadoria R. Architectural Building Protocols for Li-Fi (Light Fidelity). Academia.edu.
4. Hwaitat A., Qasem M. A Survey on Li Fi Technology and Internet of Things (IOT).

Researchgate. URL: https://www.researchgate.net/publication/339630920_A_Survey_on_Li_Fi_Technology_and_Internet_of_Things_IOT
5. Damerdash A., Aly M. Energy efficiency assessment of power electronic drivers and LED lamps in Li-Fi communication systems. Sciencedirect. URL: https://www.sciencedirect.com/science/article/pii/S2352484721011318.
6. Barry J., Kahn J. Wireless Infrared Communications. Ieeexplore. URL: https://ieeexplore.ieee.org/document/554222
7. Raay I. Li-Local: Green Communication Modulations for Indoor Localization. Academia. URL: https://www.academia.edu/46913368/_Li_Local_Green_Communication_Modulations_for_Indoor_Localization_
8. Petrosino A., Striccoli, D., Romanov, O., Boggia, G., Grieco, L.A. Fidelity for Internet of Things: A survey/ Optical Switching and Networking, Volume 48, March 2023, 100732; https://doi.org/10.1016/j.osn.2023.100732
9. Романов О., Бурлака Г., Берестовенко О., Підпалий 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
10. Romanov, O., Dong, T.T., Nesterenko, M. The possibilities for deployment eco-friendly indoor wireless networks based on LiFi technology/Proceedings of International Conference on Applied Innovation in IT, 2020, 8(1), стр. 41–48; https://icaiit.org/proceedings/8th_ICAIIT_1/1_7_Romanov.pdf
11. Romanov, O.I., Fediushyna, D.M., Dong, T.T. Model and method of Li-Fi network calculation with multipath light signals/2018 International Conference on Information and Telecommunication Technologies and Radio Electronics, (UkrMiCo), Odessa, Ukraine, 2018, pp. 1-4, DOI: 10.1109/UkrMiCo43733.2018.9047550; https://ieeexplore.ieee.org/document/9047550
12. 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 - Proceedings, 2017, 8095404.

УДК 621.395

АЛГОРИТМИ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ В SDN-МЕРЕЖІ

Романов О.І., Нестеренко М.М., Костюк К.М.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: a_i_romanov@ukr.net, nikolaiy.nesterenko@gmail.com,
kiril.kostiuk.mik@gmail.com

ARTIFICIAL INTELLIGENCE ALGORITHMS FOR LOAD BALANCING IN SDN

This paper presents Artificial Intelligence (AI) algorithms for optimizing traffic management in Software Defined Networks (SDN). It discusses the integration of monitoring and AI analysis modules to enhance load balancing and dynamic traffic reconfiguration. Leveraging AI enables networks to forecast and manage parameters intelligently, addressing challenges like low reliability and inefficient resource usage. The paper also examines popular algorithms for resource optimization and their advantages, highlighting the importance of these technologies.

Технологія SDN надає нові можливості для реконфігурації мережевого обладнання операторів та мережевої архітектури (наприклад, розділення управління та переадресації, віртуалізація, динамічна реконфігурація, централізоване управління та контроль), які вирішують проблему низької надійності мережі, низького та незбалансованого рівня використання мережевих ресурсів, високих витрат на експлуатацію та обслуговування та інше.

В свою чергу, використання алгоритмів штучного інтелекту (ШІ) надає мережі когнітивні здібності з можливістю інтелектуального прогнозування та оптимізації параметрів мережі. Використання мережі SDN з технологією ШІ не буде занадто покладатися на людський досвід, тобто ШІ допоможе контролювати та оптимізувати мережу за допомогою постійного більш точного аналізу даних та адаптивних алгоритмів.

Для розширення можливостей та функціоналу SDN-контролера можна інтегрувати додаткові модулі: моніторингу для збору додаткових параметрів мережі (обладнання) та модуль ШІ-аналізу (прогнозування) та управління. На рис. 1. показана узагальнена структура впровадження інтелектуального рівня в мережу SDN. Розглянемо призначення та взаємодію інтегрованих модулів з SDN-контролером та елементами гетерогенної мережі.

Модуль моніторингу – отримує інформацію про завантаження елементів мережі за допомогою протоколів:

SNMP/NETCONF – модифіковані протоколи управління та моніторингу визначених параметрів мережі з підтримкою протоколу OPENFLOW;

Two-Way Active Measurement Protocol (TWAMP) – даний протокол створений для збору статистики таких мережевих вендорів як Huawei (наприклад: затримка (delay), тремтіння (jitter), коефіцієнт втрати пакетів “packet loss rate”, навантаження на процесор, і т. д.);

MQTT – протокол збору телеметрії, в тому числі параметри активного мережевого обладнання, використовується для обміну повідомленнями між пристроями мережі IoT.

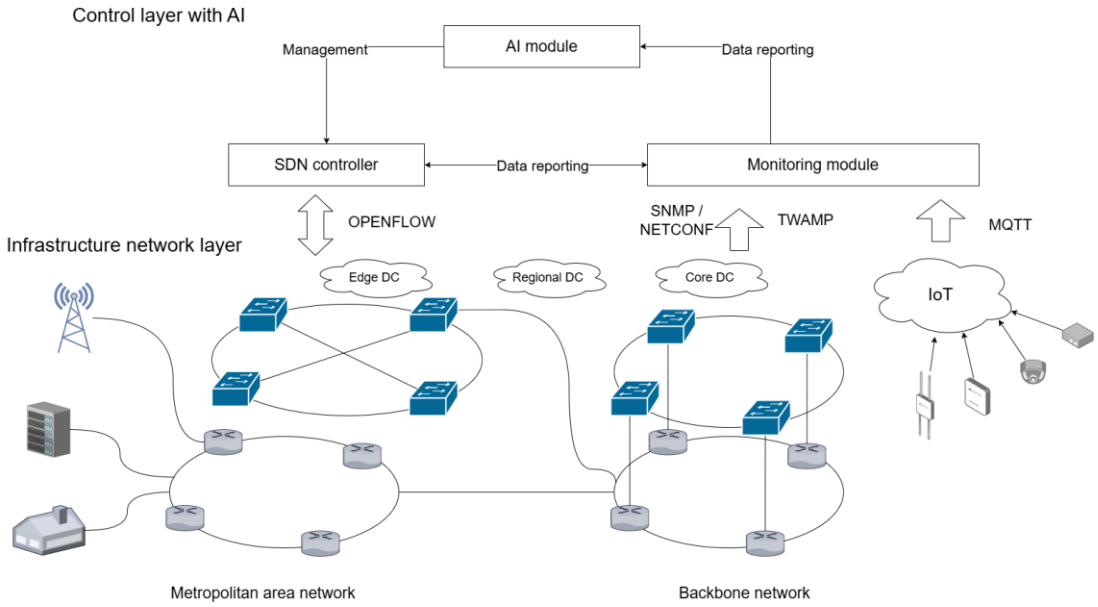


Рис. 1. Архітектура SDN-мережі з використанням ШІ.

Модуль ШІ-аналізу (прогнозування) та управління – аналізує надану модулем моніторингу статистику та формує “інтелектуальні стратегії”, що полягають в:

динамічній корекції трафіку – оптимізація шляхів проходження даних в реальному часі на основі актуальних показників завантаження, затримки, використання ресурсів та інших мережевих параметрів;

оптимізації використання ресурсів – планування і управління ресурсами (перенаправлення навантаження шляхом зміни маршруту трафіку) для досягнення рівномірного завантаження;

профілактиці перевантажень – постійне визначення потенційних зон перевантаження в мережі і завчасне вжиття заходів для балансування трафіку, щоб уникнути перевантажень окремих вузлів/маршрутів.

Причому, інтелектуальні стратегії представляють собою комплексні алгоритми і рішення, що дозволяють автоматизувати процеси управління мережею та забезпечувати її оптимізацію в умовах динамічного навантаження.

Розглянемо популярні алгоритми для оптимізації використання мережевих ресурсів та балансування навантаження в SDN-мережі:

Mapping Algorithm Based on Particle Swarm Optimization (PSO) – створений для ефективного використання наявних мережевих ресурсів. Основою алгоритму є використання методу рою частинок. Переваги алгоритму: можливість рівномірного розподілу ресурсів мережі, що зменшує навантаження на окремі вузли, збільшує сумарну пропускну спроможність групи маршрутів; невелика обчислювальна складність. Серед мінусів: ефективний для мереж з відносно невеликою кількістю вузлів (<500 вузлів), оскільки при обчисленні оптимальних маршрутів алгоритм не враховує всі можливі маршрути і шукає найоптимальніший локальний маршрут; не враховує допустиму швидкість передачі ліній, які входять до складу

маршрутів, що аналізуються;

Weight Particle Swarm Optimization (WPSO) – модифікований PSO, що додатково аналізує допустиму швидкість передачі ліній у визначених маршрутах. Основний недолік шукає найоптимальніший локальний маршрут, тобто не враховує всі можливі маршрути передачі.

Genetic Weight Particle Swarm Optimization (GWPSO) – модифікований WPSO, що покращений шляхом поєднання методу рою частинок (алгоритми PSO/WPSO) з генетичним алгоритмом. Генетичний алгоритм за рахунок своєї особливості (“мутацій” і “кросоверів”) поєднує та змінює вже проаналізовані маршрути, а саме збільшує кількість варіацій маршрутів розширюючи вибірку проаналізованих маршрутів на всю мережу, а також враховує нові, щойно додані, вузли. Впровадження генетичного алгоритму дозволило вирішити проблему розподілу ресурсів тільки локальних маршрутів, що дозволить розподіляти ресурси великих мереж (>500 вузлів). Серед недоліків можна зазначити, що алгоритм потребує більше обчислювальних ресурсів, аніж звичайні PSO або WPSO.

Використання технологій ШІ дозволяє розширити функціонал SDN-контролера за рахунок інтелектуалізації методів обробки статистичних даних та визначення інтелектуальних стратегій обробки потоків даних для балансування, прогнозування перенавантажень. На ефективність використання розглянутих алгоритмів (PSO, WPSO, GWPSO) вливає: розмірність мережі, кількість отриманих параметрів, повнота отриманих даних та потребує подальшого дослідження.

Література

1. Construction and Methods for Solving Problems at the SDN Control Level / O. Romanov et al. Emerging Networking in the Digital Transformation Age. Cham, 2023. P. 85–101. URL: https://doi.org/10.1007/978-3-031-24963-1_6.
2. Romanov, O., Nesterenko, M., Marinov, A., Skolets, S., Burlaka, H. SDN network modeling using the GUI MiniEdit/Proceedings - 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2022, 2022, стр. 637–642
3. Guo A., Yuan C. Network Intelligent Control and Traffic Optimization Based on SDN and Artificial Intelligence. Electronics. 2021. Vol. 10, no. 6. P. 700. URL: https://doi.org/10.3390/electronics10060700.
4. Directions for the Development of SDN Networks: Setting Tasks, Management Methods, Interfaces. / O. Romanov et al. 2023 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Kyiv, Ukraine, 13–18 November 2023. 2023. URL: https://doi.org/10.1109/ukrmico61577.2023.10380413
5. Event Model Algorithm with Microservice Architecture Implementation / O. Romanov et al. 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 10–12 October 2022. 2022. URL: https://doi.org/10.1109/picst57299.2022.10238498.
6. Alhilali A. H., Montazerolghaem A. Artificial intelligence based load balancing in SDN: A comprehensive survey. Internet of Things. 2023. Vol. 22. P. 100814. URL: https://doi.org/10.1016/j.iot.2023.100814.

УДК 621.395

АНАЛІЗ ТЕХНОЛОГІЙ IAC ДЛЯ РОЗГОРТАННЯ ВІДМОВОСТІЙКИХ ТА ВИСОКОНАВАНТАЖЕНИХ СЕРВІСІВ В ХМАРНОМУ СЕРЕДОВИЩІ AWS

Нестеренко М.М., Калюжний І.А.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: nikolaiy.nesterenko@gmail.com, kaluzhnyi.ivan@lll.kpi.ua

ANALYSIS OF IAC TECHNOLOGIES FOR DEPLOYING HIGHLY AVAILABLE AND HIGH-PERFORMANCE SERVICES IN THE AWS CLOUD ENVIRONMENT

This paper analyzes IaC technologies for deploying a fault-tolerant, high-load Kubernetes cluster in AWS. It explores automation, scalability, and maintainability using Terraform and Kubernetes. The study highlights best practices for cloud reliability and performance, proposing a highly available Kubernetes cluster design.

Сучасні інформаційно-комунікаційні системи масово переходять на контейнеризацію, що забезпечує гнучкість, ізоляцію та спрощує розгортання. Найпопулярнішою технологією контейнеризації є Docker, альтернативні - Podman, containerd і CRI-O. Проте використання лише систем контейнеризації створює проблеми з управлінням розробленим проектом, його відмовостійкістю, балансуванням навантаження, автоматичним масштабуванням. В зв’язку з цим, метою дослідження є визначення стеку технологій та побудова моделі кластеру для розгортання високонавантажених та відмовостійких застосунків.

Для керування контейнерами використовують системи оркестрації, які автоматизують розгортання, масштабування та забезпечують відмовостійкість. Найпопулярніші рішення: Docker Swarm (обмеженість у масштабуванні), Apache Mesos (доцільно використовувати в надвеликих масивах даних). Однією з технологій, яка забезпечує відмовостійкість і масштабування контейнерів завдяки автоматичному відновленню, балансуванню навантаження та адаптації до об’ємів трафіку є Kubernetes. Він має кластерну архітектуру (рис. 1.) і складається з наступних елементів:

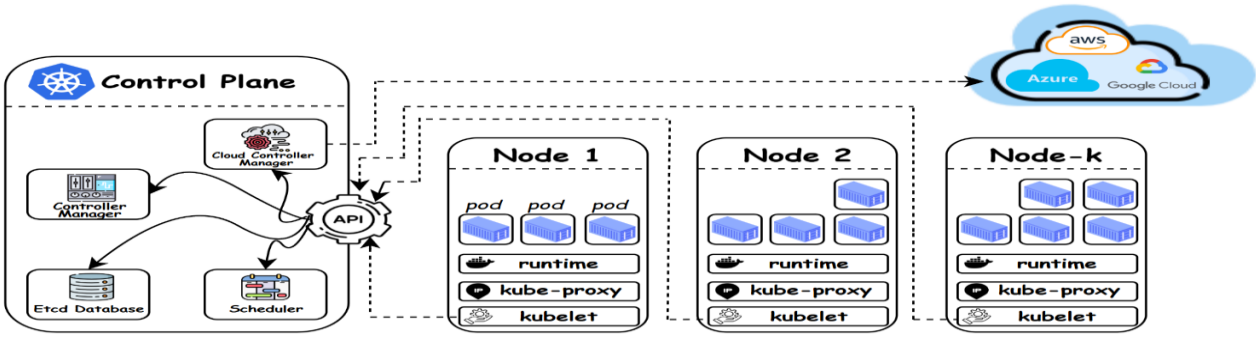


Рис. 1. Узагальнена архітектура Kubernetes кластеру.

За відмовостійкість в Kubernetes відповідають служби моніторингу стану та перезапуску подів (pod) у разі їх падіння, балансування навантаження та розподілення подів між різними нодами.

Kubernetes є універсальним рішенням для оркестрації (підтримує Docker, containerd та CRI-O) завдяки стандарту Container Runtime Interface (CRI). Також Kubernetes інтегрується з усіма великими хмарними провайдерами: AWS, Google Cloud, Azure. Kubernetes можна розгортати і на фізичних серверах або в дата-центрах, що дає змогу будувати гібридні або on-premises рішення, що робить його гнучким універсальним інструментом.

Для автоматизації розгортання, централізованого зберігання та контролю версій конфігурації використовуються Infrastructure as a Code (IaC) інструменти. Одним з найпоширеніших способів розгортання високонавантаженого та відмовостійкого Kubernetes кластеру є сервіс EKS (Elastic Kubernetes Service) на хмарній платформі AWS (Amazon Web Services).

Найбільш перспективним інструментом IaC для розгортання інфраструктури в гетерогенному хмарному середовищі, з можливістю зберігання та контролю версій конфігурації (наприклад - Git) є Terraform, який має ряд переваг: всі зміни описуються в коді (мінімізує людські помилки); попередня перевірка конфігурацій за допомогою команд для виявлення помилок; використання state file для відстеження поточного стану інфраструктури; автоматичне керування взаємозалежними ресурсами для уникнення помилок при створенні та оновленні інфраструктури; інтеграція з різними хмарними і on-premise провайдерами; декларативний підхід опису інфраструктури без необхідності написання складних скриптів. Запропоновано розгортання кластеру Kubernetes на основі AWS EKS за допомогою Terraform (рис. 2.).

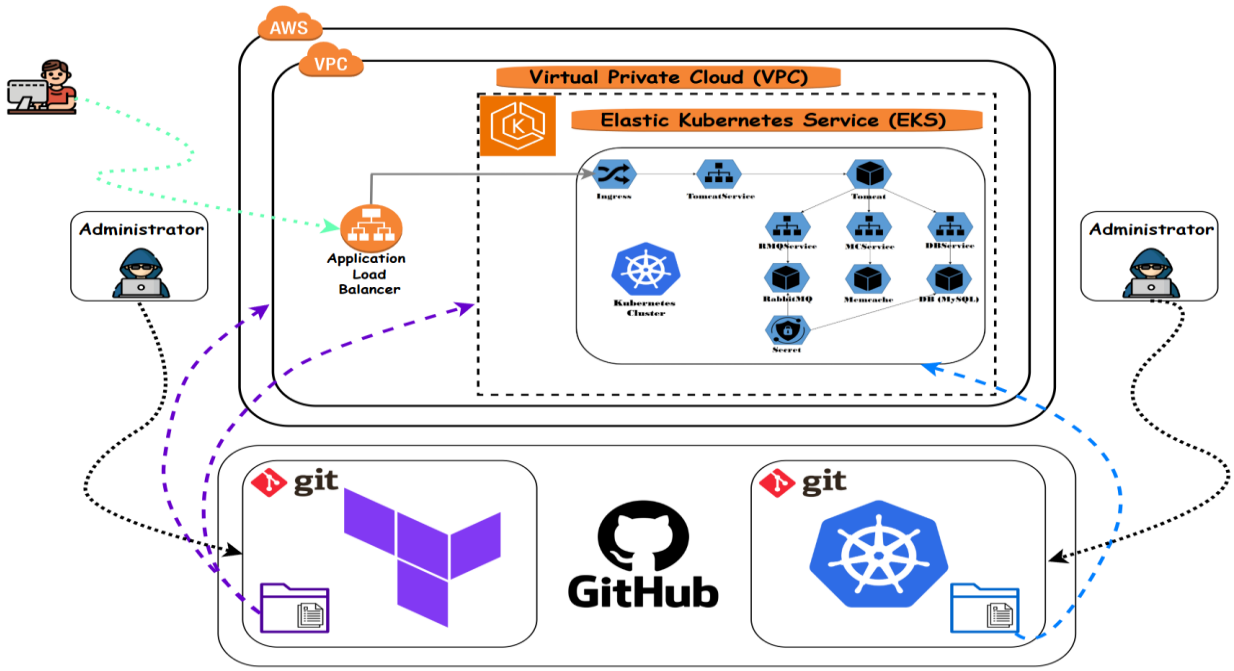


Рис. 2. Приклад схеми Kubernetes кластеру.

Terraform автоматизує створення та управління ресурсами через API зовнішніх платформ (хмарні сервіси, PaaS, SaaS тощо) за допомогою провайдерів.

Процес складається з трьох етапів:

- Write: визначається інфраструктура у конфігураційних файлах;

- Plan: створення плану змін, порівняння конфігурації з поточним станом інфраструктури;

- Apply: виконання операції створення, оновлення чи видалення ресурсів у правильному порядку, враховуючи залежності.

Тобто, Kubernetes-кластер буде розгорнуто в AWS через EKS на основі створеного VPC за допомогою Terraform. Після цього в EKS буде завантажено конфігураційні файли, що налаштують кластер відповідно до застосунку. Увесь код (Terraform і Kubernetes) керується системою контролю версій. Доступ користувачів здійснюватиметься через ALB (Application Load Balancer), який спрямовуватиме трафік до Kubernetes-кластеру.

Висновки: Підхід Infrastructure as a Code більш ефективний в управлінні хмарною інфраструктурою, завдяки автоматизації, гнучкості та відмовостійкості. Terraform, завдяки своїм перевагам, один із найпопулярніших інструментів для розгортання сервісів в AWS.

Майбутні дослідження можуть зосередитися на інтеграції IaC з різними Cloud-провайдерами, автоматизації CI/CD (Continuous Integration/Continuous

Delivery/Deployment) процесів, покращенні безпеки та оптимізації масштабованих сервісів.

Література

1. Reddy Chittibala D. Infrastructure as Code (IaC) and Its Role in Achieving DevOps Goals. International Journal of Science and Research (IJSR). 2023. Т. 12, № 1. С. 1258–1262. URL: https://doi.org/10.21275/sr24304170702.
2. Odeyinka O. J. AWS Cloud Automation : Textbook. 2nd ed. Berlin : DE Gruyter Gmbh, Walter, 2024. 366 p.
3. Romanov, O., Nesterenko, M., Boggia, G., Striccoli, D. Construction and Methods for Solving Problems at the SDN Control Level // Lecture Notes in Electrical Engineering,t2023, 965 LNEE, p. 85–101, https://link.springer.com/chapter/10.1007/978-3-031-24963-1_6
4. Романов О.І., Бурлака Г.Ю. Управління мережею SDN з використанням контролера RYU/ Вчені записки таврійського національного університету імені В.І. ВЕРНАДСЬКОГО/ Серія: Технічні науки Том 34 (73) № 5 2023, С. 59-69, DOI https://doi.org/10.32782/2663-5941/2023.5/11
5. Романов О., Бурлака Г., Берестовенко О., Підпалий 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
6. O. Romanov, V. Mankivskyi, I. Saychenko and M. Nesterenko, "Event Model Algorithm with Microservice Architecture Implementation," 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2022, pp. 561-566, doi: 10.1109/PICST57299.2022.10238498.

УДК 621.395

НАПРЯМКИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В SDN-МЕРЕЖІ

Нестеренко М.М., Устинов Д.А., Романов М.О.
Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут, Україна
Національний авіаційний університет, Україна
E-mail: nikolaiy.nesterenko@gmail.com, dmytro.ustynov@viti.edu.ua, smartboobs1927@gmail.com

DIRECTIONS IMPLEMENTING TECHNOLOGIES ARTIFICIAL INTELLIGENCE IN SDN

Integration of artificial intelligence methods and the main trends in the use of machine learning methods in SDN to improve traffic classification, prediction, routing, optimization flows, and security.

Мережі SDN мають великий потенціал за рахунок наявних програмних інтерфейсів, що дозволяє використовувати засоби штучного інтелекту (ШІ) для їх оперативної переконфігурації та оптимізації управління, навіть в режимі реального часу. Проведений аналіз показує, що найбільш ефективне застосування ШІ в SDN мережах може бути при рішенні наступних задач:

- класифікація мультисервісного трафіку на основі методів машинного навчання;
- прогнозування мережевого трафіку;
- інтелектуальна маршрутизація та оптимізація потоків даних;
- підвищення безпеки.

Розглянемо можливі рішення впровадження ШІ в цих напрямках.

Класифікація трафіку є фундаментальною для впровадження політик якості обслуговування (QoS), заходів безпеки та маршрутизації з урахуванням типу сервісів. Поточні підходи ШІ у цій галузі включають:

- навчання з учителем (supervised learning): моделі, такі як машини опорних векторів (SVM), випадковий ліс (RF), дерева рішень (DT) та *k*-найближчих сусідів (KNN), використовуються для класифікації мережевого трафіку на основі різних характеристик, таких як розмір пакету, час передачі пакету та тривалість сесії;
- глибоке навчання (deep learning): згорткові нейронні мережі (CNN), багатошарові перцептрони (MLP) та стекові автоенкодери (SAE) використовуються для більш складних завдань класифікації, особливо для зашифрованого трафіку. Підходи глибокого навчання усувають потребу в ручному проектуванні ознак і можуть досягти вищої продуктивності з великими наборами даних.
- напівконтрольоване навчання (semi-supervised learning): для вирішення проблеми обробки некласифікованих даних. Тобто напівконтрольовані

методи, такі як Лапласівський SVM, були впроваджені для класифікації трафіку з використанням як промаркованих, так і немаркованих даних, що ближче до реальних сценаріїв.

Прогнозування мережевого трафіку. Методи ШІ дозволяють контролерам SDN прогнозувати шаблони мережевого трафіку, дозволяючи проактивне розподілення ресурсів та уникнення перевантажень. Існує декілька основних підходів для використання ШІ у прогнозування трафіка, а саме: аналіз часових рядів, глибоке навчання та федеративне навчання.

Аналіз часових рядів використовує моделі, такі як авторегресійне інтегроване ковзне середнє (ARIMA) та регресія опорних векторів (SVR), використовуються для прогнозування трафіку на основі попередньо отриманих даних.

Глибоке навчання для прогнозування: довга короткочасна пам'ять (LSTM), вентильні рекурентні вузли (GRU) та рекурентні нейронні мережі (RNN) показали вищу продуктивність для прогнозування трафіку завдяки їхній здатності фіксувати часові залежності в процесі передачі трафіку.

Федеративне навчання. Цей підхід дозволяє кільком контролерам SDN спільно навчатися та використовувати моделі прогнозування без обміну необробленими даними, як наслідок підвищувати конфіденційність, одночасно отримуючи переваги від колективного інтелекту.

Інтелектуальна маршрутизація та оптимізація потоків даних. Технології ШІ можуть визначати оптимальні маршрути в режимі реального часу на основі мережевих умов.

Навчання з підкріпленням (RL): Q-навчання та інші алгоритми RL дозволяють контролерам SDN вивчати оптимальні політики маршрутизації через взаємодію з мережевим середовищем. Підхід FAST (Framework for Analyzing SDN Traffic) використовує RL для вибору шляху на основі шаблонів трафіку.

Ройовий інтелект: Алгоритми, що описують колективну поведінку децентралізованої системи із здатністю до самоорганізації, були застосовані для пошуку ефективних маршрутів у динамічних мережевих середовищах.

Глибоке навчання з підкріпленням (DRL): поєднуючи глибоке навчання з навчанням з підкріпленням, DRL використовувалось для оптимізації рішень маршрутизації в складних мережевих сценаріях.

Підвищення безпеки мереж SDN через інтелектуальне виявлення та попередження кіберінцидентів.

Виявлення аномалій: техніки навчання без учителя, такі як кластеризація та автоенкодери, допомагають ідентифікувати незвичайні зміни в мережевому трафіку, які можуть вказувати на загрози безпеки.

Виявлення DDoS-атак: моделі машинного навчання, включаючи CNN, SVM та RF, були розгорнуті для виявлення розподілених атак типу відмова в обслуговуванні (DDoS) шляхом аналізу шаблонів трафіку.

Також системи раннього виявлення вторгнень (IDS) на основі глибокого навчання можуть ідентифікувати складні атаки, навчаючись на історичних інцидентах безпеки.

Необхідно відмітити, хоча ШІ пропонує значний потенціал для мереж SDN, для його ефективного впровадження потрібно забезпечити наступні вимоги:

- обчислювальні (розрахункові) витрати (контролер SDN може стати вузьким місцем при реалізації складних алгоритмів ШІ);
- якість навчальних (вхідних) даних (продуктивність моделей машинного навчання сильно залежить від якості та репрезентативності навчальних даних);
- реалізація управління в режимі реального часу (велика кількість мережевих рішень потребують відповідей у реальному часі, що може бути складно для складних моделей ШІ);
- масштабованість (збільшення розмірності мереж масштабованість рішень ШІ стає критичною проблемою);
- безпека моделей машинного навчання (моделі ШІ можуть бути вразливими до атак зловмисників).

Інтеграція методів ШІ в SDN представляє зсув в парадигмі управління мережею, дозволяючи мережам стати більш інтелектуальними, адаптивними та автономними. Різні техніки ШІ, від навчання з учителем до глибокого навчання з підкріпленням, показують перспективи покращення класифікації трафіку, прогнозування, маршрутизації та безпеки.

Що стосується конкретно балансування навантаження та оптимізації трафіку, ШІ пропонує інструменти для прогнозування шаблонів трафіку, класифікації типів трафіку, динамічного коригування розподілу ресурсів та оптимізації рішень маршрутизації. Ці можливості стануть все більш важливими, оскільки сучасні мережі продовжують зростати в складності та масштабі, а також при появі нових технологій та послуг.

Література

1. Romanov, O., Nesterenko, M., Boggia, G., Striccoli, D. Construction and Methods for Solving Problems at the SDN Control Level // Lecture Notes in Electrical Engineering,t2023, 965 LNEE, p. 85–101; DOI:10.1007/978-3-031-24963-1_6
2. O. Romanov, V. Mankivskyi, I. Saychenko and M. Nesterenko, "Event Model Algorithm with Microservice Architecture Implementation," *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2022, pp. 561-566, doi: 10.1109/PICST57299.2022.10238498.
3. Романов О., Бурлака Г., Берестовенко О., Підпалий 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
4. O. Romanov, V. Mankivskyi, I. Saychenko and M. Nesterenko, "Event Model Algorithm with Microservice Architecture Implementation," *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2022, pp. 561-566, DOI: 10.1109/PICST57299.2022.10238498.
5. Lin B.-S. P. Toward an AI-Enabled SDN-based 5G & IoT Network. Network and Communication Technologies. 2020. Vol. 5, no. 2. P. 7. URL: https://doi.org/10.5539/nct.v5n2p7

УДК 621.39

ВИКОРИСТАННЯ ЦИФРОВОЇ СТЕГАНОГРАФІЇ В СУЧАСНОМУ КІБЕРПРОСТОРІ

Фокін Д.Г., Євдокименко М.О.
Харківський національний університет радіоелектроніки, Україна
E-mail: denys.fokin@nure.ua, maryna.yevdokymenko@ieee.org

APPLICATION OF DIGITAL STEGANOGRAPHY IN MODERN CYBERSPACE

This paper reviews recent documented cyber incidents involving the use of digital steganography in images, audio, video, and network traffic. The analysis shows that steganographic techniques can be effective in circumventing threat detection systems during cyberattacks. However, real-world use cases remain rare and poorly documented due to the complexity of both the implementation and the detection process.

В роботі розглядаються останні задокументовані кіберінциденти, пов'язані із застосуванням цифрової стеганографії у зображеннях, аудіо-, відеофайлах та мережному трафіку. Аналіз показує, що стеганографічні методи можуть бути ефективними для обходу систем виявлення загроз під час кібератак. Водночас реальні випадки їхнього використання залишаються рідкісними та недостатньо задокументованими через складність як самої реалізації, так і процесу виявлення.

Стеганографія теоретично є значним ризиком для кібербезпеки, але її задокументоване використання в реальному світі, особливо публічно повідомлене, є відносно рідкісним.

Стеганографія зображень. Зловмисники часто приховують зловмисний код або дані у файлах зображень (JPEG, PNG, BMP), оскільки зображення є найбільш поширеними мультимедійними даними. Вбудовуючи шкідливе програмне забезпечення (ПЗ) в зображення, зловмисники можуть проскочити повз антивірусні сканери та брандмауери. Пізніше приховане корисне навантаження вилучається та виконується супутнім скриптом або завантажувачем шкідливого ПЗ у цільовій системі [1].

"GO#WEBBFUSCATOR" (2022) – кампанія по розповсюдженню шкідливого ПЗ приховала зашифроване корисне навантаження всередині зображення JPEG космічного телескопа Джеймса Вебба. При звичайному перегляді зображення було фотографією галактики, опублікованою NASA, але в текстовому редакторі воно показало замаскований блок сертифіката, який містить шкідливе ПЗ, закодоване Base64. Це дозволило початковому зараженню через фішинговий документ завантажити те, що виглядало як зображення, минаючи сканери, а потім декодувати його у виконуваний файл на комп'ютері жертви [2].

Аудіо стеганографія. При належному виконанні ця методика дозволяє аудіофайлу відтворюватися без помітних змін у якості звуку, незважаючи на приховане корисне навантаження. Як стеганографія зображень, ця тактика може бути корисною для прихованої доставки шкідливого ПЗ.

"Криптомайнери в музиці" (2019) – кампанія з розповсюдження

шкідливого ПЗ, яка приховує шкідливе ПЗ у файлах WAV для встановлення криптомайнерів Monero і бекдорів. Зловмисники поєднали музику у WAV форматі із, в одному випадку, XMRig-криптомайнером, в іншому – виконуваним кодом Metasploit для налаштування віддаленого доступу який завантажувач міг вилучити з аудіофайла в пам'ять комп'ютера. В одному випадку файл WAV містив XMRig криптомайнер, в іншому – виконуваний код Metasploit для створення зворотної оболонки. Для приховування корисного навантаження зловмисники використовували LSB-заміну і псевдовипадкове кодування. Особливістю є те, що прихований код шкідливого ПЗ ніколи не з'являвся у файловій системі – він був декодований і виконувався безпосередньо в пам'яті, що значно ускладнювало виявлення. Дослідники відзначили, що це був лише другий задокументований приклад використання аудіостеганографії для впровадження шкідливого ПЗ у реальних умовах, підкресливши, що аудіостеганографія є життєздатною технікою, хоча і рідкісною [3].

Відео стеганографія. Відеофайли мають значну ємність, і ймовірність їхнього сканування на прихований вміст є навіть нижчою, ніж у випадку зображень або аудіофайлів.

Одним із останніх задокументованих випадків використання було використання відео для вилучення даних із скомпрометованої мережі. У 2014 році одна з найбільших компаній зі списку Fortune 500 зазнала витоку конфіденційної інформації через відеофайли. Дані спочатку були зашифровані, а потім вбудовані у відеофайли за допомогою загальнодоступного інструменту стеганографії, ймовірно OpenPuff, після чого зловмисники завантажили їх в загальнодоступний хмарний сервіс для обміну відео. Завдяки цьому передавання відеофайлів виглядало як звичайне завантаження користувачами легітимного контенту, що унеможливило виявлення несанкціонованого вивантаження інформації традиційними засобами безпеки [4].

Мережна стеганографія. Мережна стеганографія стосується приховування інформації в мережних протоколах без створення нових файлів що значно ускладнює її виявлення традиційними засобами аналізу трафіку. Це можна зробити, маніпулюючи корисним навантаженням пакетів, їхньою послідовністю, часовими параметрами, полями заголовка протоколу [5]. Метою є створення прихованого каналу зв'язку, який буде непомітно інтегруватися в легітимний трафік, дозволяючи зловмисникам передавати конфіденційну інформацію або управляти шкідливим ПЗ.

Одним із останніх прикладів є Pingback – шкідливе ПЗ для Windows, виявлене у 2021 році, яке використовує ICMP-тунелювання для комунікації з Command-and-Contol (C2) сервером. Замість використання HTTP або TCP Pingback здійснював надсилання та отримання команд через ICMP-пакети запиту та відповіді, використовуючи протокол, що зазвичай застосовується для діагностики мереж (утиліта ping). Використання ICMP як каналу зв'язку дає зловмисникам переваги: ICMP-трафік не має портів і рідко перевіряється брандмауерами чи засобами типу netstat. Інструменти, як Pingback, приховано

передають C2-команди в корисному навантаженні ICMP-пакетів, утворюючи непомітний двосторонній канал зв'язку з зараженими пристроями. Виявити мережну стеганографію важко, адже вона використовує дозволений трафік (ICMP або DNS), який зазвичай не аналізується глибоко, що дає змогу обходити засоби виявлення загроз і ексфільтрувати дані [6].

Підсумовуючи, сучасна цифрова стеганографія залишається складним, але ефективним інструментом. В останніх задокументованих випадках вона використовувалася переважно для прихованої доставки шкідливого ПЗ, керування зараженими системами та викрадення даних. Випадки її виявлення залишаються рідкісними, що пояснюється кількома факторами. По-перше, ця техніка є складною у реалізації, і її застосовують лише кваліфіковані зловмисники в спеціалізованих сценаріях. По-друге, методи виявлення стеганографії є недостатньо розвиненими, що ускладнює автоматизацію їхнього виявлення. По-третє, дослідження подібних атак вимагає тривалого аналізу, через брак публічних звітів залишається маловідомим. Як наслідок, хоча задокументовані випадки використання стеганографії є відносно застарілими, це не виключає її використання у складних і цільових атаках.

Література

1. The Hacker News. Steganography explained: how xworm hides inside images. The Hacker News. URL: https://thehackernews.com/2025/03/steganography-explained-how-xworm-hides.html (date of access: 16.03.2025).
2. Toulas B. Hackers hide malware in James Webb telescope images. BleepingComputer. URL: https://www.bleepingcomputer.com/news/security/hackers-hide-malware-in-james-webb-telescope-images/ (date of access: 16.03.2025).
3. Gatlan S. Attackers hide backdoors and cryptominers in WAV audio files. BleepingComputer. URL: https://www.bleepingcomputer.com/news/security/attackers-hide-backdoors-and-cryptominers-in-wav-audio-files/ (date of access: 16.03.2025).
4. Paganini P. Hackers used data exfiltration based on video steganography. Security Affairs. URL: https://securityaffairs.com/30624/cyber-crime/hackers-used-data-exfiltration-based-video-steganography.html (date of access: 16.03.2025).
5. Team Nuspire. Steganography in cybersecurity: a growing attack vector. Security Boulevard. URL: https://securityboulevard.com/2022/05/steganography-in-cybersecurity-a-growing-attack-vector/ (date of access: 16.03.2025).
6. Sharma A. New Windows 'Pingback' malware uses ICMP for covert communication. Bleeping Computer. URL: https://www.bleepingcomputer.com/news/security/new-windows-pingback-malware-uses-icmp-for-covert-communication/ (date of access: 16.03.2025).

УДК 621.39

МОДЕЛЬ МАСШТАБУВАННЯ МЕРЕЖІ НА ОСНОВІ СТОХАСТИЧНИХ ПРОЦЕСІВ ЗА УМОВ САМОПОДІБНОГО ТРАФІКУ

Компанієць В.О., Клавдієв В.П., Воронець О.М., Пустовойтов П.Є.
Національний технічний університет "Харківський політехнічний інститут", Україна
E-mail: Volodymyr.Kompaniiets@khpi.edu.ua

SCALING NETWORK MODEL BASED ON STOCHASTIC PROCESSES UNDER SELF-SIMILAR TRAFFIC CONDITIONS

A comparison of Poisson and fractal approaches to network traffic modeling is presented. It is proven that the use of stochastic processes in load forecasting allows minimizing delays and avoiding excessive resource consumption. A model is presented that provides adaptive management of network resources, creating a balance between performance and efficiency, as well as taking into account stochastic traffic characteristics.

Масштабування мереж є критичним завданням у сучасних інформаційно-комунікаційних системах, оскільки збільшення кількості користувачів та обсягів трафіку призводить до зростання навантаження на мережеву інфраструктуру.

У роботі [1] запропоновано новий метод математичного моделювання самоподібного трафіку в інфокомунікаційних мережах, який дозволяє генерувати потоки пакетів із заданим ступенем самоподібності. Цей підхід базується на використанні розподілу Парето та методу максимальної правдоподібності для оцінки параметрів моделі.

Дослідження [2] обґрунтовує методику структурно-параметричної ідентифікації та прогнозування самоподібного трафіку, що включає композицію методів глобальної та локальної оптимізації, а також вибір блочно-орієнтованих структур моделей.

Традиційні методи масштабування мереж часто не враховують динамічну природу сучасного трафіку, що може призводити до неефективного використання ресурсів. У дослідженні [3-4] розглянуто сучасні тенденції застосування технологій штучного інтелекту та машинного навчання для управління телекомунікаційними мережами та послугами. Автори акцентують увагу на використанні AI/ML (штучний інтелект/машинне навчання) для автоматизації обробки ресурсів та ізоляції між логічними та фізичними ресурсами, що є фундаментальним для мереж 5G.

Стохастичні процеси є потужним інструментом для моделювання непередбачуваних змін у мережевому трафіку та оптимізації розподілу ресурсів. У роботі [5] розглянуто застосування стохастичних методів для ефективного перерозподілу обчислювальних та мережевих ресурсів з мінімальними затримками.

Масштабування мережі в умовах самоподібного трафіку є складним

завданням, оскільки традиційні моделі керування ресурсами не враховують довготривалу залежність і високу варіативність мережевого навантаження. Самоподібний трафік проявляє властивості фрактальності та важко прогнозованих сплесків навантаження, що ускладнює розподіл ресурсів у мережах. Для ефективного масштабування необхідно використовувати математичні методи, здатні апроксимувати складні процеси та передбачати їх динаміку. У цьому контексті марківська апроксимація є перспективним підходом, що дозволяє спростити модель самоподібного трафіку, наближаючи її до керованих стохастичних систем.

Марківські випадкові процеси можуть бути використані для моделювання навантаження в мережі, оскільки вони добре підходять для опису систем із залежностями короткої пам'яті. Хоча самоподібний трафік має довготривалі кореляції, його можна апроксимувати через багаторівневі марківські моделі, що дозволяє описати зміну станів навантаження у спрощеній формі. Наприклад, можна застосувати Марківський процес із прихованими станами *(H/M/M)* або Марківські моделі черг *(M/G/1, M/M/∞)* для оцінки поведінки трафіку та адаптивного перерозподілу мережевих ресурсів. Ці позначення відносяться до систем масового обслуговування, описуваних за допомогою нотації Кендалла *(A/B/C)*.

В даній доповіді досліджується моделювання процесу, функціонування хмарної платформи для потокового відео, яка адаптивно розподіляє ресурси відповідно до кількості активних користувачів. Протягом доби трафік зазнає значних коливань: вранці навантаження мінімальне, увечері – досягає пікового значення, а впродовж дня можливі раптові сплески активності. Система повинна автоматично масштабувати обчислювальні ресурси, щоб запобігти перевантаженню та оптимізувати витрати.

Для моделювання цього процесу використовується рівняння динамічного балансування ресурсів (1), традиційно в марківських процесах λ позначають інтенсивність вхідного потоку. Водночас середня інтенсивність запитів описується функцією:

$$\lambda(t) = \lambda_0 + Asin(\omega t) + \eta(t), \quad (1)$$

де λ_0 – базова кількість запитів, A – амплітуда добових коливань, ω – частота змін, а $\eta(t)$ – стохастичний процес, що імітує випадкові стрибки трафіку.

Застосування рівняння динамічного балансування дозволяє хмарній платформі в реальному часі адаптуватися до змінного навантаження, уникаючи простоїв та перевитрат ресурсів.

Пуассонівський процес характеризується випадковими різкими сплесками навантаження, що призводить до частих і раптових змін у необхідності масштабування серверів. Натомість фрактальний процес демонструє довготривалу кореляцію, що забезпечує більш плавні зміни трафіку та стабільніше використання ресурсів.

Результати (рис. 1) вказують на важливість урахування самоподібності трафіку при проектуванні масштабованих мережевих систем. Впровадження

адаптивних алгоритмів, що базуються на аналізі фрактальних процесів, дозволяє знизити витрати на інфраструктуру та підвищити ефективність розподілу ресурсів у динамічних середовищах.

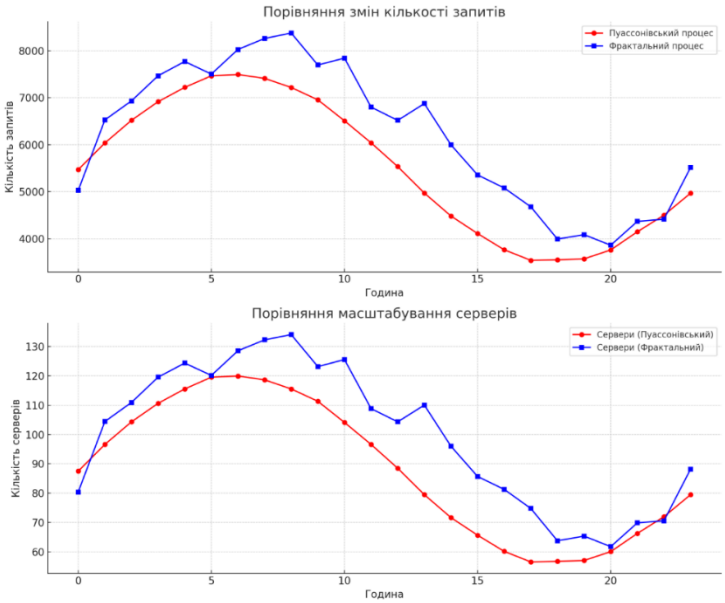


Рис.1. Масштабування ресурсів мережі при динамічній зміні навантаження.

Рівняння динамічного балансування ресурсів має широке практичне застосування в сучасних мережевих технологіях. Однією з ключових сфер його використання є програмно-конфігуровані мережі (SDN). У таких мережах контролери SDN можуть застосовувати це рівняння для динамічного перерозподілу ресурсів, реагуючи на зміни навантаження в режимі реального часу. Це дозволяє покращити ефективність використання мережевої інфраструктури та підвищити рівень якості обслуговування (QoS). Наведено, що модель забезпечує адаптивне керування мережевими ресурсами, створюючи баланс між продуктивністю та ефективністю, а також враховуючи стохастичні характеристики трафіку. Це дозволяє досягти оптимального використання інфраструктури в умовах динамічних змін навантаження.

Література

1. Пустовойтов П.Є., Компанієць В.О. Метод математичного моделювання самоподібного трафіку у інфокомунікаційних мережах // Системи управління, навігації та зв’язку, Збірник наукових праць. – Полтава: ПНТУ, 2024. – Т. 4 (78). – С. 187-189.
2. В.Корнієнко, О.Герасіна. Ідентифікація та прогнозування самоподібного трафіку інформаційно-комунікаційних мереж для систем виявлення атак // Information Technology: Computer Science, Software Engineering and Cyber Security, – Дніпро, № 1 (2022). С. 20-29.
3. М. Васильківський, О. Болдирєва, Г. Варгатюк, М. Будаш // Керування телекомунікаційними мережами з використанням технологій AI/ML. Видавництво "Телекомунікації та Інтернет-технології". – Хмельницький: ХНУ, 2021 (1). – С. 89-100.
4. Rozlomii, I. O. And Yarmilko, A. V. And Naumenko, S. V. (2022) The methods and means to improve the intelligent systems communication component's efficiency. Artificial Intelligence, vol.27 (№ 2). pp. 71-76.
5. Fontaine, X., & Smith, J. (2020). *Title of the Paper*. Proceedings of Machine Learning Research, 117, 1-10. Retrieved from https://proceedings.mlr.press/v117/fontaine20a/fontaine20a.pdf.

УДК 007.5:004.72:004.8

ОСОБЛИВОСТІ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

Чудо А.Р., Курдеча В.В.
Інститут телекомунікаційних систем,
КПІ ім. Ігоря Сікорського, Україна
E-mail: kyiv12@bigmir.net

FEATURES OF PROTECTION OF INTERNET OF THINGS DEVICES

The method for protecting IoT end devices has been 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 end devices to increase network security

За рахунок підключення різних пристроїв до Інтернету технологія Інтернету речей дає нові можливості для автоматизації, ефективності та прийняття продуманих рішень у різних сферах життєдіяльності. В зв'язку з цим особливо актуальною постає проблема захисту кінцевих пристроїв. А тому метою публікації є підвищення захищеності мережі Інтернету речей за рахунок модифікації захисту кінцевих пристроїв.

В роботі запропоновано модифікований метод захисту кінцевих пристроїв Інтернету речей(рис.1).

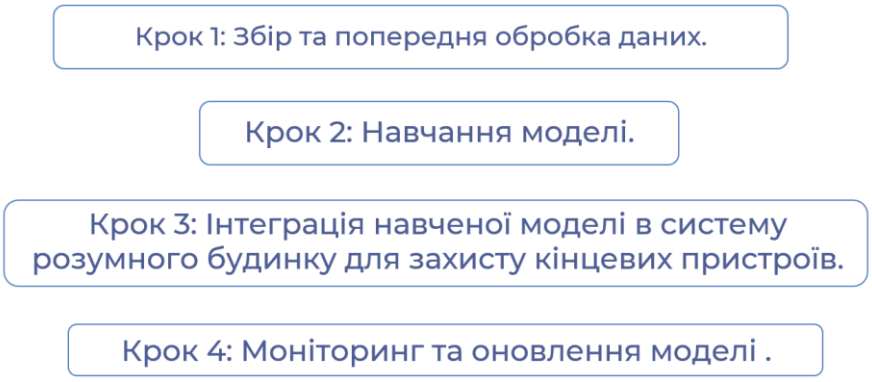


Рис.1. Модифікований метод захисту кінцевих пристроїв Інтернету речей.

Відмінністю запропонованого рішення є інтеграція навченої моделі в систему безпеки розумного будинку (рис.2). – що відповідає змінам в кроках 2 і 3 модифікованого методу (рис.1).

В першу чергу, щоб інтегрувати алгоритм машинного навчання, за допомогою якого відбувається відстеження аномального трафіку, потрібно зібрати дані з усіх датчиків.

Було взято набір даних з відкритим вихідним кодом трас трафіку зібраний з kaggle [1]. Дані були згенеровані в віртуальному середовищі, максимально наближеними до реальних. Загалом дані містять інформацію з різних датчиків розумного будинку. Ці набори даних містять зв'язок між різними вузлами IoT.

Набір цих даних в собі містять 347 935 нормальних даних та 10 017 аномальних. Також має відсутні значення в ознаках «Value» - 148 відсутніх значень, «Source Type» має 2050 відсутніх даних. Класовий показник «Normality» розділений на 8 різних класів відповідно до нормальності.

Рис.2. Модель машинного навчання модифікованого методу.

У рамках попередньої обробки, виконується два основних кроки. По-перше, виявляються та обробляються пропущені значення. Це допомагає уникнути втрати цінних даних та зберегти структуру. Другим важливим кроком є обробка несподіваних значень.

Після того, як отримано дані, потрібно очистити їх від шуму, щодо кількості екземплярів кожного класу в даних після обробки даних та вилучення з неї необхідної інформації.

Для навчання моделей набір даних був розділений у співвідношенні 80% для навчання і 20% для тестування.

За допомогою отриманих результатів відображених на багатокласових матрицях помилок, можна виділити ефективний алгоритм для цих даних.

Результати натурно-імітаційного моделювання показали, що рішення «випадковий ліс» RF зміг правильно класифікувати кожен клас, лише 403 з 1178 зразка DoS відніс до ознаки Normality, тобто визначив аномальні пакети, як нормальні. А також помилково класифікував 18 нормальних значень, як DoS. DT має фактично таку ж ситуацію, як і RF. Не на багато гірші результати отримав алгоритм машинного навчання ANN. Він не зміг

класифікувати 2 пакета SP та 1 MC. Інші ж алгоритми, дали значно гірші результати, вони не змогли класифікувати точно аномальні дані. Крім KNN він класифікував все вірно, лише 444 нормальних значень визначив як DoS.

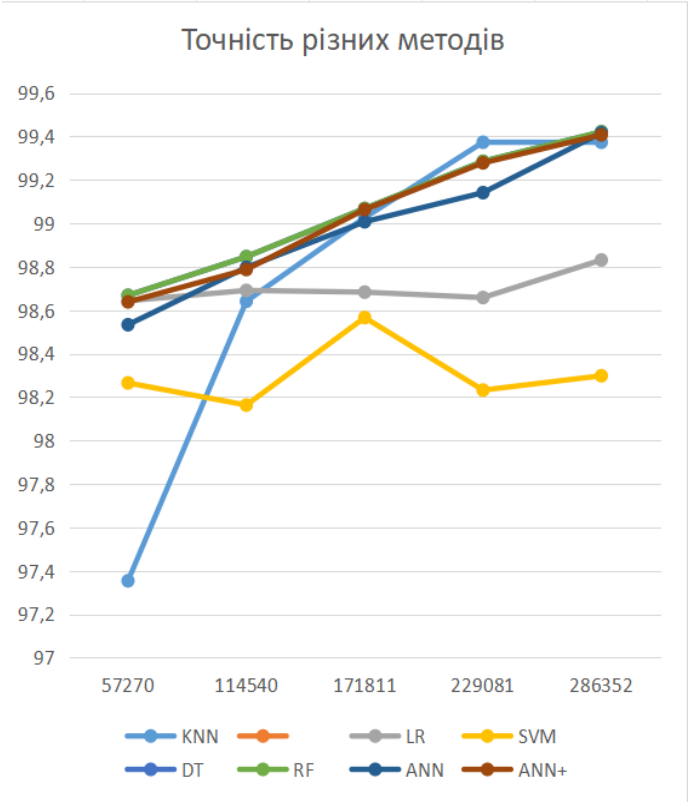


Рис. 3. Порівняння запропонованого рішення.

За результатами п'ятикратної перехресної перевірки можна дійти до таких самих висновків, як і за результатами отриманих з матриць. А саме алгоритми RF, DT та штучна нейронна мережа ANN показали майже однакові результати результати з точністю в 99.40%. Інші ж мають нижчий рівень точності.

Література

1. DS2OS traffic traces [Електронний ресурс] // Kaggle. – 2018. – Режим доступу до ресурсу: https://www.kaggle.com/datasets/francoisxa/ds2ostraffictraces.
2. Altulaihan E. Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms / E. Altulaihan, M. Almaiah, A. Aljughaiman // MDPI. – 2024. – https://doi.org/10.3390/s24020713.
3. Чудо А.Р. Курдеча В.В. Модифікований метод захисту кінцевих пристроїв інтернету речей // 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. - с.305.
4. Globa, L., Kurdecha, V., Popenko, D., Bezvuhliak, M., Porolo, Y. (2022). Data Collection and Processing Method in the Networks of Industrial IOT. In: Perakovic, D., Knapcikova, L. (eds) Future Access Enablers for Ubiquitous and Intelligent Infrastructures. FABULOUS 2022. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 445. Springer, Cham. https://doi.org/10.1007/978-3-031-15101-9_11

USD 621.372.543

DETERMINATION OF RESONATOR PARAMETERS USING THE APPROXIMATION METHOD

[1]Okhrimenko O., [1]Ilchenko V., [1]Stelnyk A., [2]Zhivkov O.
[1]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Educational and Scientific Institute of Telecommunication systems, Ukraine
[2]KTH Royal Institute of Technology
Division of Micro- and Nanosystems, Sweden
E-mail: o.okhrimenko.ti22@kpi.ua, zhyvkov@kth.se, v.i.ilchenko@kpi.ua

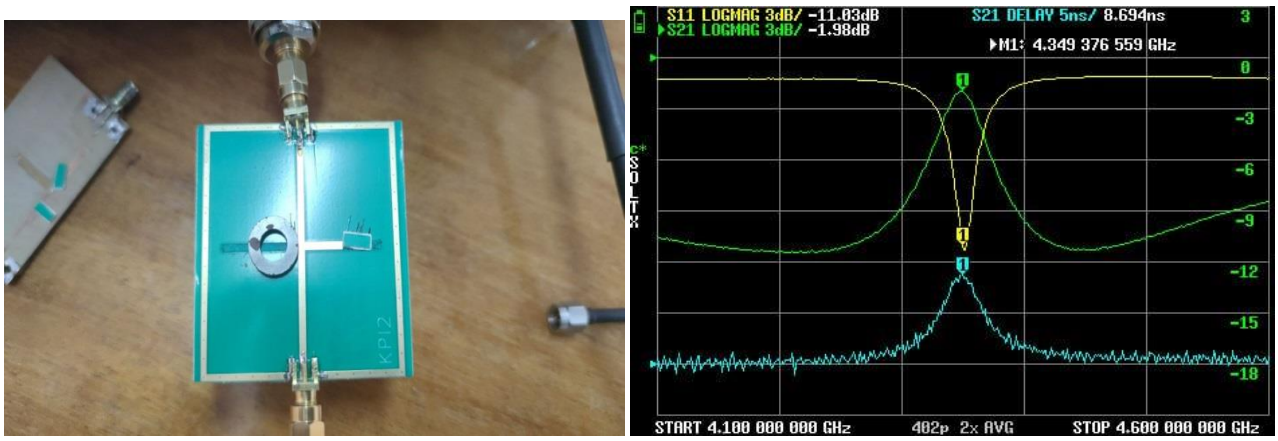
ВИЗНАЧЕННЯ ПАРАМЕТРІВ РЕЗОНАТОРІВ ЗА ДОПОМОГОЮ МЕТОДУ АПРОКСИМАЦІЇ

У доповіді розглянуто використання методу апроксимації задля визначення характеристик резонаторів через S-параметри структур, до яких вони входять.

While researching new methods of data analysis and processing, our team's attention was drawn to a paper Pompeo et al. [1] about available methods for determination of physical parameters of resonators using curve fitting [2].

We decided to investigate curve fitting further and consider its possibilities as a method that can be used to determine the parameters of resonators from the S-parameters of the structures they belong to. This procedure is generally based on approximation, which is a method of replacing an unknown function with a set of simpler functions that approximately reproduce the properties and parameters of the initial function or characteristic [2], [4]. This allows to significantly simplify the final analysis or calculations, depending on the purpose for which the approximation is used.

It is important to note that specialized computer software is used for such calculations, for example, MATLAB provides this capability [6].



a) b)

Figure 1. Two-resonator filter.
a) actual appearance**;** b) experimental measurements of S11, S21, GD.

For example, let's consider a two-resonator band-pass filter in Figure 1(a). The resonators' parameters are unknown to us - quality factor, resonant frequencies, and coupling coefficients. We are given with experimental measurements of S-parameters – Figure 1(b). From [5], we have the formulas for the calculation of S21:

$$S21 = 1 - \frac{C_{P\Sigma}}{1+C_{P\Sigma}} - \frac{C_{S\Sigma}}{1+C_{S\Sigma}},\ C_{P\Sigma} = \frac{K_{P1}}{1+j\cdot X_{P1}},\ X_{P1} = \left(\frac{f}{F_{0P1}} - \frac{F_{0P1}}{f}\right) Q_{0P1} \tag{1}$$

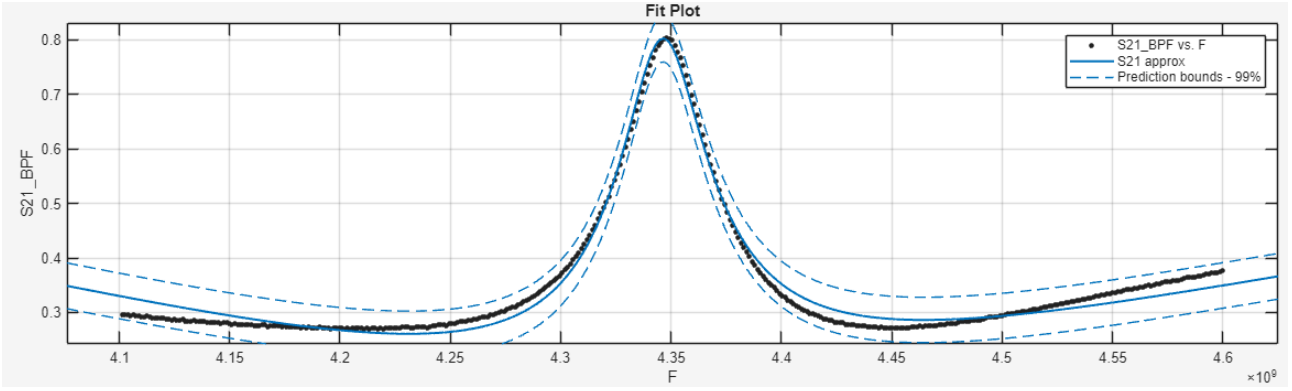
$$C_{S\Sigma} = \frac{K_{S1}}{1+j\cdot X_{S1}},\ X_{S1} = \left(\frac{f}{F_{0S1}} - \frac{F_{0S1}}{f}\right) Q_{0S1}$$

There are 6 unknown characteristics in (1):

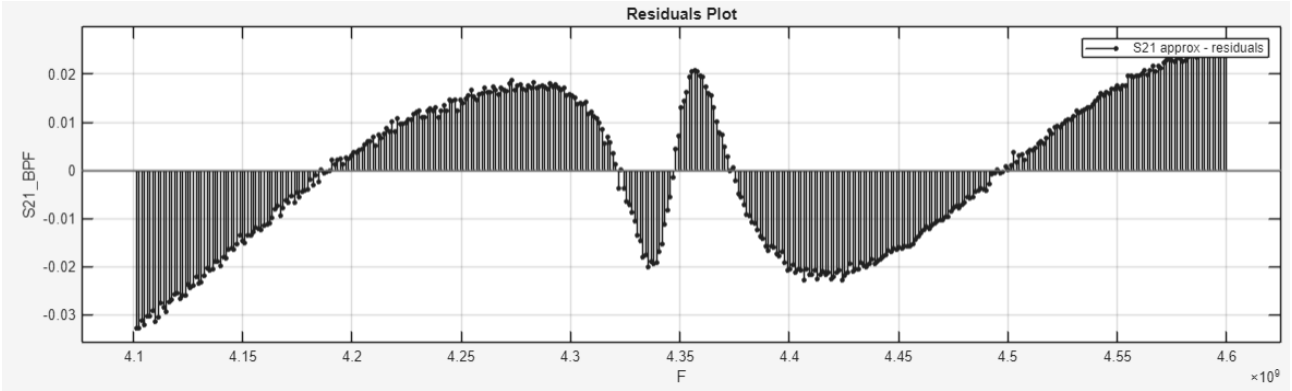
K_{P1}, K_{S1} - coupling coefficients of the resonators

F_{0P1}, F_{0S1} - resonant frequencies of the resonators

Q_{0P1}, Q_{0S1} - quality factors of the resonators



a)



b)

	Value
F_p1	4.3333e+09
F_s1	4.3461e+09
K_p1	9.6732
K_s1	8.5984
Q_0p1	25.8479
Q_0s1	1.0801e+03

c)

Goodness of Fit

	Value
SSE	0.1011
R-square	0.9834
DFE	395.0000
Adj R-sq	0.9831
RMSE	0.0160

d)

Figure 2. S21 approximation results:

a) graphical representation;
b) approximation residuals;
c) derived K, F and Q;
d) approximation quality.

Given the formulas (1) and the measurement data in Figure 1(b), it is possible to determine the unknown parameters of the band-pass filter resonators using approximation. We use MATLAB to do it [6].

As illustrated in Figure 2(a) - the approximation accurately reproduces the S21 characteristic, as proved by qualitative characteristics in Figure 2(d),. The main result of the approximation, are the coupling coefficients and Q-factors of the resonators, shown in Figure 2(c).

The main benefit of this method lies in the possibility of determining microwave characteristics (coupling coefficients, Q-factors) from experimental data, which was impossible before. As any approximation, this method requires a special approach, like choosing of the starting point and/or approximation step, as well as broader verification, which are the tasks for future study.

Acknowledgement.

This work was supported by the NATO Science for Peace Multi-Year Project G6002, "3D Materials for Energy Harvesting and Electromagnetic Sensing" and SSF Project UKR24-0008 “Electromagnetic metamaterials for communications and sensing".

References

1. Pompeo, Nicola & Torokhtii, Kostiantyn & Alimenti, Andrea & Silva, Enrico. (2025). A method based on a dual frequency resonator to estimate physical parameters of superconductors from surface impedance measurements in a magnetic field. 10.48550/arXiv.2501.11966.
2. Sandra Lach Arlinghaus, PHB Practical Handbook of Curve Fitting. CRC Press, 1994.
3. Cecil Hastings Jr., Jeanne T. Wayward, James P. Wong Jr., Approximations for Digital Computers. Princeton University Press, 1955.
4. N. I. Achieser, Theory of Approximation. Dover Pubns, 1992.
5. Рішення про реєстрацію договору, який стосується права автора на твір №7325 від 14.11.2024р Комп’ютерна програма «Filter Response Visualization Tool» Авдєєнко Г. Л. , Стоянов І.О., Живков О. П., Тичинський-Мартинюк В. Ю.
6. Imran, Omar. (2019). MatLab for Engineers.

UDC 621.391.2

ALGORITHM FOR SEPARATION OF MUTUALLY NON-ORTHOGONAL SIGNALS WITH BINARY PHASE SHIFT KEY IN PERSPECTIVE 5G MOBILE COMMUNICATION SYSTEMS

Yerokhin V.F., Vasylenko S.V.
Institute of Special Communications and Information Protection
of National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
E-mail: stddssss@gmail.com, vasylenko.phd@gmail.com

АЛГОРИТМ РОЗДІЛЕННЯ ВЗАЄМНО НЕОРТОГОНАЛЬНИХ СИГНАЛІВ З ДВІЙКОВОЮ ФАЗОВОЮ МАНІПУЛЯЦІЄЮ У ПЕРСПЕКТИВНИХ СИСТЕМАХ МОБІЛЬНОГО ЗВ'ЯЗКУ 5G

У статті наводиться опис запропонованого оптимального, за критерієм мінімуму ймовірності помилки в оцінці дискретних параметрів, алгоритму розділення двох взаємно неортогональних BPSK-сигналів, що передаються у одній частотно-часовій області.

In today's rapidly growing demand conditions for wireless services, Power-Domain Non-Orthogonal Multiple Access (PD-NOMA) technology is becoming a key element in fifth-generation (5G) communication systems. Its implementation is drive, enable the connection of a large number of devices (including various types of sensors) and improve the quality of user service.

Traditional orthogonal multiple access methods, currently actively used in fourth generation (4G) communication systems, use methods of frequency and time allocation of resources among users, which limits the number of simultaneous connections and therefore reduces the spectral efficiency of such systems. The use of PD-NOMA systems will allow to increase the efficiency of using limited spectral resources by allocating power among users in the same time and frequency domains.

Since in PD-NOMA systems users transmit signals using one frequency-time resource, differing only in power levels [1], there is a need to eliminate the mutual influence of similar (interfering) signals. In order to eliminate such interfering signals PD-NOMA systems used of the method of successive error elimination (SIC) [2]. It should be noted that the efficiency of SIC may decrease due to the accumulation of demodulation errors, especially in conditions of real interference. Also, insufficient difference in the power levels of user signals transmitted in the same frequency-time domain may lead to a further increase in the probability of errors. The above emphasizes the importance of assessing the potential interference immunity of such systems, which will allow identifying

possible vulnerabilities of modern wireless networks.

Let us consider the case when the PD-NOMA system uses mutually non-orthogonal signals with binary phase shift keying (BPSK).

From the theory of optimal nonlinear filtering it is known that the problem of a compatible, interconnected estimation of the initial phase of the carrier vibration and the discrete information parameter of the BPSK signal has already been solved [3]. In this case, to increase the signal-to-noise ratio during the removal of manipulation from the BPSK signal at the input of the phase-locked loop, used a “soft” estimation of the discrete parameters of signals. In this way, the reference (carrier) signal obtained used for quasi-coherent processing signals.

In the statistical theory of digital signal separation, there is a known algorithm for separation-demodulation of two mutually non-orthogonal digital BPSK-signals, which is optimal according to the criterion of minimum probability of error in estimating discrete information parameters of each signal [4]. This algorithm was obtained in the formulation of the classical theory of potential noise immunity, where all non-information parameters of signals that are mutually non-orthogonal over the length of the information packet are considered to be exactly known. It should be noted that the second result is generalized to the case when it is possible to process one of the signals (more powerful) quasi-coherently, and the other (less powerful) – incoherently.

The paper proposes to combine this the results and use them to separate mutually non-orthogonal BPSK-signals. According to the results of the research, it was found that when demodulating a more powerful signal, it is unnecessary to estimate the initial phase and amplitude of the carrier vibration of the less powerful signal. In addition, in order to receive the same probability of error for both signals, the difference between their instantaneous powers should be ≥ 6 dB, which will allow, when estimating the non-information parameters of the more powerful signal, to neglect the presence in the observation of the less powerful signal. In this case, the difference in the initial phases of the mutually non-orthogonal carrier BPSK-signals over the length of the information clock interval must remain slowly-variable.

In Fig. 1 presented one possible implementation option for such a quasi-coherent-incoherent demodulator of non-orthogonal BPSK-signals, which can be used in building 5G systems with using PD-NOMA technology.

The developed scheme of a quasi-coherent-incoherent demodulator of two mutually non-orthogonal BPSK-signals differs from the known one in that first, quasi-coherent reception of the first more powerful signal occurs (r_1^*), then the first received signal is compensated from the mixture at the correlator output , and only after that incoherent (quadrature) reception occurs of the second less powerful signal (r_2^*). The presence of a reactive element (RE) in the scheme allows

for an estimate of the initial phase of the more powerful signal. The decision on acceptance of the second less powerful signal is based on the addition of the in-phase and quadrature components of the signal.

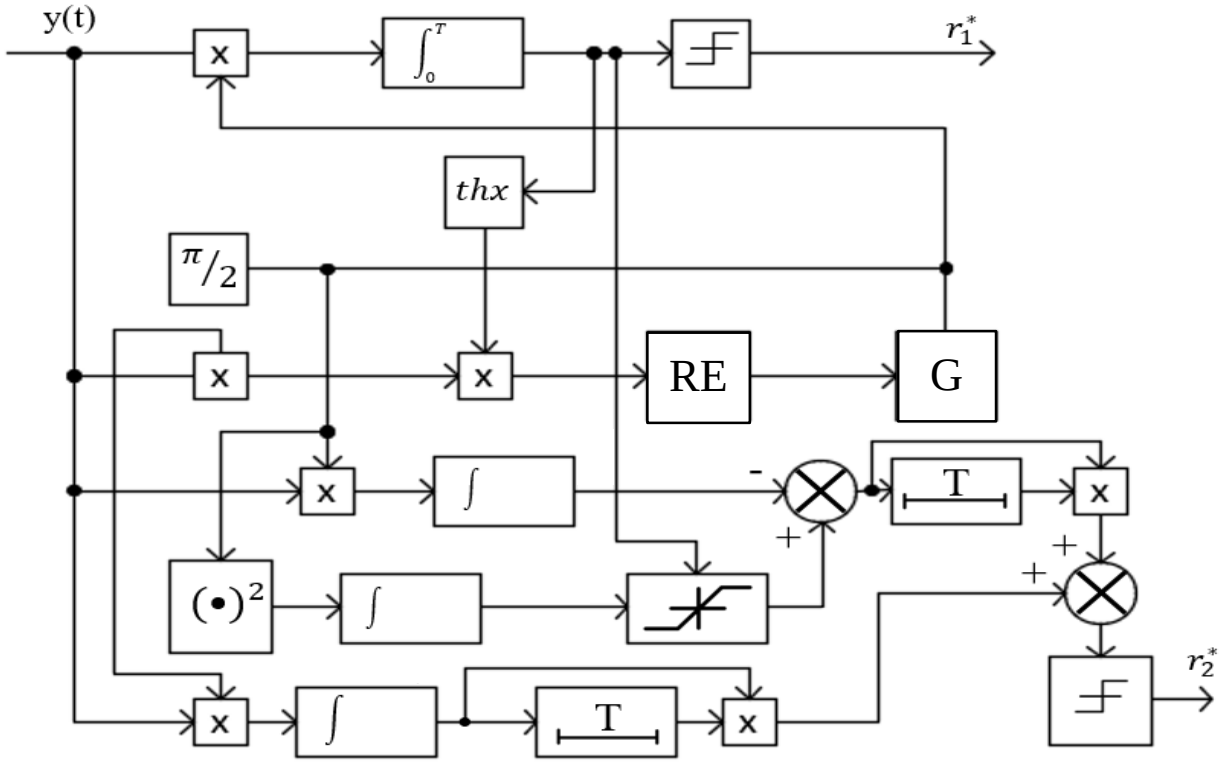


Fig. 1. Block diagram of a quasi-coherent-incoherent demodulator of mutually non-orthogonal BPSK-signals.

Conclusion. The paper proposes an algorithm for the separation-demodulation of two mutually non-orthogonal BPSK-signals, in which, when processing two similar interfering signals, it is necessary to estimate the non-information parameters (amplitude of the initial phase) of only the more powerful signal, which is processed quasi-coherently.

References

1. Islam S. M., Zeng M., Dobre O. A., & Kwak K. Non-Orthogonal Multiple Access (NOMA): How It Meets 5G and Beyond. ArXiv. 2019. abs/1907.10001. DOI:10.1002/9781119471509.w5gref032.
2. Iswarya N., Jayashree L. S. A Survey on Successive Interference Cancellation Schemes in Non-Orthogonal Multiple Access for Future Radio Access. Wireless Pers Commun. 2021. № 120. P. 1057 – 1078. DOI: 10.1007/s11277-021-08504-1.
3. Tikhonov V. I., Kharisov V.N., Smirnov V. A. Optimal filtering of discrete-continuous processes. Radio Engineering and Electronics. 1978. № 7. C. 1441 – 1452.
4. Verdu S. Multiuser Detection. Cambridge University Press. 1998. P. 451.

UDC 621.39

DEVELOPMENT OF A PARAMETRIC SYNTHESIZER FOR FREQUENCY-HOPPING SPREAD SPECTRUM SIGNALS WITH SPECIFIED CHARACTERISTICS

Igor Kovalenko, Andriy Movchaniuk
Faculty of Radio Engineering, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: igor.kovalenko.my@gmail.com

РОЗРОБКА ПАРАМЕТРИЧНОГО СИНТЕЗАТОРА СИГНАЛІВ З ПСЕВДОВИПАДКОВИМ ПЕРЕЛАШТУВАННЯМ РОБОЧОЇ ЧАСТОТИ З ЗАДАНИМИ ХАРАКТЕРИСТИКАМИ

В рамках наукової роботи по розробці амплітудного методу виявлення напряму приходу сигналів було розроблено та досліджено роботу параметричного синтезатора сигналів з псевдовипадковим перелаштуванням робочої частоти, що за своїми характеристиками наближений до джерел випромінювання, що є цільовими для даного дослідження. Отримані результати дозволяють стверджувати про можливість використання розробленого синтезатора як джерела тестового сигналу у подальшому дослідженні.

Problem Statement. In the development of new methods for determining the direction of arrival (DOA) of radio signals, an urgent issue is the synthesis of test signals that closely resemble the target signal in characteristics. This is particularly relevant for complex signals or modulations with spread spectrum, such as frequency-hopping spread spectrum (FHSS) signals, which are widely used for data transmission, control channels of unmanned aerial vehicles (UAV), and encrypted communication systems. The challenge of obtaining signals from real sources for testing newly developed algorithms is evident. The characteristics of target signals are typically determined using recordings from autonomous radio monitoring stations deployed in operational zones. Developing a synthesizer that serves as a relevant and adequate analog of a real radio signal source, the direction of arrival of which is of practical value, is an integral part of advancing innovative radio direction-finding methods.

Synthesizer Implementation. To determine the necessary characteristics of the FHSS target signal, a large volume of spectrogram recordings of real transmitters and data from open sources was analyzed (**Figure** 1).

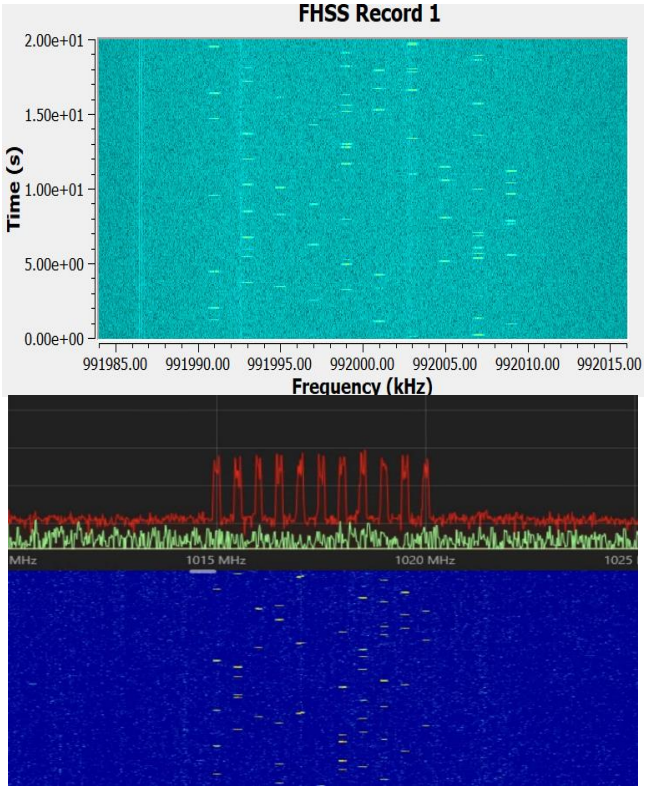


Figure 1. Recorded spectrograms from autonomous radio monitoring stations.

Experimental studies have shown that, for the signals of interest, the FHSS frequency range varies from 1 to 10 MHz, with individual channel bandwidths of 150–300 kHz and a hopping rate up to 20 Hz. Using correlation analysis of a single channel's bandwidth, a spectral fingerprint was obtained (**Figure2**), determined by the modulation type used for data transmission, specifically 2-FSK. The frequency range is predominantly sub-gigahertz, spanning 850-1025 MHz. Channel switching occurs according to a pseudo-random pattern with packet losses (gaps) of up to 30%.

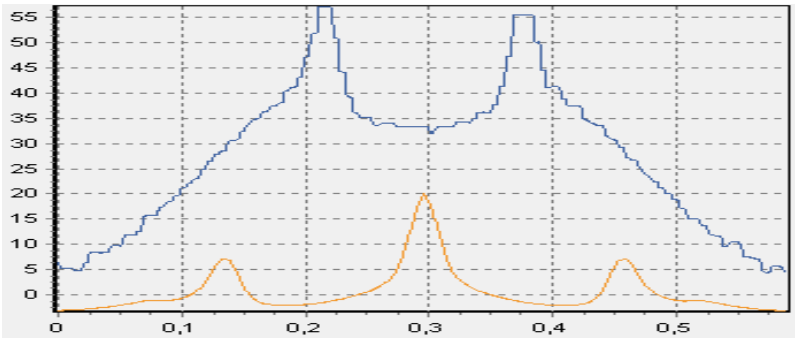


Figure 2. 2-FSK spectral fingerprint.

A review of available sources and scientific publications on this topic revealed that existing implementation approaches do not fully meet the requirements.

The development of a synthesizer capable of generating a signal with the above characteristics and allowing real-time parameter variation – essential for testing the developed direction-finding algorithms – was carried out in the GNU

Radio Companion (GRC) environment using Python and an available GRC block library.

During the formation of the functional scheme (**Figure** 3), the required structure of the FHSS signal synthesizer was determined to meet the requirements. The 2-FSK signal generator block from the GRC library is used as the primary signal source, with parameters defining a single channel's frequency bandwidth. A low-pass filter suppresses high-frequency spectral components. The carrier frequency hopping is implemented in Python using a pseudo-random number generator and an algorithm that controls frequency switching based on input parameters such as frequency range and the number of FHSS channels. The hopping rate is set in the GRC environment as an external trigger for cyclically calling the frequency-switching block. The synthesized signal is shifted into the high-frequency range using a non-recursive frequency-shifting filter from the GRC library.

Synchronization and packet skipping of FHSS signals are implemented using Python. This functional block acts as a controlled attenuator, using an external trigger and an embedded pseudo-random number generator. Considering the required packet gaps level as an input parameter, it either suppresses or allows FHSS packets to pass through the output of the FIR filter without distortion.

To simulate real-world radio wave propagation conditions more accurately, the synthesized FHSS signal is mixed with additive white Gaussian noise (**Figure** 4). The system is loaded with a virtual transmission path block.

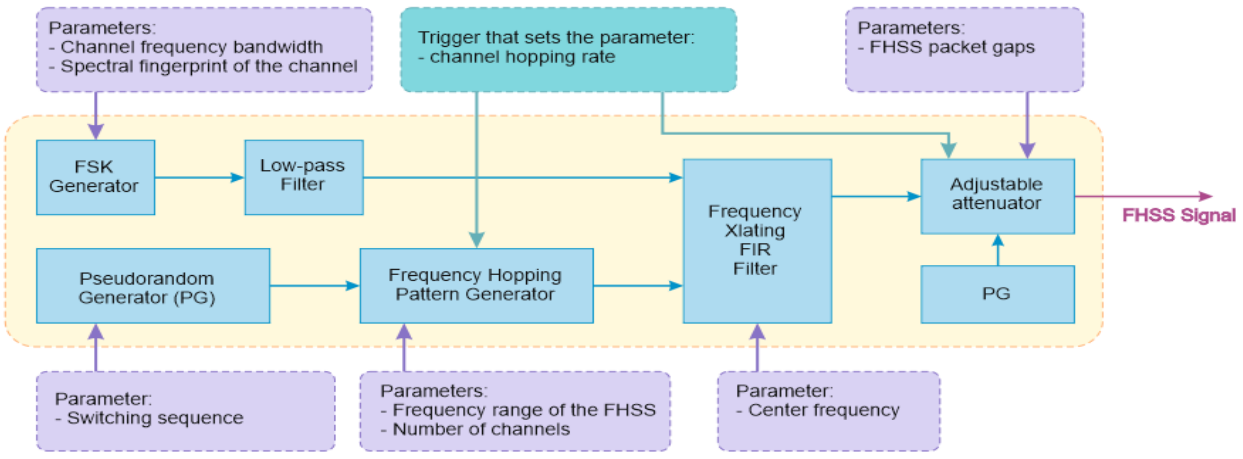


Figure 3. Functional block diagram of the developed synthesizer with the parameters and synchronization paths.

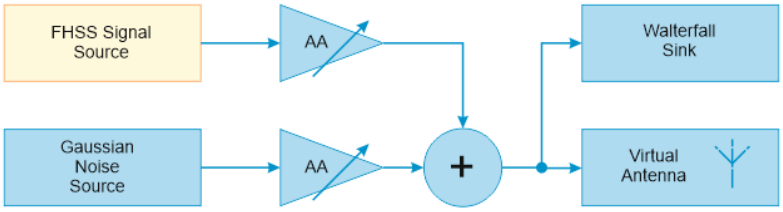


Figure 4. A block diagram of the developed synthesizer.

Conclusion. Spectrograms of FHSS signals synthesized by the developed system with various input parameter settings are presented (**Figure** 5). In addition to the specified settings, the synthesizer and noise generator have independent adjustable amplifiers (AA), enabling control over the signal and noise amplitudes and their ratio. This allows for simulation of changes in the distance to the signal source or the effect of antenna rotation – specifically, the dependence of received signal amplitude on the direction of arrival due to the antenna's directional pattern.

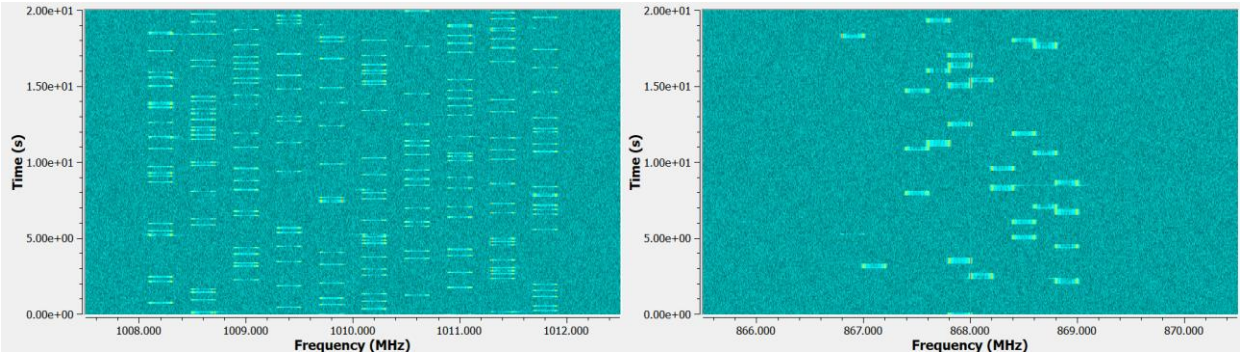


Figure 5. Spectrograms of the synthesized FHSS signals.

The provided spectrograms demonstrate that the overall appearance of the synthesized signal closely matches real FHSS signal recordings with similar characteristics. This confirms its suitability as a test input signal for developing direction-finding algorithms for spread-spectrum signal sources.

References

1. Коваленко, І. Л., Мовчанюк, А. В. (2025). Непараметричний амплітудний метод виявлення сигналів з псевдовипадковим перелаштуванням робочої частоти з низькими обчислювальними витратами. Вісті вищих учбових закладів. Радіоелектроніка. https://doi.org/10.20535/S0021347024090012
2. Коваленко І. Л.; Мовчанюк А. В. Розробка непараметричного амплітудного методу виявлення сигналів з псевдовипадковим перелаштування робочої частоти з низькими обчислювальними витратами. XIII-th International scientific and technical conference «Radioengineering Problems, Signals, Devices and Systems». Kyiv, November, 27 – 28, 2024: conference proceedings — Kyiv: 2024.
3. Solomontan, T. (2023) ‘Learning Frequency Hopping Spread Spectrum (FHSS) with GNU Radio’, Medium, August 3. Available at: https://medium.com/@solomontan_68263/learning-frequency-hopping-spread-spectrum-fhss-with-gnu-radio-7b1ab34b1b10
4. Agrim9 (н.д.) FHSS GNU Radio. Available at: https://github.com/Agrim9/FHSS_GNUradio
5. Narayan, K & Aswathy, P & Ganganna, Shivaprakash & S L, Nisha. (2022). Design and implementation of Polyphase based FHSS modulator using GNU Radio and SDR. 187-192. 10.1109/I4C57141.2022.10057873.
6. Bharadwaj, Sippee. (2015). Review of the literature of FHSS Transmitter. 10.13140/RG.2.1.1064.1762.

UDC 621.391.3

USING OF OPEN-SOURCE DIGITAL MAPS FOR ELECTRO-MAGNETIC WAVES PROPAGATION CALCULATION

Trubarov I.V.
National Technical University of Ukraine
" Igor Sikorsky Kyiv Polytechnic Institute "
E-mail:trubarov.i@gmail.com

ВИКОРИСТАННЯ ЦИФРОВИХ МАП, ОТРИМАНИХ З ВІДКРИТИХ ДЖЕРЕЛ, ДЛЯ РОЗРАХУНКІВ ПОШИРЕННЯ ЕЛЕКТРОМАГНІТНИХ ХВИЛЬ

Розглянуто можливість використання відкритих растрових цифрових картографічних даних для розрахунку поширення електромагнітних хвиль. Надано основні критерії вибору цифрових мап. Наведено порівняння цифрових мап, отриманих шляхом використання різних технологій зондування земної поверхні.

Digital maps are widely used for the numerical estimation of the signal level in different communication systems. The mostly used applications of such calculations include the calculation of the following parameters of the radio communication links: signal level and quality parameters. The calculations are performed over raster digital map layers. The result of such calculations contains the value of a required parameter for each pixel in the map layer. Such calculations make sense in case of a sufficiently sophisticated electromagnetic waves propagation model is used to properly take into account the terrain substrate over the radio communication link.

In this paper, the possibility of using of open-source digital surface maps for different parameters of radio links is considered. For estimation of signal level, different specific values may be calculated depending on the type of the communication links. For instance, for mobile communication networks, RSSI (received signal strength indicator) parameter is calculated for GSM or UMTS networks [1], and RSRP (reference signal received power) parameter is calculated for LTE networks [2]. As a quality parameter, SNIR (Signal-to-interference-plus-noise ratio) parameter is used for GSM and UMTS networks, whereas RSRQ (reference signals received quality) parameter is used for LTE networks.

The results of such calculations are typically used in the following operations: planning of radio communication networks, control the quality and availability of existing mobile radio networks, electromagnetic compatibility assurance tasks and for the estimation of power budget during the process of design of microwave line-of-sight point-to-point links [3].

The results of abovementioned calculations are typically presented as coverage raster digital map layers. To provide signal propagation calculations, different electromagnetic waves propagation models are used. One of the key factors that affects the propagation of electromagnetic waves is terrain substrate. Terrain is modelled by the elevation model.

A digital map that presents the elevation model is a raster digital map layer, each pixel of which contains the value of elevation over the reference surface. There are two types of such digital maps: digital elevation map (DEM) and digital surface map (DSM).

A DEM contains the bare-Earth surface, without all natural and built features. A DSM contains both the natural and built/artificial features of the environment. In particular, while a DEM contains only the Earth surface, a DSM also takes into account forests, buildings, other artificial objects etc. Evidently, for precise diffraction calculation, DSM is required.

In commercial software that is aimed at electromagnetic waves propagation calculation, the three separate raster digital map layers are used to support the calculation: a DEM, a layer that contains the heights of natural and artificial object on the surface of Earth and a clutter layer. Clutter layer is a raster layer of the same dimensions as DEM. It contains the information about the type of terrain for each pixel, for example: water, forest, concrete buildings etc. The clutter layer information allows to take into account the impact of the surface type. It implies using of quite sophisticated propagation models that allow to take into account this information for more precise calculation.

As a source of DEMs and DSMs, remote Earth sensing data are used. The corresponding satellite missions employ different types of radars and lidars. Since different types of objects manifest various reflection capability in different frequency bands, it is possible to build both DEMs and DSMs on the results of the measurements, if the reflection coefficient data are taken from different sensing tools on the board of a satellite.

For the electromagnetic wave propagation calculation, typically commercial software is used, and commercial digital map layers are also prepared. However, the open-source DEM and DSM data that are available on the Internet can be used for the calculations. As an example, two data sources were considered, as follows:

– Shuttle Radar Topography Mission (SRTP) [4]. The pixel size is 30 (from North to South) by 20 (from East to West) meters.

– Advanced Land Observing Satellite (ALOS) mission. ALOS Global Digital Surface Model "ALOS World 3D - 30m (AW3D30)" [5]. The pixel size is 30 (from North to South) by 20 (from East to West) meters.

It is important to understand which type of digital map, DEM or DSM, is presented by a map source. For example, Fig. 1 and Fig. 2 contain the result of the comparison of the two abovementioned maps.

In Fig. 1, the test line for comparison is created. The line presents the radio link path to be analyzed in terms of radio wave propagation. For the comparison, an urban area was selected.

In Fig. 2, the profiles, built for the test line using SRTM and ALOS data sources, are presented. As it can be seen, the SRTM data (red line in Fig. 1) represent a DEM, whereas ALOS data represent a DSM. Therefore, ALOS data shall be chosen for electromagnetic wave propagation calculation.

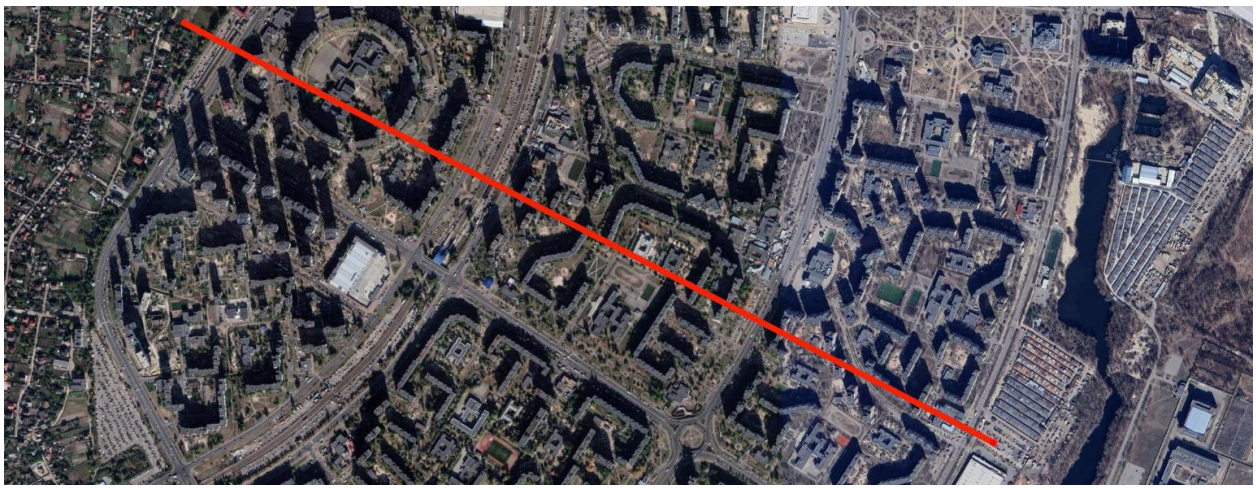


Fig. 1. Test line that simulates the radio waves propagation path for a radio link.

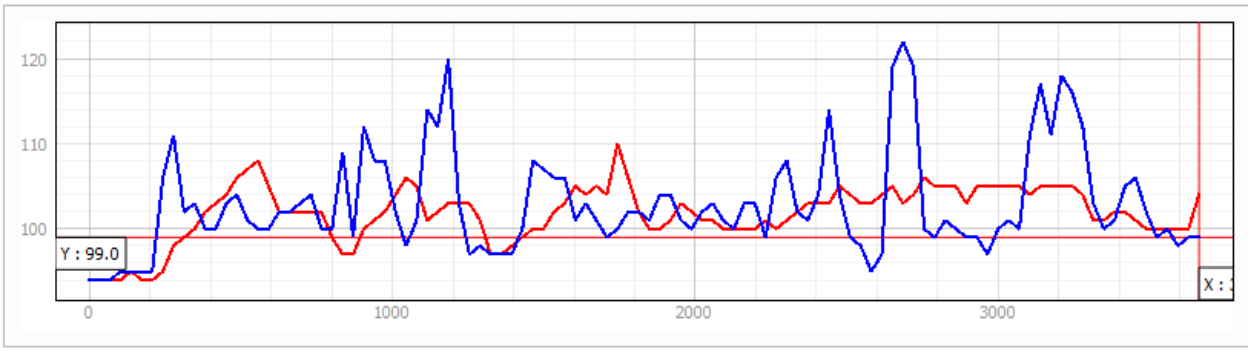


Fig. 2. Profiles of the test line, built using SRTM (red line) and ALOS (blue line).

The drawback of using open-source DSMs is the absence of clutter layer, which leads to using of the simplified propagation models that don't take into account the nature of the on-surface objects.

The strength of using open-source DSMs is using only a single value for each map pixel, which contains the total height of the surface. Therefore, there is no need to use additional map layers containing the heights of the on-surface objects.

Different comparison operations have shown that ALOS data correctly take into account different terrestrial objects, such as forests, separate trees, buildings etc. Therefore, ALOS digital map can be used for electromagnetic wave propagation calculation.

References

1. Säily, M., Sibire, G., Riddington, E. GSM/EDGE: Evolution and Performance. – Wiley, 2011
2. Sesia, S., Toufik, I., Baker, M. LTE – The UMTS Long Term Evolution: From Theory to Practice (2nd ed.). – Wiley, 2011.
3. Recommendation ITU-R P.530: Propagation data and prediction methods required for the design of terrestrial line-of-sight systems". – https://www.itu.int/rec/R-REC-P.530-18-202109-I/en
4. https://www.earthdata.nasa.gov/data/instruments/srtm
5. https://www.eorc.jaxa.jp/ALOS/en/dataset/aw3d30/aw3d30_e.htm

UDC 621.391.3

ELECTROMAGNETIC WAVES DIFFRACTION ESTIMATION FOR MICROWAVE LINE-OF-SIGHT LINKS USING OPEN-SOURCE DIGITAL SURFACE MAPS

Trubarov I.V.
National Technical University of Ukraine
" Igor Sikorsky Kyiv Polytechnic Institute "
E-mail:trubarov.i@gmail.com

ОЦІНКА ДИФРАКЦІЇ ЕЛЕКТРОМАГНІТНИХ ХВИЛЬ ДЛЯ РАДІОРЕЛЕЙНИХ ЛІНІЙ З ВИКОРИСТАННЯМ ЦИФРОВИХ МАП ПОВЕРХНІ, ОТРИМАНИХ З ВІДКРИТИХ ДЖЕРЕЛ

Розглянуто можливість використання растрових картографічних шарів, отриманих з відкритих джерел, для розрахунку факторів поширення радіохвиль. Аналіз зосереджено на оцінці дифракції електромагнітних хвиль на елементах земної поверхні як одного з ключових факторів, що впливають на енергетичний бюджет радіолінії. Розглянуто алгоритм розрахунку профіля радіолінії на основі растрового картографічного шару.

Microwave line-of-sight (LoS) communication links are essential for high-capacity wireless networks. However, signal propagation in such systems is affected by obstacles that cause diffraction, leading to signal attenuation and degradation [1]. Accurate diffraction analysis is crucial for optimal link design, and Digital Surface Maps (DSMs) have become an essential tool in this process.

DSMs provide high-resolution raster data representing terrain and built structures, which allows to model the exact propagation environment. By integrating DSMs into Geographic Information Systems (GIS), diffraction calculations can be performed with greater accuracy, ensuring that potential obstructions are identified and mitigated.

In this paper, using open-source DSMs is considered for diffraction estimation as a part of the design of line-of-sight microwave links. The International Telecommunication Union (ITU) provides several diffraction models suitable for microwave link planning. The most used of them include the following approaches:

– Knife-Edge Diffraction Model [2] is a simple yet effective method assuming a sharp-edged obstacle. While useful for basic calculations, it does not account for complex terrain variations.

– Multiple Knife-Edge Model [2] extends the single knife-edge approach to multiple obstacles, offering improved accuracy in mountainous or urban environments.

– Deygout Method [2] uses an iterative approach that estimates diffraction loss over multiple obstacles by identifying a dominant edge and computing successive diffraction effects.

– Bullington Method [2] is a simplified model that approximates

multiple obstacles as a single equivalent obstruction, reducing computational complexity.

By using DSMs, it is possible to automate the selection of relevant diffraction models and optimize antenna location to minimize signal degradation. Modern GIS tools integrate DSM data with ITU-compliant algorithms, improving reliability and efficiency in microwave network planning. The combination of high-resolution DSMs and advanced diffraction models significantly enhances the accuracy of LoS assessments, reducing deployment costs and ensuring robust communication links.

The procedure of power budget estimation of a LoS link requires generation a surface profile showing the surface heights over the signal path [3]. A DSM is a raster digital map layer, which contains values of surface height over the reference level for each raster pixel, which can be used for building a profile for a microwave link. Fig. 1 shows the fragment of a DSM, used for modelling the signal path for a microwave LoS link.

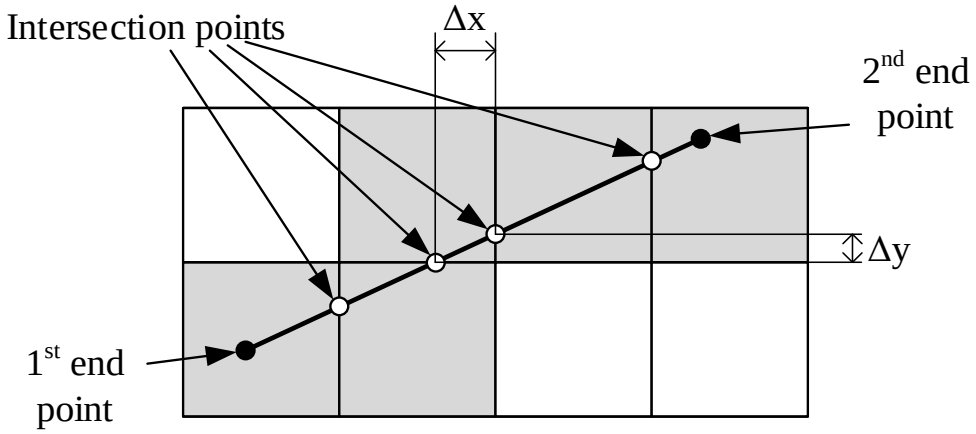


Fig. 1. Building a surface profile for a microwave LoS link.

The algorithm for building a profile includes the following steps:

– Building the line between the end points of the microwave link and calculation of the intersection points (see Fig. 1).

– Checking if the Δx and Δy (see Fig. 1) exceed the pre-defined threshold.

– Basing on the number of the intersection points, calculation of the number of pixels along the link path.

– Then, the profile as a dependence of surface height (Y axis in Fig. 2) versus distance from the 1st end point (X axis in Fig. 2) can be built. The points for X axis are taken as a uniform array consisting of the points (d_i, h_i), where d_i is the distance from the 1st end point of the link, and h_i is a surface height of this point. The distance values are calculated as follows: $d_i = i \cdot \frac{D}{N-1}$, where i is the point number, D is the distance between 1st end point and 2nd end point and N is the number of raster pixels along the path (shown as grey squares in Fig. 1).

– As a result, a link profile can be built (see Fig. 2).

For the calculations, open-source DSM can be used. In this work, the ALOS

digital maps [4] were implemented. These maps have 30 x 20 m resolution and take into account not only the Earth elevation, but also the height of terrestrial objects, such as forests, buildings etc. A drawback of using the open-sours DSMs is absence of clutter layer, which makes it impossible to consider differences in electromagnetic wave propagation in different environment (for instance, concrete, wood etc.).

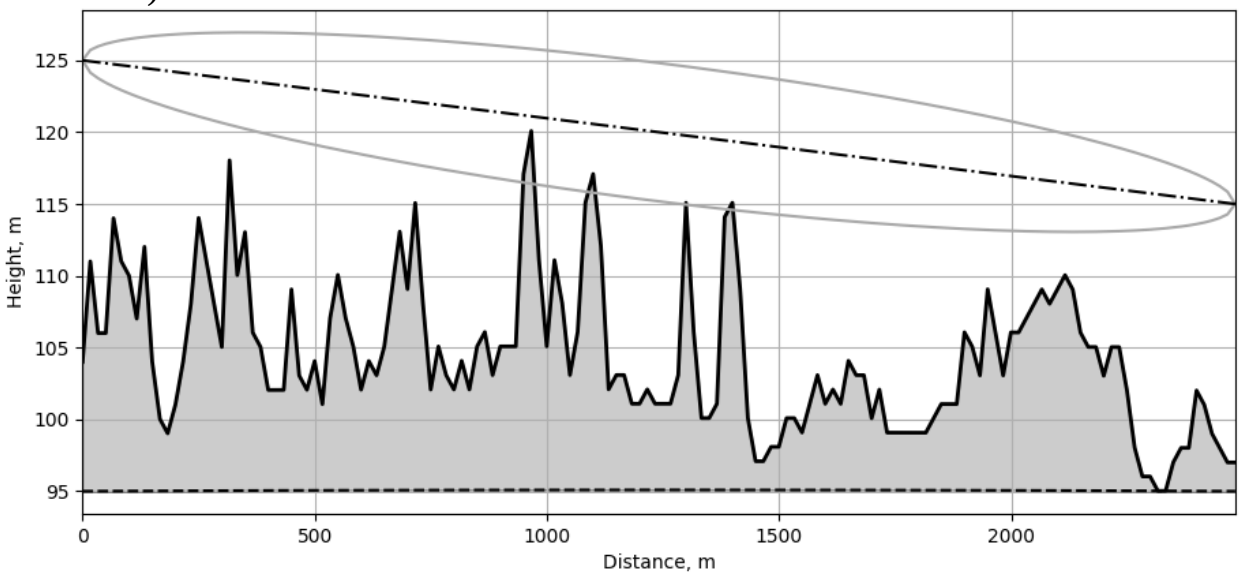


Fig. 2. Example of a microwave link profile.

To check the presented approach, Deygout method was used. The strength of this method is its ability to consider not only one or two obstacles along the wave path, but all obstacles that are essential for diffraction. As an example, for the link shown in Fig. 2, the value of power loss due to diffraction, calculated using Deygout method, is 8.9 dB. To provide the calculations, Python programming language was used, which makes the presented calculation approach independent from any commercial software.

It was shown that using ALOS DSMs and Deygout diffraction estimation approach allow to properly consider the diffraction along the signal propagation path in microwave LoS communication links. The calculations were performed for different types of terrain (rural and urban), different number of obstacles on the propagation path, various antenna heights. Good alignment with diffraction theory was observed for all combinations, which allows to consider the proposed approach reliable for the microwave LoS links planning and design.

References

1. Angueira, Pablo, and Juan Romo. Microwave Line of Sight Link Engineering. John Wiley & Sons, 2012.
2. Recommendation ITU-R P.526-10: Propagation by diffraction. – https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.526-10-200702-S!!PDF-E.pdf
3. Recommendation ITU-R P.530: Propagation data and prediction methods required for the design of terrestrial line-of-sight systems. – https://www.itu.int/rec/R-REC-P.530-18-202109-I/en
4. https://www.eorc.jaxa.jp/ALOS/en/dataset/aw3d30/aw3d30_e.htm

УДК 621.396

СИСТЕМА ПЕРЕДАВАННЯ ТА ПРИЙОМУ СИГНАЛУ ТЕЛЕВІЗІЙНОГО МОВЛЕННЯ В ТЕРАГЕРЦОВОМУ ДІАПАЗОНІ ЧАСТОТ

Авдєєнко Г.Л., Наритник Т.М., Буглак А.О.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: django2006@gmail.com

SYSTEM FOR TRANSMISSION AND RECEPTION OF TELEVISION BROADCAST SIGNAL IN THE TERAHERTZ FREQUENCY RANGE

A variant of the layout of the DVB-S/S2 television broadcasting signal transmission and reception system in the terahertz frequency range is presented. The results of laboratory studies have shown the possibility of transmitting single- and multiprogram high-definition (HD) streams in 2K and 4K formats through this system.

На сьогоднішній день в світі завдяки прогресу в галузі мікроелектроніки та практичного освоєння окремих ділянок діапазону міліметрових хвиль (30-300 ГГц) спостерігається поступовий перехід до впровадження технологій мобільного зв'язку 5G, які потенційно будуть здатні забезпечити абонентам мережі швидкість передачі даних до 10 Гбіт/с та часову затримку на рівні 5…20 мс. Також, на теперішній час такими провідними виробниками обладнання для радіорелейних ліній зв'язку (РРЛЗ) як SAF Tehnika, Ceragon та ін. розроблено лінійку радіорелейних станцій Е-діапазону (71-76 ГГц, 81-86 ГГц), які здатні забезпечити передавання та прийом інформаційних потоків на швидкості до 10 Гбіт/с при частотній смузі стовбура 2000 МГц та модуляції 128-QAM на відстань до кількох кілометрів, що цілком достатньо для того, щоб побудувати в межах великих міст транспортну мережу для з'єднання між собою базових станцій мережі 5G [1,2]. Крім того, такі РРЛЗ можуть розглядатися як альтернатива прокладанню волоконно-оптичних ліній зв'язку або їх резервування.

Велика увага вчених провідних країн світу останні кілька десятиліть також спрямована на дослідження та освоєння в різних сферах людської діяльності (бездротовий зв'язок, радіолокація, медицина тощо) короткохвильової частини діапазону міліметрових хвиль (f > 100 ГГц), яку прийнято також відносити до терагерцового діапазону (0,1 – 10 ТГц). У цьому діапазоні вже розроблено низьку макетних зразків бездротової передачі інформації, які на безліцензійній основі здатні забезпечувати завадозахищену передачу інформаційних потоків в мережах типу «точка-точка», «точка-багатоточка» зі швидкістю кілька одиниць-десятків Гбіт/с в межах прямої видимості на відстань до 2...3 км. Наприклад, в роботі [3] представлено макет терагерцової системи зв'язку, яка функціонує в діапазоні 210…230 ГГц і яка здатна передавати цифровий потік даних на швидкості до 2 Гбіт/с на відстань біля 2,03 км при потужності передавача 200 мВт. Варто відмітити, що переважна більшість сучасних публікацій з проєктування дослідних зразків бездротових ліній зв'язку терагерцового діапазону, що

представлена в науковій літературі [3,4], базується на застосуванні оптоелектронного перетворення високостабільних лазерних випромінювань для формування в терагерцовому діапазоні (ТГц) високостабільного несучого коливання гетеродину та його модуляції за допомогою оптичних модуляторів Маха-Цендера для формування модульованого радіосигналу ТГц діапазону.

У даних тезах на відміну від публікацій [3,4] представлено розроблений науковцями кафедри ТК ННІТС варіант макету системи передавання та прийому сигналу телевізійного мовлення стандарту DVB-S/S2 діапазону 130 ГГц, в якому передавальний та приймальний модуль реалізовано з використанням гетеродинів, несуча частота яких f = 64,8 ГГц сформована шляхом послідовного множення частоти термостатованого опорного кварцевого генератора NI-100M-2900 з вихідною частотою f_0 = 100 МГц та відносною нестабільністю частоти $\delta f = 5 \cdot 10^{-8}$ в 648 разів (Рис.1).

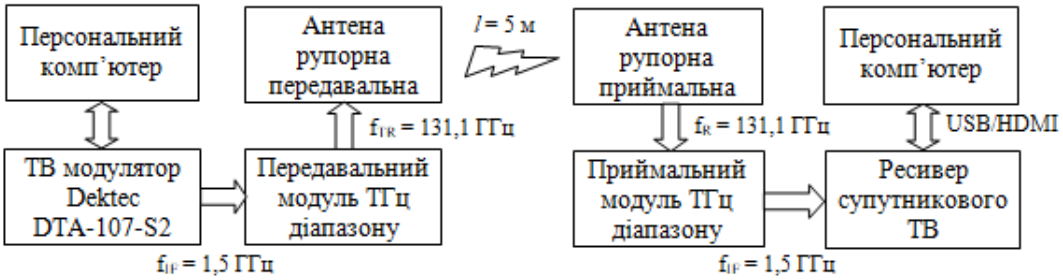


Рис.1. Структурна схема макету системи передавання
та прийому сигналу ТВ мовлення стандарту DVB-S/S2.

Формування радіосигналу ТГц діапазону з несучою частотою f_{TR} = 131,1 ГГц на передавальній стороні макету (рис.1) здійснювалось шляхом перетворення по частоті радіосигналу ТВ мовлення стандарту DVB-S/S2, який генерувався на несучій частоті f_{IF} = 1,5 ГГц за допомогою PCI-плати ТВ модулятора Dektec DTA-107-S2, яка була підключена до материнської плати персонального комп'ютера, з одно- або багатопрограмного потоку ТВ мовлення стандарту стиснення H.264, який був попередньо записаний на SSD-диск ПК у вигляді файлу з розширенням *.ts. Також файл тестового транспортного потоку для ТВ модулятора Dektec може бути сформований з будь-якого відеозапису ТВ програми або відеоконтенту (наприклад, попередньо завантаженого з Youtube) за допомогою функціоналу програмного застосунку ffmpeg [5] відповідно до рис.2.

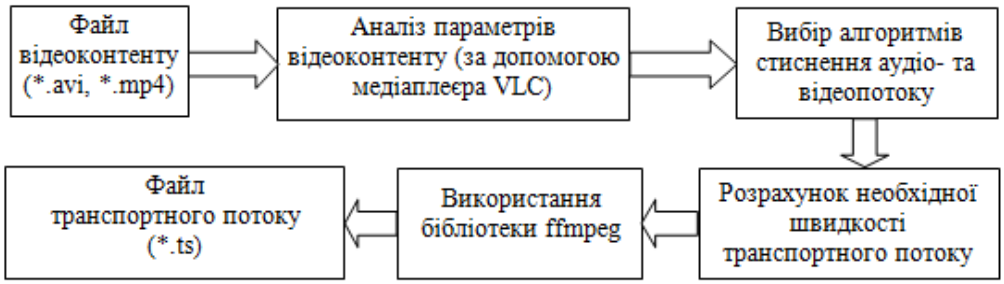


Рис.2. Формування транспортного потоку для ТВ модулятора
Dektec за допомогою програмного застосунку ffmpeg.

Для контролю параметрів сформованого на проміжній частоті

f_{IF} = 1,5 ГГц ТВ модулятором Dektec за допомогою програмного забезпечення StreamXpress (рис.3) радіосигналу ТВ мовлення стандарту DVB-S/S2, з другого ВЧ-виходу PCI-плати модулятора сигнал подавався на ВЧ-вхід PCI-плати супутникового ресивера OMICOM S2, який був доданий до материнської плати ПК передавальної сторони і який контролювався програмним пакетом CrazyScan [6] (рис.4).

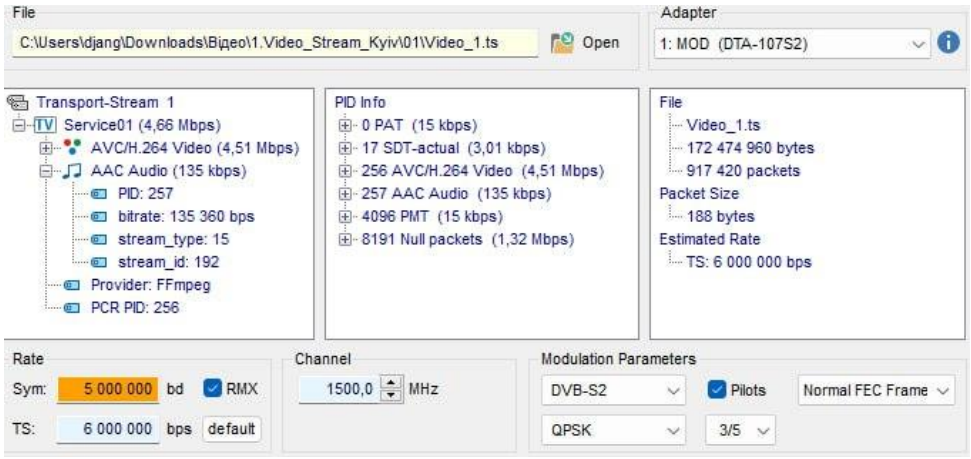


Рис.3. Вікно програмного пакету StreamXpress для формування модулятором Dektec радіосигналу ТВ мовлення стандарту DVB-S/S2 на проміжній частоті 1,5 ГГц.

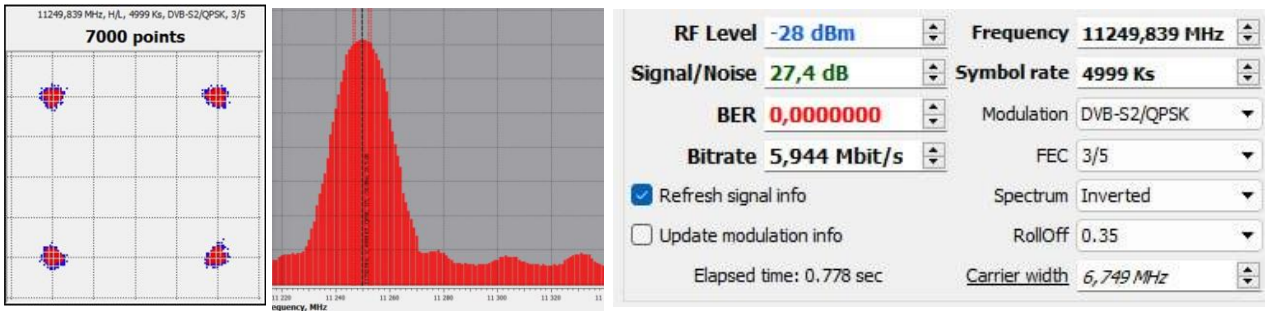


Рис.4. Вікно програмного пакету CrazyScan для контролю параметрів сформованого радіосигналу ТВ мовлення стандарту DVB-S/S2 на проміжній частоті 1,5 ГГц.

Сформований радіосигнал ТГц діапазону з вихідною потужністю -13дБм та несучою частотою 131,1 ГГц випромінювався за допомогою конічної рупорної антени в лабораторних умовах в напрямку приймальної частини макету, яка була розташована на відстані біля 5 м від передавальної (рис.5). Прийом радіосигналу ТГц діапазону здійснювався за допомогою рупорної антени та приймального модуля ТГц діапазону, який виконував перетворення частоти несучої f_{TR} = 131,1 ГГц на проміжну несучу f_{IF} = 1,5 ГГц (рис.6). Далі радіосигнал проміжної частоти надходив на ВЧ-вхід стандартного ресиверу (тюнеру) супутникового ТВ мовлення, який через інтерфейс HDMI підключався до телевізора або за допомогою конвертора HDMI/USB до ПК, в якому відеозображення та звуковий супровід переданої ТВ програми відтворювалися за допомогою медіаплеєра VLC або PotPlayer. Крім того, для контролю параметрів прийнятого ТВ сигналу стандарту DVB-S/S2 через 3-х канальний дільник потужності ТВ сигналу до виходу приймального модуля ТГц підключався аналізатор спектра Signal Hound USB-SA44B та контрольний ресивер Prof7500.

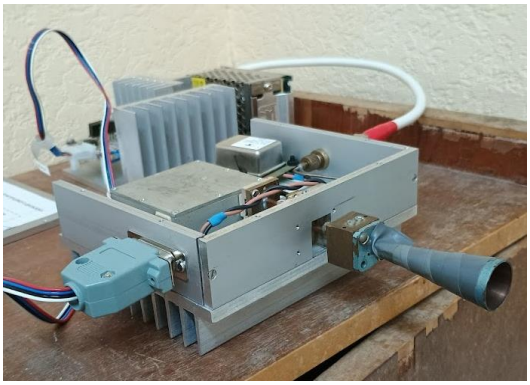


Рис.5. Фотографія передавального модуля ТГц діапазону.

Рис.6. Фотографія приймального модуля ТГц діапазону.

На рис.7 зображено спектр та сигнальне сузір'я, а на рис.8 параметри прийнятого радіосигналу ТВ мовлення з несучою частотою f_{IF} = 1,5 ГГц на виході приймального модуля ТГц діапазону.

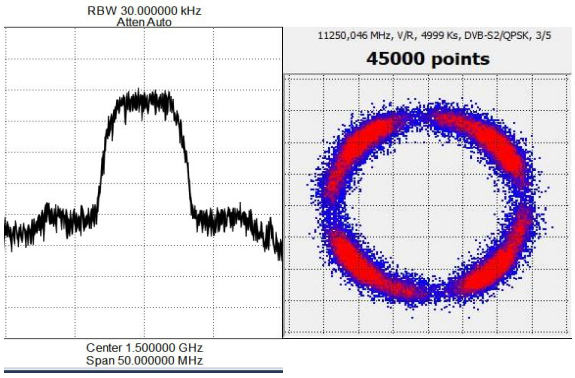


Рис.7. Спектр та сигнальне сузір'я прийнятого радіосигналу на приймальній стороні макету.

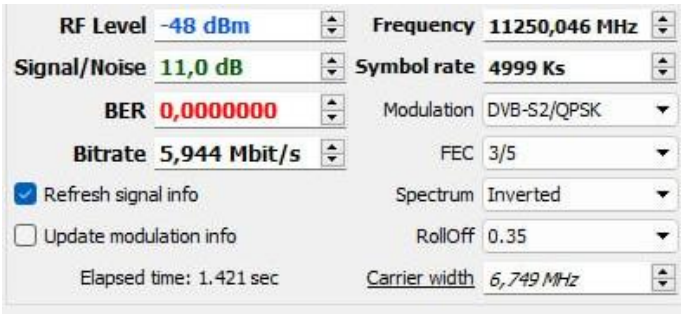


Рис.8. Параметри прийнятого радіосигналу на приймальній стороні макету.

Порівняння отриманих параметрів радіосигналу ТВ мовлення на вході передавального та виході приймального модулів ТГц діапазону (рис.4, рис.7, рис.8) показує, що сигнальне сузір'я модуляції QPSK на приймальній стороні спотворене фазовими шумами, відношення сигнал/шум зменшилось з 27 дБ до 11 дБ, проте ймовірність бітової помилки BER залишилась на рівні 10^{-7}, що було достатнім для якісного відтворення зображення ТВ програми без спотворень.

Література

1. Integra-E series. URL: https://old.saftehnika.com/en/integrae (дата звернення: 18.03.2025).
2. EtherHaul Kilo 8000 Series URL: https://www.ceragon.com/products/etherhaul-kilo-8000 (дата звернення: 18.03.2025).
3. Sen, P., Siles, J.V., Thawdar, N. et al. Multi-kilometre and multi-gigabit-per-second sub-terahertz communications for wireless backhaul applications. Nat Electron 6, 164–175 (2023). https://doi.org/10.1038/s41928-022 -00897-6
4. H. Avdieienko, A. Slyvka, O. Dykyi. Terahertz communication systems for high-definition and ultra-high-definition television transmission. Information and telecommunication sciences - 2022. - Vol.13. - №1. - pp. 4-13.
5. FFmpeg. URL: https://www.ffmpeg.org/ (дата звернення 18.03.2025р).
6. CrazyScan. URL: https://sourceforge.net/projects/crazyscan/ (дата звернення 18.03.2025р).

УДК 004.7:621.39

РОЗРОБЛЕННЯ КОМПЛЕКСУ ЛАБОРАТОРНИХ РОБІТ З ФОРМУВАННЯ ТА ДОСЛІДЖЕННЯ СИГНАЛІВ ТЕХНОЛОГІЙ МОБІЛЬНОГО ЗВ'ЯЗКУ З ВИКОРИСТАННЯМ ОБЛАДНАННЯ ROHDE & SCHWARZ

Авдєєнко Г.Л., Пікалов А.А.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: django2006@ukr.net, pikalov.andrey@lll.kpi.ua

DEVELOPMENT OF A COMPLEX OF LABORATORY WORK ON THE FORMATION AND RESEARCH OF SIGNALS OF MOBILE COMMUNICATION TECHNOLOGIES USING ROHDE & SCHWARZ EQUIPMENT

The study investigates the impact of signal imperfections in the transmitter, such as I/Q imbalance, phase noise, and radio channel parameters, including multipath propagation and interference, on the quality of the received signal. Experimental measurements were conducted using the R&S®SMJ100A vector signal generator and the R&S®FSG-13 spectrum analyzer. A set of laboratory exercises for students in the field of wireless technologies is proposed to assess the impact of signal distortions and develop methods for their compensation.

Мобільні мережі становлять основу сучасних телекомунікацій з розвитком технологій 4G, 5G та майбутнього 6G, забезпечуючи високу швидкість, пропускну здатність і мінімальні затримки. Складні умови радіоканалу через багатопроменеве поширення, інтерференцію та перешкоди потребують детального дослідження параметрів сигналів.

Розроблений лабораторний комплекс для студентів телекомунікаційних спеціальностей використовує професійне обладнання Rohde & Schwarz (векторний генератор R&S®SMJ100A та аналізатор спектру R&S®FSG-13), що дозволяє набути практичних навичок роботи з промисловим вимірювальним обладнанням та дослідити вплив різних факторів на сигнали безпроводових систем.

Комплекс спрямований на вирішення проблеми недостатньої практичної підготовки фахівців у галузі мобільного зв'язку. Еволюція від 5G до 5G-Advanced та підготовка до 6G вимагають розуміння принципів формування та обробки сигналів у складних радіоканалах, включаючи спотворення у передавачах (розбаланс I/Q, фазові шуми) та каналах поширення (багатопроменевість, інтерференція).

Однак, існуюча система підготовки спеціалістів у галузі телекомунікацій часто зіштовхується з проблемою недостатньої практичної складової. Теоретичні знання, отримані студентами, не завжди підкріплюються практичними навичками роботи з реальним обладнанням та дослідження реальних сигналів. Це призводить до розриву між академічною підготовкою

та вимогами індустрії. Саме на вирішення цієї проблеми спрямований розроблений комплекс лабораторних робіт, який дає можливість студентам працювати з професійним обладнанням та досліджувати реальні ефекти, що виникають у системах мобільного зв'язку.

Вибір обладнання Rohde & Schwarz для створення лабораторного комплексу обумовлений рядом вагомих факторів:

1. **Промисловий стандарт якості**: Rohde & Schwarz є світовим лідером у галузі виробництва вимірювального обладнання для телекомунікацій, що широко використовується провідними компаніями та дослідницькими центрами. Обладнання цієї компанії вважається еталонним, що дозволяє студентам отримати досвід роботи з найкращими професійними інструментами.

2. **Технологічна актуальність**: Компанія постійно оновлює своє обладнання та програмне забезпечення відповідно до розвитку технологій зв'язку. Зокрема, як було зазначено, на MWC 2025 Rohde & Schwarz представила інноваційні рішення під гаслом «Enabling Connections, Empowering Innovations», що демонструє фокус компанії на перехід від 5G до 5G-Advanced та розробку технологій 6G.

3. **Функціональна гнучкість**: Векторний генератор сигналів R&S®SMJ100A та аналізатор спектру R&S®FSG-13 дозволяють проводити широкий спектр експериментів з різними типами модуляції, стандартами зв'язку та умовами каналу. Це забезпечує можливість створення комплексних та різноманітних лабораторних робіт.

4. **Сумісність зі стандартами**: Обладнання Rohde & Schwarz повністю відповідає міжнародним стандартам зв'язку, включаючи IEEE 802.11, 3GPP 5G NR та інші, що дозволяє проводити дослідження сигналів у повній відповідності до реальних систем.

5. **Програмне забезпечення WINIQSIM2**: Це ПЗ дозволяє моделювати сигнали різних стандартів зв'язку з контрольованими параметрами спотворень, що є необхідним для систематичного дослідження впливу різних факторів на якість сигналу.

Розроблений комплекс лабораторних робіт структурований таким чином, щоб забезпечити поступове ускладнення завдань та охоплення різних аспектів формування та дослідження сигналів.

Кожна лабораторна робота складається з наступних етапів:

1. **Теоретична підготовка**: Студенти ознайомлюються з теоретичними основами досліджуваних явищ, математичними моделями та очікуваними результатами.

2. **Підготовка експерименту**: Налаштування обладнання Rohde & Schwarz згідно з параметрами, визначеними у завданні, програмування векторного генератора сигналів за допомогою WINIQSIM2.

3. **Проведення вимірювань**: Систематичне вимірювання параметрів сигналу при різних рівнях спотворень та умовах каналу.

4. **Аналіз результатів**: Обробка та інтерпретація отриманих даних, порівняння з теоретичними прогнозами.

5. **Розробка рекомендацій**: Формулювання висновків щодо впливу досліджуваних факторів та методів зменшення їх негативного впливу.

Впровадження запропонованого комплексу лабораторних робіт у навчальний процес суттєво підвищить якість практичної підготовки студентів, надаючи їм цінний досвід роботи з професійним обладнанням та можливість застосувати теоретичні знання на практиці. Це сприятиме формуванню важливих професійних компетенцій, включаючи розуміння принципів формування та аналізу сигналів, вміння ідентифікувати й компенсувати різні типи спотворень, а також навички оптимізації параметрів систем зв'язку.

Студенти розвинуть аналітичне мислення, навчаться аналізувати складні взаємозв'язки між параметрами сигналу та характеристиками системи, прогнозувати вплив різних факторів на якість зв'язку. Отримані під час лабораторних робіт результати можуть стимулювати науково-дослідницьку діяльність, стаючи основою для подальших досліджень, курсових та дипломних робіт. Головне, що такий підхід дозволить скоротити розрив між освітою та індустрією, допомагаючи випускникам швидше адаптуватися до роботи в реальних умовах телекомунікаційної галузі.

Розроблений комплекс лабораторних робіт з формування та дослідження сигналів технологій мобільного зв'язку з використанням обладнання Rohde & Schwarz є важливим кроком у напрямку модернізації освітнього процесу підготовки фахівців телекомунікаційного профілю. Він забезпечує систематичне дослідження впливу різних типів спотворень на параметри сигналів та дозволяє студентам набути практичних навичок роботи з професійним обладнанням.

Особливістю запропонованого комплексу є використання високоточного обладнання Rohde & Schwarz, що дає можливість досліджувати тонкі ефекти формування та поширення сигналів, які неможливо вивчити за допомогою спрощених навчальних стендів. Це дозволяє підготувати спеціалістів, здатних ефективно працювати з сучасними та перспективними технологіями мобільного зв'язку.

Впровадження даного комплексу лабораторних робіт сприятиме підвищенню якості освіти, формуванню затребуваних індустрією компетенцій та посиленню конкурентоспроможності випускників на ринку праці.

Література

1. Rohde & Schwarz. R&S®SMJ100A Vector Signal Generator -- Operating Manual.
2. IEEE Std 802.11-2020. IEEE Standard for Wireless Communications.
3. Rappaport T. S. Wireless Communications: Principles and Practice. -- 2nd ed. -- Prentice Hall, 2002.
4. "Enabling Connections, Empowering Innovations": Rohde & Schwarz Presents to the Mobile Industry at MWC 2025. Wireless Design Online, 2025.
5. 3GPP TS 38.211. "NR; Physical channels and modulation". 3rd Generation Partnership Project; Technical Specification Group Radio Access Network.

УДК 629.056.8

ФОРМУВАННЯ СИГНАЛІВ ГНСС GPS З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ SDR ДЛЯ ТЕСТУВАННЯ ПРИЙМАЧІВ СИГНАЛІВ СУПУТНИКОВОЇ РАДІОНАВІГАЦІЇ GPS

Авдєєнко Г. Л., Поворознік М.В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: django2006@gmail.com

GENERATION OF GNSS GPS SIGNALS USING SDR TECHNOLOGY FOR TESTING GPS SATELLITE NAVIGATION RECEIVERS

A variant of a hardware-software GNSS signal generator based on the HackRFOne SDR transceiver for testing GPS receivers in laboratory conditions is presented. The results of the presented research may be useful for developers of satellite radio navigation equipment.

На сьогоднішній день в світі спостерігається широке застосування навігаційної апаратури користувачів (НАК) глобальних навігаційних супутникових систем (ГНСС) GPS, GLONASS, GALILEO, Beidou різних виробників (U-Blox, SimCom, Locosys тощо) в різних сферах діяльності людини: транспорт, промисловість, сільське господарство, безпека та оборона тощо. Тому задача створення недорогих пристроїв генерування сигналів ГНСС для тестування в лабораторних, і, навіть, домашніх умовах розробленої НАК є актуальною та своєчасною. Сучасне професійне обладнання для тестування НАП володіє широким функціоналом і дозволяє одночасно формувати тестові сигнали кількох ГНСС, але коштує достатньо дорого [1]. Альтернативою професійному обладнанню для тестування НАП є формувачі сигналів ГНСС на базі технології програмно-визначувального радіо (SDR), трансивери якої на даний момент часу налічують достатньо широку номенклатуру моделей: BladeRF, HackRF One, USRP, LimeSDR, PlutoSDR та багато інших. Такі SDR-трансивери дозволяють формувати в діапазонах СВ, КВ, УКВ радіосигнали будь-якої бездротової технології шляхом програмування їх ПЛІС відповідним програмним кодом без необхідності змін в апаратній частині трансивера з вихідною потужністю (без застосування підсилювача потужності) не більше 15…20 дБм. Досвід застосування SDR-трансиверів показав, що найбільш простим та універсальним є формування тестових сигналів ГНСС GPS за допомогою програмного застосунку gps-sdr-sim, який легко встановлюється на персональний комп’ютер з операційною системою

Ubuntu [2]. При цьому алгоритм формування тестового сигналу передбачає виконання наступної послідовності дій: 1) вибір на поверхні земної кулі за допомогою картографічного сервісу Google Maps (або будь-якого іншого) точки і зчитування її географічних координат (широта, довгота, висота); 2) завантаження після попередньої реєстрації актуальних ефемерид орбітального угруповання GPS з сайту NASA [3]; 3) формування за допомогою компілятора бінарного файла з вказаними географічними координатами точки розташування відповідної часової тривалості; 4) встановлення бібліотеки драйверів для керування SDR-трансивером; 5) завантаження сформованого бінарного файла до ПЛІС SDR-трансивера (рис.1).

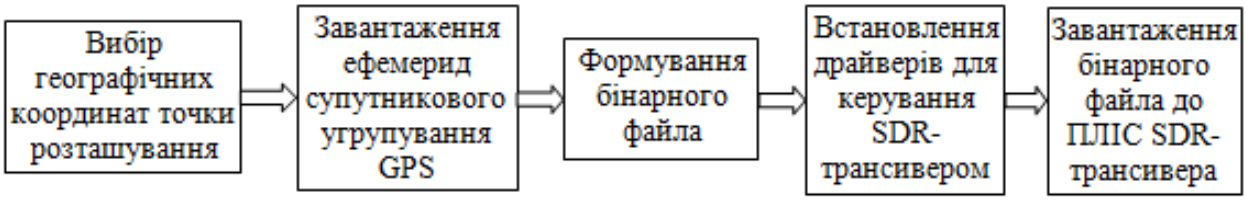


Рис.1. Алгоритм формування тестових сигналів
ГНСС GPS за допомогою бібліотеки gps-sdr-sim.

Структурна схема макету на базі формувача сигналів ГНСС GPS що була використана при проведенні тестування GPS-приймачів показана на рис.2.

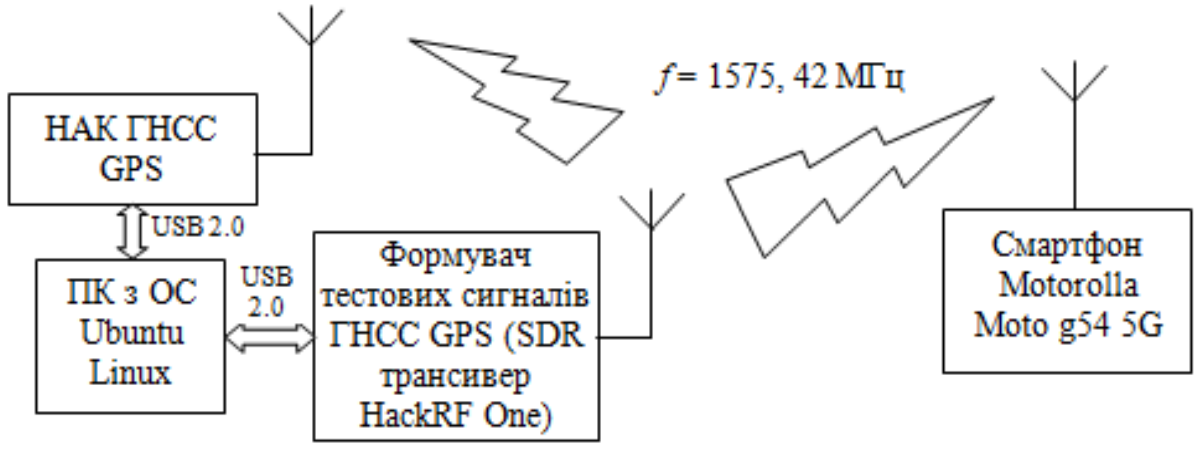
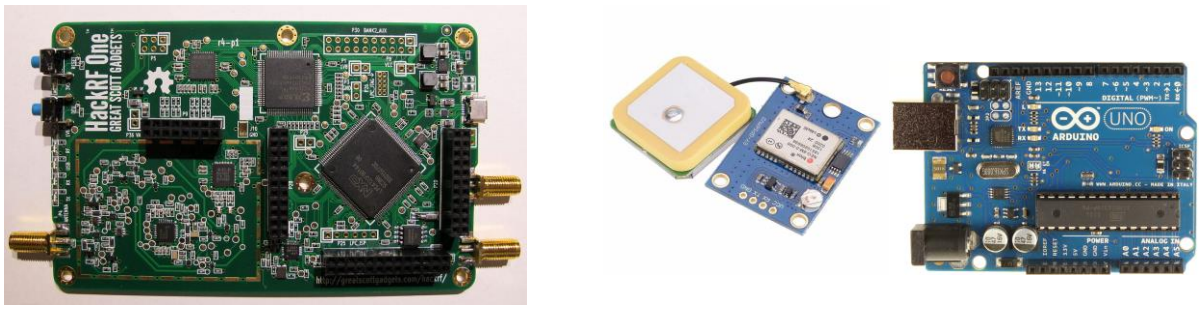


Рис.2. Структурна схема макету для тестування НАК ГНСС GPS.

При проведенні експериментального дослідження з формування сигналів ГНСС GPS з використанням онлайн-сервісу Google Maps було

задано наступні географічні координати точки розташування в межах м. Стокгольм, Швеція: широта Lat = 59.3182415º півн.ш, довгота Lon = 18.0638374 сх.д; висота над рівнем моря H = 200 м. В якості SDR-трансивера було використано трансивер HackRF One (рис.3,а) [4], що підключався повз інтерфейс USB 2.0 до персонального комп'ютера зі встановленою ОС Ubuntu Linux, а в якості НАК, що тестувались – GPS-приймач на базі GPS-модуля U-blox NEO-6M (рис.3,б) [5], який через плату мікроконтроллера Arduino Uno підключався по інтерфейсу USB 2.0 до ПК та смартфон Motorolla Moto g54 5G з вбудованим приймачем сигналів ГНСС GPS/GLONASS/GALILEO/Beidou. Формувач сигналів ГНСС GPS та ресивери, що тестувалися, були рознесені в лабораторному приміщенні один від одного на відстань біля 5 м. Для зчитування навігаційних даних від GPS-приймача на базі GPS-модуля U-blox NEO-6M по протоколу NMEA були використані програмні пакети gpsd та xgps, а для візуального відображення на карті світу точки місцеположення був використаний програмний застосунок marble [6]. Для тестування приймача сигналів ГНСС GPS, що є в складі смартфона Motorolla Moto g54 5G з ОС Android був використаний програмний застосунок GPS Test [7].



а) б)

Рис.3. Основні елементи макету: а) SDR-трансивер HackRF One;
б) GPS-модуль U-blox NEO-6M та мікроконтроллер Arduino UNO.

На рис.4,а відображено результати визначення координат місцеположення в програмному пакеті xgps при тестуванні GPS-приймача на базі GPS-модуля U-blox NEO-6M, а на рис.4,б – результати визначення координат місцеположення в програмному пакеті GPS Test при тестуванні навігаційного приймача, вбудованого в смартфон Motorolla. Порівняння отриманих результатів показало, що обидва навігаційні приймачі могли розпізнати сформовані тестові сигнали ГНСС GPS і надійно визначали задані координати місцеположення.

xgps localhc

File View Units Step of Grid Help

Satellite List

	svid	sig	PRN	Elev	Azim	SNR	qual	prRes	Used
GP	4		4	75.0	105.0	54.0			Y
GP	9		9	65.0	226.0	53.0			Y
GP	19		19	7.0	244.0	44.0			Y
GP	28		28	5.0	31.0	43.0			Y
GP	29		29	0.0	10.0	43.0			Y
GP	3		3	33.0	120.0	0.0			N
GP	6		6	0.0	0.0	51.0			N
GP	7		7	0.0	0.0	45.0			N
GP	11		11	0.0	0.0	48.0			N
GP	16		16	0.0	0.0	44.0			N
GP	20		20	0.0	0.0	44.0			N
GP	31		31	0.0	0.0	47.0			N

а)

б)

Рис.4. Результати тестування приймачів сигналів ГНСС GPS: а) U-blox; б) Motorolla.

Література

1. Labsat. Compact yet powerful GNSS testing solutions URL: https://www.labsat.co.uk/index.php/en/ (дата звернення: 12.03.2025).
2. GPS-SDR-SIM. URL:https://github.com/osqzss/gps-sdr-sim (дата звернення: 12.03.2025).
3. CDDIS NASA's Archive of Space Geodesy Data. URL:https://cddis.nasa.gov/archive/gnss/data/daily/2025/brdc/ (дата звернення: 12.03.2025).
4. Great Scott Gadgets HackRF One. URL:https://greatscottgadgets.com/hackrf/one/ (дата звернення: 12.03.2025).
5. GPS-приймач GY-GPS6MV2 на базі чіпа Ublox NEO-6M URL:https://www.mini-tech.com.ua/gps-priemnik-gy-gps6mv2 (дата звернення: 12.03.2025).
6. How to connect an usb GPS receiver with a Linux computer? URL: https://gpswebshop.com/blogs/tech-support-by-os-linux/how-to-connect-an-usb-gps-receiver-with-a-linux-computer (дата звернення: 12.03.2025).
7. GPS Test. URL: https://play.google.com/store/apps/details?id=com.chartcross.gpstest&hl=en (дата звернення: 12.03.2025).

УДК 621.39

ПРІОРИТИЗАЦІЯ ГОЛОСОВОГО ТРАФІКУ В 5G: РОЛЬ ПЛАНУВАЛЬНИКІВ У ЗАБЕЗПЕЧЕННІ QOS

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

PRIORITIZATION OF VOICE TRAFFIC IN 5G: THE ROLE OF SCHEDULERS IN ENSURING QOS

Approaches to voice traffic prioritization in 5G Standalone (SA) networks are investigated and the effectiveness of various scheduling algorithms is evaluated. Simple, QoS-oriented and adaptive methods of resource allocation are analyzed. It was found that adaptive schedulers provide the highest level of QoS for VoNR, minimizing latency and jitter. The choice of a particular algorithm depends on the performance requirements and capabilities of the network environment. These results contribute to the optimization of voice services in 5G.

Розгортання мобільних мереж п’ятого покоління (5G) формує нові вимоги до реалізації голосового зв’язку, зокрема через перехід від VoLTE до Voice over New Radio (VoNR) в архітектурі 5G Standalone (SA). Голосовий трафік у цих мережах характеризується жорсткими вимогами до затримки (latency), джитера (jitter), ймовірності втрати пакетів (packet loss rate) та гарантованої пропускної здатності (GBR – Guaranteed Bit Rate) [1]. Основним завданням радіомережі 5G є динамічне управління ресурсами, що дозволяє одночасно обслуговувати голосові сервіси (VoNR), широкосмугові передачі (eMBB) та критичні комунікації (URLLC) в умовах обмеженого спектрального ресурсу. Оскільки голосовий трафік не може конкурувати за пропускну здатність на рівних умовах із eMBB через критичні вимоги до затримки, використання адаптивних алгоритмів планування ресурсів (scheduling) є необхідною умовою забезпечення QoS у мережах 5G [2].

Голосові сервіси VoNR обробляються через QoS Flow-Based Scheduling, який реалізується шляхом встановлення QoS Identifier (5QI), що визначає параметри обслуговування пакетів у мережі. Для критичного голосового трафіку зазвичай використовується 5QI = 1, який гарантує виділення ресурсу (GBR) із затримкою ≤100 мс. Некритичний голосовий трафік із 5QI = 5, який не гарантує виділення ресурсу (Non-GBR), працює за залишковим принципом, може спричиняти погіршення якості голосового з’єднання при перевантаженні мережі [2]. Пріоритизація реалізується через виділення GBR-каналів для критичних сервісів, пріоритетне обслуговування у планувальниках MAC-рівня, механізми Head-of-Line Blocking Prevention та

динамічне коригування параметрів залежно від навантаження мережі [3].

Ефективне функціонування голосових сервісів у мережах 5G Standalone (SA) вимагає гнучкого та інтелектуального розподілу радіоресурсів, що забезпечується за рахунок алгоритмів планування (schedulers). У середовищі 5G VoNR особливу роль відіграють механізми адаптивного розподілу ресурсів, які враховують параметри радіоканалу (Channel State Information, CSI), пріоритетність трафіку (5QI), вимоги до затримки (latency) та джитера (jitter), а також загальне мережеве завантаження [4]. Алгоритми планування можна умовно поділити на три основні групи:

1) Просте розподілення ресурсів без урахування QoS:

- Round Robin (RR) – рівномірний розподіл ресурсів між усіма користувачами, незалежно від їхніх вимог до якості обслуговування. Такий підхід не забезпечує гнучкого управління радіоресурсами, що є неприйнятним для VoNR.
- Maximum Carrier-to-Interference Ratio (Max C/I) – призначає ресурси користувачам із найкращими умовами радіоканалу. Така стратегія оптимізує загальну пропускну здатність, але може призводити до деградації голосового трафіку в несприятливих умовах сигналу [4].

2) QoS-орієнтовані алгоритми планування:

- Proportional Fairness (PF) – намагається збалансувати пропускну здатність та рівномірний доступ до ресурсів, проте не гарантує стабільну якість голосових сервісів.
- Modified Largest Weighted Delay First (MLWDF) – пріоритизує потоки із найбільш критичними затримками, що робить його ефективним для голосового трафіку.
- Exponential Proportional Fair (EXP/PF) – динамічно змінює пріоритетність трафіку, комбінуючи балансування навантаження та затримку, що покращує продуктивність VoNR.

3) Адаптивні планувальники (Adaptive) – динамічно змінюють стратегію розподілу залежно від навантаження, стану каналу та вимог QoS. Застосовуються алгоритми штучного інтелекту (AI) для прогнозування стану мережі та оптимізації розподілу ресурсів. Серед переваг такого методу, висока гнучкість і оптимізація для змішаного трафіку (голос, дані). Проте реалізація адаптивних планувальників може бути досить складною [4].

На основі моделювання у програмному середовищі Matlab було проведено порівняння роботи трьох планувальників – RR, PF та Adaptive залежно від зміни рівня сигналу SNR (Signal-to-noise ratio) за ключовими

показниками QoS: середня оцінка якості MOS (Mean Opinion Score) (рис.1), середня затримка (latency) (рис.2) та джитер (jitter) (рис.3).

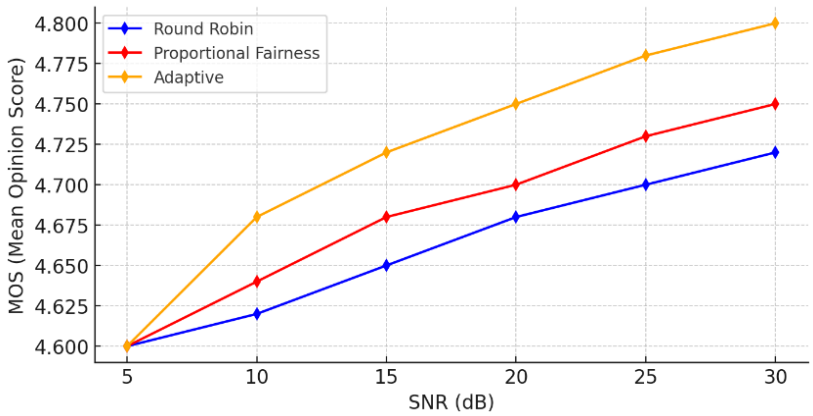


Рис. 1. Mean Opinion Score залежно від SNR

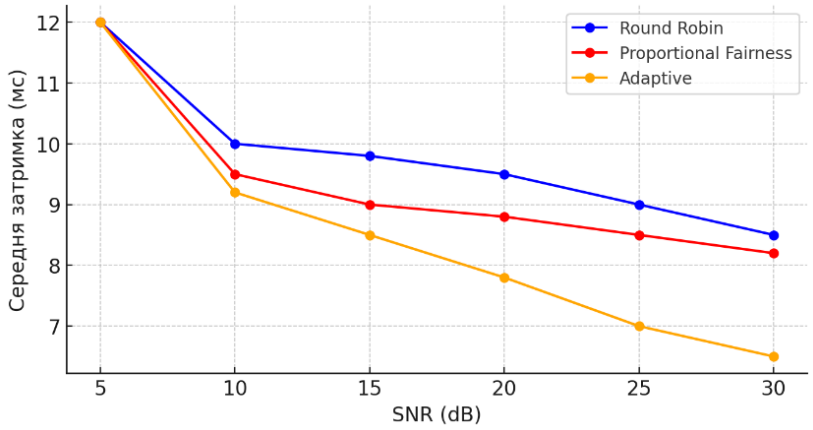


Рис. 2. Середня затримка залежно від SNR

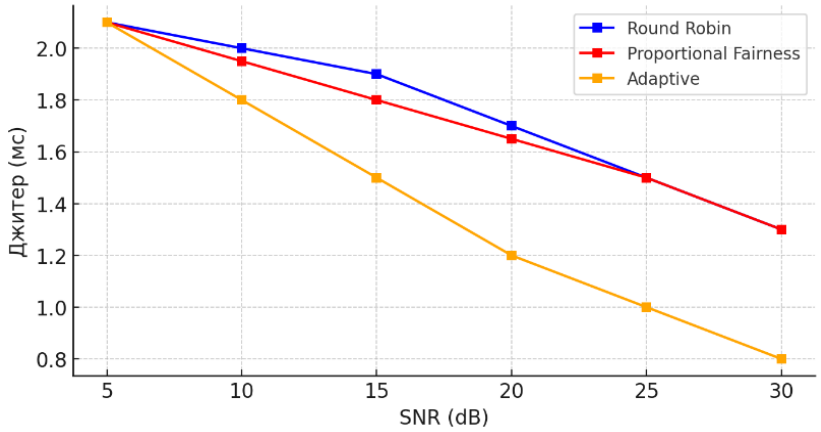


Рис. 3. Джитер залежно від SNR

Результати дослідження підтверджують, що адаптивний планувальник є найбільш ефективним рішенням для забезпечення високої якості голосових послуг у 5G Standalone (SA). Він демонструє найвищий Mean Opinion Score (MOS) на всьому діапазоні SNR, що свідчить про кращу суб'єктивну якість голосового зв'язку порівняно з традиційними підходами. З точки зору затримки та джитера, адаптивний планувальник забезпечує найнижчі

показники, динамічно коригуючи розподіл ресурсів у відповідь на зміну умов мережі та вимоги до QoS. Це дозволяє мінімізувати затримки передачі голосового трафіку та забезпечити його стабільність, що критично важливо для реального часу. Порівняно з ним, Proportional Fairness (PF) виступає як компромісний варіант, забезпечуючи збалансоване використання ресурсів, але не досягаючи необхідного рівня продуктивності для критичних голосових сервісів [5]. Round Robin (RR), хоч і забезпечує рівномірний розподіл ресурсів, є неприйнятним через високу затримку, значні коливання джитера та найнижчий рівень MOS.

Досліджено підходи до пріоритизації голосового трафіку в мережах 5G Standalone (SA) та оцінено ефективність різних алгоритмів планування. Проаналізовано прості, QoS-орієнтовані та адаптивні методи розподілу ресурсів. Встановлено, що адаптивні планувальники забезпечують найвищий рівень QoS для VoNR, мінімізуючи затримку та джитер. Вибір конкретного алгоритму залежить від вимог до продуктивності та можливостей мережевого середовища. Отримані результати сприяють оптимізації голосових сервісів у 5G.

Література

1. 3GPP TS 23.501: System Architecture for the 5G System (5GS) [Електронний ресурс] // 3rd Generation Partnership Project. – Версія 18. – 2024. – Доступно: https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/
2. Vetoshko I.P., Kravchuk S.O. Possibilities of improving the voice services quality in 5G networks // Information and Telecommunication Sciences. – 2023. – Vol.14, No 2. – P. 9-16, https://doi.org/10.20535/2411-2976.22023.9-16
3. Ветошко І.П., Кравчук С.О. Структурні особливості реалізації голосових послуг VoNR в мережі мобільного зв’язку стандарту 5G // Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки. – 2024. – Т. 35 (74), № 1. – С. 27–33. DOI: 10.32782/2663-5941/2024.1.1/04.
4. Mogensen P., Pajukoski K., Weise C. 5G QoS Design Principles and Scheduling Mechanisms // IEEE Communications Magazine. – 2023. – Vol. 61, No. 2. – P. 42-48. – DOI: 10.1109/MCOM.2023.1234567
5. Alhussein A., Rahman T., Khan M. Scheduling Algorithms for 5G Networks: Performance Analysis and Optimization // Wireless Networks. – 2022. – Vol. 28. – P. 1535-1550. – DOI: 10.1007/s11276-022-02964-x

УДК 621.396.1

ПІДВИЩЕННЯ ДОСТУПНОСТІ VOIP-СИСТЕМ

Приймак С.О., Кравчук С.О.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: serg99sb@gmail.com,

METHODS OF INCREASING VOIP SYSTEM AVAILABILITY

Permanent striving to have high-quality voice traffic over packet networks, particularly IP networks provokes a high interest among developers to improve Voice over IP (VoIP) technology. This technology assumes calls are being made over Internet Protocol data network instead of traditional public switched telephone network (PSTN).

Постійна потреба в наявності якісного голосового трафіку через пакетні мережі, зокрема IP-мережі, підтримує високий інтерес розробників до удосконалення технології голос через Інтернет-протокол VoIP (Voice over IP) [1, 2]. Дана технологія не використовує традиційну комутовану телефонну мережу загального користування PSTN (public switched telephone network); натомість виклики здійснюються через мережу передачі даних Інтернет-протоколу.

Сьогодні багато уваги приділяється наступним дослідженням, пов’язаним із подальшим розвитком VoIP-систем:

1. Висока доступність: VoIP-системи повинні забезпечувати безперервний доступ до зв'язку навіть у випадках відмов або збоїв [3]. Зазвичай, це досягається за допомогою методів резервування, кластеризації серверів та використання кількох маршрутів для передачі даних.

2. Вимоги якості обслуговування (QoS): однією з основних проблем доступності VoIP-систем є забезпечення стабільної якості передачі голосу, що включає низьку затримку, мінімальні втрати пакетів та відсутність переривань [2]. Це досягається через розподіл ресурсів, планування трафіку та адаптацію до змін у мережі.

3. Надійність і відмовостійкість: VoIP-системи мають бути захищені від різного роду збоїв, включаючи відмову серверів, збої мережі та напади DDoS (distributed denial-of-service). Дослідження в цій сфері спрямовані на розробку механізмів швидкого відновлення після збоїв.

4. Безпека: оскільки VoIP-системи функціонують через Інтернет, вони стають вразливими до атак, таких як підміна IP-адрес, перехоплення викликів, атаки на сервери реєстрації (сервери SIP (Session Initiation Protocol)) та DDoS-атаки. Підвищення доступності часто включає захист від цих ризиків через шифрування даних, автентифікацію користувачів та інші методи захисту.

5. Масштабованість: зі зростанням кількості користувачів та обсягу трафіку VoIP-системи повинні залишатися стабільними та забезпечувати

високу якість зв'язку без переривань. Тому дослідження також охоплюють розробку архітектур, які можуть масштабуватися відповідно до потреб.

Ефективність використання ресурсів: оптимізація використання мережних і обчислювальних ресурсів є важливою складовою підвищення доступності. Сучасні дослідження охоплюють різні методи компресії голосових даних, управління пропускною здатністю та мінімізації енергоспоживання.

Схема високодоступної VoIP системи.

Високодоступною VoIP-системою називається система голосового зв’язку, яка використовує IP-пакети для передачі голосу(відео, тощо) та спроектована для забезпечення безперервного функціонування, навіть у випадку збою окремих, як програмних так і апаратних компонентів, або мережних проблем. Основна мета такої системи — мінімізувати час простою, забезпечити стійкість до відмов, балансування навантаження, а також дублювання та резервування ресурсів [3].

Схему високодоступної VoIP-системи можна представити наступним чином, як показано на рис. 1.

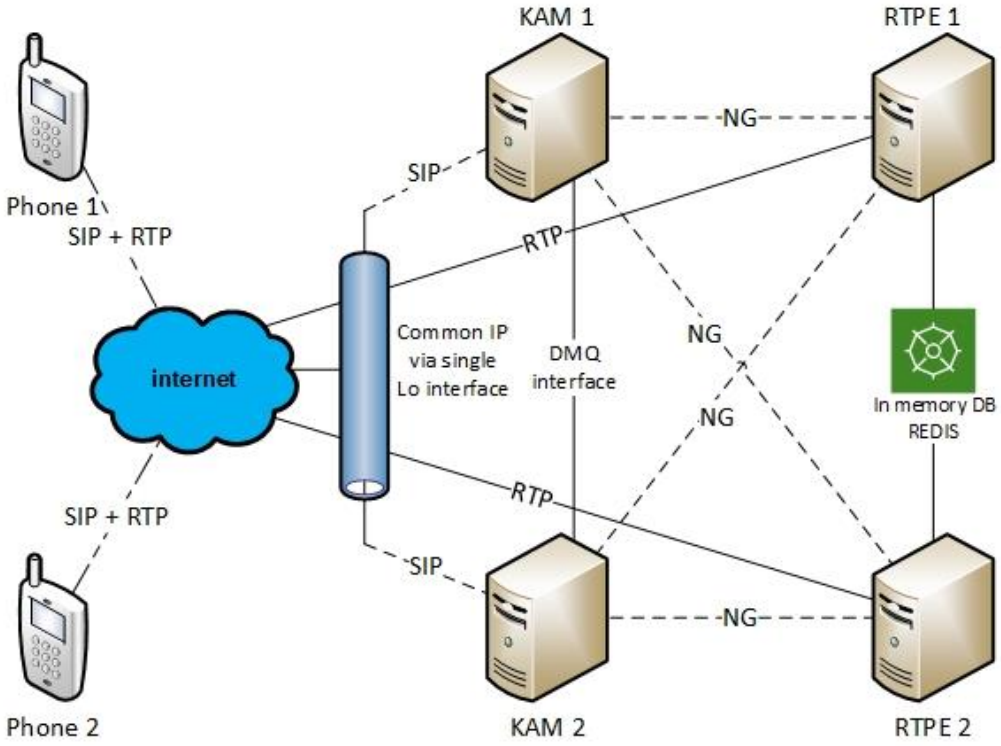


Рис. 1. Схема високодоступої VoIP системи.

Система складається з наступних компонентів:

- сервер сигналізації – KAM1, KAM2, відповідає виключно за обробку сигналізації, в даному випадку SIP;
- медіа шлюз – RTPE1, RTPE2, відповідає виключно за опрацювання голосового RTP трафіку;
- In-memory DB – REDIS, база даних для RTP транзакцій;
- абонентські термінали з підтримкою протоколу SIP – Phone 1, Phone 2.

В якості серверу сигналізації обираємо програмний SIP сервер Kamailio, а медіа шлюзом виступає RTP engine [3] - програмний продукт керування RTP трафіком. База даних REDIS використовується для маніпуляцій (накопичення, видалення) RTP транзакцій.

Між серверами сигналізацій KAM1 та KAM2 присутній логічний канал зв'язку, так званий DMQ interface [3] для обміну ідентифікаторами SIP транзакцій (SIP call id) [1], в той самий час сервера керують медіа шлюзами (RTPE1, RTPE2) за протоколом NG. В той самий час медіа-шлюзи RTPE1 та RTPE2 обмінюються RTP транзакціями за допомогою БД Redis за протоколом publish/subscribe. Час перемикання активного вузла сервера на гарячий резерв становить 1 с.

У випадку 100% функціональності системи голосовий виклик опрацьовується наступним чином: сигналізацію опрацьовує KAM1 та в той самий час він керує RTPE1, який в свою чергу відповідає за встановлення голосового RTP потоку між абонентами Phone1 та Phone2. В разі закінчення виклику одним з абонентів, KAM1 надає команду на припинення RTP потоку RTPE1 та з'єднання розривається.

Розглянемо випадки, коли будемо мати відмову одного або декількох елементів системи:

1. З'єднання було успішно встановлено за алгоритмом, описаним вище, але згодом маємо відмову сервера сигналізації KAM1. Голосовий потік продовжує функціонувати, але такий виклик «ніколи» не завершився б у разі відсутності KAM2, який контролює SIP транзакції сервера KAM1 по логічному каналу «DMQ interface». Таким чином KAM2 «підхоплює» усі активні сигнальні транзакції KAM1.

2. З'єднання було успішно встановлено за алгоритмом, описаним вище, але згодом маємо відмову RTPE1. В такому випадку, завдяки додатковому алгоритму та наявності бази даних REDIS, RTPE2 бере на себе «доопрацювання» голосового RTP потоку в той самий час як SIP Server 1 продовжує обробляти сигналізацію.

Висновок. Наведений вище метод підвищення доступності системи полягає в тому, що при відмові одного з двох серверів (KAMx та RTPEx) система не втрачає жодного встановленого виклику та має змогу опрацьовувати нові. Система має єдину точку входу (IP адрес для прийому/відправки викликів з/на зовні), яка є незмінною в разі відмови елементів системи.

Література

1. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., & Schooler, E. *SIP: Session Initiation Protocol*. RFC 3261. Internet Engineering Task Force (IETF) (2002).
2. Vetoshko I.P., Kravchuk S.O. Possibilities of improving the voice services quality in 5G networks // Information and Telecommunication Sciences. – 2023. – Vol.14, No 2. – P. 9-16, https://doi.org/10.20535/2411-2976.22023.9-16.
3. Mierla D.-C., Modroiu E.-R. "SIP Routing with Kamailio" 2022 ISBN 978-3-00-049485-7.

УДК 621.391

ПІДХІД ДО ПОБУДОВИ СТІЛЬНИКОВИХ МЕРЕЖ У ВІРТУАЛЬНОМУ СЕРЕДОВИЩІ ДЛЯ МОДЕЛЮВАННЯ 5G-МЕРЕЖ

Сколець С.С.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: serskols@gmail.com

APPROACH FOR DEPLOYMENT OF CELLULAR NETWORKS IN A VIRTUAL ENVIRONMENT FOR SIMULATING 5G NETWORKS

This work implements a model of a 4G/5G mobile network in the Mininet environment using the concept of Software-Defined Networking (SDN). The network is evaluated based on throughput and latency indicators, particularly through the simulation of a virtualized LTE network that integrates key components of 5G C-RAN. The paper describes the use of the Mininet emulator for testing a network topology that includes remote radio heads (RRH), user equipment (UE), and an SDN controller for network management. Formulas are also provided for calculating throughput using Iperf and evaluating packet delay (RTT), which affects the Quality of Service (QoS). The results of this work form the basis for further research on the impact of virtualization on the efficiency of mobile networks.

Мобільні мережі п’ятого покоління (5G) вимагають нових підходів до архітектури, управління та автоматизації. Одним із ключових рішень є централізована радіомережа (C-RAN) із віддаленими радіоголовками (RRH) та обчислювальними модулями (BBU), що розташовані в дата-центрах.

Паралельно з розвитком 5G набуває популярності концепція програмно-конфігурованих мереж (SDN), яка відокремлює управління мережею від апаратної частини, забезпечуючи гнучкість та централізований контроль. SDN інтегрується з 5G, спрощуючи управління та підвищуючи ефективність мережневих процесів.

У цій роботі реалізовано спрощену модель 4G-мережі з підтримкою SDN як крок до впровадження 5G. Мережа оцінюється за показниками затримки та пропускної здатності через моделювання в Mininet [1] — емуляторі SDN-мереж, що дозволяє тестувати LTE RAN у програмно-конфігурованому середовищі.

Спосіб віртуалізації та емуляції. Mininet — це емулятор програмно-конфігурованих мереж (SDN), що дозволяє створювати та тестувати віртуальні мережі з різними топологіями. Він підтримує віртуалізовані станції та точки доступу, використовуючи стандартні драйвери бездротових мереж Linux та модуль емуляції 80211 hwsim [2].

Емулятор реалізує SDN-підхід, де керування мережею здійснюється централізовано через контролер, який взаємодіє з комутаторами за

допомогою протоколу OpenFlow [3]. Топологія моделі складається з бездротової (LTE RAN) та дротової частин, де OpenFlow-комутатори відповідають за передачу даних, а контрольна площина керується контролером.

Середовище працює на Linux, розподіляючи пам'ять між простором ядра (для обробки бездротових інтерфейсів і протоколів) та простором користувача (для керування RRH, UE та налаштувань трафіку). Завдяки можливостям емулятора була побудована мережа з базовими станціями (RRH), мобільними користувачами (UE) та сервером, що імітує зовнішню мережу для тестування з'єднань End-to-End.

Компоненти мережі. Топологія, реалізована в емуляторі (Рис.1.), є спрощеною версією LTE-мережі відповідно до концепції C-RAN. Вона включає ключові компоненти, такі як RRH (антени базових станцій), BBU (віртуалізовані OpenFlow-комутатори), контролер та мережу EPC для маршрутизації трафіку.

Основні елементи топології:

- Контролер — використовується SDN-контролер POX [4], що керує мережею, аналізує трафік та мінімізує затримки, реалізуючи маршрутизацію на рівні L2.
- UEs (мобільні користувачі) — підключаються до RRH, мають IP/MAC-адреси, параметри антени та змінюють точки підключення за правилами асоціації.
- RRH (Remote Radio Heads) — забезпечують зв'язок між UE та контролером, виконують перемикання користувачів між зонами покриття.
- Open vSwitch — програмні комутатори, що реалізують OpenFlow, підтримують віртуалізацію мережі та дозволяють контролювати таблиці маршрутизації в реальному часі.

Така архітектура дозволяє гнучко моделювати та тестувати LTE-мережі з елементами SDN.

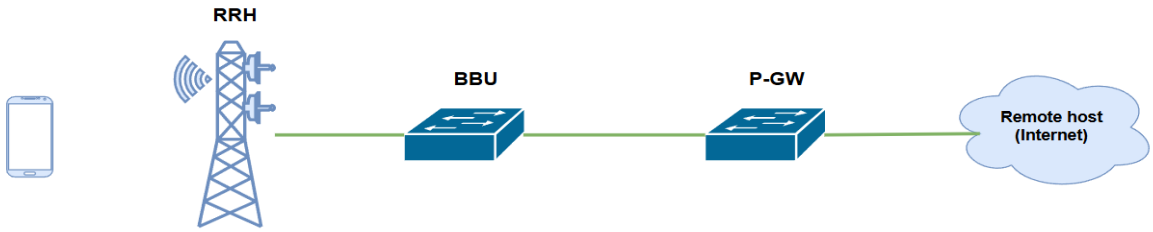


Рис. 1. Архітектура і компоненти мережі.

Реалізація LTE-модулів. Для забезпечення відповідності симуляцій специфікаціям LTE було розроблено та модифіковано програмні модулі на Python. Ці модулі реалізують функції LTE-пристроїв, включаючи мобільних користувачів та базові станції, що дозволяє емулювати бездротову взаємодію між ними.

Тестування та оцінка мережі. З огляду на можливості емулятора були прийняті такі припущення:

- BBU та RRH використовуються в контексті C-RAN, але не виконують обробку цифрових сигналів.
- Відстань між RRH і BBU не враховується через використання волоконно-оптичних ліній з високою пропускною здатністю.
- Ядро мережі відповідає за маршрутизацію, а функції S-GW та P-GW реалізовані в SDN-контролері.
- TCP/UDP-з'єднання розглядається як ідентичне для Wi-Fi та LTE.
- NFV (віртуалізація мережневих функцій) представлена через використання віртуальних комутаторів.

Для оцінки впливу SDN на мобільні мережі було проведено серію тестів на платформі Mininet. Продуктивність мережі аналізувалася за допомогою:

1. Вимірювання пропускної здатності.

Пропускну здатність пропонується вимірювати за допомогою Iperf [ ], що генерує TCP-трафік між двома точками мережі (мобільним користувачем і сервером) для моделювання E2E LTE-з'єднання.

Отримані значення будуть переведені у спектральну ефективність, поділивши на ширину каналу. Залежність SNR порівнювався з границею Шеннона:

$$C[\text{біт/с/Гц}] = \text{B}[\text{МГц}] \times \log_2(1 + SNR), \qquad (1)$$

де C – пропускна здатність, B – ширина каналу, SNR – відношення сигнал/шум.

2. Оцінка затримки пакетів (RTT).

Затримка (Latency) в LTE розрізняється на дві площини: управління та користувача. У дослідженні аналізувалася лише затримка в площині користувача, яка визначається як RTT (Round Trip Time) і впливає на якість користувацького досвіду (QoE) [5].

RTT вимірюється двома методами:

1. В кінцевому з'єднанні за допомогою ping (ICMP Echo Request) між

мобільним терміналом і IP-хостом.

2. В дротовому з'єднанні через ping між IP-хостом і антеною базової станції.

Залежність RTT від SNR отримані за формулою:

$$RTT[\text{мс}] = b_1 \times e^{(b_2 \times SNR)}, \quad (2)$$

де SNR – відношення сигнал/шум, а коефіцієнти b_1 та b_2 залежать від розміру пакету.

Висновки. У цій роботі показано реалізацію архітектури мобільної мережі 4G/5G у середовищі Mininet із використанням концепції SDN. Реалізована структура відповідає вимогам сучасних мобільних систем і може бути основою для досліджень впливу SDN на якість обслуговування (QoS) у бездротових мережах.

Розроблені модулі для підтримки LTE в Mininet дозволяють оцінювати трафік у програмно-конфігурованій мережі. Модель включає основні компоненти радіодоступу, ядра та управління мережею, що відповідають концепції 5G C-RAN.

Оцінюються показники QoS, зокрема пропускна здатність та затримка, які будуть досліджуватися на наступних етапах для порівняння з реальними вимірами та оптимізації мережневої взаємодії.

Література

1. Mininet at https://mininet.org/
2. mac80211_hwim at https://wireless.wiki.kernel.org/en/users/drivers/mac80211_hwsim
3. Сколець С. «Створення лабораторного макету мережі SDN на базі платформи Mininet з використанням контролеру Floodlight» / КПІ ІТС – Дипломна робота/ 2021 рік, с. 23-34
4. C. Fancy and M. Pushpalatha, Performance evaluation of SDN controllers POX and floodlight in mininet emulation environment; 2017 International Conference on Intelligent Sustainable Systems (ICISS), Palladam, India, 2017, pp. 695-699, doi: 10.1109/ISS1.2017.8389262
5. Kravchuk S.O. Theory of mobile infocommunication systems. System architecture: textbook. – Kyiv: Igor Sikorsky Kyiv Polytechnic Institute, 2023. – p. 636, https://ela.kpi.ua/handle/123456789/53198

УДК 004.7:621.39

ВИКОРИСТАННЯ ІНСТРУМЕНТУ "КООРДИНАТОР" У СИСТЕМІ УПРАВЛІННЯ ПРОЄКТАМИ REDMINE: РОЗШИРЕННЯ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ СИСТЕМИ НА ОСНОВІ МОДУЛЯ ДЛЯ DRUPAL САЙТУ

Руренко О.Г., Пацук В.О.
Навчально-науковий Інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: rurenko.oleksandr@lll.kpi.ua, patsuk.victoria@lll.kpi.ua

USING THE "TRACKER" TOOL IN THE REDMINE PROJECT MANAGEMENT SYSTEM: EXPANDING SYSTEM FUNCTIONALITY BASED ON A MODULE FOR A DRUPAL SITE

This work proposes a new approach to creating a telecommunications information system for a small enterprise by integrating the Redmine project management system with a Drupal site and designing a special software module for such a site based on the Drupal core.

У даній роботі пропонується новий підхід до створення телекомунікаційної інформаційної системи малого підприємства шляхом інтеграції системи управління проєктами Redmine і Drupal сайту та проєктування спеціального програмного модуля для такого сайту на базі ядра Drupal.

Розвиток комп'ютерів і інформаційних технологій спричинив низку радикальних змін у теорії та практиці проєктного менеджменту, які наразі складають базову інструментальну основу для оптимізації операційної діяльності підприємств, які орієнтовані на проєктну діяльність [4]. Такі зміни викликані передусім тим, що в ході планування та виконання проєктів у цих процесах залучено велику кількість учасників з різними проєктними ролями, і така тенденція лише зростає. За результатами останніх аналітичних досліджень Інституту проєктного менеджменту (*англ.* Project Management Institute, PMI) у семи секторах економіки, орієнтованих на проєктну діяльність, до 2027 року зростання числа учасників очікується на рівні 33 відсотків, або майже 22 мільйони нових робочих місць [1].

Новітні стилі проєктного менеджменту, такі як Scrum і Agile, хоча й створені передусім для підприємств, які спеціалізуються на розробці програмного забезпечення, успішно можуть бути використані іншими підприємствами як базовий операційний підхід до проєктного менеджменту і управління ресурсами в організації.

У даній роботі пропонується новий підхід до створення телекомунікаційної інформаційної системи малого підприємства шляхом інтеграції системи управління проєктами Redmine і Drupal сайту та проєктування спеціального модуля Drupal, який в роботі позначений як «Gant Drupal Module».

Телекомунікаційна інформаційна система Redmine – це інструмент для

керування проєктами, створений на основі фреймворку Ruby on Rails з акцентом на Agile-технології. Цей підхід до керування проєктом передбачає розбиття проєкту на етапи (ітерації) або роботи, які виконуються учасниками проєкту, і безперервно відстежуються та вдосконалюються в ході виконання проєкту.

Функціонал системи Redmine забезпечує контроль життєвого циклу окремих робіт і проєкту в цілому за допомогою спеціального програмного інструменту «Координатор» *(англ. Tracker)*, який відстежує окремі аспекти функціональної діяльності над проєктом, при цьому не нав'язує команді чи групі розробників певний метод роботи, але дозволяє організувати операційні процеси над виконанням завдань проєкту на єдиній основі. Це сприяє створенню типових для організації станів-статусів та однакових метрик, які системно використовуються аналітиками для прийняття оперативних рішень щодо дотримання темпів виконання проєкту й оптимізації ресурсів всередині компанії.

Для наочності в системі Redmine, яка інстальована на сервері в локальній мережі підприємства, демонструється проєкт створення модуля для сайту Drupal «Gant Drupal Module». Даний модельний проєкт включає наступні етапи і роботи:

I. Розроблення концепції модуля:

- Драфт концепції;
- Драфт особливостей модуля;
- Визначення основних функцій.

II. Розроблення програмної архітектури модуля:

- Розроблення конкурентних варіантів програмної архітектури;
- Попередня оцінка бюджету часу;
- Попередня оцінка бюджету ресурсів;
- Визначення попередньої ціни модуля.

III. Програмування і розроблення програмного макету модуля:

- Генерування системних файлів модуля Drupal;
  /sites/modules/custom/gantdrupalmodule/ganrdrupalmodele.info.yml
  /sites/modules/custom/gantdrupalmodule/ganrdrupalmodele.module [2];
- Створення програмного блоку «gantdrupalmodule»;
- Копіювання example.setting.local.php в settings.local.php і налаштування файлу settings.php;
- Написання коду програми модуля на PHP;
- Встановлення додаткових модулів, налаштування роутів і відлагодження програмного модуля;
- Реєстрація модуля в системі Drupal сайту і тестування;
- Інсталяція модуля в телекомунікаційній інформаційній системі організації.

Для відстеження функціональної діяльності даного проєкту використано кілька координаторів, які відображають основні етапи роботи: документація, дослідження, розробка, конфігурація, тестування, інсталяція. Налаштування переходів між статусами представлено на прикладі

координатора «Документація» (рис. 1). Наприклад, може бути дозволений перехід від статусу *«New»* до статусу *«In progress»*, але заборонений перехід від *«In progress»* до *«Closed»*. Такі налаштування виконуються аналітиком або керівником проєкта, що відображає стани-статуси видів робіт на етапах.

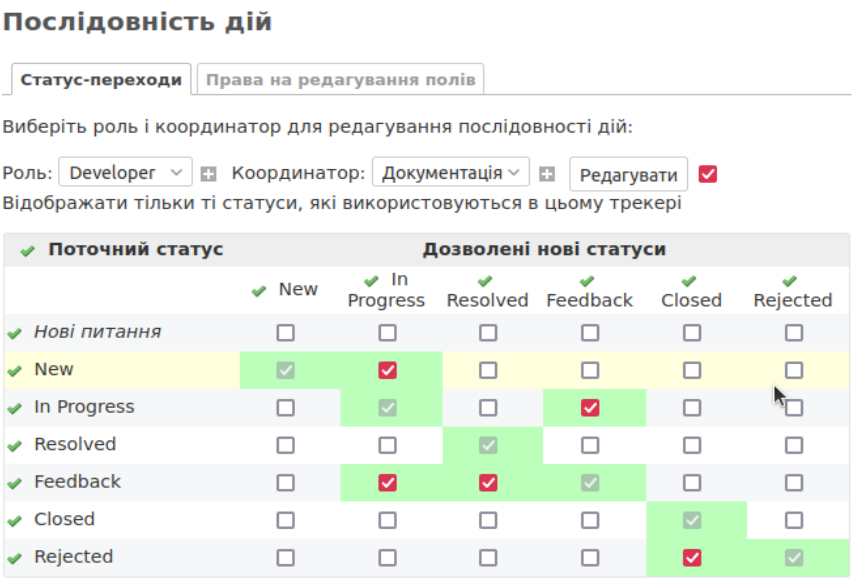


Рис. 1. Налаштування послідовності дій для координатора «Документація».

Корисним інструментом є використання діаграми Ганта в Redmine. Хоча графік Ганта і був створений Генрі Ганттом на початку 20 століття як інструмент для покращення планування та відстеження проєктів, він наразі використовується багатьма фреймворками та програмами, зокрема платформою Redmine. Він наочно візуалізує ступінь завершеності кожної з робіт у порівнянні з запланованим періодом. На прикладі діаграми Ганта щодо модульного проекту "Gant Drupal Module" (рис. 2), виділені ключові завдання.

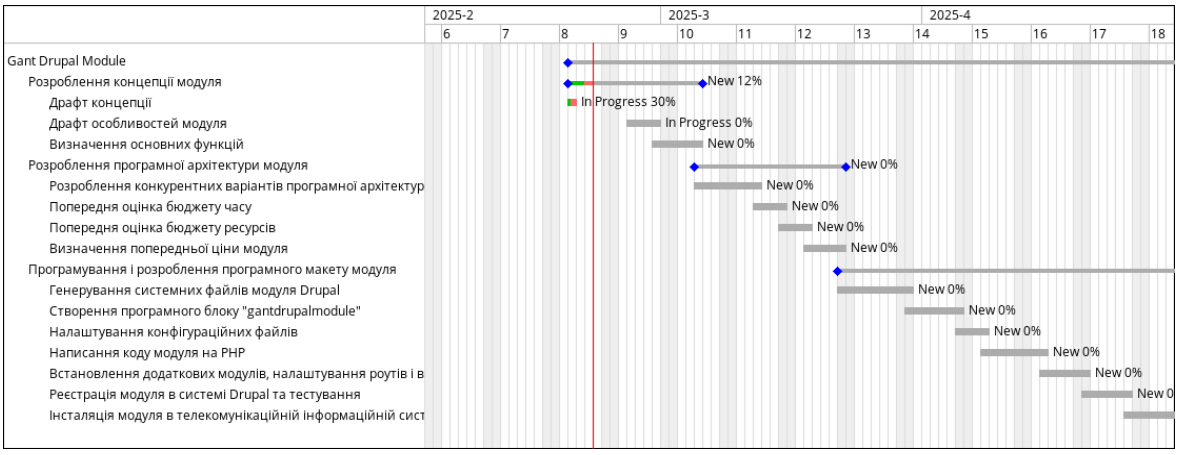


Рис. 2. Діаграма Ганта для проєкту «Gant Drupal Module».

Графічне відображення стану виконання завдань на діаграмі Ганта дає змогу користувачам швидко оцінити статус кожного завдання: *«New», «In progress», «Closed», «Resolved», «Feedback», «Rejected»* [3].

Важливим аспектом є наявність часової шкали та дедлайнів, що дозволяє зіставляти тривалість завдань із запланованими термінами. Червона вертикальна лінія позначає поточний день, що дозволяє контролювати відповідність графіку встановленим і здійснювати коригування у разі відхилень.

Діаграма Ганта також надає можливість відображення взаємозалежностей між завданнями. Деякі етапи проекту не можуть розпочатися без завершення попередніх, що дозволяє уникати конфліктів у виконанні робіт та ефективніше розподіляти ресурси.

Розроблений модуль «Gant Drupal Module» розширює функціональні можливості використання інструменту «Координатор» у системі Redmine. Впровадження такого підходу дозволяє ефективно керувати проєктною діяльністю малого підприємства за рахунок чіткої організації та контролю над виконанням завдань.

Запропонований модуль забезпечує автоматизоване відстеження етапів виконання проєкту, візуалізацію стану завдань за допомогою діаграм Ганта, що покращує комунікацію між учасниками команди проєкту.

Модуль «Gant Drupal Module» розроблено на основі бібліотеки DHTML Gant від корпорації Salesforce. Бібліотека включає гнучкий набір віджетів на JavaScript, які дозволяють будувати динамічні користувацькі віджети на основі компонентів DHTMLX. Як результат, на сайті Drupal додається нова функціональність, яка дозволяє відтворювати і редагувати діаграми Ганта, а відтак моніторити і редагувати проєкт Redmine вже на сторінці сайту Drupal.

Таким чином, інтеграція платформи Redmine з платформою Drupal сприяє створенню єдиної інформаційної системи для управління проєктами малого підприємства, що підвищує ефективність бізнес-процесів і сприяє їхній подальшій автоматизації. Подальші дослідження можуть бути спрямовані на розширення функціональності модуля і інтеграції данних між Redmine та Drupal сайтом підприємства.

Література

1. Fielding P. J. How to Manage Projects: Essential Project Management Skills to Deliver on Time, on-budget Results. – London: Kogan Page, Limited, 2019. – 256 p.
2. Платформа - Drupal. Overview - Drupal [Електронний ресурс]. – Режим доступу: https://www.drupal.org/docs/user_guide/en/index.html – Дата звернення: 17.02.2025.
3. Платформа - Redmine. Overview - Redmine [Електронний ресурс]. – Режим доступу: https://www.redmine.org/projects/redmine/wiki/Guide. – Дата звернення: 17.02.2025.
4. Lester A. Project management, planning, and control: Managing engineering, construction, and manufacturing projects to PMI, APM, and BSI standards. – 5th ed. – Amsterdam: Elsevier, 2007. – 435 p.

УДК 004.738

ШЛЯХИ ВИЯВЛЕННЯ ТА НЕЙТРАЛІЗАЦІЇ ВПЛИВУ DDOS-АТАК НА ІНОРМАЦІЙНІ РЕСУРСИ

Поковба О. Ю., Правило В. В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: pokovba.alexander@lll.kpi.ua, v.v.pravylo@ukr.net

WAYS TO DETECT AND NEUTRALISE THE IMPACT OF DDOS ATTACKS ON INFORMATION RESOURCES

The study examines normalization techniques to enhance detection accuracy. The results demonstrate that anomaly detection methods can effectively identify the onset of DDoS attacks and help mitigate malicious traffic.

Щоб ефективно виявляти різні DDoS-атаки, потрібно більше зосередитися на виявленні спільних властивостей цих зловмисних атак. Однією з таких властивостей є змінність вихідних IP-адрес, які генерують атакуючі пакети [1]. Ентропія мінливості пакетів H(Z) визначається за допомогою формули (1), яка визначається як сума Zi – об’єму пакетів, надісланих між парою з’єднань джерела та призначення (IP-адреси джерела та призначення, тобто src-dst IP) – і p(Zi) ймовірності його знаходження, вираженої шляхом нормалізації загальної кількості пакетів на Zi [2].

$$H(z) = - \sum_{i=1}^{n} zi \log(p(zi)) \quad (1)$$

Потім значення ентропії нормалізується з максимальною ентропією (2), де N - кількість різних пар зв'язку (src-dst IP).

$$H(N) = \log(N) / \log(2) \quad (2)$$

Значення ентропії вимірює, наскільки широко пакети розподіляються по розподілу. Здається, ентропія та різноманітність змінюються під час DDoS-атаки. Оскільки реальний трафік різноманітний, значення ентропії змінюються набагато різкіше, ніж будь-коли. Значення ентропії можуть змінюватися досить швидко, оскільки через характер різних служб [3], які вимагають різної швидкості передачі даних, структура потоків даних стає непостійною. Така зміна кожного другого випадку ускладнює визначення чіткого порогу виявлення DDoS-атаки. Щоб гарантувати, що він керує прийняттям обґрунтованих рішень, повинен існувати фільтр ентропійних даних, роль якого полягає у вилученні правильного набору значень [4]. Метод передбачає фільтрацію ентропійних даних із роздільною здатністю більших 10-секундних інтервалів із вибором максимумів, які можуть представляти їх для цього інтервалу (рис. 1).

$$F(z) = \max(zi, i = 1..10) \tag{3}$$

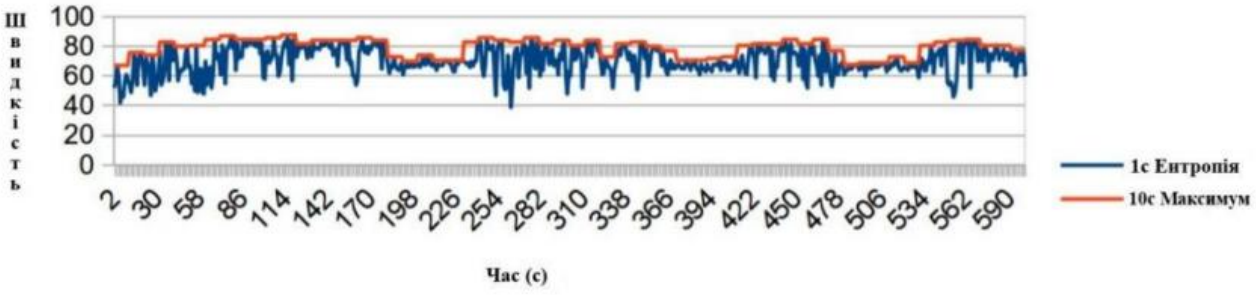


Рис.1. Найвищі значення швидкості у проміжках в 10с.

Суть запропонованої стратегії ідентифікації DDoS-атак та шкідливого трафіку полягає в інноваційному алгоритмі максимально оперативного визначення початкової точки розподіленої атаки, метою якої є знесення системи. Алгоритм також має можливість враховувати коливання сезонного навантаження, що гарантує значно більшу точність і швидкість розпізнавання атаки на її початковій стадії [5]. Крім того, було проведено ретельне дослідження, щоб підтвердити саме існування сезонних закономірностей і знайти типові сезонні періоди. Це дослідження показало, що деякі існують, тижнева і добова сезонність, і досить нечітко виражені, а також причини різкої добової сезонності.

Програмне рішення (рис. 2) застосовне для ефективного захисту «останньої милі», яка є найбільш критичним сегментом мережі. Основною функцією даного комплексу є забезпечення безпеки веб-серверів від DDoS-атак у вигляді http-флуду. Програмне забезпечення має широкий діапазон операційних систем, сумісне з усіма сучасними веб-серверами. Крім того, цей програмний комплекс можна встановлювати не тільки на фізичних серверах, а й використовувати у віртуальних хостингових середовищах, що дає можливість забезпечити масштабованість і гнучкість захисту.

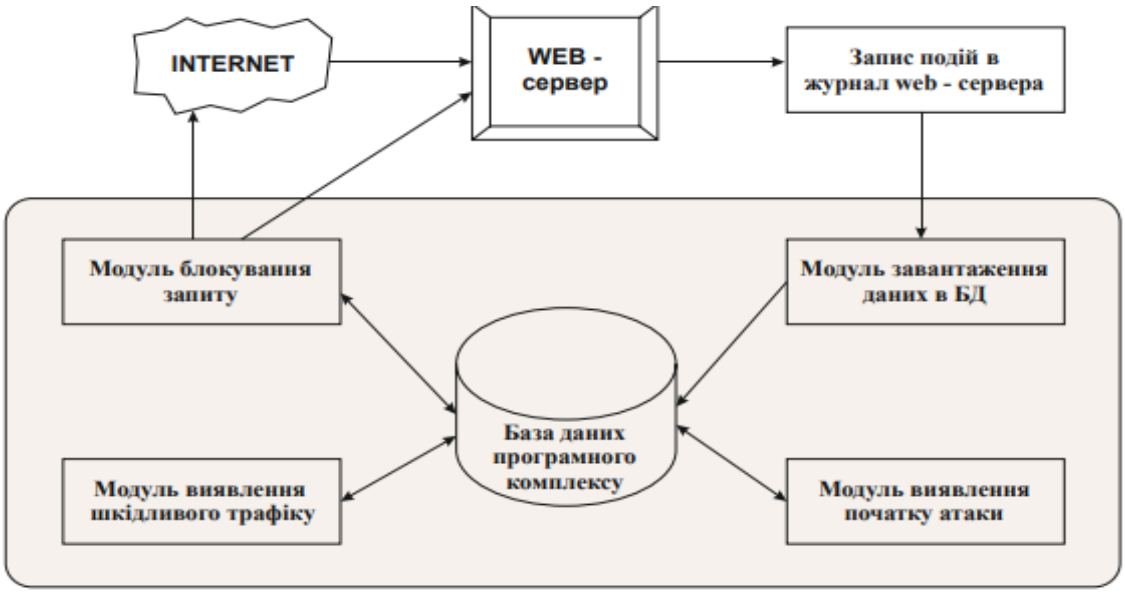


Рис.2. Архітектура програмного комплексу.

Універсальність програмного комплексу виявлення та протидії DDoS-атакам може бути реалізована не тільки для виявлення http-flood, але й для більшої кількості типів DDoS-атак. Трохи змінившись, програмне забезпечення може обробляти дані з лог-файлів різних мережевих служб, оскільки не є основним модулем, тому, крім мережевих локаторів, можна використовувати кілька інших фрагментів інформації. У цій реалізації весь програмний комплекс складається з трьох модулів і розміщується на кінцевому мережевому ресурсі. При необхідності програмні модулі можна розмістити будь-де в мережі. Так, наприклад, кінцевий сервер може мати лише завантажувач даних. Інструменти виявлення атак і фільтрації трафіку можна встановити на окремому сервері, який неможливо атакувати із зовнішньої мережі [6]. У такому встановленому програмному забезпеченні сервіс буде здатний нормально функціонувати та класифікувати трафік навіть у разі збою атакованого сервера.

Опція інсталяції доступна, якщо на захищеному вузлі не встановлено програмні модулі; звичайно, якщо дані можна отримати з мережевих локаторів та/або маршрутизаторів. В іншому випадку можна здійснити блокування трафіку на наступному вузлі [7]. Також програмний комплекс підтримує мультиінсталяцію при одночасному запуску декількох модулів виконуваного об'єкта з однаковою назвою. Наприклад, дані, на основі аналізу яких буде прийнято рішення, можуть надходити в базу з кількох джерел. На різних рівнях дані про зловмисний трафік можуть надсилатися в процесі блокування рекомендацій.

Література

1. Виявлення DDoS-атак (DDoS) Офіційний сайт компанії Cisco [Електронний ресурс]. Режим доступу : http://www.cisco.com/web/RU/products/ps5887/products_white_paper0900
2. Карта DDoS-атак в реальному часі [Електронний ресурс]. - Режим доступу: URL : http://www.digitalattackmap.com/
3. Арун Радж Кумар, П. та С. Селвакумар, "Розподілена загроза відмови в обслуговуванні (DDoS) в середовищі спільної роботи - огляд інструментів DDoSатак та механізмів відстеження", Міжнародна конференція з перспективних обчислень (IACC 2009), сс. 1275-1280, березень 2009
4. Д. Діттріх, Г. Вівер, С. Діттріх, Н. Лонг, "Інструмент атаки на розподілену відмову в обслуговуванні Mstream", травень 2000.
5. Алекс Дойал, Джастін Чжан та Хуймінг Анна Ю, "На шляху до перемоги над DDoS-атаками", Міжнародна конференція з кібербезпеки, с. 209-211, 2012 IEEE.
6. Rocky K. C. Chang, "Захист від розподілених атак на відмову в обслуговуванні на основі переповнення: Підручник", IEEE Communications Magazine, стор. 42-51, жовтень 2002.
7. AT&T Center for Internet Research at ICSI Аналіз використання рефлекторів для розподілених атак на відмову в обслуговуванні,
[online] http://www.icir.org/vern/papers/reflectors.CCR.01.pdf.

УДК 621.39

ШЛЯХИ ПІДВИЩЕННЯ ЗНАЧЕНЬ QoS В МЕРЕЖАХ 5G З УРАХУВАННЯМ ТИПУ ТРАФІКУ, ЩО ПЕРЕДАЄТЬСЯ

Правило В.В., Шумський Б.С.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: v.v.pravylo@ukr.net, shumskiy.bohdan@lll.kpi.ua

WAYS TO IMPROVE QOS IN 5G NETWORKS BASED ON THE TYPE OF TRAFFIC BEING TRANSMITTED

The paper examines the main ways to improve the quality of service (QoS) in fifth-generation (5G) networks, taking into account the type of transmitted traffic. Modern technologies that provide effective resource management and adaptive traffic management based on artificial intelligence are analyzed. Particular attention is paid to ensuring QoS for different categories of users.

Мережі п’ятого покоління (5G) є значним кроком уперед у розвитку бездротових комунікаційних технологій, забезпечуючи суттєве підвищення швидкості передавання даних, зменшення затримок та підтримку великої кількості одночасно підключених пристроїв. Однією з головних переваг 5G є можливість адаптації до різних типів трафіку, що передається мережею, забезпечуючи необхідний рівень якості обслуговування (QoS). Різні типи трафіку, такі як потокове відео, голосовий зв’язок, обмін даними між IoT-пристроями або управління критично важливими системами, мають суттєві відмінності у вимогах до пропускної здатності, затримки та надійності. Саме тому для ефективного функціонування мережі необхідно впроваджувати інноваційні підходи до керування ресурсами та оптимізації трафіку[1][2].

Одним з ключових механізмів підвищення якості обслуговування у 5G є мережна сегментація (Network Slicing) (Рис.1), яка дозволяє створювати віртуальні підмережі, оптимізовані для конкретного сценарію використання. Це дає змогу забезпечити високу пропускну здатність для мультимедійного контенту (eMBB), наднизьку затримку для критично важливих застосунків (URLLC) та підтримку великої кількості пристроїв з мінімальним енергоспоживанням у сфері Інтернету речей (mMTC) [3]. Завдяки такій гнучкості оператори можуть ефективніше розподіляти ресурси мережі та підвищувати рівень QoS для кожного користувача відповідно до його потреб.

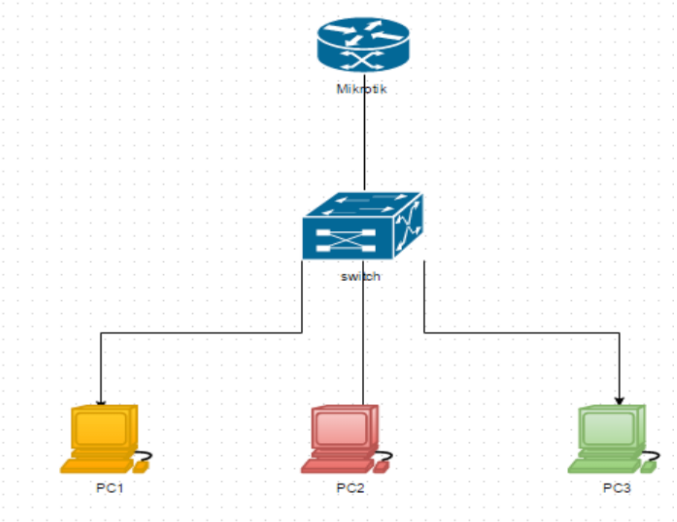


Рис.1. Приклад мережної сегментації.

Ще одним важливим підходом є оптимізація використання радіоресурсів та адаптивне управління трафіком. У 5G застосовуються алгоритми машинного навчання та штучного інтелекту, які аналізують навантаження мережі та динамічно налаштовують параметри передавання даних [4]. Це включає адаптивне масштабування ширини каналу, зміну модуляції та кодування залежно від якості радіоканалу, а також пріоритетний розподіл частотних ресурсів. Такі методи дозволяють забезпечити стабільну роботу мережі навіть у пікові періоди навантаження.

Технологія Multi-Access Edge Computing (MEC) відіграє значну роль у зменшенні затримок та покращенні QoS у 5G. Вона дозволяє переносити обчислювальні потужності ближче до кінцевого користувача, що суттєво скорочує час передачі даних та знижує навантаження на центральну частину мережі [1]. Це особливо важливо для застосувань, які потребують миттєвого реагування, таких як автономний транспорт, дистанційна хірургія, розширена реальність та автоматизовані виробничі процеси. Використання MEC також підвищує ефективність потокового передавання мультимедійного контенту за рахунок локального кешування популярних файлів та зменшення навантаження на магістральні канали передачі даних.

Забезпечення якості обслуговування в 5G також передбачає впровадження спеціалізованих механізмів для різних типів трафіку. Для відео- та аудіострімінгу використовуються адаптивні алгоритми потокового передавання, які регулюють бітрейт залежно від умов мережі, що дозволяє мінімізувати буферизацію та втрати кадрів. Для критично важливих комунікацій, таких як промислові мережі або транспортні системи V2X, застосовуються жорсткі гарантії затримок та механізми резервування каналів зв’язку. У сфері IoT, де основна увага приділяється низькому енергоспоживанню та ефективному використанню частотного ресурсу, використовуються такі технології, як NB-IoT та LTE-M, що дозволяють підключати мільйони пристроїв з мінімальним використанням смуги пропускання [5].

Окрему увагу слід приділити питанням безпеки, які безпосередньо впливають на якість обслуговування у мережах 5G. Використання розширених методів шифрування та автентифікації допомагає запобігати несанкціонованому доступу до трафіку користувачів. Впровадження блокчейн-рішень забезпечує додатковий рівень довіри та цілісності переданих даних. Крім того, застосування технологій аналізу мережевого трафіку на основі штучного інтелекту дозволяє виявляти та запобігати DDoS-атакам та іншим загрозам кібербезпеки, які можуть суттєво впливати на продуктивність мережі. [4]

Висновки. Підвищення якості обслуговування у мережах 5G є багатогранним завданням, що потребує комплексного підходу до управління ресурсами, адаптації до типу трафіку та використання передових технологій. Впровадження мережної сегментації дозволяє диференційовано підходити до обслуговування різних категорій користувачів, забезпечуючи відповідний рівень продуктивності для кожного з них. Оптимізація радіоресурсів та використання інтелектуальних алгоритмів керування трафіком сприяють ефективному розподілу пропускної здатності та мінімізації затримок. Застосування технології MEC дозволяє зменшити навантаження на основну мережу та забезпечити високу швидкість доступу до даних.

Інтеграція спеціалізованих рішень для обслуговування різних типів трафіку сприяє підвищенню якості користувацького досвіду та стабільності роботи мережі. Водночас питання кібербезпеки залишаються пріоритетними, оскільки загрози інформаційної безпеки можуть безпосередньо впливати на надійність та працездатність мережевої інфраструктури. Подальші дослідження у сфері QoS у 5G можуть бути спрямовані на розширення можливостей самонавчальних систем управління трафіком, інтеграцію з технологіями 6G та розвиток нових підходів до забезпечення інформаційної безпеки у бездротових мережах.

Література

1. Dahlman E., Parkvall S., Skold J. "5G NR: The Next Generation Wireless Access Technology." Academic Press, 2020. [ericsson.com].
2. Andrews J. G., Buzzi S., Choi W. та ін. "What Will 5G Be?" // IEEE Journal on Selected Areas in Communications. 2014. [arxiv.org ; researchers.mq.edu.au].
3. ITU-R M.2083-0. "IMT Vision – Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond."[https://www.itu.int/rec/R-REC-M.2083-0-201509-I].
4. Zhang S., Wang S., Xu H., Liu H. "5G: Towards Energy-Efficient, Low-Latency and High-Reliable Communications Networks" // IEEE Communications Surveys & Tutorials. 2019.[https://ieeexplore.ieee.org/document/8377403].
5. Cisco Annual Internet Report (2018–2023) // Cisco Systems, 2020. [https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html].

УДК 681.3:002

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПІД ЧАС ЗБЕРІГАННЯ, ОБРОБКИ ТА ПЕРЕДАЧІ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Леляк А.В., Астраханцев А.А.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: lelyak.andrey@gmail.com

ENSURING PROTECTION DURING STORAGE, PROCESSING AND TRANSMISSION OF ELECTRONIC DOCUMENTS

Electronic documents security principles are analyzed for three main implementation options: foreign passport with embedded chip, mobile driving license on a smartphone and server-based solution with a “thin” client on smartphone.

Електронне посвідчення особи – це цифрове рішення, що дозволяє громадянам підтвердити свою особистість без використання паперових документів. Основними варіантами імплементації електронних документів є імплементація згідно зі стандартом ICAO Doc 9303 [1] (закордонний паспорт з інтегрованим чіпом), імплементація згідно зі стандартом ISO/IEC 18013-5 [2] (електронне посвідчення водія) та внутрішні рішення всередині окремих країн, як-от Дія, що не забезпечують міжнародної сумісності. Рівень безпеки електронних документів є одним з вирішальних факторів [3] для переходу від паперових документів, оскільки конфіденційність, цілісність та стабільність доступу є гарантією взаємної довіри між громадянином та державою. Наприклад, для уніфікованого розв'язування типових задач безпеки електронних документів був створений регламент Європейського Союзу про електронну ідентифікацію та довірчі послуги для електронних транзакцій (eIDAS), і велика кількість країн докладають суттєвих зусиль для сумісності з цим стандартом [4].

Для порівняння шляхів розв'язання задач безпеки розглянемо три імплементації електронних документів:

1. Класичний закордонний паспорт з чіпом згідно зі стандартом ICAO Doc 9303
2. Електронне посвідчення водія в Google Wallet чи Samsung Wallet згідно зі стандартом ISO/IEC 18013-5
3. Рішення «Дія» від Міністерства цифрової трансформації України

Закордонний паспорт реалізований у вигляді пластикової картки з інтегрованим чіпом, де паспортні дані дублюються в надрукованому та електронному вигляді. Мобільне посвідчення водія реалізоване у вигляді застосунку для iOS чи Android, чутливі дані якого зберігаються на окремому захищеному чипі всередині телефону. «Дія» теж реалізована як застосунок для iOS чи Android, але дані зберігаються на віддаленому захищеному сервері.

Основними компонентами будь-якої системи електронних документів є

орган видачі, тримач та зчитувач документа. Орган видачі зберігає та керує документами, і видає їх тримачу документа. Тримач документа зберігає документ у себе на пристрої та надає його зчитувачу на вимогу. Зчитувач отримує документ від тримача та перевіряє його.

Розглянемо наступні задачі безпеки для електронних документів:

1. Уникнути несанкціонованої вичитки даних документа
2. Уникнути підслуховування каналу зв'язку
3. Автентифікувати сховище документа
4. Автентифікувати дані документу
5. Автентифікувати зчитувач
6. Отримати згоду тримача документа на передачу даних

Уникнення несанкціонованої вичитки закордонного паспорта забезпечується використанням гаманця з RFID-захистом, як і для банківських карт, що використовують схожий чіп. Для водійського посвідчення в телефоні використовуються засоби контролю доступу операційної системи такі, як вимкнення NFC, направлення NFC запитів лише до авторизованих додатків та додаткова автентифікація користувача на початку обробки повідомлень в додатку. Для рішень, що ґрунтуються на збережені даних на захищеному сервері, ця задача безпеки виконується через посилання документа лише після двосторонньої автентифікації сервера з додатком.

Основним способом захисту від підслуховування каналу зв'язку є шифрування цього каналу. Для закордонних паспортів використовується механізм PACE (Password Authenticated Connection Establishment), що формує сесійні AES ключі за допомогою даних з зони машинного зчитування (Machine Readable Zone, MRZ), надрукованої на пластику документа. Схожим чином працює шифрування каналу зв'язку для передачі електронного посвідчення водія, де AES ключі формуються з сесійних даних, унікальних для кожної передачі даних між тримачем документа та зчитувачем. Для шифрування передачі даних між «Дією» та сервером використовується протокол TLS, як і для більшості застосунків.

Для автентифікації сховища документа у випадку закордонного паспорта використовується механізм Chip Authentication, за допомогою якого формуються нові симетричні сесійні ключі на базі асиметричного статичного ключа з чіпа та асиметричного сесійного ключа зчитувача. У випадку електронного посвідчення водія використовуються механізм mDoc Authentication, під час якого тримач документа накладає електронний підпис чи рахує Message Authentication Code (MAC) на метадані документа і передає його зчитувачу разом зі своїм сертифікатом. Для рішень, що базується на збереженні даних документа на сервері, використовується класичний підхід Public Key Infrastructure (PKI), в якому застосунок та сервер обмінюються сертифікатами та перевіряють їх.

Для автентифікації даних документа у всіх рішеннях використовується цифровий підпис, що накладається органом видачі на дані документа, зберігається разом з документом, і передається разом з документом зчитувачу, щоб підтвердити автентичність цих даних.

Для автентифікації зчитувача закордонного паспорта виконується процедура Terminal Authentication, під час якої зчитувач підписує своїм приватним асиметричним ключем довільні дані, надіслані тримачем

документа, а тримач має змогу перевірити цей підпис за допомогою надісланого сертифіката зчитувача з асиметричним публічним ключем. Для електронного водійського посвідчення використовується механізм Reader Authentication, під час якого схожим чином зчитувач підписує дані, що унікальні для поточної сесії передачі даних, а зчитувач перевіряє валідність цього підпису за допомогою сертифіката зчитувача. «Дія» використовує схожий власний механізм.

Для отримання згоди тримача документа на передачу даних чи їх частини потрібен факт свідомого вибору та підтвердження користувача. Для закордонного паспорта це є демонстрація документа особі, що його перевіряє, та прикладання документа до зчитувача. Для мобільного водійського посвідчення це вибір потрібного UI елемента в застосунку на екрані телефону, а для «Дії» це демонстрація QR-коду особі, що перевіряє документ. Також протоколи зі специфікації мобільного водійського посвідчення дозволяють тримачу документа обирати, які поля документа повернути з тих, що запросив зчитувач, що поки не реалізоване в інших варіантах імплементації.

Було розглянуто три варіанти безпечного сховища електронних документів – чіп, вбудований в картку, окремий процесор в мобільному пристрої та сервер. Для розв'язання задач безпеки використовуються різні технічні засоби та протоколи, але всі перераховані рішення є в середньому достатньо безпечними для використання державними структурами. Вибір між цими варіантами імплементації електронних документів повинен базуватися на потребах держави та технічних можливостях держави та мобільних пристроях більшості громадян. Перевагою рішення з чіпом в картці є повний контроль центра видачі над комплексним рішенням електронного документа, що забезпечує високий рівень безпеки при дотриманні всіх протоколів. Рішення з захищеним процесором в телефоні є компромісним варіантом, що дозволяє зберігати електронний документ на будь-якому сучасному мобільному пристрої з високим рівнем безпеки. В такому підході можуть використовуватися більш сучасні та складні підходи до безпеки, але незахищений телефон користувача може бути використаний як додаткова точка входу в систему для нападника. Рішення зі збереженням документа на сервері є найменш вибагливим до користувацьких пристроїв, і дозволяє зосередити більшість зусиль з підвищення безпеки на віддаленому сервері. Але таке рішення потребує зв’язку з сервером як для тримача документа, так і для зчитувача для будь-якої операції.

Література

1. Machine Readable Travel Documents, ICAO Doc 9303 v8, 2021.
2. Personal identification — ISO-compliant driving licence, Part 5: Mobile driving licence (mDL) application, ISO/IEC 18013-5:2021, 2021.
3. V. Tsap, “eID Public Acceptance: Success Factors, Citizen Perception, and Impact of Electronic Identity,” Ph.D. dissertation, Tallinn University of Technology, Tallinn, Estonia, 2022.
4. A. Sharif, M. Ranzi, R. Carbone, G. Sciarretta, F. A. Marino, and S. Ranise, “The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes,” *Applied Sciences*, vol. 12, no. 24, p. 12679, Dec. 2022, doi: https://doi.org/10.3390/app122412679.

УДК 004.4

АНАЛІЗ КОНЦЕПЦІЇ ТА ПРИНЦИПІВ ФУНКЦІОНУВАННЯ МЕРЕЖ NON-TERRESTRIAL NETWORKS (NTN)

Шелест Є.В., Правило В.В., Лісовський К.С.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail:krohaenot522@gmail.com, v.v.pravylo@ukr.net, k.lisovskyi-2024@kpi.ua

ANALYSIS OF THE CONCEPT AND PRINCIPLES OF FUNCTIONING OF NON-TERRESTRIAL NETWORKS (NTN)

The basic principles and trends in the development of Non-Terrestrial Networks (NTN) are summarized. The results of simulations of signal propagation and connectivity performance in NTN systems are presented.

Розвиток телекомунікаційних технологій є ключовим фактором соціально-економічного прогресу, що зумовлює зростаючий попит на швидкісний та безперервний зв’язок. У важкодоступних регіонах традиційні наземні мережі малоефективні, тому перспективним рішенням є неназемні мережі (NTN), які використовують супутники, дрони та висотні платформи. NTN інтегруються з наземними мережами, забезпечуючи глобальне покриття та зв’язок у кризових ситуаціях. У статті аналізуються архітектура, принципи роботи та перспективи розвитку NTN в умовах впровадження технологій 5G і 6G.

Мережі Non-Terrestrial Networks (NTN) — це інноваційний підхід до забезпечення глобального покриття зв'язку за допомогою позаземних платформ, таких як супутники, висотні платформи (HAPS) та космічні системи. Вони дозволяють забезпечити зв'язок у віддалених і важкодоступних регіонах, де побудова традиційної наземної інфраструктури є неможливою або економічно невигідною.

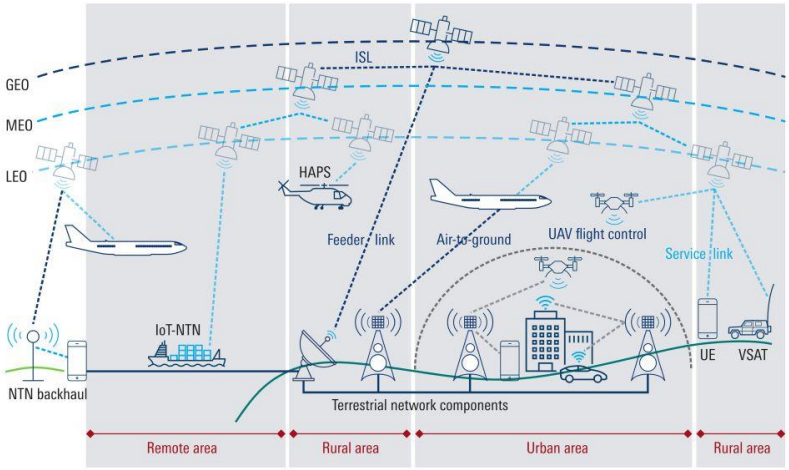


Рис. 1. Огляд можливостей підключення у NTN.

Основними компонентами NTN є геостаціонарні супутники (GEO) з високою затримкою сигналу, низькоорбітальні (LEO) для швидкого зв’язку, середньоорбітальні (MEO) як компроміс між охопленням і затримкою, висотні платформи (HAPS) для тимчасового покриття та космічні платформи для майбутнього глобального зв’язку.

Мережі NTN поділяються на три основні типи:

- Супутникові системи зв’язку — включають GEO, LEO та MEO супутники.

- Висотні платформи (HAPS) — використовуються для регіонального покриття з низькою затримкою сигналу.

- Космічні платформи — майбутній напрямок для глобального зв’язку за межами атмосфери.

Архітектура мережі NTN має багаторівневу структуру. Космічний рівень включає GEO, MEO та LEO супутники, які забезпечують глобальне покриття. Рівень висотних платформ (HAPS) складається з дронів і дирижаблів, що працюють на висоті до 20 км, забезпечуючи регіональне покриття та низьку затримку сигналу. На рівні користувача інтеграція з традиційними наземними мережами дозволяє створити безшовне покриття.

Протоколи зв’язку передбачають маршрутизацію та управління трафіком, де супутники та HAPS динамічно налаштовують маршрути залежно від стану мережі. Використання beamforming та адаптивного покриття дозволяє ефективно керувати напрямком сигналу, підвищуючи якість зв’язку та зменшуючи інтерференцію.

Забезпечення якості зв’язку включає зменшення затримки сигналу та компенсацію помилок. Використання LEO-супутників дозволяє знизити затримку до рівня традиційних мереж, а алгоритми корекції помилок покращують якість сигналу, компенсуючи спотворення, що виникають при проходженні через атмосферні перешкоди.

Управління трафіком забезпечується за рахунок динамічного перенаправлення сигналу та мінімізації втрат. Мережа автоматично змінює маршрути для уникнення перевантаження, а коригування параметрів сигналу враховує погодні умови та рівень завантаженості, що дозволяє зменшити втрати сигналу.

Переваги та застосування NTN.

Покриття у важкодоступних регіонах. NTN дозволяють забезпечити стабільний зв'язок у місцях, де наземна інфраструктура недоступна або економічно невигідна. Це охоплює пустелі, океани, гори та полярні області. Супутникові та висотні платформи забезпечують безперервне покриття незалежно від географічних умов.

Надійність зв'язку під час надзвичайних ситуацій. У випадку природних катастроф, воєнних конфліктів або пошкодження наземної інфраструктури NTN можуть оперативно відновити зв'язок. Висотні платформи та супутники забезпечують швидке розгортання покриття навіть у кризових умовах.

Військове застосування. NTN забезпечують безпечний і захищений зв'язок для військових операцій. Вони дозволяють здійснювати моніторинг, управління військовими діями та передачу оперативних даних у реальному часі навіть у зонах бойових дій.

Покращення роботи IoT (Internet of Things). NTN сприяють розвитку IoT, забезпечуючи з'єднання пристроїв у віддалених регіонах без необхідності побудови наземної інфраструктури. Це відкриває нові можливості для автоматизації, дистанційного моніторингу та управління пристроями.

Забезпечення доступу до інтернету у віддалених регіонах. NTN дозволяють забезпечити доступ до інтернету в сільських та ізольованих районах як альтернативу традиційному мобільному зв’язку. Супутникові системи, такі як Starlink від SpaceX, уже успішно забезпечують високошвидкісний інтернет у таких регіонах.

Окреслені перспективні напрямки досліджень ДР. Розраховані частоти власних коливань «квадрупольного» типу прямокутного ДР з використанням методу кінцевих елементів та методу магнітної стінки. Досліджено розподіл полів власних коливань ДР. Показано, що результати розрахунку аналітичним методом добре узгоджуються із отриманими результатами методом кінцевих елементів.

Література

1. Non-Terrestrial Networks for Energy-Efficient Connectivity of Remote IoT Devices in the 6G Era: A Survey / S. Plastras et al. *Sensors*. 2024. Vol. 24, no. 4. P. 1227. URL: https://doi.org/10.3390/s24041227.
2. Non-Terrestrial Network Basics, Advantages, and Challenges. *Keysight*. URL: https://www.keysight.com/us/en/cmp/topics/non-terrestrial-network-basics-advantages-and-challenges.html.
3. What are Nonterrestrial Networks? A Guide to NTNs - NI. *Mess- und Prüfsysteme, bei Emerson - NI*. URL: https://www.ni.com/en/solutions/semiconductor/non-terrestrial-network-test/what-is-ntn.html.
4. Non-Terrestrial Networks: The Key Tech Foundations Supporting Next-Gen Connectivity. *IQT*. URL: https://www.iqt.org/library/non-terrestrial-networks-the-key-tech-foundations-supporting-next-gen-connectivity.

УДК 621.382

АНАЛІТИЧНИЙ ОГЛЯД ОСОБЛИВОСТЕЙ ПОБУДОВИ ТА ЗАГАЛЬНИХ ВИМОГ ЯКІ ВИСУВАЮТЬСЯ ДО БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

Руренко О.Г., Гетьман О.В., Фуртат О.В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна;
Таврійський національний університет імені В.І.Вернадського, Україна
E-mail: a.rurenko@gmail.com, furtatlena@gmail.com,

ANALYTICAL REVIEW OF THE STRUCTURAL FEATURES AND GENERAL REQUIREMENTS FOR WIRELESS SENSOR NETWORKS

The wide capabilities of wireless networks served as the basis for the creation of new specialized networks, which were called sensor networks. The sources of information in them are sensors. The reduction in the size of computing devices, the increase in computing power in miniature elements made it possible to create sensors in which primary information processing is carried out and which are called sensors. Today, modern BMSs have lower deployment and maintenance costs, last longer and are more reliable. They are used in our homes, workplaces and beyond, providing new sources of control and information and bringing convenience to our personal and professional lives.

Зниження витрат на розгортання БСМ при збільшенні функціональності пов'язане зі значними успіхами в чотирьох областях: створення датчиків, напівпровідникових пристроїв на основі CMOS, нових мережевих протоколів і технології енергозбереження. Кульмінацією цих зусиль є розгортання БСМ у рамках концепції Інтернету речей(1оТ), що з'являється.

Основою будь-якої БСМ є датчики. У останні десять років спостерігається швидкий розвиток технологій з множинним зондуванням:

- мікроелектромеханічні системи(MEMS) — гіроскопи, акселерометри, магнітометри, датчики тиску, датчики піроелектричного ефекту, акустичні датчики;
- датчики на основі CMOS — температура, вологість, ємнісна близькість, хімічний склад;
- світлодіодні датчики — вимір освітленості, зондування, хімічний склад.

При об'єднанні в мережу ці датчики дозволяють використати нові застосування, такі як оптимізація управління і освітлення HVAC усередині будинків і будівель.

Більшість систем опалювання, вентиляції і кондиціонування повітря у кращому разі запрограмована на таймери і не враховують фізичну присутність людей. Використовуючи датчики MEMS, CMOS і LED для відстежування умов довкілля (вологість, температура, навколишнє світло) і присутності людей (піроелектричні, оптичні і акустичні), інтелектуальні

системи можуть бути спроектовані так, щоб різко понизити загальну потужність. Необхідно здійснювати управління електроспоживанням і освітлювальними приладами і відключати їх у разі відсутності людини або якщо навколишнє освітлення є адекватним.

Крім того, як тільки мережа датчиків буде встановлена, можуть бути реалізовані додаткові функції. Наприклад, акустичні датчики можуть використовуватися повторно для спостереження за фізичною присутністю людини впродовж дня і для виявлення розбитого скла від потенційного злому у вечірні години.

Мережеві топології безпровідних датчиків зазвичай підрозділяються на чотири категорії: однонапрямлені, двонаправлені, зоряні і комірчасті мережі.

Першими мережевими протоколами були прості односторонні лінії зв'язку, які все ще поширені в системах контролю тиску в шинах, відкривачах гаражних воріт і телевізійних пультах дистанційного керування. У міру того, як виникла необхідність у більше просунутих топологіях, розробники мереж розробили протоколи з низькою пам'яттю для двонаправлених комірчастих топологій. Крім того, в галузі відбувається перехід до стандартизованих протоколів, аналогічно переходу в MCU від звичних наборів інструкцій і до ядер на основі 8051 для 8-бітової обробки і ARM- рішень для 32-розрядних застосувань. Наявність набору стандартизованих мережевих протоколів, таких, як ZigBee, знімають навантаження на розробку і дозволяє постачальникам зосередитися на своїх конкретних застосуваннях.

Поява рентабельної топології сітки дозволяє створювати нові застосування, де традиційні топології вже не задовольняють потреби. Наприклад, додаток для домашнього освітлення може перевищувати 30 індикаторів і датчиків. Маршрутизатор Wi - Fi часто не може забезпечити покриття усього будинку через багатопроменеве розповсюдження або затінювання, але топологія сітки забезпечує надійне з'єднання з усіма місцями розташування у будинку. Крім того, топологія осередків, що надається програмним забезпеченням ZigBee, наприклад EmberZNet PRO від Silicon Labs, дозволяє працювати сотням і тисячам вузлів в одній мережі, що набагато більше, ніж в Bluetooth або Wi - Fi.

Сформулюємо деякі особливості і загальні вимоги, що пред'являються до сенсорних мереж.

1. Залежно від характеру додатків, виду джерел енергії і тривалості життєвого циклу елементів сенсорні мережі повинні мати відповідні технології обслуговування. Мережі націлені не стільки на передачу числової інформації, скільки на отримання відповіді в результаті її обробки. Тому, навіть, невелика втрата даних може привести до абсолютно неправильного результату.

2. Проблеми географічного охоплення є природними вимогами, які відсутні в інших мережах.

3. Для сенсорних мереж властиві специфічні критерії якості обслуговування. Традиційні показники QoS в них не застосовуються. Проте обслуговування БСМ має бути «хорошим». Це означає, що правильні відповіді мають бути доставлені в потрібне місце, в потрібний час.

4. Сенсорна мережа повинна надійно працювати при відмові яких-небудь вузлів, робота яких припиняється через нестачу енергії або фізичного руйнування.

5. Уся сенсорна мережа повинна продовжувати роботу впродовж усього свого життєвого циклу, а не впродовж життєвого циклу окремих вузлів. Визначення життєвого циклу мережі залежить від типу додатка.

6. Сенсорна мережа повинна задовольняти умовам масштабованості і при необхідності забезпечувати підтримку роботи великого числа вузлів.

7. Сенсорна мережа повинна мати широкий діапазон щільності розміщення вузлів, який залежить від додатка.

8. Мережа повинна мати підвищену гнучкість і можливість легкого перепрограмування вузлів в польових умовах.

9. Мережа повинна мати можливість самоконтролю, для її працездатності в умовах зміни довкілля.

10. Мережа повинна мати можливість включення додаткових ресурсів таких, як знову розгортані вузли.

Висновок. Безпроводові сенсорні мережі (БСМ) — це нова, дуже перспективна технологія отримання, передачі і зберігання інформації для різних застосувань. Вони розширюють можливості контрольних і інформаційно-вимірювальних систем, роблячи їх розподіленими в просторі. Вже перші застосування таких мереж показали, що для їх повсюдної реалізації потрібно буде виконати багато дослідницької роботи, для виконання вимог широкого класу додатків.

Література

1. Mainwaring A., Polastre J., Szewczyk R., Culler D., Anderson J. Wireless Sensor Networks for Habitat Monitoring // First ACM Workshop on Wireless Sensor Networks and Applications (WSNA). 2002. P. 88-97.
2. Bagula A. Applications of wireless sensor networks. — https://www.uonbi.ac.ke/conferences/WSN/dayl/Applications.pdf
3. Madhu A., Sreekumar A. Wireless Sensor Network Security in Military Application using Unmanned Vehicle. https://www.semanticscholar.org/paper/Wireless-Sensor-Network-Security-in-Military- using- Madhu-Sreekumar/e0aa0e813ccb502c37f03a7b91b477e35336c63d
4. Othmana M.F., Shazalib K. Wireless Sensor Network Applications: A Study in Environment Monitoring System // IEEE Sensors Applications Symposium (SAS), 2018. DOI: 10.U09/SAS.2018.8336723
5. Puccinelli D., M. Haenggi Wireless Sensor Networks:Applications and Challenges of Ubiquitous Sensing Abstract Feature // IEEE Circuits and Systems Magazine. 2005. Vol. 5, no 3. P. 19-31.

УДК 004.4

ПІДХІД ДО СТВОРЕННЯ АВТОМАСШТАБОВАНОЇ ПРОГРАМНО-КОНФІГУРОВАНОЇ МЕРЕЖІ НА ОСНОВІ KUBERNETES ТА ANTREA CNI

Рубан В.В., Алєксєєв М.О.

Навчально-науковий інститут телекомунікаційних систем
НТУУ «КПІ» ім. Ігоря Сікорського, Україна
E-mail: vladyslav.ruban20@gmail.com, alexeyev@its.kpi.ua

ANALYSIS OF KUBERNETES SOFTWARE COMPONENTS TO IMPLEMENT THE SOFTWARE-DEFINED NETWORKING APPROACH

The work is dedicated to the pressing issue of building a private cloud based on a heterogeneous environment with a dynamic architecture using users' non-alienable computing resources. Specifically, it explores the possibilities of utilizing SDN (Software-Defined Networking) technologies to create a corporate software-defined network under conditions where network load-dependent automatic scaling of its active elements occurs. These elements are implemented as containerized applications running in a cluster managed by Kubernetes. The study includes a review analysis of software components for network interaction within the cluster (CNI plugins) and justifies the use of Antrea CNI.

У сучасних комп’ютерних мережах, особливо побудованих за принципом програмно-конфігурованих мереж (SDN, Software-Defined Networking), ефективне управління обчислювальними ресурсами є критично важливим завданням. SDN розділяє контрольний та комутаційний рівні, що надає гнучкість у керуванні мережею, але також створює додаткове навантаження на центральні обчислювальні ресурси контролерів і обробки трафіку.

Kubernetes є потужною платформою для автоматизованого розгортання, масштабування та управління контейнеризованими додатками. Його механізми авто-масштабування дозволяють динамічно змінювати кількість активних компонентів на основі поточного навантаження. Це особливо актуально в контексті SDN-мереж, де навантаження на окремі елементи (контролери, балансувальники, функції обробки трафіку) може змінюватися в залежності від потоку даних та мережевих подій.

Основна проблема полягає в тому, що традиційні підходи до масштабування мережевих компонентів часто є статичними або вимагають ручного втручання, що може призводити до перевантажень або неефективного використання ресурсів. Використання Kubernetes для автоматичного масштабування активних елементів SDN-мереж дозволяє покращити адаптивність системи, підвищити її продуктивність та забезпечити оптимальний розподіл ресурсів у реальному часі. Однак інтеграція механізмів Kubernetes із мережею SDN потребує дослідження, оскільки виникають питання ефективної взаємодії, балансування навантаження та моніторингу мережевих станів.

Дана робота присвячена актуальній задачі розробки та дослідження підходів до автомасштабування елементів SDN-мереж за допомогою Kubernetes, що дозволить досягти більш ефективного використання обчислювальних ресурсів та підвищити гнучкість управління мережею.

В даній роботі у якості елемента управління мережею був обраний Antrea - мережевий плагін Kubernetes, побудований згідно специфікації CNI (Container Network Interface), оскільки його архітектура базується на принципі SDN. Antrea створює архітектуру, подібну до SDN, розділяючи панель даних (яка базується на Open vSwitch або OVS) і панель управління. Для цього Antrea встановлює агентський компонент на кожному з робочих вузлів для програмування OVS datapath, в той час як центральний контролер, що працює на вузлі плану управління, відповідає за централізовані завдання, такі як розрахунок мережевих політик [3] (див. рис 2).

Кінцевий користувач взаємодіє з кластером за допомогою K8s API Server, що є ключовим елементом в інфраструктурі Kubernetes. Кожна дія, наприклад, створення, оновлення чи видалення ресурсів кластера (pods — контейнеризоване середовище для працюючого застосунку, service — логічна надбудова для pods, тощо) проходить через цю абстракцію. Принцип роботи налаштованого кластера добре ілюструє наступна діаграма послідовностей UML (Unified Modeling Language) (див. рис. 1), на якій узагальнено показано кроки, через які проходить запит.

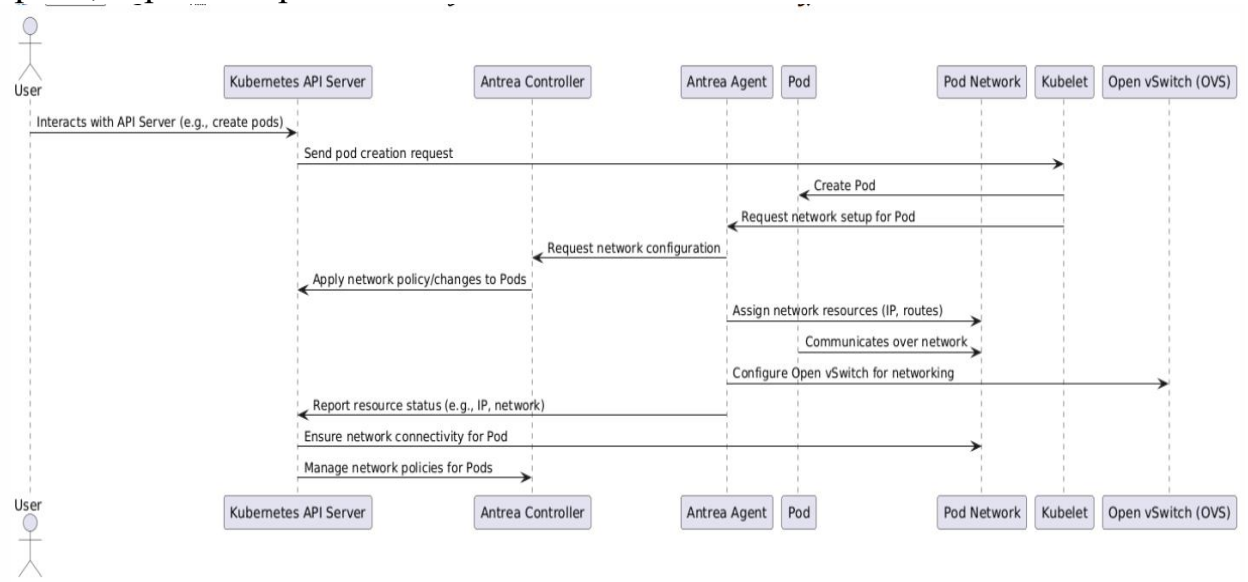


Рис. 1. Діаграма послідовностей UML, що показує логіку в K8s кластері з Antrea.

Для дослідження доцільності використання Antrea для створення автомасштабованої програмно-конфігурованої мережі на основі Kubernetes у роботі був розроблений лабораторний стенд, який складається з трьох віртуальних машин, одна з яких управляюча (controlplane), а дві інші використовуються як робочі вузли кластеру (worker nodes) (див. рис. 2). Задля перевірки продуктивності кластера з плагіном Antrea було розроблено скрипт, який автоматизує створення тестових об'єктів і симуляцію трафіку в кластері для демонстрації роботи мережевих політик, таких як AntreaNetworkPolicies та AntreaClusterNetworkPolicies [1].

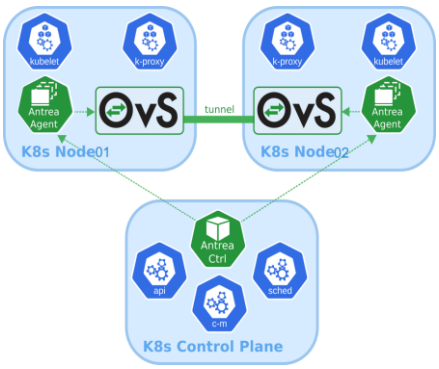


Рис. 2 - Архітектура робочого середовища.

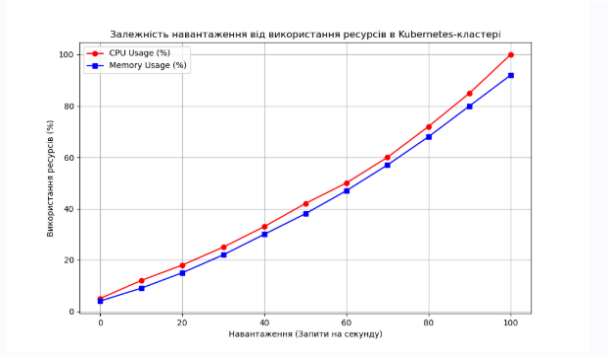


Рис. 3 а)

Рис. 3 б)

Рис. 3 в)

Рис. 3. Графіки залежності: а) навантаження від використання ресурсів в кластері; б) зміни пропускної здатності; в) часу відгуку запитів до та після застосування мережевих політик.

Висновки. Розроблений у роботі підхід та програмне забезпечення дозволило протестувати ефективність роботи та масштабування кластера з використанням Antrea. Впровадження Antrea CNI дозволило організувати взаємодію між компонентами рівня управління програмно-конфігурованої мережі безпосередньо у складі кластеру Kubernetes з використанням протоколів SDN, а також гнучко налаштовувати мережеві політики доступу між окремими обчислювальними елементами. Величина втрат продуктивності при застосуванні мережевих політик є на рівні 3-7% (див.рис.3) при однаковій структурі кластеру, але можливість роботи у середовищі Kubernetes, що дозволяє варіювати кількістю реплік активних елементів в залежності від навантаження надає суттєві переваги при роботі у динамічному середовищі, кількісні показники яких планується отримати у подальшій роботі.

Література

1. GitHub репозиторій “sdn-k8s”: Онлайн: https://github.com/wannabelll/sdn-k8s: 04.03.2024.
2. CNI Documentation. “Why develop CNI?”: Онлайн: https://www.cni.dev/docs/: 01.03.2025 18:00.
3. Antrea Docs. : Онлайн: https://antrea.io/docs/v2.3.0/ 01.03.2025 18:00.

УДК 004.4

АДАПТИВНА МУЛЬТИПРОТОКОЛЬНА АРХІТЕКТУРА IOT СИСТЕМ

Самсонов С.С., Глоба Л.С.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: s.samsonov@kpi.ua

ADAPTIVE MULTIPROTOCOL IOT SYSTEM ARCHITECTURE (AMISA)

This paper presents a brief review of application-layer protocols for resource-constrained IoT devices (MQTT, CoAP, LwM2M) and proposes an adaptive multiprotocol architecture (AMISA). The architecture allows smart switching between different protocols to optimize energy usage, reliability, and delivery guarantees in unstable network conditions.

Дослідження наукової літератури демонструє наявність великої кількості досліджень комунікаційних протоколів IoT систем. Такі протоколи прикладного рівня як Message Queing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Lightweight M2M (LwM2M) вважаються фундаментальними для використання для IoT систем з обмеженими ресурсами [1] та забезпечують енергоефективність, надійність та безпечну передачу даних.

Статті що проводять аналіз та порівняння різних протоколів прикладного рівня [2] відзначають що CoAP має мінімальну надлишкову сервісну інформацію пакетів, втім не може гарантувати 100% доставку пакетів в поганих умовах передачі, а MQTT зарекомендував себе дуже гарно для пристроїв з обмеженим ресурсом батареї в певних сценаріях. В дослідженні що глибоко порівнює MQTT, CoAP та HTTP підкреслюють сильні та слабкі сторони цих протоколів, зважаючи розмір повідомлень та хедерів, енергоспоживання, затримок та використання різних рівнів QoS (або їх аналогів) [3] [4].

Проте, у наявній літературі бракує описів IoT-систем зі «смарт» передавачами, які здатні динамічно оцінювати стан мережі та перемикатися між кількома протоколами. У такому підході важливо зважати на практичні обмеження. Наприклад, оскільки IoT пристрої є обмеженими у ресурсах, перемикання між більше ніж 2 протоколами було б непратичним. Крім того, такий підхід потрібує відповідної бекенд-інфраструктури. На практиці це означає наявність «інтерконектора протоколів» для одного з протоколів [5] і «шлюзу протоколу» для іншого.

На рис. 1 представлено адаптивну мультипротокольну архітектуру IoT системи (Adaptive Multiprotocol IoT System Architecture, AMISA), що передбачає належну бекенд-інфраструктуру для ефективного використання багатопротокольних IoT-передавачів у різних сценаріях. На відміну від існуючих типових багатопротокольних рішень, AMISA додає ще два вузли для координації роботи таких пристроїв.

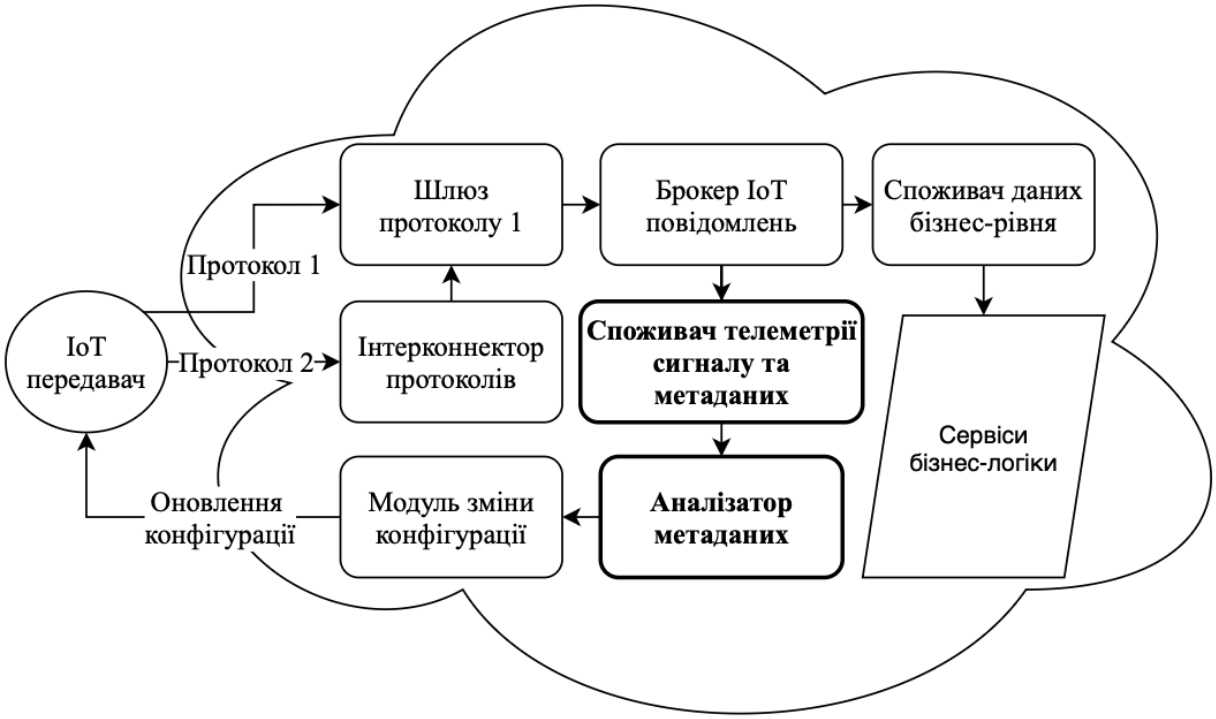


Рис.1. Адаптивна мультипротокольна архітектура IoT системи (AMISA).

Нижче розглянуто призначення кожного вузла:

IoT передавач — це передавальний пристрій, який збирає та/або агрегує дані і надсилає їх у хмару. Він обирає один із двох прикладних протоколів для передачі чергового повідомлення залежно від поточного стану мережі та конфігурації, що надходить від бекенд системи.

Інтерконектор протоколів одночасно є шлюзом для повідомлень, надісланих за допомогою Протоколу 2, і перетворювачем цих повідомлень у помвідомлення Протоколу 1. Після «перекладу» повідомлення передаються далі через шлюз Протоколу 1.

Шлюз протоколу 1 виступає «стандартною» точкою входу всіх повідомлень у систему — як безпосередньо від IoT-відправника, так і від вузла протокольного інтерконектора. За потреби цей вузол додає метадані та перенаправляє повідомлення до брокера IoT-повідомлень.

Брокер IoT-повідомлень зберігає отримані повідомлення від IoT-пристроїв. Оскільки повідомлень може бути дуже багато, наявність брокера підвищує надійність, відмовостійкість і масштабованість бекенд-системи та дозволяє різним сервісам читати лише потрібні їм дані. Такий вузол є досить типовим для систем із великою кількістю подій.

Споживач даних бізнес-рівня і сервіси бізнес-логіки відображають базову бізнес-логіку системи та не є основним предметом цього дослідження.

Споживач телеметрії сигналу та метаданих отримує релевантні дані, які допомагають визначити стан мережевого середовища (наприклад,

відношення сигнал-шум), рівень заряду батареї пристрою, тип повідомлення (наприклад, критичний звіт про збій чи звичайне «хартбіт»-повідомлення), а також ефективність доставки (наприклад, затримка, кількість повторних спроб, рівень QoS, використаний протокол).

Аналізатор метаданих обробляє дані, отримані від попереднього вузла. На базі великих вибірок статистичної інформації цей вузол приймає рішення, який протокол бажано використовувати за певних умов, і передає це рішення далі до модуля зміни конфігурації. Логіка прийняття рішення може бути реалізована за допомогою машинного навчання або ж у вигляді попередньо запрограмованих алгоритмів.

Модуль зміни конфігурації приймає рішення від попереднього вузла, трансформує його у формат придатний для оновлення конфігурації на IoT-передавачі, і надсилає таке оновлення.

В цій архітектурі важливе значення має саме оновлення конфігурації, а не прошивки передавача. Якщо ПЗ IoT передавача буде достатньо гнучким — бажаний ефект оновлення логіки вибору протоколу для відправки повідомлення може бути досягнутий за допомогою оновлення параметрів конфігурації. В порівнянні з оновленням прошивки це дозволятиме менше навантажувати мережу великою кількістю даних та уникнути ризику виходу IoT пристрою з ладу під час оновлення прошивки. При цьому слід пам’ятати що такі оновлення конфігурації не повинні відбуватися занадто часто: це дозволить аналізатору метаданих накопичити достатньо даних для аналізу та не перевантажувати мережу частими пакетами з оновленням конфігурації.

Література

1. Sharma C., Gondhi N.K. Communication protocol stack for constrained IoT systems : Proc. 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU) (25–27 Feb. 2018; Bhimtal, India). – 2018. – P. 1–6.
2. Al-Masri E., Mahmoud Q.H., Pham D., Ezeobi C., Abdelrahman S.M., Yan C., Ali A.K. Investigating messaging protocols for the internet of things (IoT) // IEEE Access. – 2020. – Vol. 8. – P. 94880–94911.
3. Naik N. Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP: Proc. 2017 IEEE International Systems Engineering Symposium (ISSE) (11–13 Oct. 2017; Vienna, Austria). – 2017. – P. 1–7.
4. Sreeraj S., Kumar G.S. Performance of IoT protocols under constrained network: a use case based approach : Proc. 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT) (15–17 Feb. 2018; Chennai, India). – 2018. – P. 495–498.
5. Dave M., Doshi J., Arolkar H. MQTT-CoAP interconnector: IoT interoperability solution for application layer protocols : Proc. 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) (7–9 Oct. 2020; Palladam, India). – 2020. – P. 122–127.

УДК 004.89

ТЕХНОЛОГІЯ NAAS ПЕРЕВАГИ ТА НЕДОЛІКИ

Глоба Л.С., Цуканов О.Ф.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: cukanov-o@ukr.net; lgloba@its.kpi.ua

NAAS TECHNOLOGY: ADVANTAGES AND DISADVANTAGES

The article examines the issue of using NaaS in telecommunications. It is shown that the use of this technology can significantly increase their efficiency. Such systems enable the creation of new content by processing large volumes of data from deep learning neural networks. This makes it possible to develop new applications faster and more cost-effectively.

У статті розглянуто проблему використання NaaS в телекомунікаціях. Показано, що використання цієї технології може значно підвищити їх ефективність. Такі системи дозволяють створювати новий контент, обробляючи великі обсяги даних з нейронних мереж глибокого навчання. Це дає можливість створювати нові додатки швидше та економічно ефективніше.

Міграція до хмарних послуг, їх широке використання та суттєва потреба в мобільності вимагає нових концепцій побудови мережі підприємства. Підприємствам потрібні більші та гнучкіші можливості разом зі зменшенням витрат на побудову власної мережі. Прикладом може бути проєкт NaaS компанії Meta Networks, який здатний задовільнити такі потреби, забезпечуючи роботу сервісів мережі та їх безпеку [1].

NaaS або Network-as-a-service є послугою «мережа як сервіс». Принцип роботи NaaS базується на використанні сервісів транспортних з'єднань, тобто є орієнтованим на продаж послуг мережі клієнтам, які не бажають або не можуть побудувати власну мережеву інфраструктуру. Сервіс включає функціонал, який забезпечує WAN-з'єднання, підключене до ЦОД, в тому числі організацію пропускної полоси на вимогу, забезпечуючи безпеку, задану якість обслуговування та інші показники. NaaS як правило є доповненням хмарних сервісів, які надаються в моделі IaaS, SaaS, PaaS.

NaaS не вимагає необхідності встановлювати обладнання, замовникам не потрібно купувати, обслуговувати та керувати ніякими RAS або VPN концентраторами. Сервіс передбачає легке налаштування політики управління безпекою.

Як і інші хмарні послуги, NaaS керується постачальником послуг і надається за фіксовану плату. Це логічний результат переходу багатьох бізнес-процесів у хмару. NaaS замінює VPN, MLPS-з'єднання, застарілі мережеві конфігурації та кілька типів локального обладнання, наприклад, балансувальники навантаження і міжмережеві екрани. NaaS справила значний вплив на архітектуру корпоративних мереж, розширюючи їх можливості [2].

По суті, NaaS - це надання мережі за передплатою. Корпоративні клієнти

часто думають, що NaaS схожа на інші хмарні послуги, але насправді вона набагато менш стандартизована, ніж SaaS, до того ж рішення для NaaS набагато складніші, що зумовлено багато в чому необхідністю застосування локального обладнання.

Для організацій, які вважають передплатний підхід до корпоративних мереж привабливим, NaaS пропонує готове рішення, що зазвичай містить обладнання, програмне забезпечення та управління за фіксованою вартістю, а послуги налаштовуються відповідно до конкретних бізнес-вимог замовника. Це дає змогу корпоративним клієнтам згладити фінансові та операційні проблеми, які виникають при постійному оновленні технологій.

Сфера застосування традиційних приватних мережевих сервісів скорочується, а сфера застосування нової моделі, заснованої на доступі, зростає. NaaS по суті є оверлейною мережею, яка забезпечує доступ до застосунків з нульовим рівнем довіри як послугу [3].

Слід зазначити, що гнучкість і масштабованість NaaS дозволяє підлаштовуватись під конкретні потреби, оскільки зміни вносять у програмне забезпечення, а не в обладнання, і такі налаштування виконують на вимогу.

Більшість проблем сумісності NaaS пов'язані з інфраструктурою, наприклад, з успадкованим обладнанням або локальними додатками, які все ще використовуються. За збігом обставин, на багатьох підприємствах деякі важливі процеси або застосунки працюють у локальних ЦОДах, а не в хмарі. І для них перехід на модель NaaS може виявитися непростим, хоча є послуги, які, безумовно, можуть полегшити це завдання.

Оскільки NaaS-з'єднання зазвичай встановлюється з використанням широкосмугового зв'язку загального користування з негарантованою доставкою, послуга доступна тільки там, де є широкосмугове підключення до Інтернету. Для багатьох можливих користувачів NaaS проблемою є потенційна втрата контролю.

Під час передачі мережевих послуг на аутсорсинг у деяких клієнтів виникають сумніви щодо оперативності обслуговування і можливості контролювати свої мережеві ресурси. У відповідь на це з'явилися спільно керовані рішення NaaS, що дають змогу клієнтам розділити з провайдерами роботу з керування мережею, пропускною спроможністю і політиками брандмауера.

Технологія NaaS (Network as a Service) продовжує розвиватися [4], і ось деякі з останніх досягнень у цій галузі:

- успішне розгортання даної технології компанією NaaS Technology Inc.- компанія оголосила початок торгів на NASDAQ, ставши першою зареєстрованою у Китаї пропозицією у цій сфері. Ця подія підкреслює зростаючий інтерес до NaaS на міжнародних ринках.

- розширення мережі зарядних станцій - NaaS Technology досягла значного успіху, охопивши 360 міст і забезпечивши доступ до зарядних станцій для більш ніж 50% міських районів Китаю, це важливий крок у розвитку інфраструктури для електромобілів.

- заміна застарілих технологій - NaaS активно замінює традиційні VPN,

MLPS-з'єднання і застарілі мережеві конфігурації, що дає змогу компаніям оптимізувати свої IT-операції та поліпшити продуктивність.

- перетворення корпоративних IT-служб - технологія NaaS допомагає розширити можливості корпоративних IT-служб, що робить її важливим інструментом для модернізації мережевої інфраструктури.

Крім того, технологія NaaS дозволяє організувати обчислювальний процес в компаніях більш ефективно за рахунок оптимізації IT-операцій. Ось кілька ключових аспектів, які варто враховувати:

- гнучкість і масштабованість: NaaS дає змогу компаніям швидко адаптуватися до мінливих вимог, забезпечуючи можливість масштабування мережевих ресурсів залежно від потреб бізнесу,

- зниження власних витрат: використання NaaS допомагає скоротити капітальні витрати на обладнання та інфраструктуру, оскільки компанії можуть орендувати необхідні ресурси у постачальників послуг,

- спрощення процесу керування інфраструкторою: постачальники NaaS беруть на себе процеси керування мережевою та обчислювальною інфраструктурою,

- безпека і доступність: NaaS пропонує вбудовані механізми безпеки та резервного копіювання, що забезпечує надійний доступ до даних і додатків у будь-який час,

- інтеграція з іншими хмарними послугами: NaaS легко інтегрується з іншими моделями хмарних послуг, такими як IaaS (Infrastructure as a Service) і SaaS (Software as a Service), що дає змогу створювати комплексні рішення для бізнесу: оптимізація мережевих процесів за допомогою NaaS компанії можуть оптимізувати свої мережеві процеси, покращуючи продуктивність і знижуючи затримки в передачі даних [5].

Таким чином, NaaS стає важливим інструментом для організації обчислювальних процесів у сучасних компаніях.

Приклади використання NaaS: віддалений доступ, тобто

- забезпечення безпечного доступу до корпоративних ресурсів для віддалених співробітників,

- хмарні додатки, тобто забезпечення високошвидкісного доступу до хмарних додатків і сервісів,

- Інтернет речей (IoT): підключення та керування пристроями IoT за допомогою надійних мережевих ресурсів.

Можна стверджувати, що технологія NaaS буде широко використовуватися сучасними компаніями, що дасть їм змогу успішно витримувати конкуренцію в сучасних реаліях бізнесу.

Література

1. https://www.it-grad.ru/blog/x-as-a-services-kak-ne-pogryaznut-v-abbreviaturax-oblachnyx-uslug
2. https://selectel.ru/blog/project-naas/.
3. https://www.dailycomm.ru/m/53851/.
4. https://www.itweek.ru/infrastructure/article/detail.php?ID=227514
5. https://naas-tech.com/.

УДК 004.02

ПОКРАЩЕННЯ КЛАСИФІКАЦІЇ ШКІДЛИВИХ URL ЗА ДОПОМОГОЮ ВЕКТОРНИХ ПРЕДСТАВЛЕНЬ НА ОСНОВІ ТРАНСФОРМЕРІВ

Глоба Л. С., Приходнюк В.В., Цуканов С.О.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: sergeyidus@gmail.com

ENHANCING MALICIOUS URL CLASSIFICATION WITH TRANSFORMER-BASED EMBEDDINGS

The basic trends in the application of transformer models for URL vectorization in malicious URL detection tasks have been summarized. The results of comparative modeling of the effectiveness of combining BERT, SBERT, and RoBERTa with neural networks (LSTM, GRU, MLP) for URL classification are presented.

Зі стрімким зростанням інтернет-трафіку у світі спостерігається значне посилення кіберзагроз, серед яких шкідливі URL-адреси (Uniform Resource Locator — Уніфікований Локатор Ресурсів) відіграють роль одного з основних векторів атак. Традиційні методи виявлення, що базуються на правилах, уже не здатні ефективно протистояти швидкій еволюції цих загроз, що підкреслює необхідність розробки більш просунутих підходів. Запропонований підхід зосереджується на аналізі сучасних технік обробки природної мови, зокрема моделей BERT (Bidirectional Encoder Representations from Transformers — Двонаправлені Кодувальні Представлення від Трансформерів), SBERT (Sentence-BERT — BERT для речень) та RoBERTa (Robustly Optimized BERT Approach — Стійкий Оптимізований Підхід BERT), у поєднанні з архітектурами нейронних мереж, такими як MLP (Multi-Layer Perceptron — Багатошаровий Персептрон), LSTM (Long Short-Term Memory — Довга Короткострокова Пам'ять), GRU (Gated Recurrent Unit — Керована Рекурентна Одиниця).
Метою роботи є не лише покращення точності класифікації, але й подолання таких викликів, як залежність від якості навчальних даних, складність моделей та високі обчислювальні витрати [8]. У цьому контексті дослідження пропонує комплексний підхід, який об’єднує передові методи векторизації та класифікації для створення надійного інструменту боротьби з кіберзагрозами.

Проблема виявлення шкідливих URL-адрес є добре дослідженою, однак сучасні методи продовжують стикатися з обмеженнями. У літературі представлено кілька підходів до вирішення цієї задачі: наприклад, один із методів пропонує виявлення фішингових URL-адрес на основі лексичних, символьних та словесних векторних ознак із використанням комбінації CNN (Convolutional Neural Network — Згорткова Нейронна

Мережа) та GRU шарів, досягаючи точності 94.4% [1], хоча відсутність порівняння з іншими сучасними методами ускладнює оцінку його ефективності; інший метод, AFSADL-MURLC [2], використовує токенізацію NLTK, вбудовування GloVe та класифікацію через GRU, досягаючи точності 98.25%, перевершуючи традиційні методи, такі як Random Forest (99.03%) чи Naive Bayes (95.37%), але поступаючись найкращим результатам; ще один підхід комбінує глибоке навчання та знання експертів для виявлення ін'єкційних атак (SQL, XSS), досягаючи точності 99.39% [4], хоча складність архітектури ускладнює практичне впровадження; гібридна модель для виявлення DDoS-атак на основі CNN та CART показала точність 97.33% [6], а модифікована версія BERT (M-BERT) [7] досягла Macro-Precision 94.42%, перевищуючи базовий BERT (91.28%), але поступаючись через гетерогенність даних. Основними викликами залишаються якість навчальних даних, складність моделей та потреба у значних обчислювальних ресурсах [8], що підкреслює необхідність нових підходів, які б поєднували високу точність із практичною реалізацією.

У цьому дослідженні класифікація URL-адрес здійснюється у два етапи: отримання векторного представлення URL та його класифікація за допомогою нейронних мереж. Для векторизації використано трансформерні моделі: BERT [10] — двонаправлена модель, яка аналізує текст у обох напрямках, забезпечуючи глибоке розуміння контексту; SBERT — покращена версія BERT для обчислення семантичної схожості між реченнями з архітектурою Siamese для швидшого генерування вбудовувань; RoBERTa — оптимізована версія BERT із динамічним маскуванням та більшим обсягом навчальних даних, що покращує узагальнюючу здатність. Векторні представлення подаються на вхід нейронних мереж: MLP із двома прихованими шарами (384 та 256 нейронів), який підходить для задач без урахування порядку даних; LSTM та GRU — рекурентні мережі, адаптовані для обробки послідовних даних, таких як текст URL-адрес.

Для оцінки ефективності підходу використано датасет "Malicious URLs dataset" [3], що містить 10,000 URL-адрес (по 5,000 шкідливих та безпечних), розділений на навчальну (80%) та тестову (20%) вибірки. Мітки класів перекодовано у числові значення: 0 для шкідливих, 1 для безпечних. Моделі реалізовано за допомогою Python та PyTorch, навчання проводилося з використанням оптимізатора Adam (learning rate 0.0001) протягом 80 епох із розміром міні-батчу 32. Для оцінки якості класифікації використано метрики: точність (accuracy), recall та precision. Експерименти показали високу ефективність запропонованих моделей: BERT + LSTM досягла найкращої точності — 99.20%, із precision 99.50% та recall 99.00% для безпечних URL-адрес і 99.60% та 99.00% для шкідливих, найкраще збалансувавши помилки першого та другого роду; BERT + GRU показала точність 99.15% із близькими показниками precision та recall; RoBERTa + LSTM досягла точності 98.65%; SBERT + GRU показала найнижчу точність — 96.30%; MLP-

варіанти досягли точності до 99.10%, але поступаються рекурентним мережам у роботі з послідовними даними.

Дослідження продемонструвало, що комбінація BERT із LSTM є найбільш оптимальним рішенням для класифікації шкідливих URL-адрес, забезпечуючи точність 99.20% та високі показники precision і recall. Моделі RoBERTa + LSTM та RoBERTa + GRU також показали конкурентні результати (98.65% та 98.75% відповідно), що робить їх перспективними для подальших досліджень. Моделі на основі MLP виявилися менш ефективними для послідовних даних, хоча й досягли високих показників (до 99.10%). Запропонований підхід підтверджує переваги використання трансформерних моделей для обробки URL-адрес, дозволяючи ефективно виявляти кіберзагрози. Рекомендується подальше вдосконалення моделей із урахуванням гетерогенності даних [3,5] та оптимізації обчислювальних витрат для реального часу. Отримані результати можуть стати основою для створення практичних систем захисту від шкідливих URL-адрес у сучасних умовах зростання кіберзагроз.

Література

1. Rasymas and L. Dovydaitis, “Detection of Phishing URLs by Using Deep Learning Approach and Multiple Features Combinations,” Baltic Journal of Modern Computing, vol. 8, no. 3, Sep. 2020, doi: https://doi.org/10.22364/bjmc.2020.8.3.06
2. A. Mustafa Hilal et al., “Malicious URL Classification Using Artificial Fish Swarm Optimization and Deep Learning,” Computers, Materials & Continua, vol. 74, no. 1, pp. 607–621, 2023, doi: https://doi.org/10.32604/cmc.2023.031371
3. Malicious And Benign URLs dataset. URL: https://www.kaggle.com/datasets/siddharthkumar25/malicious-and-benign-urls (дата звернення: 20.03.2025).
4. C. Zhao, S. Si, T. Tu, Y. Shi, and S. Qin, “Deep-Learning Based Injection Attacks Detection Method for HTTP,” Mathematics, vol. 10, no. 16, p. 2914, Aug. 2022, doi: https://doi.org/10.3390/math10162914
5. CSIC 2010 Web Application Attacks dataset https://www.kaggle.com/datasets/ispangler/csic-2010-web-application-attacks (дата звернення: 20.03.2025).
6. B. Goparaju and B. S. Rao, “Distributed Denial-of-Service (DDoS) Attack Detection using 1D Convolution Neural Network (CNN) and Decision Tree Model,” Journal of Advanced Research in Applied Sciences and Engineering Technology, vol. 32, no. 2, pp. 30–41, Sep. 2023, doi: https://doi.org/10.37934/araset.32.2.3041
7. B. Yu, F. Tang, Daji Ergu, R. Zeng, B. Ma, and F. Liu, “Efficient Classification of Malicious URLs: M-BERT - A Modified BERT Variant for Enhanced Semantic Understanding,” IEEE Access, pp. 1–1, Jan. 2024, doi: https://doi.org/10.1109/access.2024.3357095
8. F. Torregrossa, R. Allesiardo, V. Claveau, N. Kooli, and G. Gravier, “A survey on training and evaluation of word embeddings,” International Journal of Data Science and Analytics, vol. 11, no. 2, pp. 85–103, Feb. 2021, doi: https://doi.org/10.1007/s41060-021-00242-8
9. F. Torregrossa, R. Allesiardo, V. Claveau, N. Kooli, and G. Gravier, “A survey on training and evaluation of word embeddings,” International Journal of Data Science and Analytics, vol. 11, no. 2, pp. 85–103, Feb. 2021, doi: https://doi.org/10.1007/s41060-021-00242-8
10. J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, “BERT: Pretraining of Deep Bidirectional Transformers for Language Understanding,” arXiv.org, May 24, 2019. https://arxiv.org/abs/1810.04805

УДК 004.4

ОГЛЯД SIP-АТАК У VOIP-МЕРЕЖАХ

Федоров С.О., Новогрудська Р.Л.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: alternative1398@gmail.com

OVERVIEW OF SIP BASED ATTACKS IN VOIP NETWORKS

The study is devoted to the analysis of typical attacks on VoIP networks using the SIP protocol. With the growing popularity of VoIP networks, the risks associated with the security of these networks are also increasing, creating new challenges and the need to improve protection methods.

Session Initiation Protocol (SIP) - протокол ініціювання сеансу - текстовий сигнальний комунікаційний протокол, який використовується для створення, керування та завершення кожного сеансу. Він відповідає за безперебійну передачу пакетів даних через мережу. Він розпізнає запит користувача на здійснення дзвінка, а потім встановлює з'єднання між двома або більше користувачами. Після завершення дзвінка сеанс завершується. Він працює разом з іншими протоколами прикладного рівня, які ідентифікують і передають носії сеансу.

[1] визначає різні типи повідомлень, які може підтримувати SIP. Повідомлення SIP в основному поділяються на дві категорії: Запити та Відповіді. Деякі з підтримуваних запитів і відповідей SIP наведені в таблицях 1 і 2.

Таблиця 1. Запити SIP.

Запит SIP	
INVITE	Ініціювання сессії
BYE	Завершення сессії
OPTIONS	Визначення SIP-повідомлень та кодеків які розуміє UA або сервер
REGISTER	Реєстрація місцезнаходження користувача SIP
ACK	Підтвердження відповіді на запит INVITE
CANCEL	Скасувати запит INVITE (при очікуванні відповіді)
NOTIFY	Надання інформації про зміну стану, що не пов'язана з конкретною сесією
REFER	Трансфер двізнків та контакт із зовнішніми ресурсами

Таблиця 2. Відповіді SIP.

Відповідь SIP	
100 Trying	Вказує на те, що довірена особа отримала запит INVITE і обробляє його.
180 Ringing	Команда INVITE надіслана до адресата
200 OK	Сесію зв’язку створено
401	Відповідь на запит REGISTER, якщо користувач не авторизований. Не надає коректну аутентифікаційну інф-ю
403	Сервер зрозумів запит, але відмовляється його виконувати
407	Запит вимагає автентифікації користувача. Ця відповідь видається проксі-серверами
408	Відсутність відповіді на запит протягом певного часу
503	Сервер недоступний. Запит наразі виконати неможливо

Очікування щодо безпеки та конфіденційності в мережах VoIP еквівалентні вимогам до PSTN(класичних телефонних мереж), але надання захищених інтернет-послуг є набагато складнішим. SIP-повідомлення можуть містити інформацію, яку користувач або сервер бажають зберегти в таємниці.

Гнучкість і багатий набір функцій IP-телефонії на основі протоколу SIP порівняно з традиційною телефонною мережею пов'язані з додатковими ризиками для безпеки. Система IP-телефонії на основі SIP вразлива як до загальних інтернет-атак, так і до атак, специфічних для SIP. Оскільки розробка SIP в першу чергу була зосереджена на розширенні функціоналу і сумісності, існує багато можливостей для роботи над безпекою SIP.

Основні типи атак з використанням протоколу SIP можна класифікувати наступним чином [2] :

1. Підміна реєстрації SIP

SIP - це протокол управління на прикладному рівні, який може встановлювати, змінювати або завершувати користувацькі сесії. У SIP та інших протоколах VoIP, користувач користувацький агент (UA)/IP-телефон повинен зареєструватися на SIP-проксі/реєстраторі (вузлі керування), що дозволяє проксі
спрямовувати вхідні дзвінки на телефон. Підміна реєстрації відбувається коли зловмисник видає себе за дійсного користувача перед реєстратором і замінює законну реєстрацію на власну адресу. Ця атака призводить до того, що вхідні дзвінки, призначені для зареєстрованого користувача, перенаправляються на несанкціоновану адресу.

2. Модифікація SIP-повідомлень

SIP-повідомлення не мають вбудованого механізму цілісності. Виконуючи одну з атак типу «людина посередині»(man-in-the-middle) [3] (підміна IP-адреси, підміна MAC-адреси, реєстрація SIP), зловмисник може перехопити і модифікувати SIP-повідомлення, змінюючи деякі або всі атрибути повідомлення. Це може включати в себе підміну абонента, якому телефонують, в повідомленні про початок сеансу повідомлення, створюючи у жертви враження, що вона дзвонить одній людині, в той час як система з'єднує його з іншою. Змінивши SIP повідомлення, зловмисник може видати себе за абонента або перенаправити виклик за іншою адресою.

3. Скасування\завершення виклику

Зловмисник може створити SIP-повідомлення з командою Cancel або Bye і відправити його на кінцевий вузол (телефон) щоб завершити поточну розмову. Якщо зловмисник надсилає безперервний потік таких пакетів на телефон, телефон не зможе здійснювати або приймати дзвінки. Це може бути поширено на

на велику кількість телефонів, що призведе до загальносистемного збою в роботі.

4. Неправильна команда SIP

Протокол SIP покладається на hypertext markup language протокол (HTML), для передачі командної інформації. Це робить протокол SIP дуже гнучким і розширюваним для реалізації функцій VoIP. Недоліком є те, що стає дуже складно протестувати роботу SIP з усіма можливими вхідними даними. Зловмисники можуть використовувати ці вразливості, як тільки вони їх знайдуть, формуючи пакети з неправильно сформованими командами і відправляючи їх на вразливі вузли. Це призведе до погіршення роботи або виведення з ладу атакованого вузла, що зробить частину або всю систему VoIP недоступною. Це важко виправити з точки зору перевірки на помилки аналізатора повідомлень. Численні помилки та їхні експлойти, що з'являються в результаті в інтернет-браузерах показують, наскільки складно протестувати кожне можливе повідомлення, яке може бути надіслане [4].

Висновки. VoIP-мережі, як і будь-які інші мережі, піддаються атакам з боку зловмисників. SIP-протокол є однією з основних цілей цих атак.

Основні типи атак включать в себе різні способи махінацій пов’язаних з SIP, такі як підміна реєстрації SIP, модифікація SIP-повідомлень, скасування\завершення виклику, неправильні команди SIP та інші.

Важливою частиною управління мережею VoIP є збереження конфіденційності та цілісності даних, підвищення відмовостійкості, та здатність запобігати загрозам у реальному часі.

Вивчення та дослідження механізмів дій зловмисників є актуальним та важливим напрямком дослідження, що дозволить знайти способи для того щоб убезпечити широко використовувані нині VoIP-мережі, які використовують протокол SIP, від неправомірних дій.

Література

1. IETF Network Working Group. 2016. SIP: Session Initiation Protocol. Retrieved September 21, 2016. https://www.ietf.org/rfc/rfc3261.txt
2. M. Zubair Rafique, M. Ali Akbar and Muddassar Farooq. Evaluating DoS Attacks Against SIP-Based VoIPSystems, 2010, Global Telecommunications Conference.
3. David Butcher, Xiangyang Li, and Jinhua Guo. Security Challenge and Defense in VoIP Infrastructures, 2007, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS.
4. Abdirisaq M. Jama, Othman Omran Khalifa. Review of SIP based DoS attacks, 2016, International Journal of Computer Applications Technology and Research.

УДК 621.39

ХМАРНІ ТЕХНОЛОГІЇ В ТЕЛЕКОМУНІКАЦІЙНІЙ ІНДУСТРІЇ: ОГЛЯД ТА ПЕРСПЕКТИВИ

Ярмоленко В. І.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: v.yarmolenko.tz22@kpi.ua

CLOUD TECHNOLOGIES IN THE TELECOMMUNICATIONS INDUSTRY: OVERVIEW AND PROSPECTS

Cloud technologies are revolutionizing the telecommunications industry by enhancing efficiency, scalability, and cost reduction. Their implementation enables telecom operators to optimize network management, improve service quality, and reduce infrastructure expenses. Key advancements such as Network Function Virtualization (NFV), Software-Defined Networking (SDN), and AI-driven cloud solutions ensure real-time data processing and better security. Despite challenges like cybersecurity risks and migration costs, cloud technology remains a cornerstone of digital transformation, driving innovation in 5G, 6G, and beyond.

У сучасному світі телекомунікації зазнають значних змін завдяки впровадженню хмарних технологій. Вони забезпечують високу ефективність, масштабованість та зниження витрат на інфраструктуру. Застосування хмарних сервісів сприяє розвитку телекомунікаційних операторів, дозволяючи їм впроваджувати нові моделі обслуговування, оптимізувати управління мережею та забезпечувати кращу якість зв’язку.

Завдяки хмарним технологіям телекомунікаційні системи можуть швидко адаптуватися до мінливих умов ринку, інтегрувати нові послуги та забезпечувати високу продуктивність систем зв’язку. Важливо зазначити, що такі зміни відбуваються в контексті глобальної цифрової трансформації, яка визначає розвиток економіки в сучасному світі.

Основні поняття хмарних технологій

Хмарні технології являють собою модель обчислень, яка базується на використанні мережевих ресурсів для зберігання, обробки та управління даними без необхідності локального обладнання. Хмарні сервіси можуть бути поділені на три основні категорії:

- IaaS (Infrastructure as a Service) – надання інфраструктури у вигляді віртуальних серверів, мереж і сховищ даних. Це дозволяє компаніям значно скоротити витрати на придбання і підтримку апаратного забезпечення.
- PaaS (Platform as a Service) – забезпечення платформ для розробки, тестування та розгортання програмного забезпечення. Завдяки цьому підприємства можуть швидко створювати та впроваджувати нові сервіси без необхідності управління фізичною інфраструктурою.
- SaaS (Software as a Service) – доступ до програмних продуктів через інтернет без необхідності їх встановлення на локальних пристроях. Це спрощує використання програмного забезпечення і знижує витрати на його оновлення та підтримку.

Використання хмарних технологій у телекомунікаційній індустрії.

Згідно з розглянутими дослідженнями [3], хмарні технології активно впроваджуються у сфері телекомунікацій завдяки їхній здатності оптимізувати мережеві ресурси. Основні напрями їх застосування включають:

- Віртуалізацію мережевих функцій (NFV), що дозволяє операторам скорочувати витрати на фізичне обладнання та знижувати експлуатаційні витрати. Використання NFV дає змогу операторам швидко розгортати нові сервіси та адаптувати мережу до змін у навантаженні.
- Програмно визначені мережі (SDN), які забезпечують централізоване управління та гнучке налаштування трафіку. SDN дає змогу динамічно змінювати конфігурацію мережі та автоматизувати процеси управління трафіком.
- Хмарні платформи для обробки даних, що дозволяють аналізувати великі обсяги інформації в режимі реального часу та підвищують продуктивність мереж. Завдяки цьому оператори можуть оперативно реагувати на збої та прогнозувати навантаження на мережу.

Переваги хмарних технологій для телекомунікаційних операторів.

Використання хмарних технологій сприяє підвищенню конкурентоспроможності телекомунікаційних компаній. Оператори можуть зменшити витрати на фізичну інфраструктуру та технічне обслуговування. Замість розгортання власних дата-центрів вони можуть використовувати хмарні сервіси, що дозволяє значно знизити витрати капіталу. Гнучкість та масштабованість хмарних технологій забезпечують можливість швидкого розширення або скорочення ресурсів залежно від потреб, що є особливо важливим в умовах нестабільного попиту та сезонних коливань навантаження на мережу.

Реалізація безпеки та відмовостійкості є ще одним важливим аспектом – збереження даних у розподілених центрах обробки гарантує їхню цілісність і захист від збоїв. Такі технології, як шифрування даних і багаторівнева автентифікація, дозволяють мінімізувати ризики несанкціонованого доступу. Автоматизація мережевих процесів сприяє підвищенню якості обслуговування, забезпечує стабільний зв'язок і мінімізує затримки. Завдяки використанню хмарних платформ оператори можуть швидше впроваджувати нові послуги.

Централізоване управління IT-ресурсами спрощує моніторинг та адміністрування мережі, зменшує потребу в обслуговуванні та оптимізує використання технічного персоналу. Хмарні технології також допомагають розвантажувати мережі та оптимізувати трафік шляхом динамічного розподілу навантаження. Окрім цього, вони дозволяють провайдерам телекомунікацій швидко розгортати нові сервіси без необхідності значних інвестицій у власну інфраструктуру.

Виклики впровадження хмарних технологій.

Попри численні переваги, використання хмарних сервісів у телекомунікаціях має певні виклики. Одним із головних аспектів є безпека даних. Централізоване зберігання інформації підвищує ризик кібератак, що

підтверджується розглянутими дослідженнями [2]. Для мінімізації загроз необхідно використовувати сучасні системи шифрування та механізми контролю доступу, а також застосовувати багаторівневі системи захисту відповідно до міжнародних стандартів.

Ще одним викликом є залежність від інтернет-з'єднання. Якість обслуговування напряму залежить від стабільності зв'язку між користувачем і хмарним сервісом. У випадку відмови мережевої інфраструктури це може призвести до значних проблем у доступності сервісів, що наголошується в роботі [2]. Оператори змушені впроваджувати механізми резервування каналів зв'язку та автоматичне перемикання між ними.

Додатково, варто враховувати витрати на міграцію. Перехід до хмарної інфраструктури потребує значних початкових інвестицій і технічної підготовки персоналу. Крім того, необхідно зважати на можливі проблеми сумісності існуючих систем із хмарними платформами [2]. Впровадження хмарних технологій вимагає комплексного підходу, що включає оцінку ризиків, модернізацію IT-інфраструктури та адаптацію внутрішніх бізнес-процесів.

Перспективи розвитку хмарних технологій у телекомунікаціях.

У майбутньому роль хмарних технологій у телекомунікаціях буде зростати. Очікується розвиток таких напрямків: впровадження 5G та 6G для збільшення швидкості та пропускної здатності мереж, що значно розширить можливості телекомунікаційних операторів. Розвиток штучного інтелекту (AI) у хмарних сервісах сприятиме прогнозуванню навантажень і покращенню управління мережею. AI дозволить автоматизувати процеси оптимізації трафіку та забезпечувати адаптивну маршрутизацію даних. Також очікується підвищення рівня кібербезпеки завдяки вдосконаленню систем шифрування та автентифікації користувачів, що дозволить захистити мережі від загроз і забезпечити конфіденційність інформації.

Висновки. Хмарних технології є важливим фактором цифрової трансформації телекомунікаційної індустрії, сприяючи зниженню витрат, підвищенню ефективності мережевих процесів та покращенню якості обслуговування клієнтів. Хоча хмарні рішення пропонують численні переваги, вони також створюють виклики, пов'язані з безпекою, залежністю від стабільного з'єднання та високими витратами на інтеграцію. Подальше вдосконалення технологій, зокрема розвиток 5G, 6G та штучного інтелекту, відкриє нові можливості для телекомунікаційних компаній, забезпечуючи стабільність, продуктивність і безпеку мереж майбутнього.

Література

1. Нікітіна Л. О., Дженюк Н. В., Борисова Л. В. IT та технології штучного інтелекту у підготовці інженерів з телекомунікацій // Системи управління, навігації та зв'язку. – 2023. – №3. – DOI: 10.26906/SUNZ.2023.3.189.
2. Довгий С. О., Копійка О. В. IT-інфраструктура як базова складова цифрової трансформації. – Київ: ІТГІП НАНУ, 2023. – Електронний ресурс.
3. Досенко А. К. Хмарні технології: прикладні технології сучасних платформ // Вчені записки ТНУ імені В. І. Вернадського. Серія: Філологія. Журналістика. – 2022. – Ч.3. – Електронний ресурс.

UDS 621.39

COUNTERING FLASH CALLS IN 4G AND 5G WITH INNOVATIVE DETECTION AND BLOCKING TECHNIQUES

Ivan Vetoshko
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: ivan.vetoshko@ukr.net

ПРОТИДІЯ ФЛЕШ-ДЗВІНКАМ У МЕРЕЖАХ 4G ТА 5G ЗА ДОПОМОГОЮ ІННОВАЦІЙНИХ МЕТОДІВ ВИЯВЛЕННЯ ТА БЛОКУВАННЯ

Досліджено методи виявлення та блокування Flash-дзвінків у мобільних мережах 4G та 5G. Проаналізовано параметри сигналів, поведінкові аномалії трафіку та алгоритми машинного навчання. Встановлено, що поєднання ШІ-аналітики, аналізу часу встановлення виклику та моніторингу заголовків SIP/SDP підвищує ефективність виявлення. Запропоновані рішення зменшують вплив нелегітимного трафіку за рахунок оптимізації захисту мереж сигналізації.

In today's 4G and 5G mobile networks, the problem of illegitimate use of signal space to optimise the cost of business processes is becoming increasingly relevant. One of these phenomena is Flash Calls, which are short-lived incoming calls used as an alternative to SMS for user authentication. While at first glance this technology seems to be an effective solution for companies looking to reduce the cost of SMS-OTP (One-Time Password), its widespread use poses serious challenges for telecoms operators, including loss of revenue, congestion of signalling channels and the possibility of abuse by malicious actors [1]. Unlike traditional signalling attacks, such as SMS spoofing or Caller ID manipulation, Flash Calls use legitimate call establishment mechanisms in VoLTE (Voice over LTE) and VoNR (Voice over New Radio) networks. They make identification and blocking difficult due to the lack of text content and the need for urgent real-time processing. The main technical challenge is to identify such calls among legitimate calls, which requires the implementation of traffic analysis algorithms, subscriber behavioural models and the use of artificial intelligence for automated classification. Given the rapid deployment of 5G SA (Standalone) networks, there is a need to develop new approaches to detecting and blocking Flash Calls. Traditional methods, such as blacklisting or analysing signalling parameters (Call Setup Time, SIP Headers), show limited effectiveness. Therefore, more flexible solutions based on machine learning, analysis of behavioural characteristics and correlation of traffic with massive usage patterns are in demand [1].

Flash Calls are based on establishing a short-term voice connection over the mobile network without answering the call. This allows the caller to identify the user by Caller ID (CLI) or the last digits of the phone number displayed in the incoming call [1]. On LTE (4G) and 5G networks, SA Flash Calls pass through the standard signalling stack, including:

- VoLTE (Voice over LTE) - Calls are initiated via the IMS (IP Multimedia Subsystem) using SIP (Session Initiation Protocol).
- VoNR (Voice over New Radio) - a similar principle, but with advanced QoS and call processing capabilities in 5G SA.
- Basic SIP requests (INVITE, 180 Ringing, BYE) are used, which do not actually terminate the session, but generate a record in the CDR (Call Detail Record).

The main feature of Flash Calls is the extremely short interval between connection establishment and completion (usually <1 second), which distinguishes them from standard voice calls. Implementing effective methods of countering Flash Calls requires a detailed analysis of signal traffic, including monitoring call parameters and analysing behavioural anomalies within the overall traffic of a mobile operator. Given that traditional blocking mechanisms, such as Caller ID filtering or static time limits, are ineffective, operators are implementing adaptive approaches to traffic classification. One of these methods is behavioural call analysis, which involves aggregating data on user call patterns and the correlation between subscriber activity and specific parameters of a signalling session [2]. If deviations from typical scenarios are detected, the call is automatically marked as suspicious, with subsequent application of blocking or slowdown policies.

In today's 4G and 5G mobile networks, it is critical to ensure resilience to threats caused by the illegitimate use of signalling traffic, including Flash Calls. The fig.1 illustrates a typical architecture for processing signalling traffic in a mobile network, including the points of interaction between network elements, signalling gateways, and external interconnects [2]. Diagram 1 shows a two-site STP/DRA (Signal Transfer Point/Diameter Routing Agent) infrastructure used to route signal traffic between internal network elements and external 3G/4G interconnects. Interaction between the elements takes place via several protocols, including SS7 M3UA (blue), Diameter (black), EWOK (dashed), as well as TCP/IP connections for management and analytics. Management and monitoring is carried out through analytics consoles integrated with the OSS (Operations Support System), which provides control over network performance parameters [3].

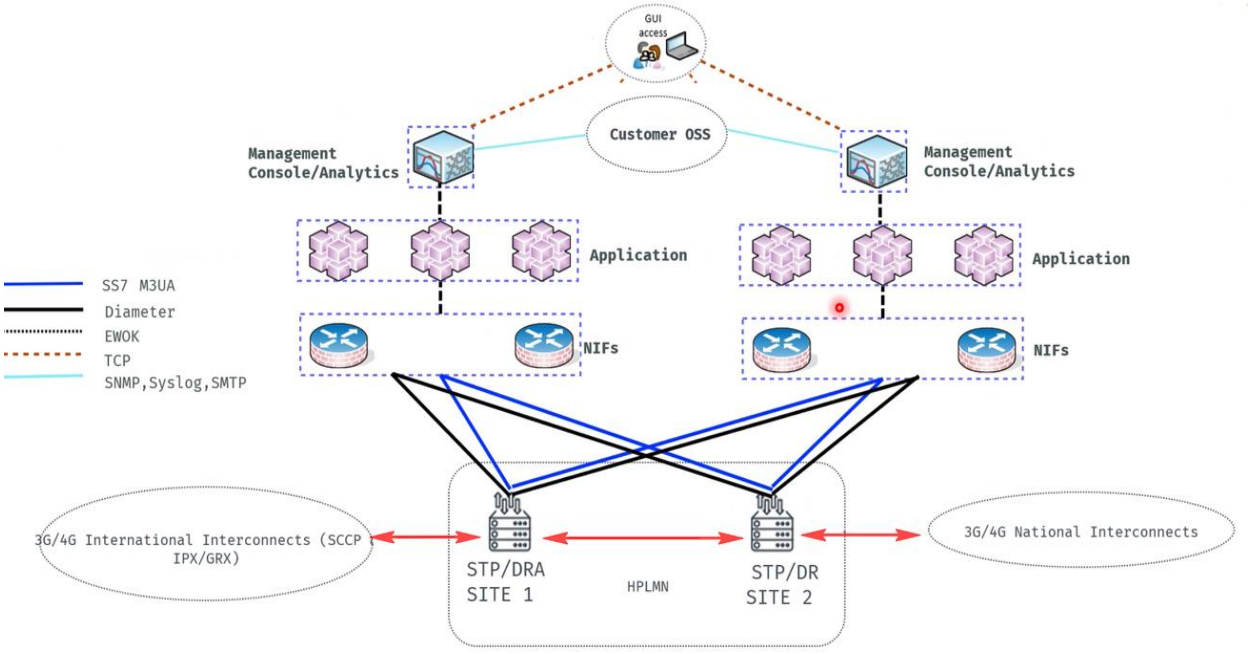


Fig. 1. Signal traffic management and fraud detection architecture.

A key feature of this architecture is the ability to centrally analyse and process signalling traffic, which allows for the identification of abnormal call patterns specific to Flash Calls. With the help of behavioural analysis algorithms integrated into the monitoring system, the operator can identify traffic that deviates from the normative parameters and automatically apply mechanisms to block or restrict unwanted calls. The dual-site distributed architecture provides increased fault tolerance and load balancing between STP/DRA nodes. This helps to minimise the impact of potential threats and abuse in signalling networks, and guarantees the stability of voice services in 4G and 5G mobile networks [3].

In 5G Standalone (SA), all VoNR calls are routed through the IMS Core without using EPC, which makes Flash Calls difficult to detect as they can masquerade as standard SIP sessions. Operators face the problem of short-lived calls that terminate before receiving 200 OKs, which are ineffective to identify through Caller ID or SIP-User Agent. SIP/SDP headers in Flash Calls may contain atypical or missing parameters, which is an indicator for analysis [2]. Particular attention should be paid to P-CSCF and S-CSCF behavioural anomalies, as an excessive number of cancelled or instantly terminated calls from a particular number range may indicate abuse. SIP header monitoring (User-Agent, P-Asserted-Identity), SDP parameter analysis, PCF QoS testing, and CDR behavioural analytics can be effective detection methods. Comprehensive analysis of signal traffic, together with the use of machine learning algorithms, will help operators to quickly identify and block Flash Calls in 5G SA [3].

Promising methods for detecting and blocking Flash Calls:

- Call Setup Time (CST) and Early Media analysis - Many Flash Calls do not reach the 200 OK stage of a SIP session, terminating before the voice channel is established. Analysing the time from INVITE to BYE or CANCEL can be a criterion for identifying suspicious calls [1].
- AI models for analysing call behaviour - Using Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM), operators can build models to detect anomalous activity. For example, Flash Calls often come in groups from different numbers in short periods of time, which can be detected through clustering.
- Using Session Border Controller (SBC) for adaptive blocking - SBCs can act as a first layer of protection by identifying suspicious SIP sessions based on several criteria, such as call establishment frequency, Caller ID matching registered numbers, and types of SIP User-Agents used [3].

Methods for detecting and blocking Flash Calls in 4G and 5G mobile networks are investigated. Signal parameters, traffic behavioural anomalies, and machine learning algorithms are analysed. It is established that the combination of AI analytics, Call Setup Time analysis, and SIP/SDP header monitoring increases the detection efficiency [2]. The proposed solutions reduce the impact of illegitimate traffic by optimising the protection of signalling networks. It was found that traditional blocking methods based on static Caller ID and SIP header filtering rules have limited effectiveness due to dynamic changes in Flash Calls patterns. Using behavioural analytics and clustering of anomalous sessions, you can detect traffic with atypical characteristics in real time. Integration of adaptive policies in Session Border Controllers (SBC) and Policy Control Function (PCF) provides flexible management of calls that match the Flash Calls profile. Further research should focus on improving distributed signal traffic analysis methods and integrating deep learning models to predict new fraudulent schemes.

References

1. Flash Calls [Electronic resource] // Mobileum. – Published: April 5, 2024. – Available: https://www.mobileum.com/products/risk-management/business-assurance/flash-calls/
2. Vetoshko I.P., Kravchuk S.O. Possibilities of improving the voice services quality in 5G networks // Information and Telecommunication Sciences. – 2023. – Vol.14, No 2. – P. 9-16. – DOI: https://doi.org/10.20535/2411-2976.22023.9-16
3. What are flash calls and how do they work? [Electronic resource] // Infobip. – Published: June 2024. – Available: https://www.infobip.com/blog/what-is-a-flash-call

УДК 004.01:004.71:004.72:004.032

УДОСКОНАЛЕНИЙ МЕТОД ІНФОКОМУНІКАЦІЙНОГО АУДИТУ

Ковальська Д. Д., Курдеча В.В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: zashkvar.youtuba01@gmail.com

ENHANCED METHOD OF INFOCOMMUNICATION AUDIT

With the growing demand for information and communication networks, the need for improved auditing methods is also increasing. This requires the implementation of more effective approaches, such as the enhanced method of infocommunication audit, which ensures a more accurate and comprehensive analysis of network infrastructure.

Продуктивне функціонування сучасного підприємства можливе тільки за умови ефективного функціонування інфокомунікаційної мережі[1]. Це обумовлено впровадженням в виробництво технологій Інтернету речей, штучного інтелекту, розподілених обчислень та сервісів хмарного середовища. В свою чергу оцінка ефективності мережі є однією з головних задач інфокомунікаційного аудиту. 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 ключових проблем при проведенні інфокомунікаційного аудиту є вплив людського фактора на точність оцінки. Навіть висококваліфіковані аудитори можуть допускати помилки або піддаватися суб’єктивним упередженням, що впливає на інтерпретацію та аналіз зібраних даних. Відмінності у досвіді, знаннях та особистих підходах можуть спричиняти неточності у висновках та знижувати надійність аудиту.

Впровадження удосконаленого методу інфокомунікаційного аудиту, заснованого на використанні спеціалізованого програмного забезпечення, дозволяє підвищити об’єктивність і точність оцінки. Автоматизовані системи аналізу мережевих інфраструктур мінімізують ризик людських помилок, забезпечують комплексну перевірку конфігурацій, аналіз трафіку та оцінку безпеки. Завдяки використанню ІКТ-інструментів можна значно покращити процес аудиту, підвищити його ефективність і забезпечити більш достовірні результати.

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 представлено удосконалений метод інфокомунікаційного аудиту мереж великих підприємств.

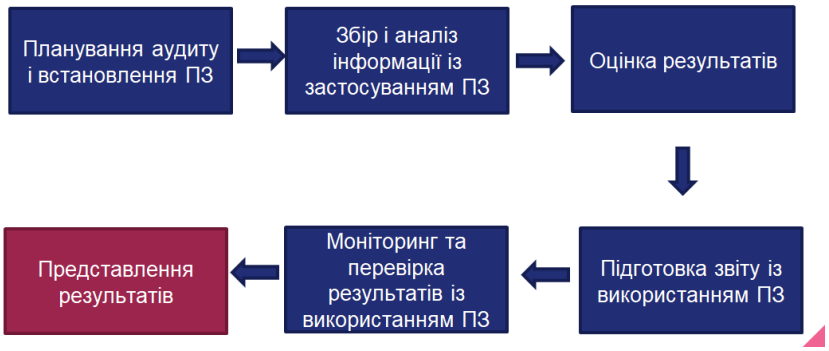


Рис.1. Вдосконалений метод інфокомунікаційного аудиту.

У межах дослідження було здійснено два натурних випробування з метою порівняння ефективності загального та розширеного методів аудиту. Початкові експерименти базувалися на традиційних підходах, що включали ручну обробку та аналіз даних, проведення тестувань вручну та суб'єктивну інтерпретацію отриманих результатів. На рисунку 2(ліворуч) представлено результати проведення звичайного інфокомунікаційного аудиту без використання програмного забезпечення.

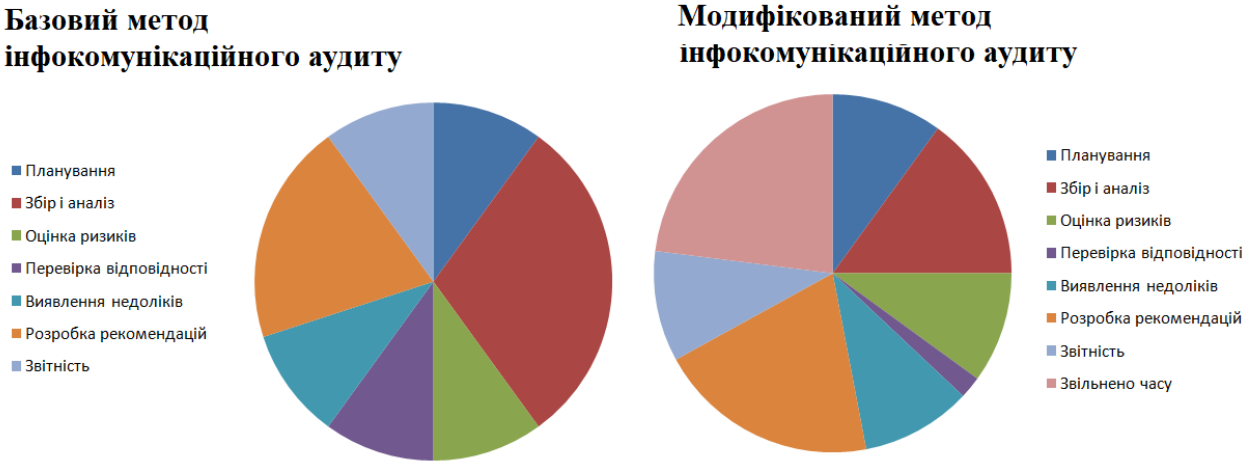


Рис.2. Результати розподілення часу при звичайному та модифікованому аудиті.

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 2 праворуч.

Впровадження удосконаленого методу інфокомунікаційного аудиту в практичне використання відкриває нові перспективи для організацій, дозволяючи підвищити якість аналізу, мінімізувати ризик помилок і зміцнити довіру клієнтів та зацікавлених сторін. Однак для досягнення максимальної ефективності важливо забезпечити регулярне оновлення та підтримку програмного забезпечення, а також підвищення кваліфікації аудиторів для оптимального використання технологічних можливостей.

Модифікація традиційних підходів до аудиту через інтеграцію сучасного програмного забезпечення є перспективним рішенням, що дозволяє суттєво покращити точність, швидкість та комплексність аналізу. Такий підхід забезпечує більш детальне виявлення вразливостей, загроз і ризиків в інфокомунікаційних системах, сприяючи підвищенню рівня безпеки та ефективності мережевої інфраструктури.

Література

1. N. Y. Mulongo, "Industry 5.0 a Novel Technological Concept," 2024 International Conference on Smart Applications, Communications and Networking (SmartNets), Harrisonburg, VA, USA, 2024, pp. 1-6, doi: 10.1109/SmartNets61466.2024.10577684.
2. M. Pooja and M. Damle, "Information Security Issues and Challenges: Perspective of Industry 4.0 Paradigm," *2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA)*, Uttarakhand, India, 2023, pp. 752-758, doi: 10.1109/ICIDCA56705.2023.10099832.
3. Current Trends in Communication and Information Technologies : [IPF: International Conference Infocommunications – Present and Future : 10th International Conference «Infocommunications – Present and Future» IPF’2020, Odesa, Ukraine, November 16–19, 2020 : Conf. Proceedings IPF 2020] / Editors: Petro Vorobiyenko, Mykhailo Ilchenko, Iryna Strelkovska. – Cham, Switzerland : Springer International Publishing, 2021. – XIX, 438 p. : ill. – (Lecture Notes in Networks and Systems (LNNS) ; Series ISSN 2367-3370 (Print) ; ISSN 2367-3389 (Electronic) ; Volume 212). – ISBN 978-3-030-76342-8 (Softcover). – ISBN 978-3-030-76343-5 (eBook). – DOI: https://doi.org/10.1007/978-3-030-76343-5.
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. Перпективи телекомунікацій : Міжнар. науково-техн. конф. студентів та аспірантів, м. Київ, 18 квіт. 2023 р.
6. S. Ushakov, L. Globa and V. Kurdecha, "EVOLVING INDUSTRY 4.0: A METHODICAL APPROACH TO OPTIMIZING IOT ONTOLOGIES FOR ENHANCED AUTOMATION," 2024 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Tbilisi, Georgia, 2024, pp. 131-134, doi: 10.1109/BlackSeaCom61746.2024.10646225.
7. Globa, L., Kurdecha, V., Popenko, D., Bezvuhliak, M., Porolo, Y. (2022). Data Collection and Processing Method in the Networks of Industrial IOT. In: Perakovic, D., Knapcikova, L. (eds) Future Access Enablers for Ubiquitous and Intelligent Infrastructures. FABULOUS 2022. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 445. Springer, Cham. https://doi.org/10.1007/978-3-031-15101-9_11

УДК 621.391

МОДЕЛЬ ЗАГРОЗ У ГЕТЕРОГЕННОМУ СЕРЕДОВИЩІ З ДИНАМІЧНОЮ АРХІТЕКТУРОЮ З НЕВІДЧУЖУВАНИМИ ОБЧИСЛЮВАЛЬНИМИ ВУЗЛАМИ ПІД КЕРУВАННЯМ KUBERNETES

Шенкаренко Т.О., Алєксєєв М.О
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: shenkarnekotaras@gmail.com, alexeyev@its.kpi.ua

THREAT MODEL IN A HETEROGENEOUS ENVIRONMENT WITH A DYNAMIC ARCHITECTURE AND INALIENABLE COMPUTING NODES MANAGED BY KUBERNETES

The work is dedicated to the pressing issue of threat modeling in a heterogeneous environment with a dynamic architecture and non-alienable computing nodes managed by Kubernetes. The proposed approach is based on the implementation of improved approaches applied during threat modeling, focusing on process optimization, data collection and analysis, threat contextualization, updating vulnerability information based on public databases, and considering the business context.

Unlike existing known solutions, the proposed enhanced threat modeling approaches include key aspects such as detailed information gathering, supply chain analysis, system compliance verification with data protection regulations (such as the General Data Protection Regulation), and the implementation of best practices from the Open Web Application Security Project (OWASP) [1] at early stages of software development.

The advantage of the proposed approach is the early detection of vulnerabilities, as the enhanced approaches focus on a detailed analysis of the future product’s documentation and architecture. This ultimately leads to resource and cost savings in product development since fixing vulnerabilities at the design stage is significantly cheaper than after the product has entered the market. Additionally, it reduces the risk of extra expenses on refactoring, testing, and releasing updates.

The study examines the experimental web environment OWASP Juicy Shop running under Kubernetes, builds a threat model using the graphical tool Threat Dragon, investigates the proposed enhanced methods, provides a statistical comparison with traditional threat modeling methods, and justifies the effectiveness of the proposed approach.

У наш час моделювання загроз стикається з низкою складнощів, пов'язаних із динамічністю ІТ-інфраструктури, зростанням атак на ланцюги постачання, та посиленням регуляторних вимог. Розвиток хмарних технологій, використання веб-додатків під управлінням Kubernetes та ускладнення мікросервісної архітектури призводять до розмивання традиційних меж довіри, що ускладнює аналіз потенційних загроз. У цьому контексті традиційні підходи до моделювання загроз, такі як STRIDE, P.A.S.T.A. та аналіз вразливостей через тестування на проникнення, все ще можуть бути корисними, де інфраструктура є менш динамічною і не включає складних інтеграцій із зовнішніми компонентами чи мікро сервісами, які зараз характерні для Kubernetes, однак вони вимагають адаптації до нових умов.

Для забезпечення безпеки програмного продукту й даних користувачів, у роботі розглядаються інструменти та пропонується покращена стратегія для моделювання загроз, яка повинна використовуватися в ранніх етапах SSDLC (Secure Software Development Lifecycle). Порівняно з традиційними, покращена стратегія включає у себе:

1. Аналіз потенційних вразливостей ланцюгів постачання. Згідно з запропонованою покращеною стратегію, необхідно визначити всі компанії та постачальників, які є частиною ланцюга постачання, включаючи не тільки основних постачальників, а й третіх осіб, таких як підрядники, субпідрядники та інші партнери. Важливо мати повний список усіх потенційних точок доступу, через які можуть бути здійснені атаки. Для аналізу відомих вразливостей в ланцюгах постачання, пропонується використовувати наступні сервіси: CVE (Common Vulnerabilities and Exposures) – це база даних, яка містить інформацію про публічно відомі уразливості в програмному забезпеченні та апаратному забезпеченні; NVD (National Vulnerability Database) – національна база даних вразливостей, яка є частиною федерального уряду США. Вона надає розширену інформацію про вразливості, їх вплив на безпеку та технічні деталі, що корисно для аналізу систем та програм, що використовуються постачальниками; Snyk – інструмент для автоматизованого сканування відкритих кодів на наявність вразливостей. Особливо корисний для оцінки безпеки у програмному забезпеченні та бібліотеках, які використовуються сторонніми постачальниками.

2. Більш глибокий збір інформації для оцінки потенційних векторів атак. Комплексний збір даних включає в себе інформацію про потоки даних, конфігурації системи, аналіз YAML-файлів маніфестів, журналів Kubernetes, мережевої активності та архітектури сервісів, тощо.

3. Інтеграція інструментів OWASP у процес моделювання. Запропонована стратегія використовує інтеграцію методології й інструментів OWASP у процес моделювання, таких як:

- OWASP Dependency-Check. Цей інструмент дозволяє здійснювати аналіз залежності й виявляти відомі уразливості в сторонніх бібліотеках та компонентах, які використовуються в додатку. В контексті Kubernetes, де додатки часто використовують контейнеризацію та інтеграцію з зовнішніми сервісами, аналіз залежності допомагає запобігти атакам через уразливості в цих компонентах.

- OWASP ASVS (Application Security Verification Standard) – це набір стандартів і рекомендацій, які визначають вимоги до безпеки веб-додатків та API

- OWASP Threat Dragon — сучасний інструмент для моделювання загроз, який забезпечує інтерактивне створення діаграм потоків даних та аналіз потенційних вразливостей у системах.

4. Урахування бізнес-контексту під час моделювання. Безпека системи повинна враховувати не лише технічні аспекти, але й особливості її бізнес-середовища. Це включає розуміння ключових вимог бізнесу, які впливають на

проектування, функціональність, підхід захисту системи та відповідність щодо вимог регуляторів [3], таких як: GDPR (General Data Protection Regulation) — захист персональних даних громадян ЄС, включаючи вимоги до отримання згоди та права на видалення даних. PCI DSS (Payment Card Industry Data Security Standard) — захист даних платіжних карток. ISO/IEC 27001 — міжнародний стандарт управління інформаційною безпекою. HIPAA (Health Insurance Portability and Accountability Act) — це федеральний закон США, ухвалений у 1996 році для регулювання захисту конфіденційності та безпеки медичної інформації.

Таким чином, процес моделювання набуває більш актуального сенсу у контексті раннього виявлення загроз й слабких місць архітектури продукту. В таблиці 1 представлено порівняння традиційних стратегій і запропонованої покращеної стратегії такого моделювання.

Таблиця 1. Порівняння традиційних і запропонованої покращеної стратегії моделювання загроз й слабких місць архітектури продукту.

Аспект	Традиційні стратегії	Покращена стратегія
Аналіз вразливостей ланцюгів постачання	Зазвичай обмежується лише основними постачальниками	Визначення всіх учасників ланцюга постачання, включаючи третіх осіб (підрядники, субпідрядники). Використання баз даних CVE, NVD, Snyk для виявлення відомих вразливостей.
Збір інформації для оцінки векторів атак	Обмежений збір інформації за допомогою стандартних журналів безпеки.	Глибокий збір інформації про потоки даних, конфігурації системи, YAML-файли маніфестів Kubernetes, мережеву активність та архітектуру сервісів.
Інтеграція інструментів OWASP	Може бути обмеженою або взагалі не використовуватися	Інтеграція таких інструментів, як OWASP Dependency-Check для аналізу залежності, OWASP ASVS для стандартів безпеки, OWASP Threat Dragon для інтерактивного моделювання загроз.
Аналіз безпеки на етапі проектування	Зазвичай обмежений лише технічними аспектами без урахування бізнесу.	Урахування не лише технічних аспектів безпеки, але й бізнес-контексту, включаючи вимоги регуляторів, таких як GDPR, PCI DSS, ISO/IEC 27001, HIPAA.
Аналіз потенційних атак на контейнеризацію	Часто не розглядається, якщо не є специфічним завданням.	Оцінка загроз для контейнеризованих додатків, зокрема Kubernetes, включаючи моніторинг контейнерів, мережевих налаштувань і доступу до внутрішніх сервісів
Регулярні перевірки та оновлення	Перевірки здійснюються після впровадження рішення, рідше в процесі розробки.	Постійний процес перевірок і оновлень, зокрема через публічні бази даних вразливостей, для виявлення нових вразливостей та актуалізації моделей загроз.

Для перевірки запропонованої покращеної стратегії моделювання загроз для Web середовища під керуванням Kubernetes було обрано проект OWASP Juice Shop, що прибирає ризики нанесення шкоди реальному середовищу й дає доступ до усієї технічної документації проекту. Це навчальний веб-додаток з відкритим кодом розроблений проектом й його основна мета — навчання розробників, фахівців інформаційної безпеки та інших спеціалістів, знаходити й усувати вразливості у веб-додатках. Цей сервіс спеціально створений для проведення практичних занять і хакатонів з кібербезпеки. Особливістю цього продукту є реалістичність, тому що він містить широкий спектр вразливостей, які зустрічаються в реальних веб-додатках, включаючи вразливості з OWASP Top-10.

Для заповнення даних моделі було зауважено наступні пункти.

1. *Причина*: визначити охоплені та не охоплені вектори атак і потенційні слабкі місця.

2. *Об'єкт оцінювання*: веб-додаток під керуванням Kubernetes, включаючи стандартний функціонал користувача й панелі адміністратора.

3. *Обсяг*: функціональність веб-додатка, зокрема механізми аутентифікації, авторизації, обробки даних користувачів та платежів.

Взаємодія з клієнтськими пристроями та зовнішніми сервісами (наприклад, платіжними шлюзами) не входить в обсяг оцінювання й моделювання.

Експериментальне моделювання загроз мало наступні фази:

1. Аналіз точок входу для ймовірної атаки на вузли системи.
2. Аналіз точок виходу.
3. Перерахунок активів системи.
4. Вектори атак для ідентифікованих активів.
5. Механізми пом'якшення ризиків.

Після заповнення всіх пунктів, було проведене графічного моделювання у програмі OWASP Threat Dragon, с заповненням вузлів архітектури й потенційні векторів атак.

У таблиці 2 приведені результати моделювання загроз для Web середовища. Дані для традиційних стратегій взяті з практичного досвіду та аналізу відкритих джерел [4].

Таблиця 2. Результати моделювання загроз.

Параметр	**Традиційні стратегії**	**Запропонована стратегія**	**Різниця**
Кількість вірно ідентифікованих загроз	70	85	21%
Точність моделювання	82%	100%	18%
Час витрачений на моделювання	Менший (31 години)	Більше (49 годин)	16%
Відповідність регулятивним вимогам згідно GDPR	Середній	Висока	

Нижче приведені розрахунки з таблиці 2, які включають точність моделювання за традиційними стратегіями для веб-сервісу OWASP Juice Shop під керування Kubernetes. Для традиційних стратегій моделювання загроз для платформи OWASP Juice Shop можна прийняти наступні дані, виходячи з типових характеристик процесу моделювання загроз без використання надмірно складних або автоматизованих методів, та загально доступних звітів різних компаній, котрі займаються кібербезпекою:

- кількість вірно ідентифікованих загроз: 70 загроз;
- кількість пропущених загроз: 10 загроз;
- кількість неправдивих позитивних результатів: 5 загроз;

$$\text{Точність моделювання} = \frac{70}{70 + 10 + 5} \times 100\% \approx 82{,}35\%$$

Оскільки за запропонованою стратегією немає пропущених загроз й неправдивих позитивних результатів, точність моделювання для веб-сервісу OWASP Juice Shop під керуванням Kubernetes буде дорівнювати 100%. Кількість вірно ідентифікованих загроз: 85 загроз.

Таким чином, різниця у точності моделювання за традиційними й запропонованою стратегією 100 - 82,35 = 17,65 %

Висновки. Завдяки покращеній стратегії моделювання, кількість вірно ідентифікованих загроз зросла на 21%, при різниці додатково витраченого часу у 16%, але моделювання відбувалось хоча і на реалістичних, але все ж таки синтетичних даних, у реальному житті цей показник може дещо відрізнятись.

Модель включає у себе вимоги регулятора GDPR, що знижує ризики на додаткове навантаження бюджету при розробці програмного продукту у майбутньому.

На відміну від приведених традиційних стратегій, покращена стратегія враховує оцінку загроз для контейнеризованих додатків, зокрема Kubernetes.

Література

1. OWASP Application Security Verification Standard. Режим доступу: https://owasp.org/www-project-application-security-verification-standard
2. AWS. "Security in Containers and Kubernetes on AWS." Режим доступу: https://aws.amazon.com
3. IT Governance Publishing, “EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide" (4th Edition)” October 15, 2020.
4. Threatmodeler. Continuous cybersecurity in 2024. Режим доступу: https://www.threatmodeler.com/continuous-cybersecurity-in-2024-what-works-and-what-doesnt/

УДК 004.4

ДОСЛІДЖЕННЯ ЗАКОНОДАВЧИХ АСПЕКТІВ ЗАХИСТУ ПРИВАТНОСТІ ПРИ ПЕРЕДАЧІ ВІДЕОДАНИХ

Солоденко М.А., Педан С.І.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: mushenok.mariia@lll.kpi.ua, stas.pedan@gmail.com

RESEARCH ON THE LEGISLATIVE ASPECTS OF PRIVACY PROTECTION DURING VIDEO DATA TRANSMISSION

An analysis of the user's private attributes contained in video data was conducted. A detailed study and comparison of legislative aspects of protecting user privacy during the transmission of video data were conducted.

У сучасному світі цифрових технологій захист приватності є одним із викликів для регуляторних органів різних країн. Зростання кількості кіберзагроз і постійне збільшення обсягів персональних даних, що передаються через мережу, підкреслюють необхідність чітких і ефективних законодавчих норм. Захист приватності при передачі відеоданих потребує уваги не лише на технічному, але й на юридичному рівні, щоб забезпечити баланс між правами користувачів та інтересами компаній [1].

Відповідно до останнього звіту компанії Ericsson про мобільність очікується, що до 2027 року об’єм відео даних, що передаються, зросте втричі та складатиме майже 80 відсотків мобільного трафіку[2]. Актуальною задачею є аналіз приватних атрибутів користувача, що передаються з відеоданими, а також дослідження сучасних законодавчих ініціатив по захисту цих даних.

Особиста інформація (Personal Identifiable Information, PII) включає будь-які дані, які дозволяють ідентифікувати особу або пов'язані з нею дані: ідентифікаційна інформація, біометричні дані, інформація про зайнятість, освітня інформація, тощо. Конфіденційні персональні дані включають інформацію про расу, сексуальну орієнтацію, фінансовий стан, геолокацію тощо. Для обробки цієї категорії даних встановлюються підвищені вимоги до конфіденційності, і компанії повинні отримати конкретну згоду споживачів для їх обробки.

Відеодані можуть містити візуальну особисту інформацію (зображення обличчя, інформація про стан здоров’я), голосові дані, текстові приватні атрибути, які попали у відеокадр (адреса електронної пошти, паспортні дані, дані водійських прав), а також конфіденційні персональні дані, що були згадані вище.

Проаналізуємо провідні законодавчі акти, що забезпечують захист приватних даних користувача при передачі відеоданих.

На міжнародному рівні ключову роль у формуванні стандартів відіграє Загальний регламент про захист даних (General Data Protection Regulation, GDPR), який був прийнятий у Європейському Союзі (ЄС). Основна мета GDPR – встановлення єдиного стандарту захисту даних у ЄС та надання суб'єктам персональних даних більшого контролю над їхньою інформацією. Водночас регламент надає бізнесу чіткі вказівки щодо збору, обробки та зберігання персональних даних, включаючи відео [3].

Каліфорнійській закон про захист приватності споживачів (California Consumer Privacy Act, CCPA) є фундаментальним регулюванням для захисту конфіденційності громадян США. CCPA надає права споживачам і зобов'язує бізнес інформувати про способи збору та обробки даних, а також дотримуватись правил безпеки [4].

Україна активно розвиває нормативну базу для захисту персональних даних в епоху цифровізації. Закон «Про захист персональних даних» (№2297-VI) забезпечує регулювання обробки даних і конфіденційності. Цей закон спрямований на забезпечення прав суб'єктів даних та сприяють інтеграції України в міжнародний простір захисту даних. Визначення термінів: «персональні дані» – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Таблиця 1. Порівняння GDPR, CCPA та Закону України.

Країна	***ЄС***	***США***	***Україна***
Законодавча норма	GDPR	CCPA	Закон «Про захист персональних даних»
Сфера дії	Усі компанії, які обробляють дані громадян ЄС	Компанії з річним валовим доходом не менше 50 мільйонів доларів, обробляють дані щонайменше 50 000 споживачів	Усі суб'єкти, які обробляють персональні дані на території України
Права суб'єктів даних	Право на доступ, виправлення, видалення, обмеження обробки, перенесення даних	Доступ до даних, право відмови від продажу, видалення	Доступ до даних, виправлення, видалення, обмеження обробки
Підстава для обробки	Згода, виконання договору, законний інтерес, захист життєвих інтересів	Згода або бізнес-потреби	Згода, законні підстави, виконання зобов'язань
Штрафи за порушення	До 20 млн євро або 4% річного доходу компанії	До $7,500 за порушення або $2,500 за ненавмисне шкоду	Адміністративні санкції, рішення суду

Продовження таблиці 1. Порівняння GDPR, CCPA та Закону України.

Країна	***ЄС***	***США***	***Україна***
Прозорість обробки	Високий рівень, зобов'язання інформувати про мету та використання даних	Вимога політик конфіденційності для споживачів	Обов'язок повідомлення суб'єктів про обробку даних
Міжнародна передача даних	Дозволяється лише до країн із належним рівнем захисту	Немає чітких обмежень, окрім внутрішніх гарантій	Дозволена за згодою суб'єкта чи при забезпеченні належного захисту
Особливості конфіденційних даних	Спеціальні обмеження на обробку даних про здоров'я, релігію тощо	Особливі вимоги до медичних і фінансових даних	Визначено окремо обробку конфіденційних даних

Українське законодавство у сфері захисту персональних даних значною мірою відповідає міжнародним стандартам, зокрема вимогам GDPR. Водночас, CCPA має свою унікальність, спрямовану на регулювання персональних даних переважно з точки зору прав споживачів і обмеженого бізнесу. Для України актуальним є подальше вдосконалення механізмів відповідності європейським стандартам, включаючи посилення контролю за виконанням норм і інтеграцію сучасних технічних заходів.

Проведено аналіз приватних атрибутів користувача, що передаються з відеоданими. Виконано дослідження та порівняльний аналіз сучасних законодавчих ініціатив по захисту приватних атрибутів користувачів, що передаються з відеоданими.

Література

1. Data Privacy Laws Worldwide | Ultimate Overview 2023. Actonic – Unfolding your potential. [Електронний ресурс] – URL: https://actonic.de/en/data-privacy-laws-worldwide-ultimate-overview-2023/#1680168010723-12077be8-9af6.
2. Mobile data traffic outlook – URL: https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/mobile-traffic-forecast.
3. General Data Protection Regulation (GDPR) – Legal Text. General Data Protection Regulation (GDPR). [Електронний ресурс] – URL: https://gdpr-info.eu/.
4. Überarbeitung L. What is CCPA?. Actonic – Unfolding your potential. [Електронний ресурс] – URL: https://actonic.de/en/knowledge-base/what-is-ccpa/.

УДК 004.4

АВТОМАТИЧНЕ РОЗПІЗНАВАННЯ ТА ЗАХИЩЕНА ОБРОБКА ДАНИХ КОРИСТУВАЧІВ В ЛОГІСТИЧНИХ СИСТЕМАХ

Коба А.О., Педан С.І.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: artemkoba04@gmail.com, stas.pedan@gmail.com

AUTOMATIC RECOGNITION AND SECURE PROCESSING OF USER DATA IN LOGISTICS SYSTEMS

The article explores the integration of automated systems for recognizing and processing handwritten recipient addresses and postal codes in modern logistics. A hybrid approach using image processing, OCR with LSTM architecture and Levenshtein distance ensures precise recognition and fuzzy matching of postal codes despite potential input errors. The proposed solution emphasizes secure data processing through encryption and localized deployment on Unix systems, safeguarding sensitive recipient information while optimizing logistics operations.

Сучасні логістичні системи дедалі більше залежать від автоматизації процесів, включаючи ідентифікацію та обробку даних отримувача. Однією з ключових проблем є розпізнавання рукописних адрес та поштових індексів отримувачів, що часто містять помилки або мають нечітке написання. Впровадження автоматизованих систем розпізнавання адрес отримувачів поштових відправлень дозволяє скоротити час їх обробки, знизити кількість помилок і підвищити ефективність логістичних операцій.

В роботі розглядається проблема автоматизованого розпізнавання та обробки рукописних адрес та індексів отримувачів у логістичних системах. Для вирішення цієї задачі необхідно проаналізувати сучасні методи оптичного розпізнавання символів (OCR) та їх застосування у логістиці, дослідити методи шифрування та захищеної передачі розпізнаних приватних даних, до яких відноситься адреса та поштовий індекс отримувача, а також розробити схему фізичної реалізації методу та його інтеграції в існуючу логістичну інфраструктуру.

На рис.1 представлений запропонований метод автоматичного розпізнавання та захищеної обробки даних користувачів в логістичних системах. Першим етапом є сканування отриманого поштового відправлення. В результаті створюється зображення, на якому присутній рукописний текст з адресою отримувача поштового відправлення.

Для покращення точності подальшого оптичного розпізнавання текстових даних, зображення проходить через послідовність алгоритмів обробки, таких як:

1. Перетворення у режим градацій сірого.
2. Обробка методом Оцу [1], який виконує зведення сірого зображення до бінарного зображення.

3. Видалення шумів зображення з послідовним використанням таких операцій математичної морфології, як розширення (дилатація) і стиснення (ерозія) [2].

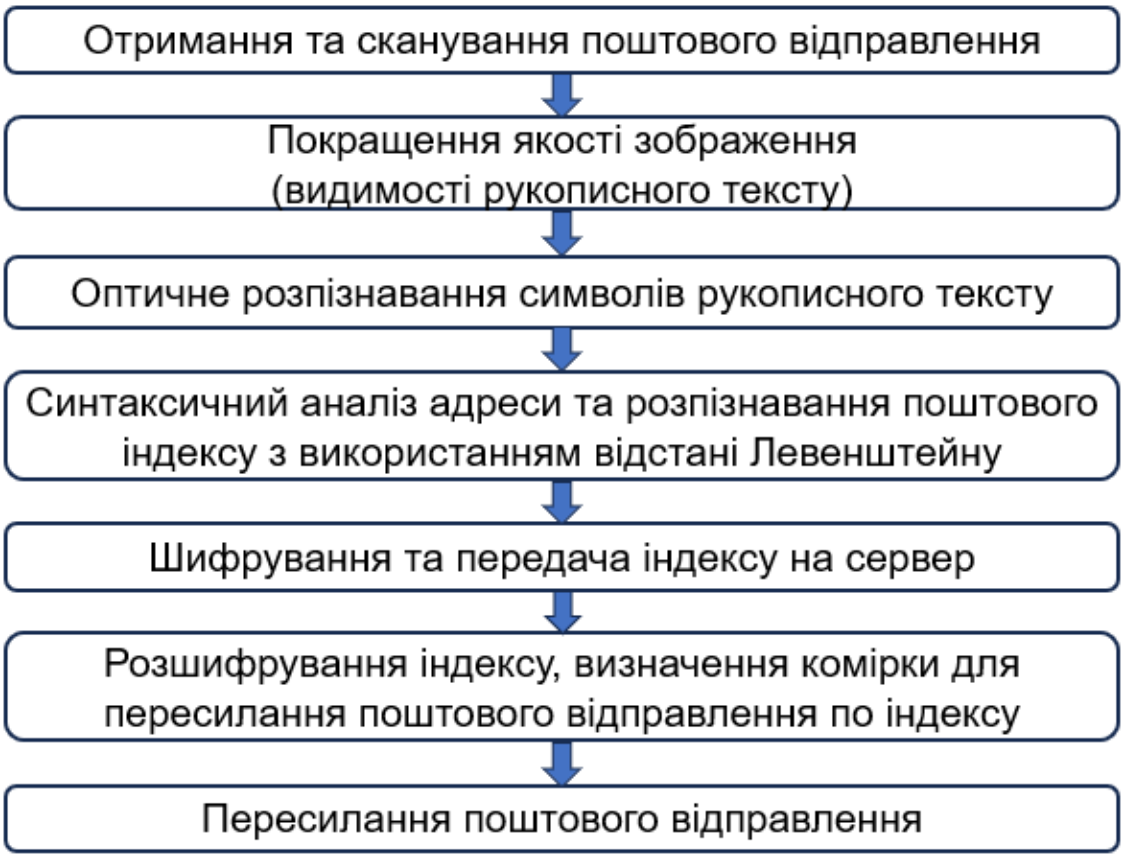


Рис. 1. Метод автоматичного розпізнавання та захищеної обробки даних користувачів в логістичних системах.

Оброблене зображення поступає на оптичне розпізнавання символів (OCR). Сучасні OCR-системи використовують алгоритми машинного навчання, зокрема згорткові нейронні мережі (CNN), рекурентні нейронні мережі (RNN) та трансформери. Їх поєднання дозволяє підвищити точність розпізнавання навіть для нерозбірливого почерку.

Для розпізнавання рукописного тексту з адресою одержувача, що включає в себе числовий поштовий індекс, може бути застосоване рішення з відкритим кодом Tesseract [3], що базується на використанні рекурентної нейронної мережі з архітектурою Довга короткочасна пам’ять (Long Short-Term Memory, LSTM) [4]. Однією з ключових особливостей LSTM є здатність "запам'ятовувати" довготривалі залежності завдяки своїм осередкам пам'яті, що робить її ідеальною для розпізнавання символів у послідовності. У рішенні Tesseract LSTM навчена обробляти текст із різними шрифтами, розмірами та умовами, забезпечуючи адаптацію до "складних" даних, включно з рукописними текстами чи спотвореннями.

Наступним етапом є синтаксичний аналіз адреси та розпізнавання поштового індексу з використанням відстані Левенштейна [5]. Відстань

Левенштейна є фундаментальною концепцією в задачах нечіткого пошуку тексту. Ця метрика вимірює "відстань" між двома текстовими рядками, визначаючи мінімальну кількість операцій (вставок, видалень або замін символів), необхідних для перетворення одного рядка в інший. У задачах нечіткого пошуку вона використовується для знаходження найбільш схожих записів у словнику даних, навіть якщо текстовий ввід містить помилки або варіації. Використання такого підходу дозволяє знайти в розпізнаному тексті адреси одержувача значення поштового індексу, що міститься в словнику, не дивлячись на вміст однієї або декількох помилок оптичного розпізнавання тексту.

В логістичній системі сервіс по обробці зображення, оптичному розпізнавання тексту та пошуку поштового індексу повинен бути розгорнутий на Unix системі на базі Raspberry Pi, оскільки дані отримувача відносяться до конфіденційної інформації, що потребує підвищеного захисту та мінімізації передачі таких даних за межі пристрою, що їх зберігає.

Фінальними етапами автоматизації процесу передачі відправлень є захищена передача розпізнаного поштового індексу на сервер, що визначає траєкторію подальшого руху відправлення.

Таким чином, розроблений метод автоматичного розпізнавання рукописних адрес та індексів отримувачів демонструє високу ефективність у вирішенні задач логістичних систем. Застосування сучасних OCR-алгоритмів, зокрема LSTM-моделей, дозволяє досягти точності розпізнавання навіть у випадках нечіткого або спотвореного написання. Використання відстані Левенштейна забезпечує коректне визначення поштових індексів, знижуючи вплив помилок розпізнавання. Локалізація обробки даних на базі пристроїв Raspberry Pi гарантує безпеку конфіденційної інформації, що є критично важливим у логістиці. Запропоноване рішення має потенціал для подальшої інтеграції та вдосконалення, відкриваючи нові можливості для автоматизації в логістичних процесах.

Література

1. M. Sezgin & B. Sankur (2004). Survey over image thresholding techniques and quantitative performance evaluation. Journal of Electronic Imaging. **13** (1): 146 - 65. doi:10.1117/1.1631315
2. Методи класифікації об’єктів, що рухаються/ Пашко А.О.: Електронне видання, 2019, 52 с.
3. Tesseract OCR. [Електронний ресурс]. – Режим доступу до ресурсу: https://github.com/tesseract-ocr/tesseract
4. Klaus Greff; Rupesh Kumar Srivastava; Jan Koutník; Bas R. Steunebrink; Jürgen Schmidhuber (2015). LSTM: A Search Space Odyssey. arXiv:1503.04069
5. Клещ, К. О., & Царьов, М. О. (2023). МОДИФІКАЦІЯ АЛГОРИТМІВ НЕЧІТКОГО ПОШУКУ ДЛЯ ВИКОРИСТАННЯ ТАБЛИЦІ ПОДІБНОСТІ СИМВОЛІВ. Таврійський науковий вісник. Серія: Технічні науки, (3), 21-28. https://doi.org/10.32782/tnv-tech.2023.3.3

УДК 004.4

ПОБУДОВА ЗАПИТІВ ДО ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ДЛЯ ВИРІШЕННЯ ТЕЛЕКОМУНІКАЦІЙНИХ ЗАДАЧ

Ільченко М.В., Іщенко М.О., Педан С.І.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: michael13ilch@gmail.com, ishchenkomaria391@gmail.com, stas.pedan@gmail.com

CONSTRUCTION OF LARGE LANGUAGE MODELS PROMPTS FOR SOLVING TELECOMMUNICATION PROBLEMS

Application of prompt engineering techniques in telecommunications, with a focus on optimizing the performance of large language models (LLMs) for a range of tasks, such as customer support, network management, and the personalization of information requests, specifically regarding the implementation of software products are researched. Analysis of basic prompt design principles, including few-shot learning, role prompting, chain-of-thought reasoning, multi-step prompting, iterative prompt engineering and refinement are conducted. Current challenges and future direction of LLMs usage in the telecommunications sector are also outlined.

У 2023 році у світі виникла новітня галузь наукового пошуку - інженерія запитів як результат стрімкого розвитку великих мовних моделей (ВММ), що відкриває безпрецедентні можливості для телекомунікаційної галузі. Реалізація потенціалу цих моделей вимагає ефективної інженерії запитів. У роботі досліджується застосування методик інженерії запитів у телекомунікаціях, з акцентом на оптимізації продуктивності ВММ для вирішення низки технічних задач, таких як підтримка клієнтів, управління мережею та персоналізація інформаційних запитів.

ВММ можуть генерувати нові текстові дані та тренуються на величезних обсягах текстових даних із різних джерел. ВММ продемонстрували вражаючі можливості в різних завданнях обробки природної мови, таких як узагальнення тексту, відповіді на запитання, аналіз настроїв, генерація коду та машинний переклад. Вони також можуть створювати історії, вірші, жарти, тексти пісень, зображення, аудіо та код, усе це керується текстовими запитами [11].

Продуктивність ВММ істотно залежить від якості вхідних запитів. Передбачається, що ВММ будуть інтегровані в усі наші робочі процеси [7]. Метою цієї роботи є дослідження сучасних підходів до побудови запитів ВММ для вирішення актуальних задач у телекомунікаційній галузі.

Термін "інженерія запитів" почав активно застосовуватися у науковій літературі з 2023 року. Нині існує ціла низка загальних методик інженерії запитів, які можна пристосувати для галузевих потреб, наприклад для сфери телекомунікацій [4, 5, 10]. До основних типів запитів ВММ належать такі:

1. Навчання з кількома прикладами [2, 9] – це надання ВММ декількох прикладів запитів клієнтів і бажаних відповідей. Приклад: аналіз мережевого

трафіку через надання ВММ низки типових прикладів аномальної активності.

2. Рольова побудова запитів [10] надає ВММ певну роль, на зразок роль "(Уявіть, що) Ви - … ." Наприклад, коли телекомунікаційна компанія використовує чат-боти для підтримки клієнтів, то для отримання кращих відповідей можна використовувати рольове підказування на зразок: "Ви - досвідчений технічний спеціаліст телекомунікаційної компанії. Відповідайте на запитання клієнтів чітко та лаконічно." Це допоможе чат-боту краще зрозуміти контекст та надавати точніші відповіді.

3. Міркування за допомогою ланцюга думок [1, 8] скеровує ВММ на покроковий процес міркування, щоб допомогти ШІ розбити проблему на менші кроки та зробити висновок. Наприклад: "Клієнт повідомляє, що інтернет не працює. Спочатку перевірте, чи підключений маршрутизатор. Потім перевірте, чи є з'єднання з інтернетом. Якщо з'єднання є, перевірте налаштування мережі."

4. Багатоступеневі запити [6] передбачають розбиття складного запиту на послідовність простіших кроків. Кожен крок використовує результати попереднього аби поступово наблизитися до кінцевого рішення. Уявімо, що нам потрібно діагностувати проблему з повільним інтернетом у клієнта. Ми можемо використовувати багатоступеневі запити:

Крок 1: Збір інформації про проблему. Крок 2: Визначення типу з'єднання та обладнання. Крок 3: Перевірка основних параметрів мережі. Крок 4: Діагностика можливих причин. Крок 5: Надання рекомендацій.

5. Ітеративна побудова та уточнення запитів [3]. Прикладом є сценарій, коли мережевий адміністратор намагається діагностувати періодичну втрату пакетів у критичній бізнес-мережі.

Ітерація 1: початковий запит: "Проаналізуй останні журнали мережі щодо втрати пакетів і визнач потенційні причини." Ітерація 2: уточнення (фокус на конкретному часовому проміжку). Ітерація 3: подальше уточнення (глибоке занурення в пропускну здатність). Ітерація 4: цілеспрямоване дослідження (фокус на аномальній активності).

Кожна ітерація базується на попередній відповіді. Запити стають все більш конкретними та цілеспрямованими.

Зазначимо, що наведена вище класифікація не є єдино можливою Наприклад, у праці Джулс Вайт [10] наводиться складніша класифікація з дещо відмінного ракурсу, позаяк вона групує шаблони запитів за їхньою функціональністю або метою, наприклад, "Семантика вхідних даних", "Взаємодія" тощо. Це відрізняється від класифікації за техніками, такими як "навчання з кількома прикладами" або " міркування за допомогою ланцюга думок ", які описують конкретні методи побудови запитів.

Як зазначають дослідники, перспективи окресленого напрямку допоможуть вирішити питання мережевих аномалій, моделювання мереж, сталого розвитку та екологічної безпеки, причому успіх ВММ у телекомунікаційній сфері буде залежати від спеціалізованих наборів даних при створенні базових моделей для телекомунікацій [5].

Розвиток ВММ відкриває нові можливості для комунікацій 6G,

наприклад, оптимізація та управління мережею, дозволяючи користувачам вводити вимоги до завдань у ВММ природною мовою. Покращення знань ВММ про комунікації, а також можливостей логічного міркування може значно підвищити потенціал ВММ для комунікацій 6G.

Отже, інженерія запитів є критично важливим компонентом ВММ в цілому та у телекомунікаційній галузі зокрема. Так, інжиніринг запитів дозволяє створювати запити, які генерують код для конкретних задач в телекомунікаціях (наприклад, можна використовувати LLM для оптимізації наявних кодів, автоматичного створення скриптів для налаштування мережевого обладнання, розробки протоколів, аналізу трафіку та великих обсягів даних, що генеруються мережами). Використання ефективних принципів розробки запитів допомагає покращити здатність ВММ аналізувати дані мереж, діагностувати та вирішувати їхні проблеми, покращувати безпеку та адаптувати ШІ до потреб споживача. Виклики сьогодення, пов'язані з ВММ, стимулюють оптимізацію їхнього використання в телекомунікаційному секторі.

Таким чином, в роботі розглянуті основні принципи розробки запитів ВММ, включаючи навчання з кількома прикладами, рольові запити, міркування за допомогою ланцюга думок, багатоступеневі запити, ітеративні запити з уточненнями та продемонстроване їхнє застосування у сфері телекомунікаційних задач. Також окреслено проблеми, виклики і перспективи використання ВММ у телекомунікаційному секторі.

Література

1. "Chain-of-Thought Prompting Guide." PromptHub. Accessed [12 February 2025]. https://www.prompthub.us/blog/chain-of-thought-prompting-guide
2. "Few-Shot Learning." Nebius Blog. Accessed [12 February 2025]. https://nebius.com/blog/posts/few-shot-learning
3. "Iterative Prompt Engineering and Refinement." DataCamp. Accessed [12 February 2025]. https://campus.datacamp.com/courses/chatgpt-prompt-engineering-for-developers/advanced-prompt-engineering-strategies?ex=13
4. Lin, Xingqin et al., "A Primer on Generative AI for Telecom: From Theory to Practice." arXiv, August, 16, 2024 https://arxiv.org/abs/2408.09031
5. Maatouk, Ali et al. “Large Language Models for Telecom: Forthcoming Impact on the Industry.” IEEE Communications Magazine 63 (2023): 62-68. https://arxiv.org/pdf/2308.06013
6. "Multi-Step Prompting." DataCamp. Accessed [12 February 2025]. https://campus.datacamp.com/courses/chatgpt-prompt-engineering-for-developers/advanced-prompt-engineering-strategies?ex=5
7. "The Rise of the Prompt Engineer – and Why It Matters." World Economic Forum. May 4, 2023. https://www.weforum.org/stories/2023/05/growth-summit-2023-the-rise-of-the-prompt-engineer-and-why-it-matters/
8. Wei, Jason et al., "Chain-of-Thought Prompting Elicits Reasoning in Large Language Models," arXiv, February 22, 2023, https://arxiv.org/abs/2201.11903
9. "What Is Few-Shot Learning?" IBM. Accessed [12 February 2025]. https://www.ibm.com/think/topics/few-shot-learning
10. White, Jules et al., "A Prompt Pattern Catalog to Enhance Prompt Engineering with ChatGPT," arXiv, February 22, 2023, https://arxiv.org/abs/2302.11382
11. Britto, Ricardo, Timothy Murphy, Massimo Iovene, Leif Jonsson, Melike Erol-Kantarci, and Benedek Kovács. 2023. “Telecom AI Native Systems in the Age of Generative AI -- An Engineering Perspective.” https://arxiv.org/abs/2310.11770

УДК 004.4

МІКРОКОМП'ЮТЕР RASPBERRY PI В ПРОЄКТАХ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Іщенко М.О., Могильний С.Б.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: ishchenkomaria391@gmail.com, isearch@ukr.net

RASPBERRY PI MICROCOMPUTER IN INFORMATION SECURITY PROJECTS

Raspberry Pi microcomputers have taken a prominent place in radio engineering systems. This is due, first of all, to their high performance with low power consumption. Also, the presence of Ethernet, Wi-Fi, Bluetooth ports and available GPIO pins makes them popular in IoT and Edge Computing systems. Implemented projects in the field of information security of electronic communications are considered.

Останні моделі мікрокомп'ютерів Raspberry Pi мають чотириядерний процесор (рис.1), Wi-Fi 2.4 ГГц та 5.0 ГГц 802.11ac, Blue і порт Gigabit Ethernet, з підтримкою PoE. Решта основних параметрів, які є основою для використання їх в системах електронних комунікацій, наведена в табл.1, а в табл.2 – короткий аналіз реалізованих проєктів.

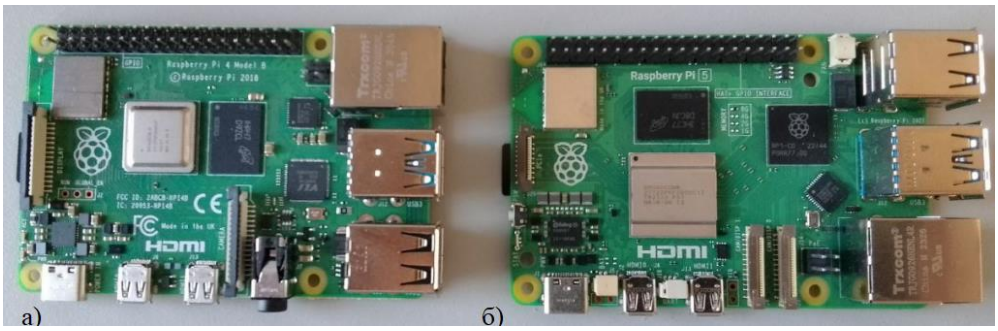


Рисунок 1. Мікрокомп'ютери Raspberry Pi 4B (а) і Raspberry Pi 5 (б).

Таблиця 1. Параметри мікрокомп'ютерів, важливі для реалізації проєктів.

	Raspberry Pi 4	**Raspberry Pi 5**
CPU	ARM-Cortex A72 (чотири ядра)	ARM-Cortex A76 (чотири ядра)
Частота CPU	1.5/1.8 ГГц	2.4 ГГц
SDRAM	LPDDR4-3200 SDRAM (1ГБ, 2ГБ, 4ГБ, 8ГБ)	LPDDR4X-4267 SDRAM (4ГБ, 8ГБ і 16ГБ)
Живлення	5V/3A DC (через USB-C порт чи GPIO)	5V/5A DC (з підтримкою Power Delivery)
Годинник реального часу	Немає	Годинник реального часу та роз'єм для батареї
PCIe	Немає	Інтерфейс PCIe 2.0 x1 для швидкої периферії

Таблиця 2. Проєкти з інформаційної безпеки з використанням мікрокомп’ютерів.

	Проєкт	**Короткий опис**	**Версія Raspberry Pi**
1	CIRClean USB Key Sanitizer [2]	Інструмент, який дозволяє безпечно та надійно сканувати сумнівні USB диски на наявність шкідливих програм і вірусів, не підключаючи їх безпосередньо до комп’ютера	Raspberry Pi 3B+
2	Travel Router [3]	Компактний маршрутизатор на OpenWRT забезпечує додатковий рівень безпеки, створюючи приватну ізольовану мережу для пристроїв, захищаючи їх від прямого впливу зловмисників	Raspberry Pi 3B+ або 4B
3	Tor Router [4]	Служба маршрутизації для мережі Tor	Raspberry Pi 3B+
4	Password Manager [5]	Сучасний менеджер паролів із багатофакторною автентифікацією, резервними копіями, сертифікатом SSL, віддаленим доступом і розширеною безпекою	Raspberry Pi Zero
5	Pi-Hole Ad Blocker [6]	Потужний блокувальник реклами на мережевому рівні	Raspberry Pi 3B+
6	VPN server [7]	Особистий VPN-сервер з використанням OpenVPN	Raspberry Pi 3B+ або 4B
7	Intrusion Detection System [8]	Системи виявлення вторгнень (IDS) на інструментах Snort і Suricata з відкритим кодом	Raspberry Pi 3B+ або 4B
8	Honeypot [9]	Система-приманка, яка відманює потенційних зловмисників від наших важливих активів, дозволяючи нам спостерігати та аналізувати їхню тактику	Raspberry Pi 3B+
9	Wi-Fi Security Audits [10]	Інструмент для перевірки безпеки мережі Wi-Fi з попередньо завантаженими інструментами Aircrack-ng, Kismet і Wifite для аудиту	Raspberry Pi 3B+ або 4B
10	Dashboarding with Grafana [11]	Елегантна інформаційна панель для центру операцій	Raspberry Pi 3B+
11	Network Scanner [12]	Автоматичний сканер мережевих пристроїв, який надсилає сповіщення на пошту при підключенні нової системи до мережі	Raspberry Pi 4B
12	Kali Linux Hacking Lab [13]	Kali Linux записується на картці microSD. За замовчуванням цей образ містить метапакет kali-linux-default, який є набором інструментів для пентестера	Raspberry Pi 4B або 5
13	Private Cloud Storage [14]	Власна приватна персональна хмара, яка працює з нашої домашньої мережі, до якої можна отримати доступ із-за меж цієї мережі	Raspberry Pi 4B або 5

Використання наведених вище проєктів дозволяє досліджувати методи забезпечення інформаційної безпеки в реальних умовах функціонування, проектувати та тестувати нові рішення в сфері безпеки та захисту передачі даних.

Література

1. *Могильний С.Б.*. Мікрокомп'ютер RaspberryPi– інструмент дослідника: посібник. – К.: 2014. – 340 с.
2. CIRCLean - USB key sanitizer. [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://circl.lu/projects/CIRCLean/
3. Raspberry Pi x OpenWRT Travel Router. [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://tristam.ie/2023/582/
4. Onion Pi. [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://learn.adafruit.com/onion-pi/overview
5. How to Self-Host Bitwarden Password Manager on Raspberry Pi Zero. [Електронний ресурс]. – 2025. – Режим доступу до ресурсу: https://www.makeuseof.com/self-host-bitwarden-password-manager-raspberry-pi-zero/
6. Pi-hole. Network-wide Ad Blocking. [Електронний ресурс]. – 2025. – Режим доступу до ресурсу: https://pi-hole.net/
7. PiVPN.The simplest way to setup and manage a VPN, designed for Raspberry Pi™. [Електронний ресурс]. – 2024. – Режим доступу до ресурсу: https://www.pivpn.io/
8. Turn your Raspberry Pi into an intrusion detection system with Pi.Alert. [Електронний ресурс]. – 2024. – Режим доступу до ресурсу: https://www.xda-developers.com/turn-your-raspberry-pi-into-an-intrusion-detection-system/
9. HoneyPi – An easy honeypot for a Raspberry Pi. [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://trustfoundry.net/2017/08/22/honeypi-easy-honeypot-raspberry-pi/
10. *Shao-Long WANG, Jian WANG, Chao FENG and Zhi-Peng PAN*. Wireless Network Penetration Testing and Security Auditing. [Електронний ресурс]. – 2025. – Режим доступу до ресурсу: https://www.researchgate.net/publication/310662676_Wireless_Network_Penetration_Testing_and_Security_Auditing
11. Install Grafana on Raspberry Pi. [Електронний ресурс]. – 2024. – Режим доступу до ресурсу: https://grafana.com/tutorials/install-grafana-on-raspberry-pi/
12. Build a Raspberry Pi Scanner that Tracks the Devices Connected to Your Local Network. [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://makezine.com/projects/build-raspberry-pi-network-scanner/
13. Kali on Raspberry Pi 4 - User Instructions. [Електронний ресурс]. – 2025. – Режим доступу до ресурсу: https://www.kali.org/docs/arm/raspberry-pi-4/
14. Build Your Own Raspberry Pi Cloud Server With Nextcloud. [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.makeuseof.com/raspberry-pi-nextcloud/

УДК 004.4

МЕТОД ПОКРАЩЕННЯ ЯКОСТІ ПЕРЕДАЧІ БЕЗПРОВІДНОГО СИГНАЛУ НА ЗБІЛЬШЕНУ ВІДСТАНЬ

Михайловський В.В., Педан С.І.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: vladyslav.mykhailovskyi@gmail.com, stas.pedan@gmail.com

METHOD FOR IMPROVING THE QUALITY OF WIRELESS SIGNAL TRANSMISSION OVER LONGER DISTANCE

A method to enhance the quality of wireless signal transmission through the stabilization of a transmitting device's position, based on the optical flow calculation of video frames with the underlying surface, is proposed. This method can be applied in various scenarios, such as establishing connections with unmanned aerial vehicles, controlling autonomous vehicles, and operating industrial IoT systems. By ensuring high-quality signal transmission over long distances, even in conditions of complex surface relief and the presence of radio interference, the proposed method proves to be highly effective.

Зі зростанням попиту на високошвидкісний бездротовий зв’язок збільшується кількість викликів, пов’язаних із передачею даних на значні відстані. Мобільні мережі, Wi-Fi-з’єднання, супутниковий інтернет та IoT-пристрої працюють у середовищах, де стабільність сигналу може значно змінюватися в залежності від фізичних перешкод, рівня електромагнітного шуму, погодних умов та інших чинників. Однією з основних проблем є згасання сигналу, викликане як природним зменшенням потужності через велику відстань, так і ефектами багатопроменевого поширення, коли сигнал відбивається від різних поверхонь і досягає приймача із затримкою.

Традиційні методи підвищення якості безпровідного зв’язку включають збільшення потужності передавача, зміну частотного діапазону, використання кодів корекції помилок, адаптивне налаштування параметрів передачі сигналу та використання фазованих антенних решіток для формування вузькоспрямованих пучків сигналу. Однак ці методи не завжди забезпечують стабільне з’єднання в умовах мобільності передавачів і приймачів. У випадку мобільних пристроїв, безпілотних літальних апаратів (БПЛА) або систем із плаваючими платформами зміщення антен може спричиняти значні коливання рівня сигналу, що ускладнює підтримання якісного зв’язку.

Одним із перспективних підходів до вирішення цієї проблеми є використання аналізу оптичного потоку відеосигналу для автоматичної стабілізації положення передавачів та приймачів. Оптичний потік є методом обчислення зміщення об’єктів у просторі на основі аналізу послідовності відеокадрів. Оптичний потік визначає схему видимого руху об'єктів, поверхонь і граней у зоровій сцені, спричинюваного відносним рухом спостерігача та сцени, а також розподіл видимих швидкостей руху візерунку яскравості в зображенні [1]. Цей метод широко застосовується у

сферах робототехніки, автономного транспорту, систем керування БПЛА та комп'ютерного зору. Використання оптичного потоку для стабілізації безпровідного зв'язку дозволяє коригувати положення антен у реальному часі, компенсуючи рух пристрою та покращуючи якість сигналу.

На рис. 1 представлена схема пристроїв, що приймають участь в передачі сигналу на збільшену відстань. Оригінальний сигнал Відправника приймається Ретранслятором, який підсилює його та передає Отримувачу. Для забезпечення якості сигналу, що ретранслюється, положення Ретранслятору повинно бути стабільним у просторі. Ретранслятор використовує відеокамеру, що знімає поверхню під ним. Послідовність відео кадрів використовується для розрахунку оптичного потоку. Ці результати використовуються для компенсації небажаних рухів Ретранслятору у просторі.

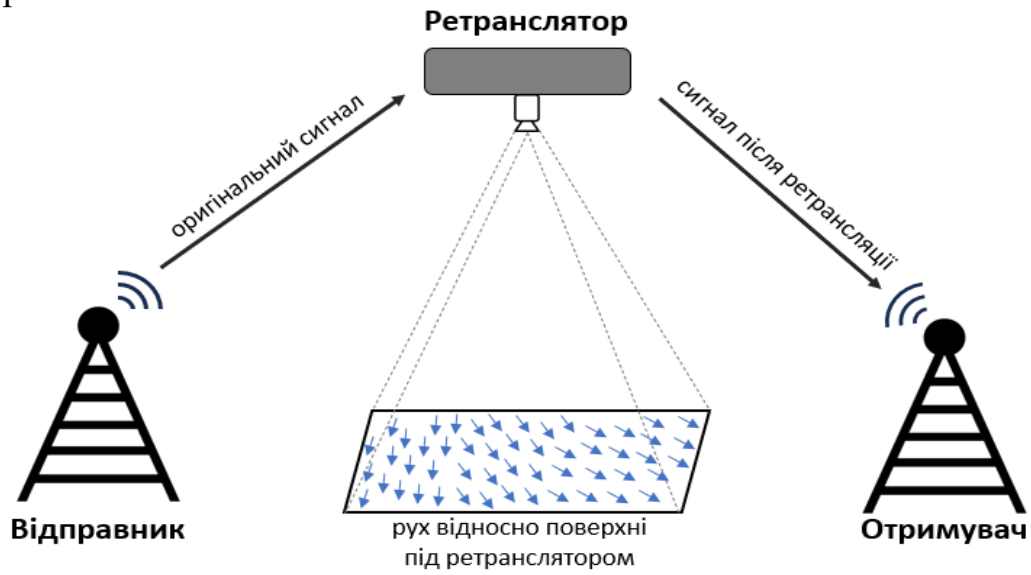


Рис. 1. Схема пристроїв, що забезпечують
передачу сигналу на збільшену відстань.

Метод стабілізації просторового положення пристрою ретранслятора для підвищення якості передачі сигналу складається з наступних кроків (рис. 2):

1. Сигнал з відеокамери ретранслятора, що направлена на поверхню під ним, перетворюється на послідовність відео кадрів.

2. Використовуючи часову послідовність кадрів, пристрій розраховує вектори оптичного потоку по осям x, y, z. Для розрахунку оптичного потоку можуть бути використані класичні методи, такі як диференціальний метод Лукаса-Канада [2], так і методи, які базуються на моделях машинного навчання, таких як FlowNet [3] або архітектури Трансформер [4].

3. Розрахунок корекції положення ретранслятору відбувається на основі даних оптичного потоку, а також даних про поточне положення пристрою. Оцінка змін якості сигналу в результаті попередніх корекцій положення пристрою є сигналом зворотного зв'язку і може використовуватися для підвищення точності подальших розрахунків корекції положення.

4. Завершальним кроком є корекція положення пристрою ретрансляції у 3D просторі на основі розрахунків, проведених на кроці 3.

Рис. 2. Метод корекції положення у просторі пристрою, що ретранслює сигнал.

Практичне застосування запропонованого методу може бути корисним у різних сферах, зокрема у мобільних бездротових мережах (стабілізація антен базових станцій у випадках нестабільного положення), безпілотних літальних апаратах (коригування положення передавача на БПЛА для підтримки стабільного сигналу з наземною станцією), автономних транспортних засобах (забезпечення якісного зв'язку між транспортними одиницями у складних умовах міського середовища), промислових IoT-системах (покращення стабільності зв'язку між мобільними сенсорами у виробничих приміщеннях або на відкритих майданчиках).

Запропонований підхід є особливо ефективним у системах, де необхідно підтримувати стабільний рівень сигналу в умовах змінного середовища та обмежених ресурсів каналу зв'язку. Використання аналізу оптичного потоку у поєднанні з традиційними методами покращення стабільності сигналу дозволяє значно підвищити ефективність бездротових мереж та зменшити втрати даних.

Таким чином, аналіз оптичного потоку відеосигналу є перспективним напрямком для підвищення якості безпровідного зв'язку. Подальші дослідження у цьому напрямку можуть бути зосереджені на оптимізації алгоритмів обробки відеосигналу, інтеграції методу з нейронними мережами для автоматичної адаптації параметрів зв'язку та розширеному тестуванні у реальних умовах експлуатації.

Література

1. Horn, Berthold K.P.; Schunck, Brian G. (August 1981). Determining optical flow (PDF). Artificial Intelligence (англ.). 17 (1–3): 185—203. doi:10.1016/0004-3702(81)90024-2.
2. B. D. Lucas and T. Kanade (1981), An iterative image registration technique with an application to stereo vision. Proceedings of Imaging Understanding Workshop, pages 121-130.
3. Dosovitskiy, Alexey; Fischer, Philipp; Ilg, Eddy; Hausser, Philip; Hazirbas, Caner; Golkov, Vladimir; Smagt, Patrick van der; Cremers, Daniel; Brox, Thomas (2015). FlowNet: Learning Optical Flow with Convolutional Networks. 2015 IEEE International Conference on Computer Vision (ICCV). IEEE. pp. 2758–2766.
4. Alfarano, Andrea; Maiano, Luca; Papa, Lorenzo; Amerini, Irene (2024). "Estimating optical flow: A comprehensive review of the state of the art". Computer Vision and Image Understanding. 249: 104160. doi:10.1016/j.cviu.2024.104160.

УДК 004.62:004.7:681.5:007.5

РОЗРОБКА МЕДІА-КОНТЕНТУ ДЛЯ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ ЗА ДОПОМОГОЮ UNREAL ENGINE

Дядюра К.О., Курдеча В.В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: diadiura.kirill@lll.kpi.ua

DEVELOPING MEDIA CONTENT FOR INTERNET OF THINGS SYSTEMS USING UNREAL ENGINE

The purpose of this publication is an attempt, using practical experience, to apply this solution in the field of infocommunications to improve the quality of modeling, management, and operation of Internet of Things systems.

Unreal Engine (UE) – це передове рішення, яке використовується для розробки 3D-контенту, створений компанією Epic Games. Його використовують для створення відеоігор для різноманітних платформ (таких як ПК, консолі та мобільні пристрої), а також для фільмів, реклами, використовують також і для створення віртуальної та доповненої реальності, архітектурних візуалізацій, симуляцій тощо. Метою даної публікації є спроба, використовуючи практичний досвід, застосувати дане рішення в сфері інфокомунікацій для підвищення якості моделювання, управління та роботи систем Інтернету речей.

UE надає можливості для створення різноманітного цифрового контенту, серед яких: відеоігри, фільми та кінематографічні сцени, створення рекламних роликів та сінематиків, віртуальна та доповнена реальність, симулятори та навчальні проєкти (використовується для інженерних, військових та медичних тренажерів).

А отже, відповідно UE може бути застосованим в інфокомунікаціях для створення 3D-візуалізацій покриття мереж, моделювання станцій зв’язку чи супутникових мереж.

На сьогоднішній день відома невелика кількість проектів в застосуванні UE в сфері телекомунікацій. Наприклад, компанія Exadel розробила симулятор мобільної мережі після стихійного лиха для телеком-оператора, використовуючи геопросторові дані та UE для оцінки відмов базових станцій та стратегій відновлення без шкоди справжній мережі, а Blare Tech спочатку використовувала UE для моделювання 5G-покриття у міських умовах, візуалізуючи рівні сигналу на 3D-карті місцевості. До того ж, Another Reality Studio створила VR-тренажер монтажника стільникових веж на UE [1;2].

Процес застосування UE для створення контенту для системи Інтернету речей пропонується розглядати наступним чином – рис. 1.

Рис.1. Процес застосування UE для створення контенту для мереж Інтернету речей.

До складових процесу відносяться наступні кроки:

1. Першим кроком створення будь-якого контенту є підготовка чіткого технічного завдання (далі – ТЗ), тобто документу, який опише суть, мету та кінцеве бачення продукту. до необхідного.

2. На основі даного документу виконується другий крок – це збір «референсів»[3] і створення розкадровки, а також збір прикладів оточення та зовнішнього вигляду персонажів/головного об’єкту (якщо готового не передбачено ТЗ) – рис.2.

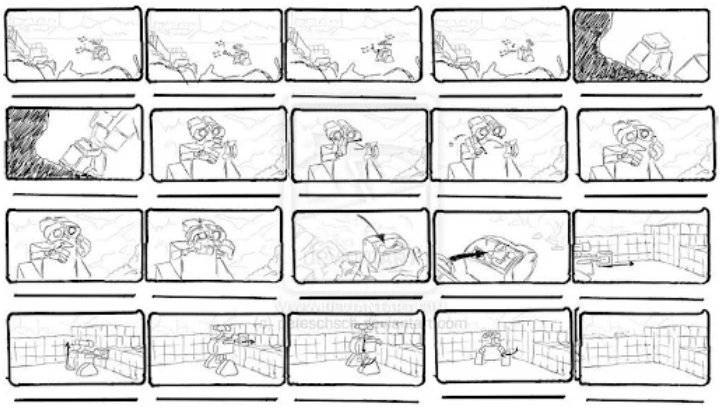


Рис.2. Збір референсів при створенні контенту Інтернету речей.

Це не менш важливий крок, який дає можливість на основі прикладів та намальованих кадрів створити вже наочне бачення як буде виглядати продукт, щоб у разі потреби одразу змінити концепцію чи деякі окремі кадри.

3. Тепер маючи кадри та чіткі приклади, що має бути зображено, створюється блокінг, базова версія. Використовуючи спочатку примітивні елементи, а після вже більш детальні, відтворюється у сирому вигляді вже 3D візуалізація продукту, що дозволяє вже побачити вигляд кінцевого продукту, виправити помилки.

Рис.3. Вигляд базової версії на різних етапах створення.

4. Отже, затвердивши та виправивши всі помилки зовнішнього вигляду та технічного завдання, маючи кінцевий базовий вигляд продукту, можна приступити до останнього кроку – наповнення, а саме – додавання матеріалів, зовнішнього вигляду, потрібного стилю графіки, налаштування світла тощо.

Таким чином, можливо застосувати технічні засоби Unreal Engine для під’єднання до IoT-систем. Зокрема, за рахунок протоколу MQTT. А отже це дає можливість напряму підключитися до брокера MQTT і отримувати/надсилати телеметрію з сенсорів у реальному часі, фактично “оживляючи” 3D-сцену даними зі справжніх пристроїв. Окрім MQTT, Unreal підтримує й інші методи зв’язку. Є можливість використовувати WebSocket-з’єднання –доступні плагіни (наприклад, EasyWebSocket) для інтеграції через Blueprints, що дозволяє отримувати потоки даних безперервно.

Література

1. Using Serious Gaming to Simulate Disaster Recovery for a Major Telco - Режим доступу: https://exadel.com/news/serious-gaming-for-a-major-telco/ - Назва з екрана (дата звернення: 17.03.2025).
2. Virtual Safety Training Project Overview - Режим доступу: https://anotherreality.studio/case-studies-old/virtual-safety-training/ - Назва з екрана (дата звернення: 17.03.2025).
3. UFS: Анімаційні фільми - Режим доступу: https://filmschool.com.ua/animacijne_kino - Назва з екрана (дата звернення: 17.03.2025).
4. Smart home embedded system | Zero OS — Режим доступу: https://thefwa.com/cases/smart-home-embedded-system-zero-os-p2 — Назва з екрана (дата звернення: 17.03.2025).

УДК 004.72:004.62:331.4:614.7

СИСТЕМА ЕКОЛОГІЧНОГО МОНІТОРИНГУ НА ОСНОВІ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

Щербина Н.Є. Курдеча В.В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: shcherbina.nikita@lll.kpi.ua

ECOLOGICAL MONITORING SYSTEM BASED ON INTERNET OF THINGS TECHNOLOGY

The task of environmental monitoring is to prevent emergency and dangerous situations in order to save human life and health. Therefore, the effectiveness and reliability of such monitoring should be as high as possible. The purpose of the publication is to increase the reliability and efficiency of environmental monitoring through the Internet of Things.

Метан є одним із найшкідливіших парникових газів, який здатен спричиняти значний вплив на зміну клімату. Викиди цього газу в газовидобувній промисловості становлять серйозну екологічну проблему, так як неконтрольовані витоку можуть сприяти глобальному потеплінню та економічним втратам через втрату цього ресурсу. Міжнародні екологічні стандарти та державні регуляції зобов'язують вести контроль рівню викидів метану, що вимагає впровадження ефективних технологій моніторингу. Традиційні методи вимірювання, такі як ручні перевірки, не здатні забезпечити постійний контроль та оперативне реагування на витоки. Тому актуальною задачею є розробка та вдосконалення IoT-систем для автоматизованого моніторингу викидів метану на газових свердловинах.

Наразі існує декілька підходів до моніторингу газових викидів. Одним з них є вищезазначені ручні вимірювання, який є традиційним методом, що включає використання газоаналізаторів та періодичних інспекцій персоналу. Недоліками можна вважати низьку оперативність та значну залежність від людського фактору.

Мобільні наземні системи моніторингу - це автомобілі, які оснащені газоаналізаторами та системами збору даних. Вони пересуваються майданчиками, або територією газових родовищ, фіксуючи під час цього зміни концентрації метану у повітрі.[1]. Перевагами є високі точності вимірювань, виявлення витоків газу без встановлення великої кількості стаціонарних датчиків та можливість мобільного розгортання на нових об'єктах. Але звідси випливають і недоліки: великі витрати на персонал, неможливість цілодобового моніторингу та менша ефективність через специфіку логістики.

Тому пропонується система моніторингу на основі технології Інтернету речей[2-5]. Модифікація даної системи відбувається за рахунок технології LPWAN (табл. 1), яка застосовується замість або сумісно з іншими системами зв'язку [6]

Таблиця 1. Порівнянь характеристик LPWAN та GSM для систем екологічного моніторингу.

Параметр	LPWAN	GSM
Діапазон дії	До 15км	до 5км (3G, 4G), до 1км (5G)
Споживання енергії	Дуже низьке, пристрої можуть працювати роками на батареї	Високе, потребує постійного живлення або заряджання
Пропускна здатність	Низька (0,3 – 50 кб/с), підходить для малих обсягів даних	Висока (до 1 Гб/с у 5G), для потокових даних
Масштабованість	Висока	Обмежена операторами
Наявність покриття	Потрібно розгортати власну мережу	Глобальне покриття мобільних операторів
Застосування	Ідеальне для IoT, моніторингу довкілля, «розумного» міста	Підходить для передачі великих обсягів даних

На рис.1 зображено систему моніторингу метану з використанням IoT технології. Стаціонарні та автономні датчики вимірюють концентрацію метану та надсилають дані через LPWAN до найближчих станцій. Станції отримують ці дані та пересилають їх через мережу до сервера, який обробляє дані та зберігає їх у хмарі.

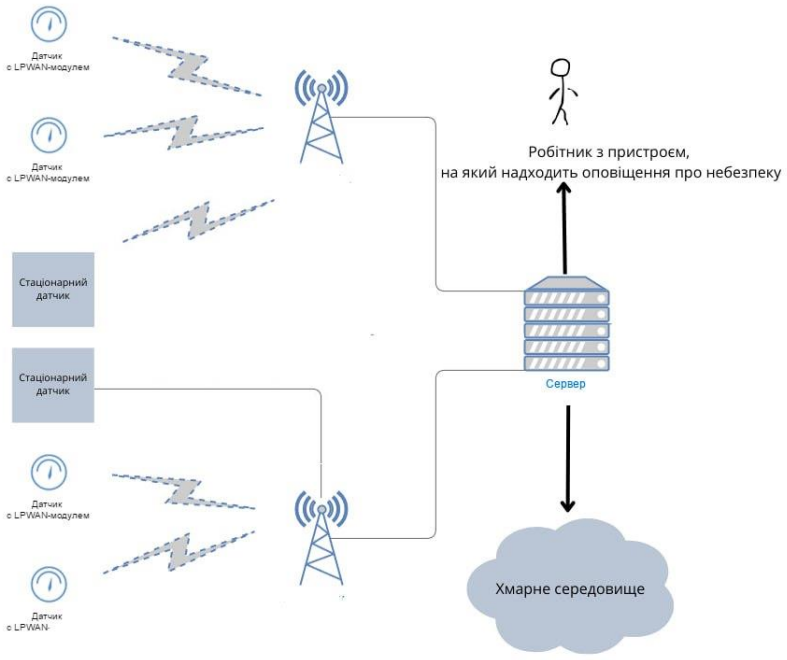


Рис. 1. Модифікована система екологічного моніторингу та сповіщення на основі технології Інтернету речей.

Якщо виявлено небезпечну концентрацію газів, то сервер надсилає оповіщення робітнику, який отримує сповіщення на свій пристрій. Ця система дозволяє оперативніше реагувати на потенційні витоки, зводячи ризики до мінімуму.

Отже, модифікована система для моніторингу викидів метану, яка відрізняється від існуючих рішень використанням LPWAN/LoRaWAN, дозволить знизити енергоспоживання та забезпечити зв’язок сенсорів на великих відстанях; інтеграція з хмарною платформою дозволить отримувати дані у реальному часі, відслідковувати виявлення аномалій та прогнозувати потенційні витоки.

Запропоноване рішення дозволить значно підвищити ефективність моніторингу, забезпечити швидке реагування на екологічні ризики та знизити витрати на контроль викидів. Така система може бути впроваджена як «головна», так і в доповнення до уже існуючих систем екологічного моніторингу.

Література

1. Picarro and NTT-AT Deploy Natural Gas Pipeline Inspection Solution for Teiseki Pipeline Corporation in Japan https://www.picarro.com/gas/picarro_and_nttat_deploy _natural_gas_pipeline_inspection_solution_for_teiseki_pipeline
2. S. Ushakov, L. Globa and V. Kurdecha, "EVOLVING INDUSTRY 4.0: A METHODICAL APPROACH TO OPTIMIZING IOT ONTOLOGIES FOR ENHANCED AUTOMATION," 2024 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Tbilisi, Georgia, 2024, pp. 131-134, doi: 10.1109/BlackSeaCom61746.2024.10646225.
3. Ushakov Serhii and Kurdecha 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
4. 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 2022. Lecture Notes in Networks and Systems, vol 809. Springer, Cham. https://doi.org/10.1007/978-3-031-46880-3_13
5. Eduard Siemens, Vasyl Kurdecha, Serhii Ushakov, "INTERNET OF THINGS DATA TRANSFER METHOD USING NEURAL NETWORK AUTOENCODER" Information and Telecommunication Sciences, 2023, #1, DOI: 10.20535/2411-2976.12023.9-15
6. Солоденко М.А., Курдеча В.В. ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ ЗБОРУ ІНФОРМАЦІЇ ВУЗЛІВ ІНТЕРНЕТУ РЕЧЕЙ //XVIII Міжнародна науково-технічна конференція "Перспективи телекомунікацій" ПТ-2024: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2024. – с.167.

УДК 004.7:658.6:658:8

МОДИФІКОВАНИЙ ПРОЦЕС ОБРОБКИ ЗАЯВОК В ІНФОКОМУНІКАЦІЙНІЙ СИСТЕМІ ДЛЯ ЗАБЕЗПЕЧЕННЯ ОПЕРАЦІЙНОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

Бачук М.І., Курдеча В.В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: bachuk.maxym@lll.kpi.ua

MODIFIED APPLICATION PROCESS IN THE INFORMATION AND COMMUNICATION SYSTEM FOR ENSURING THE OPERATIONAL ACTIVITIES OF AN ENTERPRISE

The main existing solutions for infocommunication systems for retail trade were considered, their shortcomings were analyzed, and a strategy was developed to optimize the operational activities of the enterprise by integrating chatbots into the system.

В умовах стрімкого розвитку технологій та розширення сфери надання послуг, зокрема роздрібної торгівлі, головним рішенням автоматизації операційної діяльності підприємства стають інфокомунікаційні системи. Вони дозволяють забезпечити ефективне управління бізнес-процесами підприємства(Табл.1). Метою даної публікації є пропозиції щодо модифікації інфокомунікаційної системи підприємства для підвищення ефективності його операційної діяльності.

Таблиця 1. Порівняння інфокомунікаційних рішень операційної діяльності.

Система	Призначення	Переваги	Недоліки
ERP	Управління всіма процесами компанії, такими як ресурси, фінанси, склад, CRM	Комплексний підхід управління бізнес-процесами	Висока вартість та складність впровадження
POS	Обробка продажів, платежів та товарообігу	Легка інтеграція та швидкість обслуговування	Обмежена функціональність, можлива додаткова інтеграція з іншими системами
CRM	Управління клієнтською базою	Покращена взаємодія з клієнтами та обробка надходження заявок	Потребує інтеграції з іншими системами або маркетплейсами
WMS	Оптимізація складу	Точність обліку товарообігу	Потрібна інтеграція з ERP

POS-системи відносяться до таких систем та дозволяють вести облік товару, допомагають з веденням бухгалтерського обліку, зокрема з обробкою платежів та продажів. Недоліком таких систем є відсутність інтеграції клієнтських модулів, таких як CRM.

WMS-системи забезпечують підприємство оптимізацією логістики, веденням обліку товарообігу та залишків самого товару. ERP-системи охоплюють усі напрямки ведення бізнесу роздрібної торгівлі та не тільки. Основним недоліком є висока вартість та складність впровадження.

CRM-системи допомагають з підтримкою клієнтської бази. Деякі з них дозволяють отримувати замовлення з урахуванням того, що ця система інтегрована до інших систем або ж маркетплейсів, що допомагає додатково оптимізувати роботу підприємства в введенні обліку.

Порівняння даних рішень (табл. 1) показує необхідність модифікації інфокомунікаційної системи підприємства для підвищення ефективності операційної діяльності.

На рис. 1 описано процес надходження заявки клієнта до CRM-системи з односторінкового сайту та подальшої її обробки.

Основною проблемою такої системи надходження заявки є саме кінцевий результат обробки в месенджері, оскільки зазвичай на це йде багато часу. Для клієнтів є важливим не якість ведення листування, а швидкість відповіді представника компанії. Чим швидше буде оброблена заявка клієнта, тим більше шансів утримати потенційного покупця. Одним з можливих рішень в такому випадку є впровадження чат-ботів та інтеграція їх до CRM-системи.

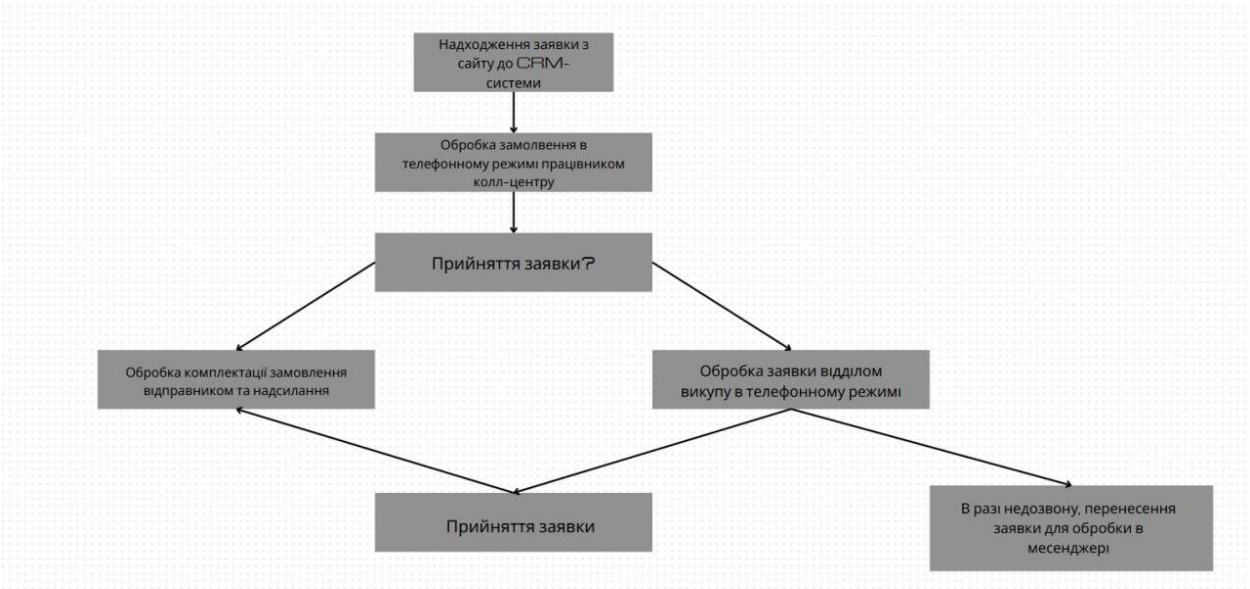


Рис 1. Процес надходження заявки та подальшої її обробки.

Основними месенджерами для обробки звернень клієнтів в Україні залишаються Телеграм та Вайбер. На відміну від СМС-розсилок та телефонної обробки заявок, комунікація в месенджерах безкоштовна. Процес розробки таких ботів можна розбити в декілька етапів. Перш за все, бот повинен бути зареєстрований для того, щоб отримати API Token, який знадобиться для інтеграції бота. Щоб створити бот у Вайбері потрібно пройти реєстрацію бізнес-акаунта для отримання API ключа на Viber Partner.

Наступним кроком вирішення є вибір технології розробки. Зазвичай для Телеграм-ботів використовується Python, зокрема python-telegram-bot,

aiogram, pyTelegramBotAPI. Для реалізації чат-боту в Вайбері за допомогою Python використовується viberbot.

Після етапу розробки бот можна інтегрувати до CRM-системи за допомогою API CRM, щоб забезпечити автоматизовану передачу заявок та їх обробку. Модифікована структура надходження заявки з інтеграцією бота наведена на рисунку 2.

Рис 2. Модифікований процес обробки заявки в удосконаленій інфокомунікаційній системі підприємства.

Отже в даній роботі було модифіковано процес обробки заявки за рахунок застосування чат-ботів в інфокомунікаційній системі підприємства роздрібної торгівлі. Дане рішення призвело до покращення показників операційної діяльності підприємства (зменшується часозатратність). Окрім того, покращено процес комунікації з клієнтами підприємства.

Література

1. É. Marcon, G. A. Marodin and A. G. Frank, "Combining Organizational and Social Factors to Support Industry 4.0 Implementation: A Sociotechnical and Configurational Analysis of Technology Adopters," in *IEEE Transactions on Engineering Management*, vol. 72, pp. 146-160, 2025, doi: 10.1109/TEM.2024.3506991.Ковальська Д. Д., Курдеча В.В., Якорнов Є.А. МЕРЕЖЕВИЙ АУДИТ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ //XVIII Міжнародна науково-технічна конференція "Перспективи телекомунікацій" ПТ-2024: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2024. – с. 161.
2. S. Ushakov, L. Globa and V. Kurdecha, "EVOLVING INDUSTRY 4.0: A METHODICAL APPROACH TO OPTIMIZING IOT ONTOLOGIES FOR ENHANCED AUTOMATION," 2024 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Tbilisi, Georgia, 2024, pp. 131-134, doi: 10.1109/BlackSeaCom61746.2024.10646225.
3. Globa, L., Kurdecha, V., Popenko, D., Bezvuhliak, M., Porolo, Y. (2022). Data Collection and Processing Method in the Networks of Industrial IOT. In: Perakovic, D., Knapcikova, L. (eds) Future Access Enablers for Ubiquitous and Intelligent Infrastructures. FABULOUS 2022. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 445. Springer, Cham. https://doi.org/10.1007/978-3-031-15101-9_11
4. B. Kumar, Y. Anjali, M. Mudholkar, P. Mudholkar, P. V. Bharati and N. Abdullayeva, "IoT-Enabled Asset Management and Tracking in Organizations," *2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES)*, Lucknow, India, 2024, pp. 1-5, doi: 10.1109/IC3TES62412.2024.10877428.

УДК 004.43

АВТОМАТИЗОВАНА СИСТЕМА КОНТРОЛЮ МІКРОКЛІМАТУ В ТЕПЛИЦЯХ НА БАЗІ ANDROID

Самолюк М.І., Суліма С.В.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: itssulima@gmail.com

AUTOMATED MICROCLIMATE CONTROL SYSTEM IN GREENHOUSES BASED ON ANDROID

The use of automated technologies to control the microclimate in home greenhouses can significantly improve the efficiency of growing plants. The creation of a mobile application for remote monitoring and control of greenhouse parameters is a key step in improving this process.

Інтелектуальний Android-додаток для автоматизованого контролю мікроклімату в домашніх теплицях являє собою значний прогрес у сільськогосподарських технологіях, використовуючи можливості Інтернету речей (IoT) і штучного інтелекту (ШІ) для оптимізації умов росту рослин. Сприяючи моніторингу та управлінню найважливішими параметрами навколишнього середовища, такими як температура, вологість і вологість ґрунту, в режимі реального часу, ця програма дозволяє користувачам підвищити продуктивність і стійкість тепличного господарства. Зростаючий глобальний попит на ефективні сільськогосподарські практики підкреслює актуальність інтелектуального Android-додатку для автоматизованого контролю мікроклімату в домашніх теплицях, особливо в умовах, коли зміна клімату впливає на традиційні методи ведення сільського господарства і ставить під загрозу продовольчу безпеку в усьому світі [1, 2].

Запропонована програма має зручний інтерфейс, який дозволяє безперешкодно взаємодіяти з різними датчиками і системами управління, гарантуючи, що користувачі, включаючи дрібних фермерів, можуть легко впроваджувати передові технології, не потребуючи значних технічних знань і досвіду. Інтеграція алгоритмів штучного інтелекту підвищує автоматизацію тепличних операцій за рахунок прогнозування змін навколишнього середовища та оптимізації використання ресурсів, що сприяє як підвищенню якості врожаю, так і зниженню операційних витрат [3]. Крім того, додаток сприяє доступності на різних пристроях, обслуговуючи ширшу аудиторію та сприяючи більш інклюзивному підходу до сучасних сільськогосподарських практик [4].

Схематичне представлення загальної структури інформаційної системи показано на рис. 1.

Основні функціональні можливості додатку включають:

- Зареєструватися та увійти в систему.
- Додавати теплиці за допомогою QR-коду.

- Відстежувати дані датчиків в режимі реального часу (температура, вологість, світло, вологість ґрунту, рівень води).
- Створювати власні плани вирощування або використовувати попередньо визначені шаблони.
- Ручне керування автоматизованими системами.
- Керування модулями теплиці (освітлення, насос, охолодження).
- Пуш-сповіщення про критичні події.

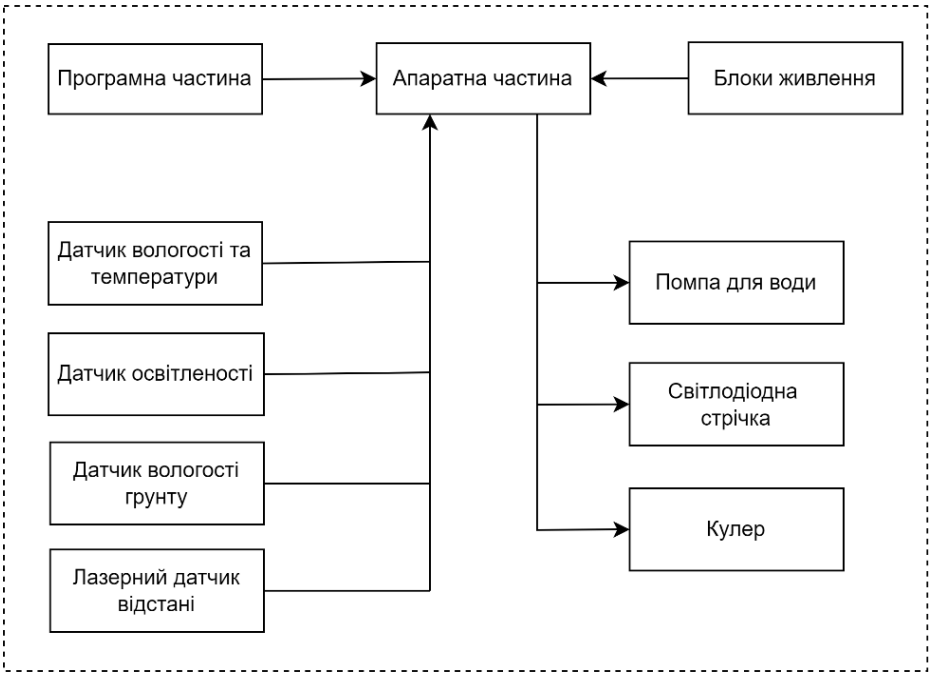


Рис.1. Схематичне представлення загальної структури інформаційної системи.

Додаток використовує HTTPS для безпечного зв'язку та bcrypt для хешування паролів. Spring Security обробляє аутентифікацію та авторизацію на стороні сервера. Логічне представлення взаємодії між компонентами застосунку показано на рис. 2.

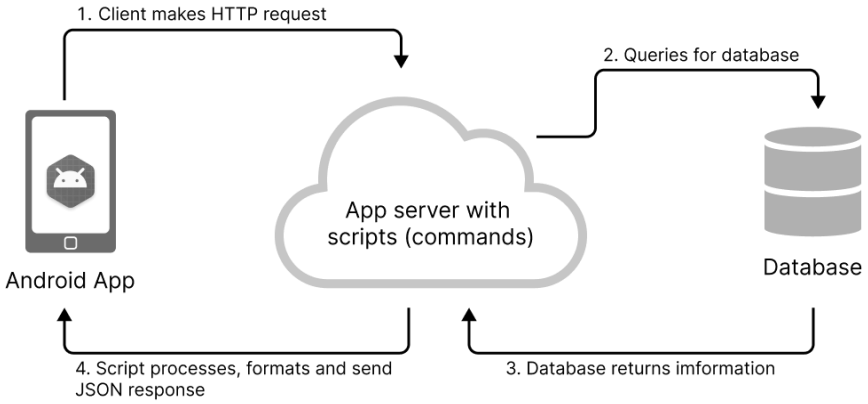


Рис.2. Логічна схема взаємодії компонентів застосунку.

Серверна частина була реалізована у вигляді застосунку, який працює в хмарному середовищі. Її функціональність забезпечується за допомогою мови Kotlin та фреймворку Spring Boot. Клієнтська частина представлена у вигляді Андроїд-застосунку. Її структура організована відповідно до сучасних стандартів мобільної розробки.

На головній сторінці додатку відображаються всі поточні параметри, які характеризують процес вирощування рослини. Завдяки перемикачам, розташованим на картках із показниками, користувач може активувати ручний режим налаштування, якщо потрібно внести тимчасові зміни до певних параметрів, таких як температура чи вологість. У нижній частині екрану знаходиться панель навігації, що забезпечує перехід між основними розділами програми.

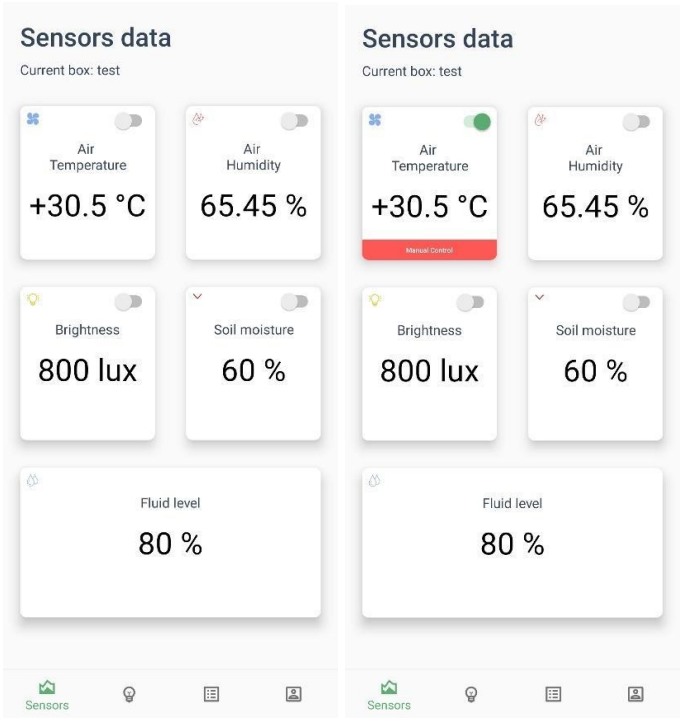


Рис.3. Основний екран додатку.

Загалом, інтелектуальний додаток для Android для автоматизованого контролю мікроклімату стоїть на передовій сучасних сільськогосподарських рішень, сприяючи підвищенню ефективності та сталості в тепличному середовищі, одночасно сприяючи більшій залученості різних груп користувачів. Очікується, що його подальший розвиток відіграватиме ключову роль у формуванні майбутніх сільськогосподарських практик на тлі зростаючих екологічних викликів.

Література

1. K. M. Al-Aubidy, M. M. Ali, A. M. Derbas and A. W. Al-Mutairi, "Real-time monitoring and intelligent control for greenhouses based on wireless sensor network," 2014 IEEE 11th International Multi-Conference on Systems, Signals & Devices (SSD14), Barcelona, Spain, 2014, pp. 1-7, doi: 10.1109/SSD.2014.6808765.
2. Cutting-Edge Technologies for Microclimate Monitoring in Greenhouses: How Gadgets Help Preserve Plants. Vanegexfol.com, https://vanegexfol.com/. Accessed 8 Feb. 2025.
3. Gul, Danish, and Rizwan Ul Zama Banday. "Transforming Crop Management Through Advanced AI and Machine Learning: Insights into Innovative Strategies for Sustainable Agriculture." AI, Computer Science and Robotics Technology, vol. 1, no. 4, 2024, pp. 123-145. IntechOpen, doi:10.5772/acrt.20240030.
4. Lee M-H, Yao M-H, Kow P-Y, Kuo B-J, Chang F-J. An Artificial Intelligence-Powered Environmental Control System for Resilient and Efficient Greenhouse Farming. Sustainability. 2024; 16(24):10958. https://doi.org/10.3390/su162410958.

УДК 621.39

ПІДХІД ДО РЕСУРСОЕФЕКТИВНОГО NETWORK SLICING НА БАЗІ NETWORK FUNCTIONS VIRTUALIZATION

Матвєєв Є.В., Суліма С.В.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: itssulima@gmail.com

AN APPROACH TO RESOURCE-EFFICIENT NETWORK SLICING BASED ON NETWORK FUNCTIONS VIRTUALIZATION

The paper discusses an approach to optimizing resource management in 5G and 6G networks using Network Slicing and Network Functions Virtualization (NFV) technologies. The integration of machine learning methods is proposed to ensure efficient resource allocation between network slices.

Розподіл мережі на сегменти дозволяє створювати кілька віртуальних мереж, або «слайсів», на одній фізичній інфраструктурі, пристосованих до конкретних вимог додатків. Ця можливість має вирішальне значення для задоволення різноманітних потреб у послугах, таких як розширений мобільний широкосмуговий зв'язок, наднадійний зв'язок з низькою затримкою та зв'язок з Інтернетом речей (IoT), що робить її важливою сферою вивчення та впровадження в сучасних телекомунікаціях [1-3]. Важливість оптимізації управління ресурсами в цьому контексті полягає в її потенціалі для підвищення ефективності, продуктивності та масштабованості мережі при мінімізації операційних витрат. Ключовими поняттями в цьому процесі оптимізації є динамічний розподіл ресурсів, інтелектуальне розбиття мережі на сегменти та методи оптимізації на основі штучного інтелекту, які мають на меті полегшити коригування мережевих ресурсів у реальному часі відповідно до мінливих потреб. Хоча ці методи обіцяють значне поліпшення використання ресурсів і якості послуг, вони також представляють складності, пов'язані з впровадженням і управлінням, які необхідно вирішити, щоб використовувати весь їхній потенціал [4].

Оскільки телекомунікаційний ландшафт продовжує розвиватися з появою технологій 5G і майбутніх технологій 6G, фокус на оптимізації управління ресурсами для розгалуження мережі буде мати вирішальне значення для вирішення проблем і використання можливостей, пов'язаних з цим трансформаційним зрушенням в мережевій архітектурі [5, 6].

Основний внесок даного дослідження полягає у застосуванні алгоритмів машинного навчання для оптимізації Network Slicing у поєднанні з NFV:

1. Інтелектуальне управління ресурсами – розроблено модель, яка аналізує історичні дані про навантаження мережі та прогнозує оптимальний розподіл ресурсів.

2. Динамічне масштабування – запропонований підхід дозволяє адаптувати параметри мережі в режимі реального часу, знижуючи

ймовірність перевантаження окремих сегментів.

3. Оптимізація використання NFV – інтеграція запропонованого алгоритму з NFV дозволяє гнучко змінювати конфігурацію мережі без додаткових витрат на обладнання.

Запропонована модель складається з наступних компонентів:

1. Модуль збору даних – відстежує параметри мережі в реальному часі, збираючи інформацію про трафік, пропускну здатність та затримки.

2. Модуль прогнозування (XGBoost) – аналізує історичні дані для передбачення оптимального розподілу ресурсів.

3. Модуль управління ресурсами – виконує автоматичне масштабування ресурсів залежно від поточного навантаження.

4. Модуль інтеграції з NFV – забезпечує динамічну конфігурацію мережевих функцій без необхідності зміни фізичного обладнання.

5. Модуль моніторингу та адаптації – постійно аналізує ефективність використання ресурсів та коригує параметри мережі в режимі реального часу.

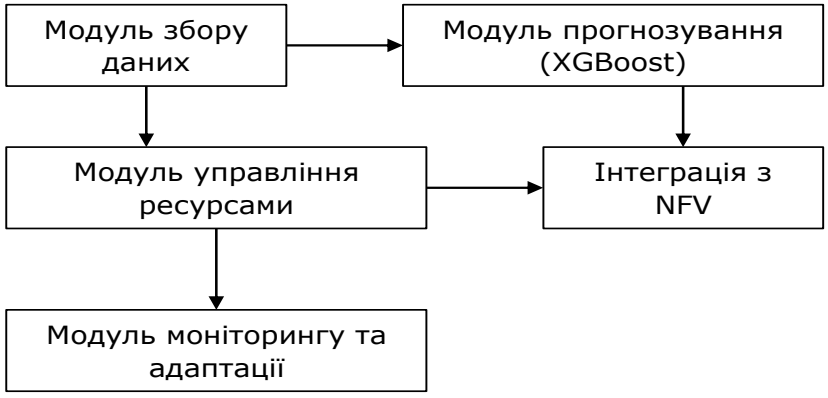


Рис.1. Графічна схема моделі.

Загальний принцип роботи:

Дані збираються → передаються в XGBoost для прогнозування → на основі прогнозу здійснюється управління ресурсами → зміни інтегруються в NFV → моніторинг контролює ефективність і за необхідності коригує стратегію. Для навчання моделі необхідно правильно підготувати дані.

Таблиця 1. Приклад набору даних.

Слайс	**Тип**	**Мін. CPU**	**Мін. RAM**	**Мін. BW**	**Навантаження (%)**	**Оптимальний CPU**	**Оптимальний RAM**	**Оптимальний BW**
Слайс1	eMBB	20	10	30	70	30	15	40
Слайс2	URLLC	15	10	20	50	20	12	25
Слайс3	mMTC	10	5	10	30	12	8	15

Після навчання оцінюємо ефективність моделі.

Середньоквадратична помилка (MSE): середнє квадратичне відхилення між прогнозованими та реальними значеннями:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(y_{\text{pred}}^{i} - y_{\text{true}}^{i})^2$$

де y_{pred}^{i} — це передбачене значення, а — y_{true}^{i} реальне значення.

MSE є дуже популярною функцією втрат у задачах регресії через кілька причин. По-перше, якщо між прогнозованими і реальними значеннями є велика різниця, MSE дає значно більше значення, що дозволяє моделі зосереджуватися на точності для важливих прогнозів. Крім того, MSE має гарні математичні властивості, що робить її зручною для аналізу і оптимізації. Вона є диференційованою функцією, що дозволяє використовувати стандартні методи оптимізації, такі як градієнтний спуск. Таким чином, вибір MSE як функції втрат забезпечує стабільність і ефективність навчання моделі в задачах регресії.

Корисність коефіцієнта детермінації R2R^2: Коефіцієнт детермінації вимірює, яка частина варіації в залежній змінній може бути пояснена моделлю. Він варіюється від 0 до 1, де 1 означає, що модель абсолютно точно передбачає всі значення, а 0 — що модель не має прогностичної сили.

Для оцінки ефективності було проведено симуляційне моделювання. Аналіз показав, що використання алгоритму XGBoost для управління ресурсами дозволяє зменшити затримки в мережі на 15–20% та підвищити ефективність використання ресурсів на 25% у порівнянні з традиційними методами.

Інтеграція машинного навчання та NFV у процес управління ресурсами дозволяє знизити експлуатаційні витрати, підвищити продуктивність та покращити якість обслуговування.

Література

1. Li, Xin, et al. "Network Slicing for 5G: Challenges and Opportunities." IEEE Internet Computing, vol. 21, no. 5, Aug. 2017, pp. 20-27.
2. Ulema, Mehmet. "5G Network Slicing - Part 1: Concepts, Principles, and Architectures." IEEE Communications Magazine, 2017, pp. 70-71.
3. Subedi, P., Alsadoon, A., Prasad, P.W.C. et al. Network slicing: a next generation 5G perspective. J Wireless Com Network 2021, 102 (2021). https://doi.org/10.1186/s13638-021-01983-7.
4. GeeksforGeeks, "What is Network Virtualization?" GeeksforGeeks. [Online]. Available: https://www.geeksforgeeks.org/what-is-network-virtualization/. [Accessed: Feb. 10, 2025].
5. G. Singh, "Explain the concept of Network Slicing in 5G," Telecom Trainer, Jan. 6, 2024. [Online]. Available: https://www.telecomtrainer.com/explain-the-concept-of-network-slicing-in-5g/. [Accessed: Feb. 10, 2025].
6. Andrade, M., & Wickboldt, J. A. (2025). A Study on 5G Network Slice Isolation Based on Native Cloud and Edge Computing Tools. arXiv preprint arXiv:2502.02842.

УДК 004.7

СПОСІБ ПЕРЕРОЗПОДІЛУ ЕЛЕКТРОЕНЕРГІЇ В МЕРЕЖІ MICROGRID НА БАЗІ ОНТОЛОГІЧНОЇ МОДЕЛІ

Степанов Г. О., Новогрудська Р. Л.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: glib4400@gmail.com

A METHOD OF REDISTRIBUTION OF ELECTRICITY IN A MICROGRID NETWORK BASED ON AN ONTOLOGICAL MODEL

The paper examines the key operational modes of Microgrids, including grid-connected, islanded, black start, peak load shaving, renewable integration, and emergency modes. A dynamic energy redistribution method based on an ontological model is proposed, utilizing real-time monitoring and adaptive decision-making. The method analyzes the balance between energy generation and consumption, prioritizes critical loads, and dynamically manages energy flows. The ontological model facilitates the integration of data from generation, storage, and distribution components, ensuring automated system adjustments and interoperability between different devices.

У процесі розробки стратегії перерозподілу електроенергії в мережі Microgrid важливо враховувати різні сценарії її роботи.

Нормальний режим роботи (Grid-Connected Mode). У цьому режимі Microgrid підключена до основної електромережі та працює синхронно з нею. Електроенергія може як споживатися з мережі, так і передаватися до неї залежно від балансу генерації та споживання всередині Microgrid.

Острівний режим (Islanded Mode). У випадку відключення від основної мережі (наприклад, через аварію або планове обслуговування) Microgrid переходить в автономний режим.

Режим відновлення після аварії (Black Start). Після повного знеструмлення Microgrid повинна мати можливість самостійно відновити роботу без залежності від основної мережі. Це вимагає наявності джерел енергії, здатних ініціювати процес відновлення, та координації між компонентами системи для поступового підключення навантажень.

Режим пікового навантаження (Peak Load Shaving). У періоди високого споживання електроенергії Microgrid може зменшувати навантаження на основну мережу, використовуючи власні генератори або системи зберігання енергії.

Режим інтеграції відновлюваних джерел енергії (Renewable Integration Mode). Зі збільшенням частки відновлюваних джерел, таких як сонячні панелі та вітрові турбіни, Microgrid повинна ефективно керувати змінністю їх генерації.

Режим аварійного реагування (Emergency Mode). У випадку критичних ситуацій, таких як природні катастрофи або техногенні аварії, Microgrid може забезпечувати електроенергією критично важливі об'єкти, відключаючи некритичні навантаження для збереження ресурсів та підтримки життєво важливих функцій [1].

Для оптимального управління керованими пристроями як на стороні постачання, так і на стороні споживання, у координованому режимі застосовується гібридна система, основана на технології багатоагентних систем. У цій системі розглядаються центральний координатор Microgrid, розподілені елементи, відновлювальні джерела енергії, система зберігання енергії та сервісні компоненти. Реалізована архітектура зв'язку та ієрархія передачі повідомлень, що здійснюється через обмін інформацією між центральним координатором та системами відновлювальних джерел енергії. Протягом кожного періоду прийняття рішень синергія досягається через обмін повідомленнями, які передають дані про доступну потужність від відновлювальних джерел енергії до систем управління енергоспоживання [2]. Кожен елемент управління споживанням енергії регулює енергоспоживання та генерацію, враховуючи інформацію, завдання, робочий стан пристроїв та вимоги до споживання електроенергії, з максимальною метою мінімізації витрат на електроенергію та досягнення максимального рівня комфорту. Потім обсяг електроенергії, що обмінюється між мережею, передається центральному координатору. Підсумовуючи всі транзакції з мережею, центральний координатор у співпраці з системою зберігання електроенергії може регулювати систему зберігання на основі різних факторів, таких як чистий попит на потужність, ціни на та можливість обміну з мережею для виконання цілей та обмежень системи.

Визначаючи компоненти системи збору та обробки інформації, ми можемо виділити компоненти, які безпосередньо стосуються збору, обробки та передачі інформації в контексті системи Microgrid. Система Microgrid складається з компонентів для генерації енергії, зберігання енергії, управління та перерозподілу. До них належать системи для моніторингу та управління енергетичними потоками, такі як компоненти зберігання, що відслідковують рівень заряду, стан батарей і ефективність зберігання енергії. Компоненти управління інтегрують дані з різних джерел енергії та систем зберігання, а компоненти перерозподілу моніторять напругу та контролюють комутацію для забезпечення стабільності мережі. Інтерфейси користувачів надають доступ до даних і моніторингу стану енергосистеми, а користувачі системи відповідають за аналіз зібраної інформації та прийняття рішень [3].

Логіка роботи системи на основі онтологічних правил

- Отримуємо інформації про рівні генерації, стан сховищ, навантаження та активність споживачів.
- Визначаємо, які джерела та сховища можуть бути задіяні залежно від критеріїв перерозподілу:
- Вибираємо джерела генерації залежно від вартості та доступності, та перерозподіляє між підстанціями залежно від балансу генерації та споживання:
- Займаємося моніторингом оновлення параметрів у реальному часі, автоматично коригуючи перерозподіл.
- Надаємо операторам та аналітикам візуалізовані дані про поточний стан системи.

Для ефективного перерозподілу електроенергії пропонується алгоритм, який ґрунтується на динамічному аналізі вхідних параметрів. На першому етапі аналізується баланс між виробленою та спожитою енергією. Якщо генерація перевищує попит, енергія або спрямовується в сховища, або перерозподіляється серед споживачів. Якщо ж генерація недостатня, система або активує резервні джерела, або вводить обмеження на некритичні навантаження. Важливою частиною алгоритму є пріоритизація споживачів. Критично важливі об'єкти, отримують безперебійне енергопостачання, тоді як вторинні навантаження можуть бути тимчасово обмежені.

Система працює в реальному часі, постійно моніторячи параметри та адаптуючи розподіл енергії. Якщо виникають аварійні ситуації, алгоритм автоматично вживає заходів: коригує напругу через комутаційне обладнання або активує резервні джерела живлення.

Література

1. K. M. Son, K. Lee, D. -C. Lee, E. -C. Nho, T. -W. Chun and H. -G. Kim (2009), “Grid interfacing storage system for implementing microgrid”, 2009 Transmission & Distribution Conference & Exposition: Asia and Pacific, P. 1-4.
2. A. Anvari-Moghaddam, J. M. Guerrero, A. Rahimi-Kian and M. S. Mirian (2016), “Optimal real-time dispatch for integrated energy systems: An ontology-based multi-agent approach”, 2016 IEEE 7th International Symposium on Power Electronics for Distributed Generation Systems (PEDG), P. 1-7.
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.

УДК 004.4

ПІДХІД ДО АВТОМАСШТАБУВАННЯ КЛАСТЕРІВ KUBERNETES НА ОСНОВІ ПЕРСОНАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ РЕСУРСІВ КОРИСТУВАЧІВ

Ковальов А.В., Алєксєєв М.О.
Навчально-науковий інститут телекомунікаційних систем
НТУУ «КПІ» ім. Ігоря Сікорського, Україна
E-mail: andreyjester32@gmail.com, alexeyev@its.kpi.ua

APPROACH TO AUTOSCALING KUBERNETES CLUSTERS BASED ON PERSONAL COMPUTATIONAL RESOURCES OF USERS

The approach to Kubernetes cluster autoscaling based on users' personal computing resources is relevant, as it allows optimizing the utilization of existing devices and reducing server hardware costs amid growing computational power demands. Currently, existing solutions are primarily designed for cloud environments and static clusters, including Kubernetes Autoscaler, Cluster API, metal3-io, and other node management automation tools. However, these solutions have certain drawbacks, such as a high dependence on cloud providers, limited flexibility in integrating heterogeneous resources, and complexity in managing short-lived computing agents.

This work focuses on developing an approach that enables automatic scaling of Kubernetes clusters by leveraging users' personal devices, utilizing Cluster API and metal3-io capabilities for node registration and lifecycle management. The efficiency of the proposed solution has been experimentally validated through the deployment of a prototype, demonstrating successful scaling from a single worker node to multiple nodes without significant failures. This confirms the potential for real-world implementation of the proposed approach.

Сучасні телекомунікаційні сервіси та застосунки часто працюють у середовищі контейнерів Kubernetes, що став де-факто стандартом для оркестрації контейнерів. Важливою перевагою Kubernetes є здатність масштабувати застосунки та інфраструктуру під змінне навантаження (еластичність). Горизонтальне масштабування виконується як на рівні контейнерів (подів), так і на рівні вузлів кластера. Для автоматизації масштабування кластерів у Kubernetes використовується компонент Cluster Autoscaler – інструмент, що автоматично змінює кількість вузлів у кластері залежно від поточних потреб у ресурсах. Зокрема, коли ресурсів не вистачає для запуску нових контейнерів (подів), Cluster Autoscaler знаходить відповідну групу вузлів і додає новий вузол; якщо ж деякі вузли тривалий час недовантажені, він може видалити зайві вузли, оптимізуючи витрати ресурсів. Однак типова реалізація автомасштабування кластерів розрахована передусім на інтеграцію з хмарними провайдерами. Cluster Autoscaler взаємодіє з API хмарного середовища для створення або видалення віртуальних машин, які виконують роль вузлів. Подібна схема добре працює в публічних або приватних хмарах, де доступні ресурси можуть бути швидко виділені через API. Натомість у середовищі без хмарного провайдера (наприклад, на власному апаратному забезпеченні, on-premises або на периферійних пристроях) постає проблема: як автоматично додавати вузли кластера на фізичному обладнанні? У випадку bare-metal (фізичних серверів) відсутній універсальний хмарний

API для створення нового вузла, тому необхідне альтернативне рішення для інтеграції з Kubernetes. З іншого боку, у багатьох організаціях та спільнотах є невикористані обчислювальні ресурси – персональні комп'ютери користувачів, робочі станції, локальні сервери, які простоюють або використовуються не на повну потужність. Виникає ідея залучити ці ресурси до спільної групи для обчислень. Концепція волонтерських обчислень показала, що пристрої користувачів можуть успішно виконувати наукові та інші завдання, об'єднуючись у розподілені обчислювальні мережі (наприклад, проєкт BOINC використовує потужності персональних комп'ютерів добровольців). Запропонований у цій статті підхід поєднує ідею використання зовнішніх (користувацьких) ресурсів із механізмами автомасштабування Kubernetes. Метою є створення гібридної інфраструктури, де кластер Kubernetes за потреби автоматично розширюється за рахунок вузлів, наданих користувачами, без залучення традиційних хмарних ресурсів. У роботі використано сучасні інструменти автоматизації керування кластером – Cluster API та суміжні проєкти. Cluster API – це проєкт спільноти Kubernetes, що забезпечує декларативне керування життєвим циклом кластерів (створення, масштабування, оновлення) за допомогою Kubernetes API. Одним із інфраструктурних провайдерів для Cluster API є Metal³ – набір засобів для керування фізичною (bare-metal) інфраструктурою з використанням Kubernetes. Metal³ інтегрується з Cluster API, дозволяючи йому виступати інструментом для створення вузлів на реальних машинах. У даній роботі Cluster API та Metal³ використовуються для автоматизованого приєднання/від'єднання фізичних хостів (серверів) до кластеру Kubernetes. Персональні комп'ютери користувачів розглядаються як такі «фізичні хости», що можуть динамічно ставати частиною спільного кластера. Запропонований підхід полягає в тому, що кластер Kubernetes може автоматично залучати додаткові вузли із зовнішньої групи обчислювальних ресурсів, які надаються користувачами. На відміну від стандартного сценарію, де нові вузли – це віртуальні машини у хмарі, тут нові вузли – це фізичні машини (або віртуальні машини на локальному обладнанні), що знаходяться поза початковим кластером. Кожен такий вузол належить окремому користувачу або організації та зазвичай не є частиною кластера постійно. Система повинна мати змогу реєструвати доступні вузли, додавати їх до кластера при зростанні навантаження та видаляти (вивільняти) коли потреба в додаткових ресурсах зникає. Рішення будується на архітектурі з використанням Cluster API. Передбачається наявність керувального кластеру (management Cluster), який виконує роль "контролера" для основного робочого кластеру (workload Cluster). У нашому випадку ці ролі можуть бути об'єднані: наприклад, один кластер може одночасно запускати робочі навантаження та містити контролери Cluster API (конфігурація кластера, в якій робочі навантаження та компоненти керування кластером працюють одночасно на одному кластері). Контролери Cluster API оперують спеціальними ресурсами Kubernetes для опису інфраструктури: Cluster, Machine, MachineSet, MachineDeployment тощо. З їх допомогою визначається склад кластера (включно з кількістю вузлів) у декларативний спосіб. Для інтеграції фізичних машин користувачів використано інфраструктурний провайдер Metal³. Проєкт Metal³ надає компонент Bare Metal Operator (BMO) (див. рис. 1), який керує об'єктами типу BareMetalHost – вони представляють собою доступні фізичні вузли з інформацією про спосіб доступу для їхнього ввімкнення та розгортання (через BMC, IPMI тощо).

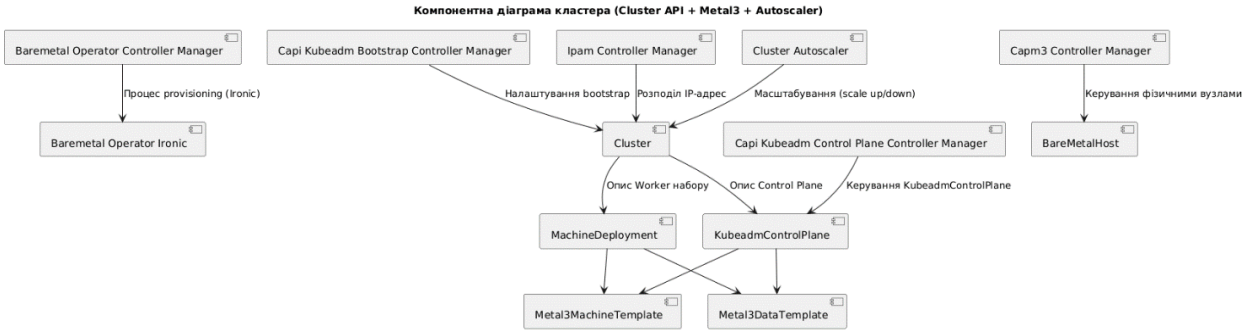


Рис. 1. Компонента діаграма кластеру.

Перед початком масштабування адміністратор реєструє персональні машини користувачів у системі як об’єкти BareMetalHost (наприклад, через додавання їх MAC-адрес, IP для управління та облікових даних доступу до їх BMC). Таким чином формується група потенційних вузлів, які готові до приєднання. Альтернативно, якщо безпосереднього доступу для автоматичного розгортання ОС на вузлі немає, може застосовуватися підхід агентського типу: на машині користувача заздалегідь встановлено необхідне програмне забезпечення (середовище виконання контейнерів, наприклад, containerd або CRI-O, що відповідають за запуск та керування контейнерами), і вона реєструється як готовий хост у кластері управління (аналогічно концепції Bring Your Own Host, BYOH). У даній роботі у реалізації зроблено акцент на використанні Metal³ та Bare Metal Operator для повної автоматизації процесу додавання вузла. Коли навантаження на кластері зростає (наприклад, з’являються нові поди, які не були розподілені планувальником Kubernetes (scheduler), тобто не можуть бути розміщені через нестачу ресурсів на існуючих вузлах), спрацьовує Cluster Autoscaler. Він працює як окремий компонент у кластері і постійно відслідковує невідпрацьовані запити на ресурси. У даній роботі Cluster Autoscaler налаштований у режим роботи, в якому замість API хмарного провайдера використовується інтерфейс прикладного програмування Cluster API для управління ресурсами (прапор --cloud-provider=Clusterapi при запуску). У такій конфігурації при необхідності масштабування Cluster Autoscaler не звертається до зовнішнього провайдера напряму, а створює новий об’єкт Machine (або збільшує репліку MachineDeployment) через API Kubernetes. Контролер Cluster API виявляє, що потрібен новий вузол, і ініціює процес його створення за допомогою провайдера Metal³. На стороні Metal³ Bare Metal Operator шукає вільний зареєстрований BareMetalHost, щоб призначити його новому Machine. Вибраний хост автоматично переходить у процес підготовки: через інтеграцію з OpenStack Ironic йому завантажується образ операційної системи і виконується конфігурування Kubernetes-вузла (наприклад, через cloud-init запуск kubeadm join). Після завершення цього процесу новий вузол підключається до кластеру Kubernetes (відображається в списку kubectl get nodes) і стає готовим для розміщення обчислювальних завдань, реалізованих у вигляді подів Kubernetes (див. рис. 2).

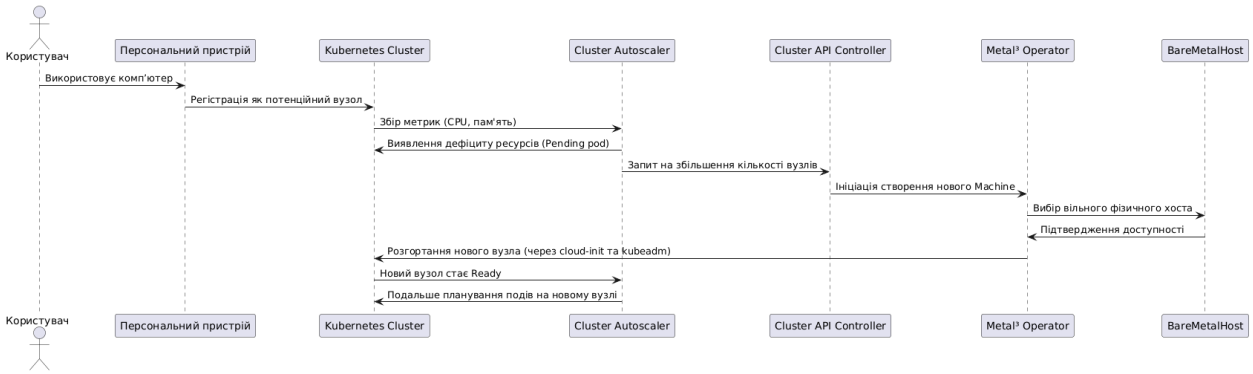


Рис. 2. Схема процесу реєстрації робочих вузлів.

Таким чином, кластер збільшується на один вузол. Весь цикл – від детектування нестачі обчислювальних ресурсів до моменту повного підключення та готовності нового вузла виконувати навантаження – виконується автоматично. Аналогічно, у разі тривалого простою ресурсів, Cluster Autoscaler може вирішити видалити зайвий вузол: тоді через Cluster API відповідний об’єкт Machine буде видалено, що призведе до від’єднання фізичного вузла (вузол повертається до початкового стану зареєстрованого об'єкта BareMetalHost (стану готовності для наступного підключення). Варто зазначити, що використання Metal³ у зв’язці з Cluster API фактично надає засоби Kubernetes для управління апаратними вузлами як об’єктами кластеру. Такий підхід узгоджується з концепцією Kubernetes-native infrastructure, коли інфраструктура (сервери) управляється так само, як і застосунки, через декларативні API. У даній роботі це дозволило досягти мети – автоматизувати залучення персональних машин.

У рамках даної роботи розгорнуто експериментальну інфраструктуру, реалізовано експериментальний сценарій із залученням персональних обчислювальних ресурсів користувачів, що емулюються за допомогою віртуальних машин. Використано кластер Kubernetes версії 1.30, у якому встановлено контролери Cluster API (версія v1beta1) та провайдер Metal³. Було зареєстровано декілька (2 шт.) віртуальних BareMetalHost як доступних вузлів – вони грали роль "персональних комп’ютерів" в експерименті. Кожному хосту призначено параметри BMC (емуляція через virtual BMC) та підготовлено завантажувальний образ з Kubernetes (CoreOS-based). Cluster Autoscaler розгорнуто як под (контейнер) у цьому ж кластері і налаштовано на автоматичну ідентифікацію групи вузлів (об'єктів Machine), придатних для масштабування. Параметри (або межі) масштабування кластера, що визначають мінімальну та максимальну допустиму кількість вузлів встановлені: мінімальна кількість вузлів = 1, максимальна = 2 (1 початковий + 1 додатковий). Моніторинг стану кластера здійснювався засобами Kubernetes (метрики використання CPU/RAM) та логів Cluster Autoscaler. На рис. 3 представлено етапи процесу автоматичної реєстрації нового вузла до Kubernetes-кластера за допомогою Metal³ та Cluster API:

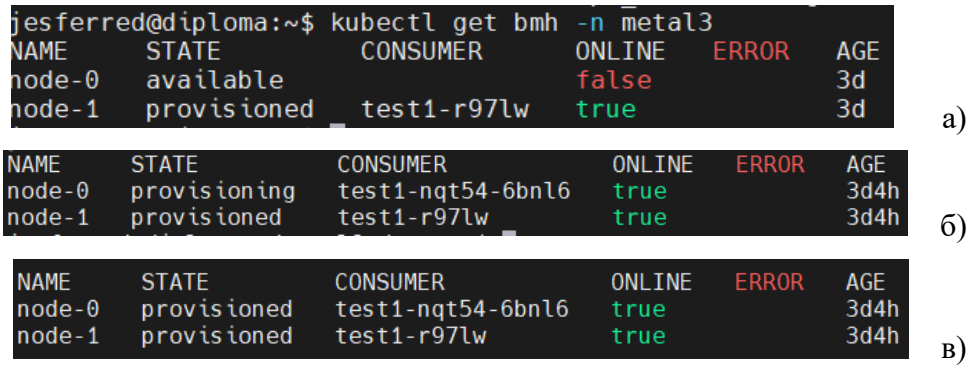


Рис. 3. Процес реєстрації нового вузла
а) Вузол готовий до приєднання (available) – це стан, коли вузол (BareMetalHost) зареєстрований у системі, але ще не приєднаний до робочого кластера;
б) Вузол приєднується (provisioning) – виконується автоматичний процес конфігурації, встановлення ОС, запуск необхідних сервісів, вузол перебуває у процесі інтеграції з кластером;
в) Вузол приєднаний (provisioned) – вузол повністю інтегровано в кластер, він готовий приймати навантаження та запускати поди Kubernetes.

Висновки. У даній роботі представлено новий підхід до автомасштабування кластерів Kubernetes, який базується на залученні персональних обчислювальних ресурсів користувачів. Сформовано архітектуру рішення з використанням Cluster API та Metal³, що дозволяє автоматично додавати/видаляти вузли кластера на основі зовнішніх (нехмарних) ресурсів. Реалізовано прототип та проведено експерименти, які підтвердили ефективність підходу: кластер успішно масштабується від 1 до 2 вузлів і назад без ручного втручання, забезпечуючи необхідні ресурси під час пікового навантаження.

Отримані результати свідчать, що спільне використання Kubernetes з інструментами керування інфраструктурою (Cluster API, Bare Metal Operator) відкриває можливість створення динамічних гібридних кластерів, де частина ресурсів надається добровільно учасниками або використовується за принципом спільноти.

Література

1. Смаглюк В.О., Алєксєєв М.О. Керування клієнтськими обчислювальними ресурсами з динамічним життєвим циклом у корпоративній мережі. Інфокомунікаційні та комп'ютерні технології, 2022, №2(04), с. 134–142.
2. Kubernetes Cluster Autoscaler – Офіційна документація. Kubernetes Documentation. – URL: https://Kubernetes.io/docs/concepts/Cluster-administration/node-autoscaling/
3. Metal³ Project – Metal3.io. Офіційний вебсайт проекту Metal³. – URL: https://metal3.io/
4. Cluster API Provider BYOH (Bring Your Own Host). GitHub Repository – vmware-tanzu/Cluster-api-provider-bringyourownhost. – URL: https://github.com/vmware-tanzu/Cluster-api-provider-bringyourownhost/
5. CNCF Blog – Kubernetes Cluster API reaches production readiness with v1.0. Cloud Native Computing Foundation, 6 Oct 2021. – URL: https://www.cncf.io/blog/2021/10/06/Kubernetes-Cluster-api-reaches-production-readiness-with-version-1-0/
6. BOINC: A Platform for Volunteer Computing. Berkeley Open Infrastructure for Network Computing (BOINC) Overview. – URL: https://boinc.berkeley.edu/

УДК 621.37

МОДЕЛЮВАННЯ РІВНЯ ПРИЙНЯТОГО СИГНАЛУ ЗАСОБОМ РАДІОМОНІТОРИНГУ НА БЕЗПІЛОТНОМУ ЛІТАЛЬНОМУ АПАРАТІ

Бугайов М.В.
Житомирський військовий інститут імені С.П. Корольова, Україна
E-mail: karunen@ukr.net

MODELING THE RECEIVED SIGNAL STRENGTH BY UAV-BASED RADIO MONITORING DEVICE

UAV-based spectrum sensing provides a number of significant advantages including improved energy availability of radio emitters. Modeling the received signal strength, taking into account terrain and the location of obstacles, will allow to estimate the location of radio emitters.

Стрімкий розвиток безпілотних літальних апаратів (БпЛА) стимулює їх впровадження для вирішення найрізноманітніших завдань, зокрема ведення радіомоніторингу (РМ) [1-4]. Для виявлення та оцінювання параметрів невідомих джерел радіовипромінювання (ДРВ) необхідно розробити математичну модель сигналу, яка буде враховувати ефекти поширення радіохвиль для рухомого засобу РМ.

Засіб РМ будемо описувати такими параметрами: смуга пропускання та чутливість приймача, швидкість сканування, форма діаграми спрямованості (ДС) антени, швидкість та траєкторія руху БпЛА. До основних параметрів ДРВ будемо відносити: координати ДРВ, потужність випромінювання, частотно-часові параметри сигналів, форму та орієнтацію в просторі ДС антени, швидкість руху ДРВ. Канал поширення радіохвиль будемо характеризувати ступенем прояву ефектів відбиття, дифракції, розсіювання та інтерференції в різних діапазонах частот та швидкістю їх зміни при переміщенні БпЛА.

Для ультракороткохвильового діапазону основними факторами, що впливають на рівень прийнятого сигналу є втрати на поширення, затінення, завмирання та неізотропність ДС антен ДРВ та БпЛА. Доплерівським зсувом частоти в даних умовах можна знехтувати.

Для оцінювання потужності прийнятого засобом РМ сигналу з частотою f в момент часу t будемо використовувати модель, що враховує крім імпульсної характеристики каналу поширення неізотропність ДС антени ДРВ та РМ:

$$P_r(t,f)=P_t\underbrace{\left(\frac{\mathrm{c}}{4\pi r(t)f}\right)^{\nu(t)}}_{1}\underbrace{\frac{1}{\chi(t,f)}}_{2}\underbrace{m(t,f)}_{3}\underbrace{G_r\left(\theta(t),\gamma(t)\right)G_t\left(\theta(t),\gamma(t)\right)}_{4}. \quad (1)$$

де P_t – потужність випромінювання ДРВ;

c – швидкість поширення радіосигналів;

$r(t)$ – відстань між ДРВ та засобом РМ;

$\nu(t)$ – коефіцієнт втрат на поширення радіохвиль, який залежить від типу навколишнього середовища і знаходиться в межах 2-6;

$\chi(t, f)$ – випадкова величина затінення;

$m(t, f)$ – складова багатопроменевого поширення;

$G_r(\theta(t), \gamma(t))$ – коефіцієнт підсилення антени ДРВ в напрямку на антену РМ;

$G_t(\theta(t), \gamma(t))$ – коефіцієнт підсилення антени РМ в напрямку на антену ДРВ;

$\theta(t)$ – азимут;

$\gamma(t)$ – кут місця.

Математичну модель потужності прийнятого сигналу (1) можна розглядати як добуток чотирьох функцій часу, які змінюються з різною швидкістю.

Повільна (1), що визначається зміною дальності між передавальною і приймальною антенами. При цьому значення коефіцієнта втрат на поширення радіохвиль $\nu(t)$ змінюється в часі за рахунок переміщення засобу РМ через різні середовища. Відстань між ДРВ та БпЛА визначається траєкторією його польоту.

Швидка (2), що визначається ефектом затінення і описується кореляційною відстанню затінення, яка залежить від розміру перешкоди і складає від кількох до десятків метрів [5]. Під час зміни відстані між ДРВ та засобом РМ дана просторова мінливість змінюється на часову і масштабується швидкістю переміщення БпЛА.

Дуже швидка (3), що визначається багатопроменевим поширенням. Для статистичного опису радіоканалу із рухомим приймачем використовують розподіл Релея (Райса). Даному розподілу підпорядковуються значення обвідної прийнятого сигналу в каналі без частотно-селективних завмирань, тобто обвідна окремої багатопроменевої складової.

Швидкість відносного переміщення засобу РМ та ДРВ визначає наскільки швидко змінюється рівень прийнятого сигналу. Часовий інтервал між мінімумами (максимумами) рівня завмирань складає наближено півперіоду частоти Допплера, що відповідає переміщенню приймача (передавача) на половину довжини хвилі несучої частоти сигналу.

Складова впливу неізотропності ДС антен засобу РМ та ДРВ (4) може проявлятися на усі інші складові в залежності від їх форми та параметрів руху БпЛА. Припускаємо, що ДС антени ДРВ не змінюється в часі. Тоді даний фактор є детермінованим проте невідомим. Ступінь впливу даного чинника на рівень прийнятого сигналу визначається формою ДС та її орієнтацією відносно засобу РМ на БпЛА.

На рис. 1 наведено схему переміщення БпЛА на площині відносно одного ДРВ та пояснення втрат сигналу на різних ділянках траєкторії польоту. Якщо відсутнє затінення, то будемо вважати, що є умови прямої видимості і завмирання підпорядковані розподілу Райса, які мають меншу глибину порівняно із завмираннями Релея. Також припускаємо, що антена засобу РМ є неспрямованою.

При знаходженні БпЛА із засобом РМ в положенні 1 є умови прямої видимості, він знаходиться найближче до ДРВ та в максимумі ДС його

антени. Тому рівень прийнятого сигналу буде високим із незначними пульсаціями, що спричинені завмираннями Райса.

У другому положенні відсутня пряма видимість через затінення, що спричинить логарифміно-нормальне затухання та завмирання Релея. Засіб РМ знаходиться в максимумі ДС. Тому на прийнятий сигнал впливатимуть швидкі та дуже швидкі глибокі завмирання.

У третьому положенні між ДРВ та БпЛА є пряма видимість і засіб РМ знаходиться в мінімумі ДС антени ДРВ. Тому в даній точці простору рівень прийнятого сигналу буде невисоким із неглибокими завмираннями Райса.

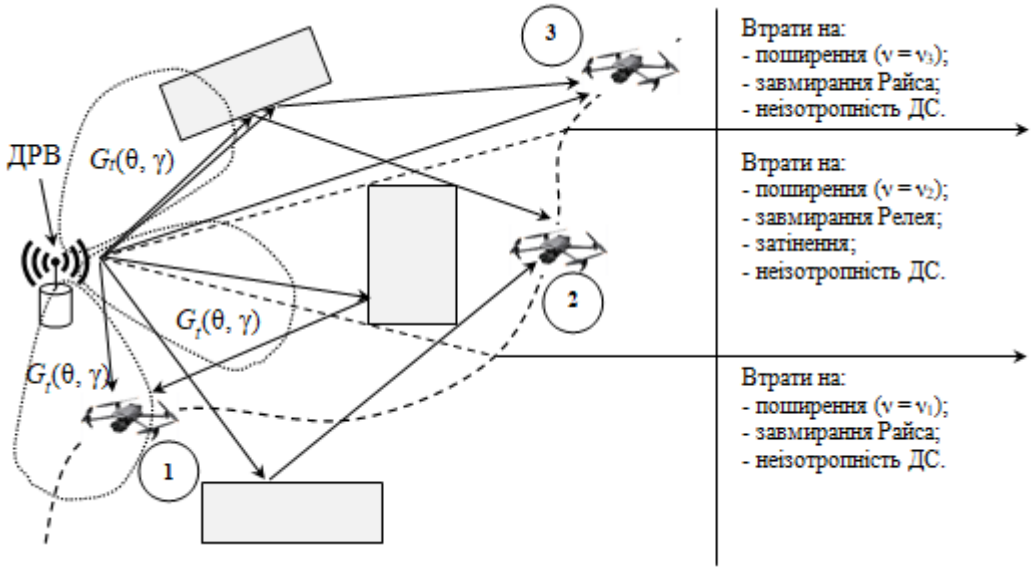


Рис. 1/ Схема переміщення БпЛА відносно одного ДРВ/

Якщо середня потужність випромінювання ДРВ P_t не змінюється в часі, то оброблення виміряних значень потужності прийнятого сигналу засобом РМ з урахуванням рельєфу місцевості та розміщення інших об'єктів (будівель, дерев) на маршруті польоту БпЛА дозволить наближено оцінити розміщення ДРВ за умови його незмінного положення. Збільшення кількості прольотів за різними маршрутами дозволить підвищити точність оцінювання координат ДРВ. Самі маршрути польоту БпЛА також підлягають оптимізації з урахуванням апріорних даних щодо можливого положення ДРВ та карти місцевості.

Література

1. Gul N., Kim S. M, Ali J, Kim J. UAV aided virtual cooperative spectrum sensing for cognitive radio networks. PLoS One, 2023 Vol. 5, 36 p. doi: 10.1371/journal.pone.0291077.
2. Shen F., Ding G., Wang Z., Wu Q. UAV-Based 3D Spectrum Sensing in Spectrum-Heterogeneous Networks. IEEE Transactions on Vehicular Technology, 2019, vol. 68, no. 6, pp. 5711-5722. doi: 10.1109/TVT.2019.2909167
3. Jasim M. A. et al. A Survey on Spectrum Management for Unmanned Aerial Vehicles (UAVs). IEEE Access, 2022, vol. 10, pp. 11443-11499. doi: 10.1109/ACCESS.2021.3138048.
4. Du X. et al. UAV-Assisted Three-Dimensional Spectrum Mapping Driven by Spectrum Data and Channel Model. Symmetry, 2021, Vol. 13(12). doi: 10.3390/sym13122308.
5. Karagiannis G. A., Panagopoulos A. D. Dynamic Lognormal Shadowing Framework for the Performance Evaluation of Next Generation Cellular Systems. Future Internet, MDPI, 2019, vol. 11(5), pp. 1-18. doi:10.3390/fi11050106.

УДК 621.382

ПЕРЕВАГИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ ДЛЯ ТРЕНУВАННЯ САПЕРІВ

[1]Рибачик І.К., [2]Козленко О.В., [3]Булигіна Л.В.
[1]*Політехнійний ліцей НТУУ «КПІ» м.Києва,*
[2,3]*НТУУ «Київський політехнічний інститут імені Ігоря Сікорського», Україна*
E-mail: ilya.ribachik@gmail.com, ovkozlenko@gmail.com, lus0561@gmail.com

ADVANTAGES OF USING VIRTUAL REALITY TECHNOLOGIES FOR DEMINER TRAINING

The use of virtual reality technologies in training systems for sappers can significantly improve the quality of training of military personnel and reduce risks to their lives. The article examines the prospects and advantages of using virtual reality technologies for demining.

Питання розмінування у сучасному світі залишається актуальним і важливим завданням, оскільки нерозірвані міни та вибухові пристрої становлять серйозну загрозу життю людей в різних країнах світу. В Україні це питання стоїть гостро і є однією з нагальних потреб суспільства. Хоча в світі вже розробляється обладнання, яке використовується під час процесу розмінування, застосування лише таких машин недостатньо. Розроблені технології не здатні працювати на певних типах ґрунту, а також на гірських ландшафтах, пагорбах або вузьких ділянках. Тому ручне розмінування залишається ключовим напрямком гуманітарного розмінування**.** Крім того, ручне розмінування вважається більш точним та більш екологічним, ніж механічне розмінування. Цей процес вимагає уваги до деталей та великої обережності, щоб уникнути травм та смертей. У цьому контексті розвиток сучасних технологій, таких як віртуальна реальність, може значно полегшити процес навчання розмінуванню та зменшити ризики для людей, які займаються цією діяльністю. Це важливо й тому, що в Україні відчувається дефіцит спеціалістів з розмінування.

Вивченням проблем розмінування території, розробкою шляхів модернізації протимінної безпеки в Україні, дослідженням способів вдосконалення ефективних вибухонебезпечних засобів та механізмів займалися такі вчені та експерти, як Б. Ворович, М. Бутенко, О. Ковбаса, О. Передрій. Способи розмінування місцевості та фактори, які впливають на виконання завдань з розмінування, розглядали науковці Національної академії сухопутних військ імені гетьмана Петра Сагайдачного Р.Л.Колос та Ю.О.Фтемов [2]. Шляхи щодо вирішення питань розмінування території України з акцентом на підвищення ефективності розмінування в умовах збройного конфлікту на базі Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського досліджував Б. О. Ворович [1]. Перспективи використання VR-симуляторів у військовій сфері (для підготовки до бойових дій, навігації, рятувальних операцій) описували А.Г. Ткачук та О.О.

Добржанський [3].

За останні кілька років віртуальна реальність стала надзвичайно популярною технологією у галузі навчання, в тому числі і військового навчання. Імітації реальних подій дають змогу військовим повністю зануритися у віртуальне середовище. Вони можуть використовувати VR-симулятори для підвищення своєї ефективності та зниження ризику травмування під час навчання [3].

Впровадження технологій VR в навчальний процес дозволить майбутнім саперам віртуально працювати з різними типами вибухонебезпечних об'єктів, навчаючи їх реагувати на них швидко і ефективно. Крім того, симулятори дозволяють підвищити рівень реалізму тренувань і зменшити ризик для життя сапера.

Використання можливостей віртуальної реальності для навчання саперів має низку переваг.

– По-перше, використання даної технології дозволяє створити реалістичне віртуальне середовище, яке може імітувати різні сценарії небезпечних ситуацій, з якими можуть стикатися сапери. Це дає їм можливість навчатися в безпечній обстановці, максимально наближеній до реальності.

– По-друге, віртуальна реальність дозволяє саперам отримати практичний досвід в будь-який час і в необхідній кількості, таким чином розвиваючи кінестетичну пам'ять.

– По-третє, використання віртуальної реальності дозволяє інструкторам контролювати та спостерігати за процесом навчання саперів, а також збирати дані про їхні дії та реакції, що може бути корисним для подальшого вдосконалення систем тренувань.

Навчання може відбуватися будь-де і в будь-який час, є можливість додавати сценарії, змінювати ландшафт та створювати нові умови для тренування.

Тренувальна система для демінерів з VR може бути успішно впроваджена в навчальних закладах на уроках Захисту України та в організаціях, що займаються підготовкою рятувальників, розширюючи можливості таких курсів. Застосування технологій віртуальної реальності в тренувальних системах для саперів може значно поліпшити якість навчання, підготовку військових та зменшити ризики для їхнього життя.

Література

1. Ворович Б. О. Шляхи вирішення проблемних питань розмінування території України / Б. О. Ворович // Збірник наукових праць центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. – 2020. – № 2. – С. 143–149. – [Електронний ресурс]. – Режим доступу: https://doi.org/10.33099/2304-2745/2020-2-69/143-149 (дата звернення: 2.09.2024).
2. Організація виконання робіт з розмінування місцевості від вибухонебезпечних предметів / Р. Л. Колос, Ю. О. Фтемов // Військово-технічний збірник. - 2017. - № 17. - С. 53-60. - [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/UJRN/vtzb_2017_17_12 (дата звернення 4.12.2024).
3. Ткачук А.Г., Добржанський О.О. Застосування VR-технологій у військовій робототехніці. - [Електронний ресурс]. – Режим доступу: https://conf.ztu.edu.ua/wp-content/uploads/2023/06/192.pdf (дата звернення 18.11.2024).

UDC 004.77:004.78:004.92

ARCHITECTURE OF AUDIOVISUAL SYSTEM IN INTERNET OF THINGS

Kovalchuk S.S., Kurdecha V.V.
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: serghkoval1337@ukr.net

АРХІТЕКТУРА АУДІОВІЗУАЛЬНИХ СИСТЕМ В ІНТЕРНЕТІ РЕЧЕЙ

У статті наводиться огляд проблематики в питанні аудіовізуальних систем у системах Інтернету речей в контексті безпеки, енергоживлення, сумісності із наведенням технічних рішень.

A review of issues in the issue of audiovisual systems in Internet of Things (IoT) systems in the context of security, power supply and interoperability.

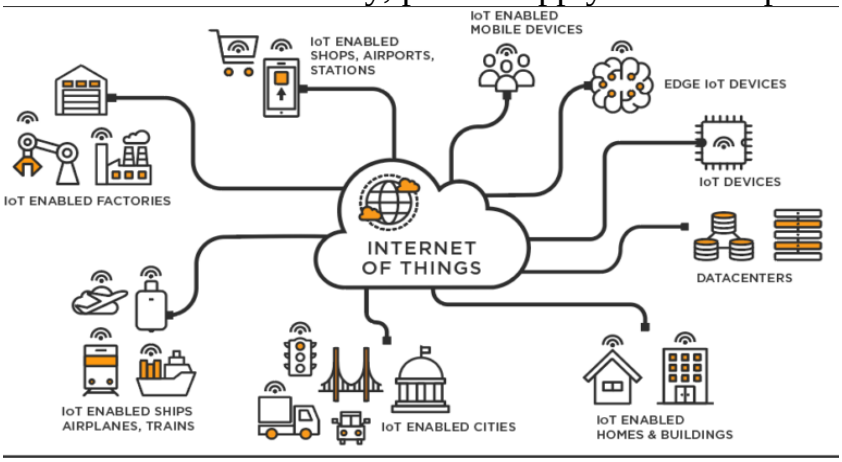


Fig. 1. Possibilities of IoT.

The Internet of Things is a key element in shaping modern frameworks in various areas of life, contributing to improved efficiency, reduced costs and enhanced security [1]. The audiovisual framework in the Internet of Things encompasses a range of tools, including video recorders, sound modules, displays, detectors, and applications for data manipulation and transmission. Even in the field of audiovisual technologies with significant potential, several issues hinder the optimal application of audiovisual systems in the Internet of Things [2]: compatibility and integration; security; high network load; energy efficiency [3].

New technologies are actively being introduced to tackle these challenges. AI automates system configuration and optimizes audio and video signal processing [4]. The implementation of 5G and fiber-optic networks minimizes data transmission delays, which is especially vital for streaming services and interactive platforms. Blockchain technology enhances intellectual property security, while energy-efficient algorithms help reduce resource consumption, improving overall system efficiency. Additionally, these systems are built based on specific models.

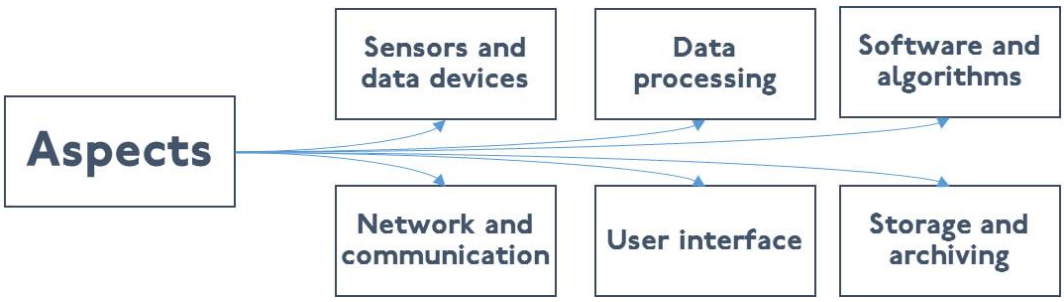


Fig. 2. Aspects of audiovisual systems (AVS).

The main models of audiovisual systems include systems with video and audio integration, where simultaneous transmission of image and sound enables full two-way communication, commonly used in video conferencing and surveillance. Another category consists of systems with sensors and interactive devices, often found in IoT applications such as security systems that utilize cameras and speakers to monitor activity and notify users. Additionally, audiovisual technologies play a key role in multimedia entertainment and advertising, supporting interactive exhibitions, marketing campaigns, and large-scale media events.

Despite technological obstacles, video and sound systems on the Internet have high potential for improvement. The generation and synchronization of images and audio through AI helps automate tasks in various industries, such as journalism, healthcare, or smart city settings [5].

Fig. 3. Architecture levels AVS in IoT.

Such innovations can contribute to more engaging and personalized experiences for users, for example, flexible multimedia systems that respond to the user's emotions or physical functions through specialized devices.

Video and audio equipment are a key function of Internet connectivity today, and they grow more useful every year. Identifying technical and security obstacles will allow these networks to achieve unprecedented achievements, improving the lifestyle of global citizens.

Modeling an audiovisual system involves two main approaches: simulation modeling and full-scale (physical) modeling. Simulation modeling relies on mathematical or software models to predict system behavior, assess noise impact, and evaluate sound and image transmission quality without creating physical prototypes. Tools like MATLAB, Simulink, and Python libraries (SciPy, OpenCV) enable virtual simulations of signal processing and distortion correction, allowing for early-stage optimization and error prevention.

Full-scale modeling, on the other hand, involves building a real prototype and testing it in actual conditions, considering factors like lighting, acoustics, and external interference. This approach ensures accurate evaluation of cameras, microphones, and displays, identifying real-world challenges such as signal delays or noise. While simulation provides a cost-effective way to refine system performance, full-scale testing validates its practical reliability. Combining both methods enhances the accuracy and efficiency of audiovisual systems.

The integration of audiovisual systems into the Internet of Things (IoT) offers great potential but also presents challenges related to security, power efficiency, and interoperability. Advances in AI, 5G, blockchain, and energy-efficient algorithms are helping to address these issues by optimizing data transmission, enhancing security, and reducing resource consumption. Additionally, the combination of simulation and full-scale modeling ensures both theoretical optimization and real-world validation of system performance. As these technologies continue to evolve, overcoming technical barriers will lead to more interactive, efficient, and intelligent audiovisual solutions, ultimately enhancing user experiences and fostering smarter, more connected environments.

References

1. *How is IoT impacting the audio-visual industry (Reader Forum).* RCR Wireless, 2024. Available at: https://www.rcrwireless.com/20240628/internet-of-things-4/how-is-iot-impacting-the-audio-visual-industry-reader-forum.
2. M. Tsukada, K. Ogawa, M. Ikeda, T. Sone, K. Niwa, and S. Saito, "Software Defined Media: Virtualization of Audio-Visual Services," *Proceedings of the 2017 IEEE International Conference on Communications (ICC)*, 21-25 May 2017, IEEE. DOI: 10.1109/ICC.2017.7996610. Available at: https://ieeexplore.ieee.org/document/7996610.
3. F. Renna, J. Doyle, V. Giotsas, and Y. Andreopoulos, "Query Processing for the Internet-of-Things: Coupling of Device Energy Consumption and Cloud Infrastructure Billing," *Proceedings of the 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 04-08 April 2016, Berlin, Germany, IEEE. DOI: 10.1109/IoTDI.2015.37. Available at: https://ieeexplore.ieee.org/document/7471353.
4. D. Jadhav, S. Agrawal, S. Jagdale, P. Salunkhe, and R. Salunkhe, "AI-Driven Text-to-Multimedia Content Generation: Enhancing Modern Content Creation," *Proceedings of the 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, 03-05 October 2024, IEEE. DOI: 10.1109/I-SMAC61858.2024.10714771. Available at: https://ieeexplore.ieee.org/document/10714771.
5. D. M. Harris, & S. L. Harris, *Цифровая схемотехника и архитектура компьютера (2-е изд.)*. Питер, 2013. ISBN 978-0-12-394424-5.
6. 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.
7. L. Globa, V. Kurdecha, I. Ishchenko and A. Zakharchuk, "An approach to the Internet of Things system with nomadic units developing," 2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), Lviv, Ukraine, 2017, pp. 248-250, doi: 10.1109/CADSM.2017.7916127.
8. 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.

УДК 519.8

ПРЕДСТАВЛЕННЯ ЕВОЛЮЦІЇ ДЛЯ МОДЕЛЬНОЇ ІНТЕГРАЛЬНОЇ ГРИ ЗБЛИЖЕННЯ З ДРОБОВИМИ ІНТЕГРАЛАМИ РІМАНА-ЛІУВІЛЯ

Гетьман О.В., Руренко О.Г., Фуртат О.В.
Навчально-науковий інститут телекомунікаційних систем
НТТУ «КПІ імені Ігоря Сікорського»,
Таврійський національний університет імені В.І.Вернадського, Україна
E-mail: lgetman78@gmail.com, a.rurenko@gmail.com, furtatlena@gmail.com

REPRESENTATION OF THE EVOLUTION FOR THE MODEL INTEGRAL GAME OF APPROACH WITH RIEMANN-LIOUVILLE FRACTIONAL INTEGRALS

In this paper, we obtain a representation of the evolution for a model integral game with fractional Riemann-Liouville integrals. The representation of the evolution of the game is expressed in terms of the generalized Mittag-Leffler matrix function.

В роботі отримано представлення еволюції для модельної інтегральної гри зближення з дробовими інтегралами Рімана-Ліувіля. Представлення еволюції гри виражається в термінах узагальненої матричної функції Міттаг-Леффлера.

Застосування методів дробового числення в теорії керування викликає значний інтерес у дослідників, оскільки на відміну від класичних диференціальних моделей таких процесів дозволяє апроксимувати динамічні процеси з пам’яттю і вивчати їх спадкові особливості [1, 2].

В роботі розглянута модельна ігрова задача зближення для системи інтегральних рівнянь з дробовими інтегралами Рімана-Ліувілля. Подібні ігрові задачі були визначені в [3], де показаний зв’язок таких ігор з більш широкими класами ігрових задач зближення для динамічних систем з вольтерівською еволюцією.

Для функції $f(x)$, визначеної на $(0,\infty)$, дробовий інтеграл Рімана-Ліувілля порядку β представляється як

$$J_t^{\beta}\left(f(t)\right) = \frac{1}{\Gamma(\beta)}\int_0^t (t-\tau)^{\beta-1} f(\tau)d\tau, \beta > 0, \qquad (1)$$

при чому $J_t^{\beta} f(t) = f(t)$ для $\beta = 0$, де $\Gamma(\ \ )$ - гамма-функція Ейлера. Рівняння (1) може бути представнено у вигляді згортки функцій

$$J_t^{\beta} f(t) = \frac{t^{\beta-1}}{\Gamma(\beta)} * f(t). \qquad (2)$$

Нехай в n-мірному евклідовому просторі R^n заданий керований процес, динаміка якого описується системою інтегральних рівнянь

$$z(t) = z_0 + \frac{A}{\Gamma(\delta)}\int_0^t (t-\tau)^{\alpha-1} z(\tau)d\tau + \frac{B}{\Gamma(\beta)}\int_0^t (t-\tau)^{\beta-1}\phi\big(u(\tau), v(\tau)\big)d\tau, \alpha > 0, \beta > 0 \quad (3)$$

тут $z(t)$- вимірна (по Лебегу) і обмежена вектор-функція, A, B - $n \times n$ квадратні матриці, $\phi(u, v), \phi: U \times V \to R^n$ - функція, яка вважається неперервною за сукупністю змінних u, v, таких, що $u \in U$, $v \in V$, де U, V- деякі компактні множини в R^n.

Окрім еволюції процесу (3), задана деяка термінальна множина M^*, яка представлена у вигляді

$$M^* = M_0 + M, \quad (4)$$

де M_0- лінійний підпростір в R^n, а M- компактна множина, така, що $M \in K(L)$, де L- ортогональне доповнення до M_0 в R^n.

Наміри першого (u) і другого (v) гравців протилежні. Перший гравець намагається вибирати керування в своєму класі керувань таким чином, щоб якнайшвидше привести траєкторію процесу (3) на термінальну множину (4), а другий — максимально відкласти момент зближення з термінальною множиною M^*.

Метою роботи є встановлення достатніх умов закінчення гри на умовах першого гравця за деякий гарантований час зближення $t < \infty$ і знаходження керувань для першого гравця в класі контркерувань.

Далі без доведення приведемо деякі властивості дробових інтегралів, які відомі в теорії дробового числення і будуть нами використані в роботі.

Властивість 1 ([2], властивість 2.5):

$$J_t^{\alpha}\left(t^{\beta-1}\right) = \frac{1}{\Gamma(\alpha)}\int_0^t (t-\tau)^{\alpha-1}\tau^{\beta-1}d\tau = \frac{\Gamma(\beta)}{\Gamma(\beta+\alpha)}t^{\beta+\alpha-1} \quad (5)$$

Властивість 2 ([2], лема 2.3):

$$J_t^{\alpha}J_t^{\beta}\left(f(t)\right) = J_t^{\alpha+\beta}\left(f(t)\right) \quad (6)$$

В роботі [3] була визначена матрична функція Міттаг-Леффлера. Представимо матричну функцію Міттаг-Леффлера у вигляді наступного матричного ряду

$$E_{\alpha,\beta}(A) = \sum_{k=0}^{\infty}\frac{A^k}{\Gamma(\alpha k + \beta)}, \alpha > 0, \beta > 0 \quad (7)$$

Для отримання представлення еволюції гри розглянемо еквівалентну до (3) систему інтегральних рівнянь

$$z(t) = z_0 + AJ_t^{\alpha}z(t) + BJ_t^{\beta}\phi(t), \alpha > 0, \beta > 0 \quad (8)$$

в якій через $F(t)$ позначимо праву частину: $F(t) = z_0 + BJ_t^{\beta}\phi(t)$. Для пошуку розв'язку системи інтегральних рівнянь (8) використаємо метод послідовних наближень (метод Пікара). Це означає, що розв'язок $z(t)$системи (8) будемо шукати у вигляді нескінченного функціонального ряду:

$$z(t) = z_0(t) + z_1(t) + z_2(t)... \tag{9}$$

Початкове наближення $z_0(t)$ нехай дорівнює $F(t)$. Тоді $z_0(t) = F(t) = z_0 + BJ_t^{\beta}\phi(t)$, а наступні наближення обчислюються за формулою:

$$z_k(t) = AJ_t^{\alpha} z_{k-1}(t), k = 1,2,... \tag{10}$$

Для $z_1(t)$ отримаємо наступний вираз:

$$z_1(t) = AJ_t^{\alpha} z_0(t) = AJ_t^{\alpha}\left(z_0 + BJ_t^{\beta}\phi(t)\right) = AJ_t^{\alpha} z_0 + A \times BJ_t^{\alpha} J_t^{\beta}\phi(t). \tag{11}$$

Розв'язок $z_1(t)$ можна переписати в більш компактному вигляді

$$z_1(t) = A\frac{t^{\alpha}}{\Gamma(\alpha+1)} z_0 + A \times BJ_t^{\alpha+\beta}\phi(t), \tag{12}$$

оскільки перший інтеграл в (11) обчислюється: $AJ_t^{\alpha} z_0 = A\frac{t^{\alpha}}{\Gamma(\alpha+1)} z_0$, а подвійні дробові інтеграли: $A \times BAJ_t^{\alpha} AJ_t^{\beta}\phi(t) = A \times BJ_t^{\alpha+\beta}\phi(t)$ спрощуються на підставі напівгрупової властивості дробових інтегралів (6) (*Властивість 2*).

Далі знайдемо наближення $z_2(t)$. Оскільки

$$z_2(t) = AJ_t^{\alpha} z_1(t) = AJ_t^{\alpha}\left(A\frac{t^{\alpha}}{\Gamma(\alpha+1)} z_0 + A \times BJ_t^{\alpha+\beta}\phi(t)\right),$$

тоді після аналогічних спрощень отримаємо:

$$z_2(t) = A^2\frac{t^{2\alpha}}{\Gamma(2\alpha+1)} z_0 + A^2 \times BJ_t^{2\alpha+\beta}\phi(t).$$

Можна показати, що для $k \geqslant 1$ справедлива рекурентна формула

$$z_k(t) = A^k \frac{t^{k\alpha}}{\Gamma(k\alpha+1)} z_0 + A^k \times B J_t^{k\alpha+\beta} \phi(t), \quad (13)$$

а відтак, розв'язок (9) можна представити у вигляді функціонального ряду

$$z(t) = z_0 + B J_t^{\beta} \phi(t) + A \frac{t^{\alpha}}{\Gamma(\alpha+1)} z_o + AB J_t^{\alpha+\beta} \phi(t) + A^2 \frac{t^{2\alpha}}{\Gamma(2\alpha+1)} z_o + A^2 B J_t^{2\alpha+\beta} \phi(t) + \ldots + A^k \frac{t^{k\alpha}}{\Gamma(k\alpha+1)} z_o + A^k B J_t^{k\alpha+\beta} \phi(t) + \ldots \quad (14)$$

Отриманий розв'язок $z(t)$ у вигляді ряду (14) при $k \to \infty$ можна переписати таким чином:

$$z(t) = \sum_{k=0}^{\infty} \frac{A^k t^{k\alpha}}{\Gamma(k\alpha+1)} z_0 + \sum_{k=0}^{\infty} \frac{A^k t^{k\alpha+\beta-1}}{\Gamma(k\alpha+\beta)} B * \phi(t). \quad (15)$$

В термінах матричної функції Міттаг-Леффлера (7) $z(t)$ виражається наступною формулою

$$z(t) = E_{\alpha,1}(At^{\alpha}) z_0 + E_{\alpha,\beta}(At^{\alpha}) t^{\beta-1} B * \phi(t), \quad (16)$$

а відтак представлення еволюції для інтегральної гри (3), (4) має вигляд:

$$z(t) = E_{\alpha,1}(At^{\alpha}) z_0 + \int_0^t E_{\alpha,\beta}\left(A(t-\tau)^{\alpha}\right)(t-\tau)^{\beta-1} B \phi\big(u(\tau), v(\tau)\big) d\tau, \alpha > 0, \beta > 0 \quad (17)$$

.

Можна показати, що отриманий розв'язок $z(t)$ у вигляді системи рівнянь (17) описує еволюцію гри для іншого класу ігрових задач, коли динаміка процесів описується дробовими похідними Капуто [2]. Такі ігрові задачі вивчалися в [5]. Таким чином встановлено зв'язок між класами ігрових задач для окремих модельних еволюційних динамічних ігор зближення.

Література

1. Monje C.A., Chen Y.Q., Vinagre B.M., Xue D, Fejiu V. Fractional Order Systems and Control - Fundamentals and Applications.
2. Kilbas A.A., Srivastava H.M., Trujillo J.J. Theory and Applications of Fractal Differential Equations. — Elsevier: Amsterdam, the Netherlands, 2006.
3. Eidelman S.D., Chikrii A.A., Rurenko A.G. Quasilinear integral games of approach // Доповіді НАН України. -1998. -7. -С.92-98.
4. Chikrii A.A. Conflict-controlled processes. — Boston-London-Dordrecht: Kluwer Academ. Pub., 1997. — 424 P.
5. Чикрий А.А., Эйдельман С.Д. Обобщенные матричные функции Миттаг-Леффлера в игровых задачах для еволюционных уравлений дробового порядка // Кибернетика и системный анализ. -2000. -3. -С.3-31.

УДК 621.382

АНАЛІТИЧНИЙ ОГЛЯД ПРИКЛАДІВ ЗАСТОСУВАННЯ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

Руренко О.Г., Гетьман О.В., Фуртат С.О.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна;
Таврійський національний університет імені В.І.Вернадського, Україна
E-mail: a.rurenko@gmail.com, furtatsergij@gmail.com,

ANALYTICAL REVIEW OF WIRELESS APPLICATION EXAMPLES SENSOR NETWORKS

Recent advances in network and material science technologies are leading to widespread deployment of large-scale wireless sensor networks (Wireless Sensor Networks, WSS).

Together with wireless sensor networks of the new generation, these technologies were very different from those developed only 5...10 years ago. Today, modern BSMs have lower deployment and maintenance costs, work longer and are more reliable. They are used in our homes, workplaces and beyond, providing new sources of control and information and bringing convenience to our personal and professional lives.

Основними перевагами безпроводових мереж, в порівнянні з традиційними кабельними, являються простота розгортання і підключення до них нових користувачів, а також мобільність користувачів в зоні її дії.

Охорона і моніторинг довкілля представляють одну з найбільш затребуваних сфер застосування БСМ. В основному метою створення таких мереж є своєчасне виявлення і локалізація лісових пожеж. Велике число первинних перетворювачів, забезпечених засобом передачі даних, розкидається з повітря на певній території лісового масиву, що дозволяє виявляти і локалізувати лісові пожежі. Датчики, що містяться у вказаних перетворювачах, призначені для виявлення полум'ю, тепла і газів, хімічних сполук, що утворюються при горінні. За допомогою GPS здійснюється точна геолокація перетворювачів. Завдяки такій мережі здійснюється не лише локалізація лісових пожеж, але і відвертання таких, оскільки після установки мережа також може отримувати і передавати значення температури і відносної вологості для визначення вірогідності пожежі в зоні, що знаходиться під наглядом. В результаті обробки інформації, що отримується на центральному пункті, виробляється сигнал «тривоги». Оператори постійно мають карту розподілу температур. Розподілена сенсорна мережа при необхідності може встановлювати зв'язок між рятувальниками, що здійснюють пошукові і рятувальні роботи в заданому районі. Існують мережі моніторингу землетрусів і виміру напруги земної поверхні після землетрусів, мережі стеження за активністю вулканів і інші. Усі вони використовують акселерометричні датчики.

Не менш значиму роль грають мережі, пов'язані з моніторингом стану водойм і попередженням повеней. По периметру водосховища встановлюються датчики рівня води(звичайно це поплавкові пристрої, що спрацьовують досягши заданого рівня води у водоймі). Впродовж усього

основного часу датчик знаходиться в режимі «сну», завдяки чому досягається істотна економія енергії, батареєю живлення.

Контроль за «дикою» природою. Вивчення дій людської присутності на рослини і тварин в умовах «дикої» природи представляє практичний інтерес і забезпечується шляхом розгортання спеціалізованих сенсорних мереж. Для багатьох популяцій порушення звичного місця існування часто має вирішальне значення. Особливо це стосується колоній морських птахів. 20 % яєць гине із-за 15-хвилинного відвідування місць гніздування людиною. При повторному відвідуванні птаха взагалі можуть покинути гнізда. Сенсорні мережі дозволяють стежити за поведінкою і життям диких тварин особливо у важкодоступних місцях.

Контроль екологічних параметрів широко застосовується в інтелектуально керованому сільському господарстві. Використовуючи комбінацію датчиків, таких як вологість, температура і світло, вдається визначити ризик замерзання, можливі хвороби рослин і по вологості ґрунту визначити вимоги до поливу. Сенсорні мережі дозволяють створити комфортні умови для росту домашніх рослин, контролювати умови в розплідниках і уважно слідкувати за забезпеченням високих показників росту вибагливих культур, таких як виноградні лози або тропічні фрукти, де найменші зміни клімату можуть вплинути на кінцевий результат. Обробка статистичних матеріалів дозволяє визначити оптимальні умови для кожної окремої культури, порівнюючи з показниками, отриманими при найкращих врожаях.

Спеціалізовані безпроводові сенсорні мережі використовуються в тваринництві з метою оптимізації умов вирощування тварин. Вони дозволяють контролювати температуру народження тварин для підтримки її на заданому рівні, вимірювати рівні газів, що утворюються худобою, таких як метан(CH4), аміак(Нз) і сульфід водню(H2S). Датчики вібрації і руху дозволяють визначати рівень стресу у тварин, контролюючи нестійкість стада.

Контроль стану будівель і інженерних споруд здійснюється з метою визначення їх надійності. Використовуються датчики інклінометричного типу для виміру мікротріщин, що виникають в результаті землетрусів і структурних змін фундаментів, датчики відносних переміщень елементів конструкції мостів і інших інженерних споруд .

Так, зокрема, робиться моніторинг структурної надійності мостів(SHM) на основі обробки показів великого числа датчиків переміщень, об'єднаних в єдину сенсорну мережу. У Каліфорнії, наприклад, 13 % з 23000 мостів вважаються структурно недостатніми, тоді як 12 % з 600000 мостів країни мають задовільний рейтинг. Нью-Йорк може виявитися першим містом з безпроводовим мостовим моніторингом, здійснюваним безперервно і цілодобово.

Окрім контролю надійності, у великих будівлях розгортаються мережі клімат-контролю. Вони забезпечують виміри рівня заповнення, температури і витрати повітря, зменшення втрат енергії за рахунок належного регулювання вологості, вентиляції, кондиціонування повітря.

Автомобільний і залізничний транспорт мають рухливі об'єкти, що взаємно переміщаються один відносно одного, тому існує безліч

безпровідних мереж, що забезпечують надійний зв'язок між ними. Необхідність автоматизації процесу диспетчеризації транспортних засобів в місцях їх концентрації(гаражі, залізничні вузли) привела до створення спеціалізованих сенсорних мереж, що забезпечують збір і обробку даних, що отримуються від великого числа датчиків. Це датчики, що вказують місце розташування, переміщення, стан і ідентифікаційну інформацію об'єктів. В якості одного з прикладів подібних численних мереж можна привести сенсорну мережу автоматизованого автодрому. АПК «Автоматизований автодром» призначений для автоматизації процесу контролю рівня професійної підготовки осіб, що навчаються водінню автомобіля. Є сукупністю апаратних і програмних засобів, що дозволяють організувати і автоматизувати процес об'єктивного контролю професійних навичок водіння автотранспорту. Він включає три взаємозв'язані підсистеми:

- полігон автодрому, обладнаний засобами розмітки і навігації;
- автомобіль, обладнаний комп'ютерною системою, сенсорними пристроями і засобами передачі інформації;
- диспетчерський пункт, обладнаний засобами спостереження і управління процесом тестування.

Устаткування автодрому дозволяє в автоматизованому режимі: фіксувати результати виконання випробувальних вправ за спеціально розробленою методикою в умовах, максимально наближених до реального дорожнього руху; видавати результат іспиту без участі екзаменатора (з повним розшифруванням помилок).

Уся інформація з датчиків автоматизованого стеження, розташованих на використовуваних автомобілях, передається по безпровідній локальній мережі в диспетчерський пункт, де оперативно обробляється і виводиться на дисплей диспетчерові.

Висновок. Резюмуючи, можна стверджувати, що безпровідні сенсорні мережі (БСМ) — це нова, дуже перспективна технологія отримання, передачі і зберігання інформації для різних застосувань. Вони розширюють можливості контрольних і інформаційно-вимірювальних систем, роблячи їх розподіленими в просторі. Вже перші застосування таких мереж показали, що для їх повсюдної реалізації потрібно буде виконати багато дослідницької роботи, для виконання вимог широкого класу додатків.

Література

1. Deploying a wireless sensor network on an active volcano / G. Werner-Allen, K. Lorincz, M. Welsh, O. Marcillo, J. Johnson, M. Ruiz, J. Lees // IEEE Internet Computing. 2006. Vol. 10, no 2. P. 18-25.
2. Mainwaring A., Polastre J., Szewczyk R., Culler D., Anderson J. Wireless Sensor Networks for Habitat Monitoring // First ACM Workshop on Wireless Sensor Networks and Applications (WSNA). 2002. P. 88-97.
3. Bagula A. Applications of wireless sensor networks. — https://www.uonbi.ac.ke/conferences/WSN/dayl/Applications.pdf
4. Madhu A., Sreekumar A. Wireless Sensor Network Security in Military Application using Unmanned Vehicle. https://www.semanticscholar.org/paper/Wireless-Sensor-Network-Security-in-Military- using- Madhu-Sreekumar/e0aa0e813ccb502c37f03a7b91b477e35336c63d

УДК 621.396.946

АЛЬТЕРНАТИВНІ НАВІГАЦІЙНІ СИСТЕМИ НА БАЗІ НАНОСУПУТНИКІВ

Явіся В.С., Лисенко О.І., Тимофеєв Є.М.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: yavisya42@gmail.com

ALTERNATIVE NAVIGATION SYSTEMS BASED ON NANOSATELLITES

The safety of land and air transportation depends to a large extent on the quality of satellite navigation systems. Interference in signal transmission or coding can cause serious emergencies. One of the ways to increase the autonomy of navigation is to use nanosatellite constellations that reduce dependence on global navigation systems.

В умовах сьогодення визначення місцезнаходження різноманітних об'єктів здійснюється шляхом використання супутникових навігаційних систем. Їх функціонування є ключовим фактором для забезпечення безпеки руху як надводних, так і повітряних суден. Все більшого поширення набувають сервіси, що дозволяють контролювати вантажні перевезення та відстежувати транспортні засоби. Навігаційні додатки на мобільних гаджетах значним чином спрощують процедуру пошуку об'єктів за відомим адресом та знаходження оптимальних маршрутів. Таким чином, якість роботи навігаційних систем безпосередньо впливає не лише на безпеку, але й на рівень комфорту та якість життя сучасного суспільства.

Підвищення точності, надійності та стабільності навігаційних систем можливе завдяки поступовій інтеграції аеронавігаційних систем різних країн у єдину глобальну мережу, що є одним із ключових аспектів глобалізації світової економіки. Такий підхід відповідає Глобальній експлуатаційній концепції, розробленій Міжнародною організацією цивільної авіації (ICAO – International Civil Aviation Organization). Концепція передбачає перехід на сучасні технології CNS/ATM (Communication, Navigation and Surveillance/Air Traffic Management – зв'язок, навігація, спостереження та управління повітряним рухом) та об’єднання аеронавігаційних систем окремих країн у єдину мережу [1].

Технологія CNS/ATM базується на активному використанні Глобальних навігаційних супутникових систем (GNSS – Global Navigation Satellites System) для навігаційного супроводу повітряних суден на всіх етапах польоту. Впровадження цієї концепції передбачає поступове скорочення ролі наземних навігаційних засобів як основних джерел координатної інформації [1].

Системи GNSS надають можливість високоточного визначення місцезнаходження об'єктів на значних територіях, що значно перевищує функціональні можливості наземних навігаційних засобів. Проте використання лише супутникових технологій як основного джерела

навігаційних даних супроводжується низкою ризиків, які можуть суттєво вплинути на безпеку польотів, надійність транспортних перевезень та роботу телекомунікаційних мереж, що використовують безпілотні літальні апарати. Основними факторами ризику є [1]:

- низький рівень енергетичної потужності навігаційних сигналів, що підвищує вразливість GNSS-приймачів до активних радіозавад як природного, так і штучного походження.
- можлива монополізація GNSS окремими країнами, що може призвести до навмисного погіршення якості навігаційних показників, кодування або відключення сигналів у разі виникнення політичної або економічної нестабільності.
- глобальний характер GNSS обумовлює високу залежність від окремих елементів системи (космічних апаратів, наземних станцій керування тощо), що може спричинити масштабні збої у функціонуванні системи в різних регіонах планети.

Для мінімізації потенційних негативних наслідків необхідно створення альтернативних навігаційних систем, які можуть виступати в якості основних, резервних або додаткових засобів позиціонування. Такі системи, відповідно до положень концепції CNS/ATM, мають відповідати наступним вимогам [1]:

- наявність функціональних можливостей, аналогічних GNSS, у частині навігаційного забезпечення.
- забезпечення точності визначення координат, яка не поступається показникам GNSS.
- повна незалежність від супутникових систем GNSS у процесі функціонування.
- можливість інтеграції з перспективними супутниковими системами для підвищення точності, цілісності, безперервності та експлуатаційної готовності в різних географічних районах.

Необхідність створення альтернативних засобів аеронавігації, незалежних від GNSS, є очевидною. Зниження впливу зазначених негативних факторів може бути досягнуто шляхом реалізації комплексу заходів, що включають [1]:

- застосування спеціалізованих алгоритмів, які ґрунтуються на комбінованих методах визначення просторових координат у багатопозиційних системах;
- використання методів синхронізації без залучення атомних еталонів часу та даних GNSS;
- оптимізацію просторового розташування радіомаяків;
- формування складних сигналів із унікальними індивідуальними характеристиками;
- використання сучасної елементної бази, що забезпечує компактність, високу обчислювальну потужність та енергоефективність апаратури;

- створення бортових багатофункціональних приймачів, сумісних з пристроями GNSS, що мінімізує необхідність конструктивних змін в наявному обладнанні або дозволяє повністю їх уникнути.

Для більшості країн світу ризик втрати сигналів навігації унаслідок їх відключення або шифрування з боку монополістів GNSS (GPS, ГЛОНАСС) залишається актуальним. Збереження незалежності в таких умовах можливе лише шляхом розгортання власних навігаційних систем. Одним із перспективних напрямів є використання угруповань наносупутників (НС). Завдяки порівняно низькій вартості створення та виведення на орбіту, кількість елементів такої системи може бути значною. Це, разом із синхронізацією випромінюваних сигналів, забезпечить достатній енергетичний рівень сигналу на вході приймача навіть за умов активних навмисних радіоперешкод.

В умовах складної радіоелектронної обстановки підвищення енергетики навігаційних сигналів у заданій зоні може бути досягнуто завдяки використанню спрямованих антен на борту НС та забезпеченню необхідного просторового положення супутників.

Орієнтація супутників традиційно здійснюється за допомогою двигунів-маховиків та магнітних виконавчих органів, проте такі системи не забезпечують можливість зміни орбіти. Найбільш ефективним рішенням є комбінована система управління, що поєднує магнітні котушки для стабілізації та орієнтації, а також іонні двигуни [2].

Надкомпактні іонні двигуни застосовуються для корекції орбіти НС, вони дозволяють значно подовжити термін служби апаратів. Робоча маса зберігається всередині двигуна в рідкому вигляді, а при виході через мікроскопічний отвір іонізується та прискорюється в електричному полі [3, 4].

Таким чином, створення власної навігаційної системи на основі угруповання НС із комбінованою системою управління, синхронізацією сигналів, орієнтацією та стабілізацією просторового положення дозволить підвищити незалежність України в галузі аеронавігації.

Література

1. 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. DOI: 10.1109/INFOCOMMST.2018.8632097.
2. Явіся В.С. Гібридна система орієнтації телекомунікаційних наносупутників // Тринадцята міжнародна науково-технічна конференція «Перспективи телекомунікацій». Матеріали конференції. – К.: КПІ ім. Ігоря Сікорського. – 2019. – С. 273-275.
3. Adam Zewe. MIT engineers develop a fully 3D-printed electrospray engine // https://news.mit.edu/2025/mit-engineers-develop-fully-3d-printed-electrospray-engine-0212.
4. Innovation News Network // https://www.innovationnewsnetwork.com/deploying-compact-fuel-efficient-satellite-engine-space/17036.

УДК 621.396.946

ВАРІАНТ ПОБУДОВИ РЕГІОНАЛЬНОЇ СУПУТНИКОВОЇ КОМУНІКАЦІЙНОЇ СИСТЕМИ

Явіся В.С., Лисенко О.І., Тимофеєв Є.М.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: yavisya42@gmail.com

OPTION OF BUILDING A REGIONAL SATELLITE COMMUNICATION SYSTEM

The author analyzes the ways of building communication satellite systems that are represented in the Ukrainian telecommunications market. To meet the needs of citizens and government agencies in satellite communications services, it is proposed to use a single geostationary satellite.

На сучасному етапі супутниковий зв'язок є ефективним засобом організації доступу до широкого спектру послуг – від телефонного зв'язку та високошвидкісного Інтернету до побудови корпоративних мереж для передачі даних. Такий зв'язок оптимально підходить для встановлення комунікацій між віддаленими регіонами та зонами зі слабко розвиненою інфраструктурою.

Популярність супутникового зв'язку пояснюється його ключовими перевагами, серед яких висока пропускна здатність, можливість роботи у важкодоступних районах та побудова мережі без фізичних комутаційних пристроїв. Якість послуг, що надаються операторами, значною мірою залежить від архітектури системи супутникового зв'язку.

В Україні послуги супутникового зв'язку надаються такими операторами, як Inmarsat, Thuraya, Iridium, Starlink та Globalstar [1, 2]. За орбітальним розташуванням ці системи поділяються на дві групи: геостаціонарні (Inmarsat, Thuraya) та низькоорбітальні (Iridium, Starlink, Globalstar).

Inmarsat експлуатує мережу з одинадцяти супутників на геостаціонарній орбіті (~36000 км), які забезпечують 98% глобального покриття, за винятком полярних регіонів. Thuraya використовує три супутники, що охоплюють переважно Європу, Африку та Азію, залишаючи «білі плями» в Північній та Південній Америці, а також на полюсах.

Оператором Thuraya на геостаціонарну орбіту запущено лише три супутники. Один із них вичерпав свій ресурс, проте залишається на орбіті як резервний. Два активних супутники забезпечують зону покриття, в якій спостерігаються «білі плями» над Світовим океаном, на суходолі в Північній і Південній Америці, а також у районах обох полюсів Землі.

Кожен супутник Inmarsat та Thuraya, що знаходиться на геостаціонарній орбіті, створює сотні високопотужних сфокусованих променів. Їх можна оперативно налаштовувати для забезпечення необхідної пропускної здатності мережі в регіонах з підвищеним попитом на послуги,

шляхом розширення зони покриття або збільшення кількості променів.

Встановлення з’єднання всередині мережі в межах зони покриття здійснюється без залучення наземних станцій. Підключення абонентських терміналів до наземних мереж оператор Inmarsat забезпечує через три наземні станції, тоді як оператор Thuraya використовує лише одну [1, 2].

Термін експлуатації супутників становить від 12 до 15 років.

Серед низькоорбітальних супутникових систем, які забезпечують 100% покриття поверхні Землі, вирізняється оператор Iridium.

Система Iridium включає 77 супутників, з яких 66 є активними та розміщені на шести приполярних орбітах. Унікальний механізм міжсупутникового зв’язку дозволяє передавати сигнал від одного супутника до іншого без ретрансляції на Землю. Завдяки цьому для обслуговування викликів Iridium теоретично може функціонувати з однією наземною станцією сполучення (всього працюють дві такі станції).

Супутники Iridium розташовані на висоті 780 км над поверхнею Землі [1, 2].

Супутники Globalstar виконують функції повторювачів із прямою ретрансляцією сигналу. У складі угрупування діють 48 активних супутників та 4 резервні, які розташовані на висоті 1414 км. Підключення до наземних мереж забезпечується мережею шлюзових станцій, що дозволяє одночасно працювати з наземними станціями не менше ніж 40 супутникам.

Через відсутність міжсупутникового зв’язку апарати потребують прямого з’єднання зі станцією для надання послуг користувачам. Така організація мережі дозволяє надавати клієнтам локалізовані в межах певного регіону телефонні номери для терміналів супутникового зв’язку. Однак за відсутності станцій у віддалених регіонах сервіс недоступний, навіть якщо супутники знаходяться над цими територіями. Це обмеження залишає без покриття полюси та деякі регіони Африки й Азії.

До недавнього часу на навколоземній орбіті не було жодного супутника системи Starlink, проте нині вона є однією з найбільших супутникових систем зв'язку. Попри незавершене розгортання, система вже функціонує та поступово змінює світ, зокрема відіграючи важливу роль у підтримці України під час повномасштабного російського вторгнення [3].

Архітектура системи Starlink включає три основні компоненти: низькоорбітальне супутникове угрупування, мережу наземних станцій і користувацькі термінали.

Більшість супутників системи Starlink знаходиться на орбітах висотою 540-550 км, що сприяє значному зниженню затримки сигналу для кінцевих користувачів. Наступний етап розвитку проєкту передбачає розгортання додаткового угруповання з 7518 апаратів на висоті 330-350 км, що є найнижчою орбітою серед існуючих систем супутникового зв'язку. Дані супутники функціонуватимуть у V-діапазоні [3].

У майбутньому компанія SpaceX планує розширити кількість активних супутників до 42 тисяч. Попри масштабність цієї кількості, завдяки досягненням у зниженні вартості запусків та серійному виробництві

супутників, такий план виглядає цілком реалістичним порівняно з очікуваннями кількарічної давності.

Тривалість експлуатації супутників систем Iridium, Starlink та Globalstar становить приблизно 7-10 років.

На сьогодні в Україні значна кількість користувачів, зокрема відомчі структури, використовують послуги супутникового зв'язку. Наразі ці послуги переважно надаються закордонними телекомунікаційними компаніями. Водночас зміни у міжнародному політичному середовищі потенційно можуть призвести до припинення обслуговування українських абонентів.

Альтернативним рішенням для мінімізації таких ризиків є створення власної регіональної системи супутникового зв'язку. Аналіз основних принципів побудови таких систем свідчить, що супутники на геостаціонарній орбіті мають низку переваг над низькоорбітальними системами. До основних переваг належать: можливість обслуговування користувачів без необхідності використання наземних станцій, стабільний рівень сигналу у радіоканалі, відсутність ефекту Доплера, спрощена організація зв'язку та більший термін служби супутників.

Для створення зони обслуговування системою супутникового зв'язку в межах всієї території України потрібний лише один геостаціонарний супутник, тоді як для низькоорбітальних систем необхідно залучити кілька десятків апаратів. Таким чином, створення супутникової системи на базі геостаціонарного супутника є економічно доцільним рішенням.

Водночас слід враховувати основні недоліки таких систем, зокрема перевантаженість геостаціонарної орбіти на окремих ділянках, значне загасання сигналу та істотні затримки при його передачі [4,5].

Отже, для задоволення потреб мешканців України та державних установ у супутниковому зв'язку, достатньо вивести на геостаціонарну орбіту лише один супутник.

Література

1. Sattrans, сайт компанії: Супутниковий Інтернет. http://sattrans.ua/index.php?route=common/home.
2. Satphone, сайт компанії: Статті про супутникові телефони, обладнання та супутниковий зв'язок. https://satphone.com.ua/.
3. Starlink: Як влаштована система глобального супутникового інтернету. https://universemagazine.com/starlink-yak-vlashtovana-systema-globalnogo-suputnykovogo-internetu.
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. DOI: 10.1109/INFOCOMMST.2018.8632097.
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. pp. 123-125. DOI: 10.1109/UkrMiCo47782.2019.9165399.

УДК 621.396.96:004.62

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ MIMO ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖ

Тимофеєв Є.М., Лисенко О.І.
Навчально-науковий інститут телекомунікаційних систем
НТУУ «КПІ» ім. Ігоря Сікорського, Україна
E-mail: timofeeevzh@gmail.com

APPLICATION OF MIMO TECHNOLOGY TO IMPROVE THE EFFICIENCY OF MOBILE SENSOR NETWORKS

This paper explores the use of cooperative MIMO (Multiple-Input Multiple-Output) technology to enhance the performance and energy efficiency of mobile sensor networks. It examines the key advantages of implementing MIMO technology, including increased data transmission rates and reduced power consumption, particularly in wireless communication environments. The authors highlight how cooperative MIMO can address challenges in sensor networks by optimizing resource utilization and extending network lifetime. The paper also includes a case study demonstrating the positive impact of cooperative MIMO on energy efficiency during data transmission. Overall, this research provides valuable insights into the potential of MIMO technology for improving the performance and sustainability of mobile sensor networks.

Мобільні сенсорні мережі (МСМ) відіграють ключову роль у сучасних бездротових системах, зокрема в екологічному моніторингу, управлінні інфраструктурою та smart city. Одним із основних викликів, з якими стикаються ці мережі, є зростання обсягу переданих даних і потреба в енергоефективності. Одним із можливих рішень є впровадження технології MIMO (Multiple-Input Multiple-Output), яка дозволяє підвищити пропускну здатність і надійність зв'язку за рахунок використання кількох антен для одночасної передачі і прийому даних [1].

Використання адаптивного формування променів (beamforming) у рамках MIMO дає змогу зменшити інтерференцію та покращити якість сигналу. Цей підхід дозволяє мобільним сенсорним мережам динамічно налаштовувати антенні конфігурації в реальному часі. Розподілене MIMO, яке включає кілька вузлів для спільної передачі даних, допомагає знизити рівень перешкод і підвищити ефективність мережі, хоча це вимагає складної координації між вузлами.

Аналіз алгоритмів оптимізації ресурсів, які можуть знижувати енергоспоживання та підвищувати пропускну здатність, виявляє проблеми з обмеженими обчислювальними ресурсами вузлів. Крім того, вдосконалення мережевих протоколів для адаптації до динамічних умов роботи, таких як оптимізація маршрутизації та управління потоком даних, є важливим для забезпечення надійності та зниження втрат сигналу. Масштабованість мережі також є критичним аспектом, який дозволяє забезпечити ефективну роботу

МСМ у різних конфігураціях [2].

Це дослідження спрямоване на вивчення нових підходів для створення більш ефективних, енергоощадних та надійних бездротових систем зв'язку для мобільних сенсорних мереж.

Мобільні сенсорні мережі (МСМ) мають вирішальне значення для ефективного моніторингу та передачі даних у різних галузях, таких як контроль навколишнього середовища, промисловий моніторинг, охорона здоров'я та безпека. Однак, їхнє ефективне функціонування стикається з кількома проблемами:

1. Обмежена пропускна здатність;
2. Високе енергоспоживання;
3. Інтерференція та багатопроменевість;
4. Масштабованість.

Впровадження технології **MIMO** (Multiple Input Multiple Output) є перспективним рішенням цих проблем. Вона дозволяє значно збільшити пропускну здатність, покращити надійність зв'язку та знизити вплив інтерференції завдяки використанню кількох антен на передавачі та приймачі. Це дозволяє суттєво підвищити продуктивність мобільних сенсорних мереж.

Проте, інтеграція технології MIMO в МСМ стикається з певними труднощами, серед яких:

- Технічна складність;
- Динамічні умови.

Актуальність дослідження полягає в розробці методів і алгоритмів для ефективного впровадження MIMO у мобільні сенсорні мережі, що дозволить вирішити зазначені проблеми та підвищити їх ефективність. Зокрема, важливим є розробка енергоефективних алгоритмів для управління ресурсами мережі, оптимізації маршрутизації та зниження впливу інтерференції [3].

Одним із ключових покращень, яке може забезпечити технологія MIMO у мобільних сенсорних мережах (МСМ), є *зниження енергоспоживання та підвищення пропускної здатності.*

Для більш конкретного прикладу покращення ефективності мобільних сенсорних мереж (МСМ) за допомогою MIMO, розглянемо *реальний сценарій* з використанням експериментальних даних. Ми порівняємо енергоспоживання, час передачі даних та надійність зв'язку для мережі з MIMO та без MIMO [4-5].

Сценарій:

1. **Мережа без MIMO**:

- Кожен сенсорний вузол передає дані окремо до базової станції.
- Використовується одна антена для передачі та прийому.
- Енергоспоживання на передачу даних розраховується за формулою:

$$E = P \cdot t$$

де P — потужність передачі, t — час передачі.

2. **Мережа з MIMO**:

- Використовуються 2 антени для передачі та 2 антени для прийому (2x2 MIMO).

- Вузли кооперуються для передачі даних, що дозволяє зменшити потужність передачі кожного окремого вузла.

- Енергоспоживання розраховується з урахуванням коефіцієнта енергоефективності MIMO.

Вихідні дані:

- **Кількість вузлів**: 10.

- **Відстань до базової станції**: 50 метрів.

- **Потужність передачі без MIMO**: 100 мВт на вузол.

- **Потужність передачі з MIMO**: 60 мВт на вузол (завдяки кооперації).

- **Час передачі без MIMO**: 0.5 секунди на вузол.

- **Час передачі з MIMO**: 0.3 секунди на вузол (завдяки паралельній передачі).

- **Надійність зв'язку без MIMO**: 80%.

- **Надійність зв'язку з MIMO**: 95% (завдяки зменшенню інтерференції).

Розрахунки:

1. **Енергоспоживання без MIMO**:

$$E_{\text{без MIMO}} = 10 \cdot (100\ \text{мВт} \cdot 0.5\ \text{с}) = 500$$

2. **Енергоспоживання з MIMO**:

$$E_{\text{з MIMO}} = 10 \cdot (60\ \text{мВт} \cdot 0.3\ \text{с}) = 180$$

3. **Економія енергії**:

$$\text{Економія} = \frac{500 - 180}{500} \cdot 100\% = 64\%$$

4. **Час передачі**:

- Без MIMO: 10 вузлів передають дані послідовно, загальний час:

$$t_{\text{без MIMO}} = 10 \cdot 0.5\ \text{с} = 5\ \text{с}$$

- З MIMO: вузли передають дані паралельно, загальний час:

$$t_{\text{з MIMO}} = 0.3\ \text{с}$$

Для візуалізації ефективності MIMO побудуємо графік, який порівнює енергоспоживання при передачі даних з використанням MIMO та без нього. Використаємо Python та бібліотеку ***matplotlib***.

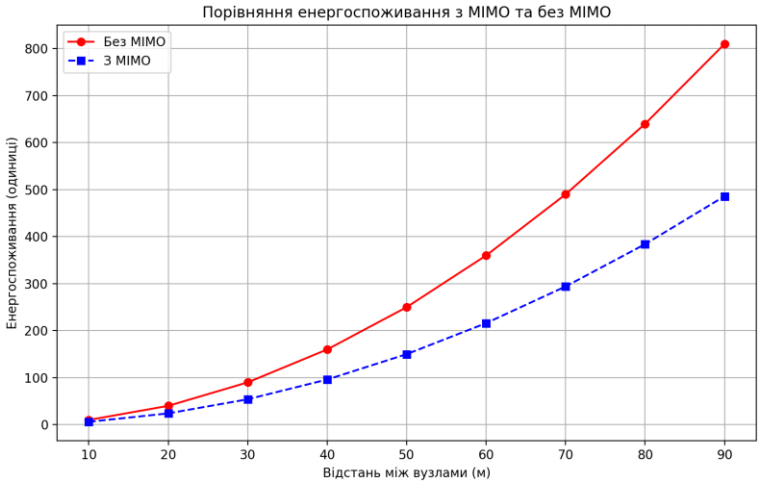


Рис.1. Порівняння енергоспоживання з MIMO та без MIMO.

Використання MIMO у мобільних сенсорних мережах дозволяє:
- Значно знизити енергоспоживання (на 64% у даному прикладі).
- Прискорити передачу даних (у 16 разів у даному прикладі).
- Підвищити надійність зв'язку (з 80% до 95%).

Це робить MIMO ключовою технологією для покращення ефективності МСМ, особливо в умовах обмежених енергетичних ресурсів та високих вимог до швидкості передачі даних.

Висновки. Технологія MIMO є перспективним рішенням для покращення ефективності мобільних сенсорних мереж. Її впровадження дозволяє значно знизити енергоспоживання, підвищити пропускну здатність, скоротити час передачі даних та забезпечити надійність зв'язку. Незважаючи на технічні виклики, подальші дослідження та розробки дозволять повністю реалізувати потенціал MIMO для створення ефективних, енергоощадних та надійних мобільних сенсорних мереж.

Література

1. Tymofeiev, Y., Lysenko, O., Yavisya, V., & Novikov, V. (2024). Enhancing the performance of mobile sensor networks through cooperative MIMO. In Mechanisms of Development of the Scientific and Technical Potential of Modern Society: Collection of abstracts of XL International Scientific and Practical Conference (Sept. 25-27, 2024, Salzburg, Austria) (pp. 77–79). Salzburg: ISU. ISBN 978-617-8427-43-6. DOI: https://doi.org/10.70286/isu-25.12.2024.
2. Тимофєєв Є.М., Лисенко О.І., Явіся В.С., Новіков В.І. (2024). Кооперативне MIMO з використанням комбінованої акустичної та магнітно-індукційної технології**.** Матеріали міжнародної науково-практичної конференції «Актуальні проблеми та інноваційні технології у сфері гуманітарного розмінування, цивільного захисту, критичної інфраструктури та екологічної безпеки для повоєнного відновлення України». 6-7 листопада 2024 року.
3. Кравчук С.О., Голубничий О.Г., Тараненко А.Г., Потапов В.Г., Ткалич О.П. Системи зв’язку з рухомими об’єктами: Підручник. – Спец. видання. – К.: Вид-во ТОВ «Спринт-Сервіс», 2012. – 452 с.
4. Бакулін М.Г., Варукіна Л.А., Крейнделін В.Б. Технологія MIMO: принципи та алгоритми. – М.: Гаряча лінія – Телеком, 2014. – 244 с.
5. Бунін С.Г., Войтер А.П., Ільченко М.Ю., Романюк В.А. Самовпорядковані радіомережі з надширокосмуговими радіосигналами. – К.: НПП «Видавництво «Наукова думка» НАН України». – 444 с.

УДК 621.396.1

АЛГОРИТМ АДАПТИВНОГО УПРАВЛІННЯ ЕЛЕКТРОЖИВЛЕННЯМ ВУЗЛІВ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

[1]Дрегало Б.О., [1]Лисенко О.І., [2]Алєкссєва І.В., [1]Новіков В.І.
[1]Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
2Фізико-математичний факультет КПІ ім. Ігоря Сікорського, Україна
E-mail: novikov1967@ukr.net

ALGORITHM FOR ADAPTIVE POWER CONTROL OF WIRELESS SENSOR NETWORK NODES

To analyze the energy consumption of nodes, a mathematical model was developed that takes into account the energy consumption of nodes in three main operating modes: active, standby, and sleep modes, and an algorithm was proposed that dynamically switches nodes between different modes based on monitoring environmental conditions and load levels.

Управління електроживленням вузлів безпроводових сенсорних мереж (БСМ) є ключовим чинником, що визначає їхню ефективність, стабільність та тривалість функціонування [1]. Враховуючи обмежені енергоресурси сенсорних вузлів, забезпечення максимально можливої економії енергії є критично важливим завданням для подовження життєвого циклу мережі та підтримання її продуктивності на високому рівні. Поняття управління електроживленням в контексті БСМ охоплює комплекс методів та рішень, спрямованих на мінімізацію енергетичних витрат без шкоди для якості передачі даних і надійності зв'язку.

Методи управління електроживленням, що застосовуються в сучасних БСМ, включають різноманітні підходи, зокрема оптимізацію протоколів маршрутизації, використання режимів зниженого енергоспоживання, адаптивне налаштування параметрів вузлів, а також інтелектуальне планування передачі даних. Ці методи дозволяють забезпечити баланс між мінімізацією енергетичних витрат і збереженням стабільної продуктивності системи, що є надзвичайно важливим для мереж, де заміна або зарядка батарей вузлів є практично неможливими або складними [2].

Математичне моделювання енергоспоживання вузлів в БСМ є одним із ключових етапів розробки ефективних методів зниження енерговитрат вузлів. Основною метою такого моделювання є створення алгоритмів, які забезпечують мінімальне споживання енергії без втрати якості передавання даних та функціональних можливостей мережі. Прикладами таких алгоритмів є наступні алгоритми;

1. LEACH (Low-Energy Adaptive Clustering Hierarchy): Алгоритм кластеризації, який рівномірно розподіляє енергетичне навантаження, обираючи головні вузли на основі рівня заряду батареї. Це дозволяє зменшити кількість передач між вузлами та базовою станцією [3].

2. TEEN (Threshold Sensitive Energy Efficient Sensor Network Protocol): Використовує порогові значення для активації вузлів. Передача даних здійснюється тільки при перевищенні критичних значень параметрів, що значно знижує витрати енергії [4].

3. HEED (Hybrid Energy-Efficient Distributed Clustering): Оптимізує вибір головних вузлів, враховуючи залишковий заряд батарей та розташування вузлів в мережі [5].

Для аналізу енергоспоживання вузлів було розроблено математичну модель, яка враховує енерговитрати вузлів у трьох основних режимах роботи: активному, режимі очікування та режимі сну та запропоновано алгоритм, який динамічно перемикає вузли між різними режимами на основі моніторингу умов середовища та рівня навантаження.

Формула для загального енергоспоживання вузла виглядає наступним чином:

$$E_{total} = E_{active} + E_{idle} + E_{sleep}$$

де:

E_{total} — загальне енергоспоживання вузла;

E_{active} — енергія, витрачена вузлом у активному режимі;

E_{idle} — енергія, витрачена вузлом у режимі очікування;

E_{sleep} — енергія, витрачена вузлом у режимі сну.

Кожен з режимів характеризується власними енергетичними параметрами:

1. Активний режим (E_{active}): під час передачі чи приймання даних вузол споживає найбільше енергії. У цьому режимі середнє енергоспоживання складає близько 50 мАгод.

2. Режим очікування (E_{idle}): вузол готовий до приймання сигналів, але не виконує активної передачі. Енергоспоживання в цьому режимі є значно нижчим і складає близько 10 мАгод.

3. Режим сну (E_{sleep}): вузол перебуває у стані низького енергоспоживання, при цьому мінімально підтримує свою функціональність. Споживання енергії в цьому режимі складає лише 1 мАгод.

Запропонована модель дозволяє оцінити загальні витрати енергії кожного вузла залежно від його тривалості перебування в кожному режимі. Наприклад, якщо вузол працює в активному режимі протягом 2 годин, у режимі очікування — 5 годин, і в режимі сну — 17 годин, його загальне енергоспоживання можна розрахувати за формулою:

$$E_{total} = (50 \cdot 2) + (10 \cdot 5) + (1 \cdot 17) = 100 + 50 + 17 = 167 \text{ мАгод.}$$

Це дає змогу оптимізувати роботу мережі, враховуючи, що вузли мають максимально використовувати режим сну для економії енергії.

Алгоритм, який динамічно перемикає вузли між різними режимами на основі моніторингу умов середовища та рівня навантаження, включає наступні кроки:

1. Моніторинг стану вузла:

Перевірка активності (кількість пакетів на секунду);

Аналіз рівня залишкового заряду батареї.

2. Прийняття рішень:

Якщо активність низька, вузол переходить у режим очікування.

Якщо залишковий заряд вузла знижується нижче встановленого порогу, зменшується частота пробудження.

При високому рівні навантаження вузол переходить у активний режим.

3. Оптимізація передачі даних:

Використання методів агрегації даних для зниження кількості передач.

Таким чином, у доповіді запропоновано математичну модель енерговитрат вузлів БСМ, яка враховує енерговитрати вузлів у трьох основних режимах роботи: активному, режимі очікування та режимі сну та алгоритм, який динамічно перемикає вузли між різними режимами на основі моніторингу умов середовища та рівня навантаження.

Напрямом подальших досліджень є оцінка ефективності запропонованого алгоритму за різних параметрів та умов функціонування БСМ.

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. Основи побудови безпроводових сенсорних мереж [Електронний ресурс]: навч. посіб. для здобувачів ступеня бакалавра за освіт. програмою «Інженерія та програмування інфокомунікацій» спец. 172 Електронні комунікації та радіотехніка / КПІ ім. Ігоря Сікорського; уклад.: С. О. Кравчук та ін. – Електрон. текст. дані (1 файл). – Київ: КПІ ім. Ігоря Сікорського, 2024. – 313 с.
3. Heinzelman W. R., Chandrakasan A., Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks //Proceedings of the 33rd annual Hawaii international conference on system sciences. – IEEE, 2000. – С. 10 pp. vol. 2.
4. Alsafi S., Talab S. A. Threshold sensitive energy efficient sensor network protocol //International Journal of Academic Engineering Research (IJAER). – 2020. – Т. 4. – С. 48-52.
5. Younis O., Fahmy S. HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks //IEEE Transactions on mobile computing. – 2004. – Т. 3. – №. 4. – С. 366-379.

УДК 621.396.1

АНАЛІЗ МЕТОДУ РОЗПОДІЛЕНОГО ВИХІДНОГО КОДУВАННЯ СТИСНЕННЯ ДАНИХ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

[1]Третяк А.В., [1]Лисенко О.І., [2]Алєксєєва І.В., [1]Новіков В.І.
[1]Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
[2]Фізико-математичний факультет КПІ ім. Ігоря Сікорського, Україна
E-mail: novikov1967@ukr.net

ANALYSIS OF THE DISTRIBUTED SOURCE CODING USING SYNDROMES METHOD FOR DATA COMPRESSION IN WIRELESS SENSOR NETWORKS

The features of the application of the distributed source coding method for data compression in wireless sensor networks are analyzed.

Для зменшення витрати енергії, пов’язані з передачею даних та підвищення ефективності використання каналів зв’язку з обмеженою смугою пропускання в безпроводових сенсорних мережах (БСМ) застосовуються методи стиснення даних [1-2]. Розподілене кодування — це метод обробки даних, який дозволяє стискати інформацію з кількох джерел (наприклад, сенсорів), які генерують корельовані дані, без потреби прямого обміну інформацією між джерелами.

Кожне джерело стискає свої дані незалежно, передаючи лише мінімально необхідну інформацію. Декодування виконується в центральному вузлі, який використовує як отримані стисливі дані, так і "sideinformation" (допоміжну інформацію, яка може бути корельованими даними від інших джерел). Розподілене кодування вирішує проблеми, які виникають у системах із розподіленими джерелами даних, котрі зустрічаються у БСМ. У безпровідних сенсорних мережах кожен сенсор має обмежений запас енергії. Найбільші витрати енергії пов’язані з передачею даних. Замість передавання повного набору даних, розподілене кодування дозволяє сенсорам передавати тільки стислі дані (синдроми), що значно знижує витрати енергії. У системах із високою кількістю джерел (наприклад, сотні чи тисячі сенсорів) передача великих обсягів даних створює перевантаження каналу зв’язку. Розподілене кодування скорочує кількість переданих даних. Дані, які генеруються джерелами, що знаходяться у близькості (наприклад, сенсори температури), часто корельовані. Замість передачі всіх даних, розподілене кодування використовує цю кореляцію для стиснення.

Метод розподіленого вихідного кодування (англ. Distributed source coding using syndromes, DISCUS) [3] базується на теоремі Слепіана-Вулфа, котра теоретично обґрунтувала можливість стиснення корельованих джерел без втрати ефективності, навіть якщо кодування виконується незалежно. Розподілене кодування підходить для великих систем, де централізовані підходи можуть стати вузьким місцем через обмеження обчислювальної потужності чи пропускної здатності.

Висока кореляція між даними означає, що значення, зібрані різними сенсорами, мають схожі або залежні одне від одного значення. Це часто спостерігається у фізичних системах, де сусідні сенсори вимірюють параметри в одній і тій самій області (наприклад, температуру, вологість, тиск). Тобто якщо сенсор S1 вимірює температуру 25°C, а сенсор S2, розташований поруч, вимірює 24°C або 26°C, то дані S1 та S2 корельовані. У таких випадках ми можемо використати знання про значення одного сенсора (або групи сенсорів) для передбачення або точного відновлення значення іншого. Кореляція дозволяє зменшити надлишковість у даних. Замість передачі повного набору даних, можна передавати тільки відмінності або мінімальну кількість інформації (синдроми), достатню для відновлення даних у центральному вузлі.

Центральний вузол мережі використовує кореляцію наступним чином:

1. Центральний вузол знає дані одного або кількох сенсорів (Y) як допоміжну інформацію. Це може бути або повні дані сусіднього сенсора, або вже відновлені дані.

2. Синдром, отриманий від джерела, визначає набір можливих значень (косет).

3. Кореляція з допоміжною інформацією дозволяє звузити цей набір до одного правильного значення.

4. Вузол виконує операцію декодування, використовуючи матрицю H, яка визначає, як саме стискати й декодувати синдроми.

5. Знаходиться значення, яке відповідає отриманому синдрому і найближче до допоміжної інформації.

Параметри котрі повинні бути встановлені заздалегідь на вузлі наступні:

1. Матриця H, яка визначає, як стискаються дані і як декодуються синдроми. Центральний вузол повинен мати ту саму матрицю H, яка використовується у сенсорах.

2. Центральний вузол повинен знати, яким чином дані корельовані тобто знати модель кореляції (наприклад, максимальна різниця значень між сенсорами).

3. Центральний вузол повинен отримувати або вже мати дані від сусідніх сенсорів, щоб використовувати їх як допоміжну інформацію для відновлення стислих даних.

4. Вузол повинен мати алгоритм для обчислення можливих значень із синдрому (кандидатів) і вибору правильного значення на основі кореляції.

Розглянемо наступний приклад стискання бітів інформації в DISCUS

Початковий обсяг даних: X має розмір 1024 байти (тобто $1024 \times 8 = 8192$біт).

Якщо X і Y майже ідентичні (висока кореляція), то $H(X|Y)$ буде набагато меншим за $H(X)$, тобто якщо кореляція між джерелами 90%, то $H(X|Y)$ буде близько 10% від $H(X)$.

Припустимо що $H(X)=8192H(X)=8192$ біт (початкова ентропія X). Рівень кореляції між X і Y — 90% (відповідає $H(X|Y)=10\% \times H(X)$). Тоді $H(X|Y)=0.1 \times 8192=819.2$ біт.

Обсяг стиснутої інформації819.2 біт=819.2/8=102.4 байта.

Отже, обсяг інформації після стиснення зменшиться з 1024 байт до 102 байт, що відповідає коефіцієнту стиснення = 1024/102.4≈10.

Якщо початковий обсяг даних становить 1024 байти, то за умов високої кореляції (90%) обсяг стиснутої інформації може зменшитися до 102 байт (близько 10 разів). Ефективність стиснення залежить від ступеня кореляції між X і Y. Якщо кореляція нижча (наприклад, 50%), обсяг даних зменшиться менше (приблизно в 2 рази).

Розглянемо наступний приклад БСМ (рис.1), яка вимірює температуру в певній зоні. У мережі є кілька сенсорів (S1,S2,S3), які передають дані в центральний вузол температуру в зоні, де вона змінюється плавно (наприклад, через рівномірне нагрівання чи охолодження).

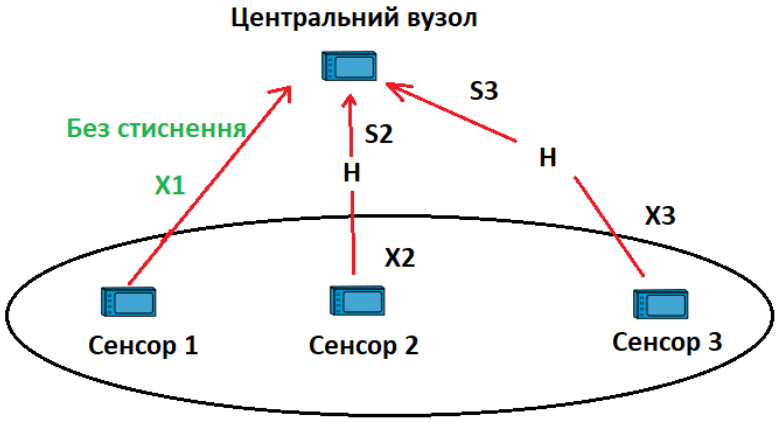


Рис. 1. Приклад використання методу DISCUS.

Вимірювання температури:

S1:{25,26,25,27,26}

S2:{26,27,26,28,27}

S3:{27,28,27,29,28}

Ці дані мають високу кореляцію через близьке розташування сенсорів. Відмінність між S1 і S2 зазвичай не перевищує 1°C.

Якщо не використовувати метод DISCUS, то кожен сенсор передає повний набір своїх даних. S1,S2,S3 передають по 5 значень (по 1 байту на кожне значення). І загальна кількість переданих даних: 3×5=15 байт.

Передача за допомогою DISCUS

Кожен сенсор кодує свої дані у вигляді синдрому.

Центральний вузол вже знає значення сусідніх сенсорів (вони передаються або вже декодовані).

Сенсор S2 використовує S1 як допоміжну інформацію. Відмінності між S1 і S2 [1,1,1,1,1]

У двійковому вигляді: [1,1,1,1,1] кодується в компактний синдром.

Передається лише синдром (2–3 біти замість 8 біт).

Сенсор S3 використовуєS2 як допоміжна інформація. Відмінності між S2 iS3: [1,1,1,1,1]

Знову передається лише синдром. Центральний вузол отримує дані S1 у повному вигляді {25,26,25,27,26}.Синдроми від S2 та S3.За допомогою S1 і синдрому від S2, вузол відновлює дані S2 {26,27,26,28,27}. За допомогоюS2 і синдрому від S3, вузол відновлює дані S3 {27,28,27,29,28}.

Аналіз використання методу DISCUS наведено в таблиці 1.

Таблиця 1. Обсяг переданої інформації з методом DISCUS.

Параметр	**Розмір (байт)**
Загальна кількість переданих даних(S1,S2,S3)	15
Повні дані для S1	5
Синдроми для S2 і S3	1.25
Загальний обсяг	7.5
Коефіцієнт стиснення	2.00

Стиснення в методі DISCUS напряму залежить від кореляції між даними сусідніх вузлів або джерел. Чим вища кореляція, тим менший обсяг інформації потрібно передавати, оскільки центральний вузол може ефективніше відновити дані з використанням допоміжної інформації.

Таким чином, у доповіді проведено аналіз сучасного методу стиснення даних БСМ DISCUS. Напрямом подальших досліджень є експериментальне дослідження ефективності методів стиснення, таких як MRCQ, DIMENSIONS, S-LZW-MC, оцінка їх продуктивності за такими критеріями, як коефіцієнт стиснення, використання пам’яті, кількість операцій та середньоквадратичної помилки, якщо присутня, з використанням ПЗ Matlab2024b.

Література

1. Akyildiz I. F. et al. A survey on sensor networks //IEEE Communications magazine. – 2002. – Т. 40. – №. 8. – С. 102-114.
2. Nelson M., Gailly J. L. The data compression book 2nd edition //M & T Books, New York, NY. – 1995.
3. 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.

УДК 621.396.1

МОДЕЛЬ ПРОГНОЗУВАННЯ ТОПОЛОГІЧНИХ ЗМІН ЛІТАЮЧИХ СЕНСОРНИХ МЕРЕЖ НА ОСНОВІ ВИКОРИСТАННЯ РЕКУРЕНТНИХ НЕЙРОННИХ МЕРЕЖ

[1]Кошмак А.І., [1]Лисенко О.І., [2]Алєксєєва І.В., [1]Новіков В.І.
[1]Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
[2]Фізико-математичний факультет КПІ ім. Ігоря Сікорського, Україна
E-mail: novikov1967@ukr.net

A MODEL FOR PREDICTING TOPOLOGICAL CHANGES IN FLYING SENSOR NETWORKS BASED ON THE VICINITY OF RECURRENT NEURAL NETWORKS

To achieve a high level of adaptability of routing methods in flying sensor networks, a vicarious model for predicting topological changes based on the vicarious recurrent neural networks using a long short-term memory.

Розвиток технологій літаючих сенсорних мереж (ЛСМ) відкриває нові можливості для передачі, обробки та аналізу інформації [1-3]. У зв'язку з необхідністю забезпечення ефективної маршрутизації в ЛСМ, виникає потреба у вдосконаленні існуючих та створенні нових методів маршрутизації, які враховують специфіку таких мереж, пов’язану з динамічними змінами топології, обмеженими енергетичними ресурсами, високою мобільністю вузлів та складністю середовища передачі даних. Урахування та інтеграція цих аспектів є необхідною умовою для забезпечення стабільної та надійної роботи ЛСМ в умовах складних і динамічних сценаріїв експлуатації.

Для досягнення високого рівня адаптивності методів маршрутизації у ЛСМ було запропоновано використання моделі прогнозування топологічних змін на основі використання рекурентних нейронних мереж (РНМ, англ. Recurrent neural network, RNN) із механізмом довгої короткочасної пам’яті (англ. Long short-term memory, LSTM) [4]. Структурна схема запропонованого рішення, яка відображає основні етапи обробки даних, включаючи прогнозування та оновлення маршрутів представлено на рис. 1.

На схемі зображено, як дані з сенсорів, що збирають координати вузлів і їхню швидкість, подаються у вигляді часових рядів на вхід модулю прогнозування. Цей модуль складається з кількох шарів LSTM, які аналізують часові залежності в рухах вузлів і формують прогноз майбутніх положень. На основі отриманого прогнозу виконується оцінка стабільності з'єднань між вузлами, і за необхідності коригуються маршрути передачі даних.

Рекурентна нейронна мережа отримує на вхід три основні параметри: координати вузлів (x, y) та їхню швидкість. Модель спочатку проходить навчання на синтетичних або реальних даних, які відображають поведінку вузлів у різних сценаріях. Під час роботи мережі прогнозовані значення координат дозволяють передбачити розриви зв’язків у мережі та забезпечити своєчасне оновлення маршрутів.

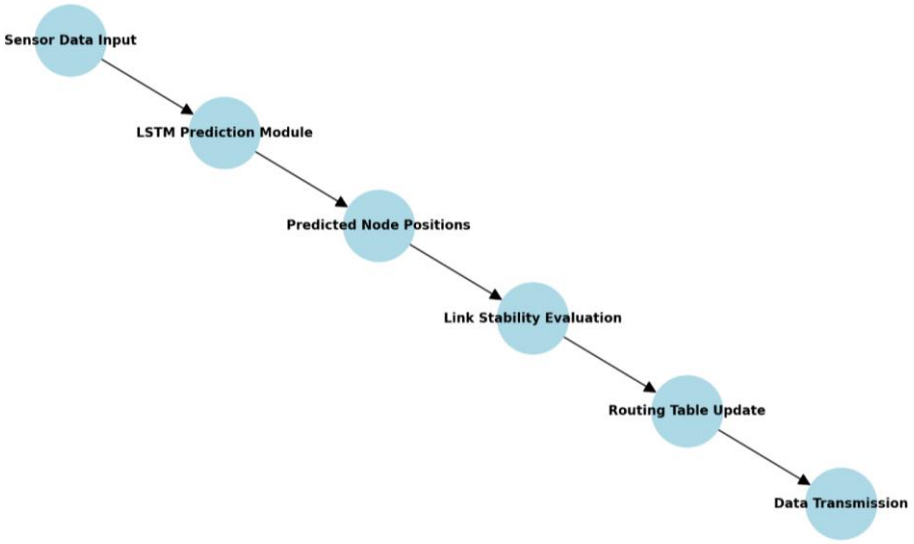


Рис. 1. Структурна схема прогнозування топологічних змін та оновлення маршрутів у ЛСМ.

Реалізація нейронної мережі відбувається через бібліотеку TensorFlow. У запропонованому коді на рис. 2 описана модель, яка використовує два шари LSTM для вилучення залежностей з даних. Перший шар забезпечує обробку короткочасних залежностей, а другий фокусується на довгих взаємозв’язках між вузлами мережі. Для запобігання перенавчанню використовується регуляризація у вигляді Dropout.

Запропонований код демонструє основний процес створення та навчання рекурентної нейронної мережі для прогнозування майбутніх положень вузлів у літаючих сенсорних мережах. Ця мережа використовує вхідні послідовності даних, які містять координати вузлів (x, y) та їхню швидкість (v), щоб передбачати їхні майбутні параметри. Такий підхід дозволяє алгоритмам маршрутизації заздалегідь враховувати можливі зміни топології мережі.

Архітектура моделі побудована на базі двох шарів довгої короткочасної пам'яті , що є основою для обробки часових залежностей. LSTM-шари здатні зберігати інформацію про попередні стани в мережі, дозволяючи моделі враховувати динаміку змін у русі вузлів. Перший LSTM-шар обробляє короткочасні залежності між вхідними даними, тоді як другий фокусується

на довготривалих взаємозв'язках, що є важливим для складних сценаріїв динамічних мереж. Додатково використовується регуляризація у вигляді Dropout. Dropout знижує ймовірність перенавчання, випадково виключаючи частину нейронів із процесу навчання. Це забезпечує стійкість моделі до змін у даних та покращує її узагальнюючі здібності.

Навчання моделі здійснюється за допомогою навчальних даних (x_train та y_train), які представляють часові послідовності координат вузлів та їхніх швидкостей, а також прогнозовані значення для наступних часових кроків. Важливою частиною цього процесу є використання валідаційних даних, що дозволяють оцінити продуктивність моделі на раніше невідомих наборах даних. Такий підхід запобігає перенавчанню та забезпечує можливість адаптації до реальних сценаріїв роботи мережі.

```
import tensorflow as tf
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import LSTM, Dense, Dropout


input_dim = 3
output_dim = 3  ь
time_steps = 10


model = Sequential([
    LSTM(64, return_sequences=True, input_shape=(time_steps, input_dim)),
    Dropout(0.2),
    LSTM(32, return_sequences=False),
    Dropout(0.2),
    Dense(output_dim, activation='linear')
])

model.compile(optimizer='adam', loss='mean_squared_error')


history = model.fit(
    x_train, y_train,
    epochs=50,
    batch_size=32,
    validation_data=(x_val, y_val)
)
```

Рис. 2. Код для реалізації прогнозування топологічних змін у ЛСМ із використанням LSTM.

Ключовим компонентом є функція втрат, яка в цьому випадку представлена середньоквадратичною похибкою (mean_squared_error). Ця функція використовується для оцінки точності моделі, визначаючи різницю

між реальними координатами вузлів та передбаченими. Оптимізація здійснюється за допомогою алгоритму Adam, що дозволяє ефективно налаштовувати ваги нейронної мережі та забезпечує швидку збіжність навіть для великих наборів даних.

Результатом навчання є модель, яка може обробляти поточні дані з вузлів мережі, прогнозуючи їхні майбутні положення. Наприклад, у реальній системі модель отримує на вхід послідовності даних про координати та швидкості вузлів, обробляє їх через LSTM-шари та видає прогнозовані значення координат. Ці значення передаються маршрутизатору, який на основі прогнозу оновлює маршрути передачі даних. Це дозволяє забезпечити безперервність з'єднання, зменшити затримки передачі та уникнути втрат пакетів у мережі.

Таким чином, запропонований підхід дозволяє інтегрувати прогнозування топологічних змін у процес маршрутизації. Окрім високої точності, модель демонструє гнучкість та стійкість до змін у топології мережі. Подальші вдосконалення можуть включати оптимізацію архітектури моделі, вибір гіперпараметрів або використання глибших мереж для обробки складніших залежностей.

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. Dupond S. A thorough review on the current advance of neural network structures //Annual Reviews in Control. – 2019. – Т. 14. – №. 14. – С. 200-230.

UDC 621.391.3

INTEGRATION ECOSYSTEM OF WIRELESS SENSOR NETWORKS AND THE INTERNET OF THINGS

Oliinyk D.I., Koshkarov S.A., Nizhnyi D.A.
National Institute for Strategic Studies, Ukraine,
Chernivtsi Cooperative Professional College of Economics and Law, Ukraine,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: danaolijnuk@gmail.com, steve_ko@ukr.net, nizhnyi.danyil@lll.kpi.ua

ІНТЕГРАЦІЙНА ЕКОСИСТЕМА БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ ТА ІНТЕРНЕТУ РЕЧЕЙ

У статті наводиться опис концепції інтеграційної екосистеми бездротових сенсорних мереж та Інтернету речей, що базується на синергії сучасних технологій зв'язку, хмарних обчислень та інтелектуальних алгоритмів для забезпечення ефективного збору, передачі та обробки даних.

Окреслено ключові технічні та стратегічні межі розвитку даної екосистеми, зокрема впровадження технологій 5G/6G, субтерагерцових систем, штучного інтелекту та віртуальних середовищ, що сприяють формуванню нової цифрової економіки та створенню умов для розгортання інтерактивних систем майбутнього.

Wireless sensor networks (*WSN*) are of increasing interest for scientific research and play a major role in the deployment of the Internet of Things (*IoT*) and the formation of the Metaverse [1].

Symbiotic technologies such as artificial intelligence (*AI*), cloud computing, big data and wireless systems IMT -2020 (5G), combined with the power *of IoT*, opens up new possibilities for their use in telecommunications, information technology and other "smart" industries of metaverse. Significant progress has been observed in the development by the International Telecommunication Union (*ITU)* 5G technology and the implementation of generally accepted standards for the approval of sixth generation (6G) radio interface technology [2].

In the future, these technologies are aimed at creating densely distributed, interacting and self-organizing networks of international mobile communications (*IMT*) with the joint allocation of radio resources of different heterogeneous systems to improve resource utilization and enhance system performance. In turn, with the widespread deployment of base stations (BS), edge servers, and intelligent devices, mobile networks provide a new platform for ubiquitous data collection,

storage, exchange, and computation. These are potential factors of semantic communications of future mobile distributed/collaborative machine learning (ML).

Recent advances *in AI* in image, video and audio signal processing, data analysis, among other things, have allowed wireless communication to move towards an intelligent paradigm, in particular, architecture, protocols, and algorithms for IMT. The rapid growth of mobile data and traffic flow motivates the implementation of new technologies to improve the efficiency of radio spectrum use (*Spectrum Engineering, SE*), energy efficiency improvement (*Energy Efficiency, EE*) and sensor deployment density. Actually, *WSNs* refer to networks of spatially separated and dedicated sensors and devices interconnected by radio signals, which are capable of relay messages from one element to another.

In this context, research into subterahertz (THz) technologies is playing a significant role. It is predicted that in the future, these technologies will enable exceptional data rates for 5G and 6G wireless communication systems, especially for intelligent communication between devices falling under the category of *IoT*. The transition from the current 5G millimeter wave (mmW) technology to the THz spectrum will provide unprecedented solutions that will guarantee higher transmission speeds and channel capacity for any wireless communication system. One of the technologies that will contribute to achieving communication at frequencies up to THz, providing low path loss and power with reliable and fast data transmission, is the implementation of terahertz high-gain antennas. THz antennas are suitable for IoT applications that require fast data transmission, as they provide high-speed wireless connectivity for 5G and 6G. Compared to other wireless technologies, these applications include high-definition video streaming, virtual reality (VR), augmented reality (AR), mixed reality (MR), and waves for real-time sensor data collection. In this virtual space, the basic microparticle may not be a biological cell, but a binary code (0 and 1), or even a quantum bit (qubit). AI is able to construct a multi-level digital continuum, where elementary binary or quantum units form complex structures - from virtual organisms to entire ecosystems and societies.

The compatibility and growth of shared ecosystems on this basis is shaping a new digital world and unlocking its potential, fueling the next wave of recombinant

innovation and defining the next evolution of the Internet. It is built on decentralized blockchain technologies, a metaverse, and non-fungible tokens (NFTs).

According to the definition proposed by the International Telecommunication Union ITU-T FGMV-20 focus group, the metaverse is considered as “an integrated ecosystem of virtual worlds that offers immersive experiences that change existing ones and create new values” [3]. For example, three-dimensional (3D) virtual AI agents in virtual reality (VR) or holograms in augmented reality (AR) can establish new possible forms of interaction in the metaverse, in which traditional channels give way to interactive ones. In the metaverse, everyone can create their own avatar and freely explore the simulated environment. Similarly, in the metaverse, remote or hard-to-reach places can be recreated, processes can be simulated, etc. It is obvious that the increased level of interaction and immersion offered by the metaverse opens up unprecedented opportunities and challenges for scientific research *on WSNs* in the context of deployment *IoT*. Ukraine is part of this growing segment of the market for computing power, AI, cloud and edge capabilities, spatial content creation, software and specialized knowledge, as it leverages VR, AR and MR capabilities [4].

The metaverse already represents the integration of digital and real economies, which will define the next generation of digital economy involving immersive technologies (immersion in the virtual world), holographic principles (property of quantum gravity), tactile communications and new media beyond 8K image resolution, etc [5]. For the development and evolution of the metaverse, VR/AR/MR technologies in combination with the integration of information and communication technologies act as the main tool that will be crucial in the future [6]. According to expert forecasts, the metaverse market will reach $2.1 billion in 2025. The annual growth rate of this market (CAGR 2024-2030) is expected to be 40.03%, leading to a projected market size of US $16.1 billion by 2030. In this regard, there is a need to form a systemic approach to creating a new digital space that would be simultaneously effective, stable and socially significant based on a multi-level model of building a metaverse. One example of addressing these issues

is the “Development Plan for the Metaverse Industry in China”, which directly addresses VR as the foundation of the metaverse and defines strategic goals for the development of VR technologies in industry, education and entertainment, including the integration of AI and 5G [7] In addition, countries such as India, South Africa, and Vietnam are actively implementing augmented reality and AI in key industries by integrating physical objects with their connection to *WSNs.* IoT allows these objects to collect and share data, which has far-reaching implications for improving efficiency, resource allocation, and quality of life. *WSNs* are an effective-distributed data collection technology that will play a major role in IoT deployment, but issues related to reliability, autonomy, cost, and accessibility to application domain experts still limit their widespread use.

Conclusion. The integration of IoT with WSNs is a revolutionizing way of interacting with the world and offers significant potential for increasing efficiency, productivity, and connectivity across sectors of the economy. In addition, addressing strategic challenges requires long-term digitalization efforts and continuous data review, which are the basis for the network economy model. This requires further understanding of how to address the challenges and opportunities of the metaverse, and in what direction to further explore potentially new forms of interaction. *IoT* with *WSNs.*

References

1. Internet of Things: Wireless Sensor Networks. URL: *https://www.iec.ch/basecamp/internet-things-wireless-sensor-networks*
2. Recommendation ITU-R M.2160-0 (11/2023) M Series: Mobile, radiodetermination, amateur and related satellite services Framework and overall objectives of the future development of IMT for 2030 and beyond. URL: *https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2160-0-202311-I%21%21PDF-E.pdf*
3. ITU-T Focus Group Technical Specification FGMV-20 (2023), Definition of metaverse.URL: *https://www.itu.int/en/ITU-T/focusgroups/mv/Pages/default.aspx*
4. Metaverse: market data & analysis. URL: *https://www.statista.com/study/132822/metaverse-market-report/*
5. Robert Silva. “8K Resolution – Definition and Explanation of 8K Video Resolution”. About.com. Archived from the original on January 14, 2012. Retrieved February 12, 2014.
5. Report ITU-R M.2516-0 (11/2022) Future technology trends of terrestrial International Mobile Telecommunications systems towards 2030 and beyond. URL: *https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2516-2022-PDF-E.pdf*
6. The third session of the 14th National People's Congress concluded in Beijing.URL: http://www.miit.gov.cn

УДК 621.396.4

ЗАДАЧІ ПЛАНУВАННЯ ТРАЄКТОРІЇ ПОЛЬОТУ ГРУПИ БПЛА ДЛЯ ЗБОРУ ДАНИХ З ВУЗЛІВ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ

Романюк В.А.[1], Гримуд А.Г.[2]
[1]*Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Україна*
[2]*Національний університет оборони України, Україна*
E-mail: romval2016@gmail.com; grimood@ukr.net

TASKS FOR PLANNING THE FLIGHT TRAJECTORY OF A MULTI-UAVS FOR DATA COLLECTION FROM NODES A WIRELESS SENSOR NETWORK

An improved algorithm for constructing a flight trajectory and collecting multi-UAV data from wireless sensor network nodes is proposed to achieve certain objective control functions.

Розглядається безпроводова сенсорна мережа (далі – БСМ) з незв'язними наземними стаціонарними вузлами, які випадковим чином розташовані на важкодоступній території, де відсутня будь-яка комунікаційна інфраструктура. 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 комунікаційних аероплатформ (далі – КА), які побудовано на базі безпілотного літального апарату (далі – БпЛА) [1-4]. Сенсорні вузли здійснюють збір даних (моніторинг) параметрів зовнішнього середовища (об'єктів, цілей), їх збереження та подальшу передачу до комунікаційної аероплатформи при наявності з нею радіозв'язності.

Однією з найважливіших завдань збору даних є завдання планування траєкторії польоту БпЛА, тобто визначення набору точок у просторі.

Процес планування траєкторії польоту для збору даних групи БпЛА здійснюється наземним центром управління, в процесі польоту та збору даних кожна КА корегує заплановане рішення згідно реальних умов та параметрів вузлів мережі (координати, рівень енергії батарей та обсяг даних) на момент польоту та визначеного пріоритету цільових функцій [1-3].

Мета роботи – провести класифікацію задач планування траєкторії польоту (зависання) групи БпЛА та визначити алгоритми їх рішення.

Основними цільовими функціями процесу збору даних КА з вузлів БСМ можуть бути: мінімізація часу (граничний час) збору даних $T_{зб}$, максимізація часу (визначений час) функціонування вузлів мережі $T_{ф}$, мінімізація кількості КА тощо [1, 2]. Реалізація цих оптимізаційних задач залежить від прийнятого рішення по траєкторії польоту КА для збору даних з вузлів сенсорної мережі.

Постановка та рішення задачі планування траєкторії польоту групи БпЛА залежить від вихідних даних (рис.1): кількість вузлів, КА та їх параметри (однорідні або неоднорідні); наявність або відсутність мобільних пунктів зарядки батарей БпЛА; кількість (одна або декілька) та локація

(однакова або різна) точок вильоту та повернення КА; способи обльоту БСМ (за територією або за точками збору даних); створення повітряної мережі (для передачі даних моніторингу на базову станцію та координації своїх дій з іншими КА) або ні, наявність перешкод (заборонених зон) польоту тощо.

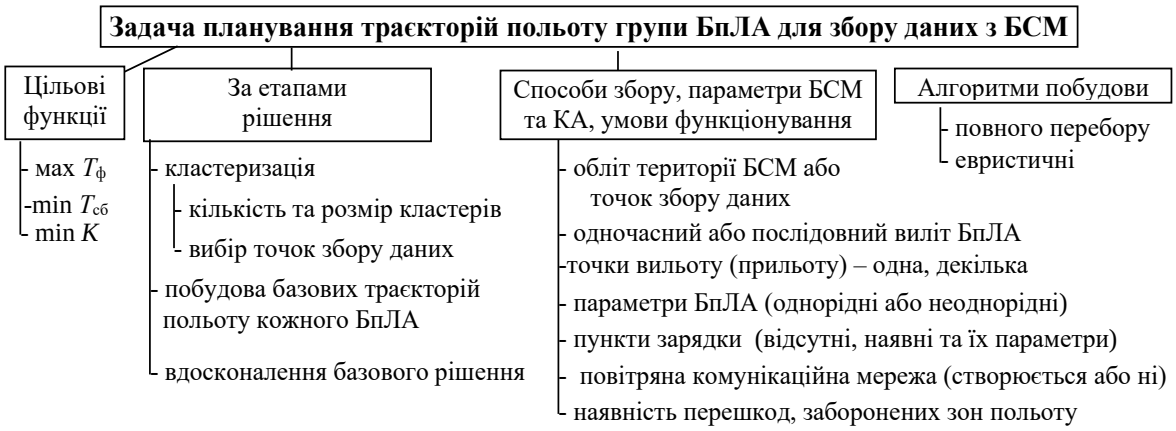


Рис. 1. Класифікація задач планування траєкторії польоту групи БпЛА.

Будувати траєкторію групи БпЛА можна двома основними способами:

1. Реалізувати обліт всієї площі (території) розташування вузлів БСМ. Наприклад, розбиття на квадрати територію БСМ (здійснити накладання сітки), розподіл квадратів між КА та їх обліт за певними відомими алгоритмами: за смугами, за периметром, за спіраллю, зігзаг тощо [3]. Однак такий спосіб призводить до значного часу обльоту вузлів мережі КА, хоча він фактично реалізується тільки при первинному обльоті КА мережі для збору інформації про поточні параметри вузлів.

2. Віртуальна кластеризація вузлів мережі з визначенням у просторі точок збору даних та побудова траєкторії польоту КА між точками збору даних.

Постановка задачі. Дано: наземна безпроводова БСМ значної розмірності з незв'язною топологією. Збір даних моніторингу здійснює декілька (K) комунікаційних аероплатформ. Виліт (приліт) групи КА здійснюється одночасно з визначеної точки, політ здійснюється зі створенням повітряної мережі, яка застосовується в якості каналу управління польотом БпЛА.

Необхідно: визначити траєкторію польоту кожної БпЛА для досягнення певних цільових функцій (мінімізація часу збору, максимізація часу функціонування мережі тощо)

Припущення: для збору даних з сенсорних вузлів КА використовують радіоканали прямої видимості, розмір кластера радіозв'язності КА-вузли визначається висотою польоту та параметрами прийомопередавачів (антен) вузлів та КА, протоколом канального рівня, обмін даними в кластері між БпЛА та вузлами здійснюються в процесі засисання в точках збору та в процесі польоту.

Задача побудови траєкторії польоту групи БпЛА можна віднести до задачі пошуку найкоротшого шляху для декількох комівояжерів (MTSP, Multi Traveling Salesman Problem algorithm). Метою MTSP є мінімізація

загального часу виконання місії. Однак в нас інша мета – мінімізувати максимальний час збору T_k даних серед *k*-БпЛА (задача minmaxT_k).

Загалом рішення задачі пошуку найкоротшого шляху для декількох комівояжерів є *NP*-складною [4]. Отримане точного рішення в реальному часі для БСМ значної розмірності стає не можливим. Тому доцільно використовувати евристичні алгоритми пошуку рішення.

Найпростіше рішення по плануванню траєкторії польоту групи КА – побудувати траєкторію обльоту для одного БпЛА, яку потім розподілити на сегменти для рішення задачі комівояжера для кожного БпЛА групи [4].

Тому спочатку проводиться віртуальна кластеризація мережі з адаптацією розміру кластерів (використовується алгоритм кластерного аналізу FOREL (FORmal Element)) з врахуванням координат вузлів, їх взаємного розташування, обсягу даних, енергії батарей та пріоритету цільових функцій [1-3] та визначенням майбутніх точок зависання (збору) даних траєкторії БпЛА [1, 2]. Потім обраховуємо оптимальну траєкторію обльоту всіх точок збору для одного БпЛА [3]. Далі плануємо траєкторію кожного БпЛА за рахунок поділу загальної траєкторії на певні ділянки. Будуємо базові траєкторії БпЛА (застосування алгоритму рішення завдання про циклове покриття фіксованої потужності *k* мінімальної ваги (Minimum-weight k-Size Cycle Cover Problem, Min-k-SCCP) [4]). Отримані базові рішення ітераційно покращуємо за допомогою запропонованих евристик, які перерозподіляють точки збору між траєкторією з більшим часом до траєкторії з меншим часом.

Таким чином, розглянуті завдання планування траєкторії групи КА для збору даних з БСМ. Запропонований евристичний алгоритм планування траєкторії польоту групи БпЛА, якій складається з наступних кроків: кластеризація мережі з визначенням точок збору даних, побудова траєкторії польоту для одного БпЛА, розбиття траєкторії одного КА на К-траєкторій, покращення рішення по досягненню визначених цільових функцій.

Побудована імітаційна модель процесу збору даних групою БпЛА дозволила провести оцінку ефективності запропонованих рішень та показати перевагу в порівнянні з відомими рішеннями.

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.
3. Романюк В.А., Гримуд А.Г. Алгоритми побудови траєкторії комунікаційної аероплатформи для збору даних з вузлів безпроводової сенсорної мережі. Communication, informatization and cybersecurity systems and technologies, 2024. № 6. p.186 – 203. https://doi:10.58254/viti.6.2024.15.186.
4. Zhen Qin, Aijing Li, Chao Dong, Haipeng Dai, Zhengqin Xu. Completion Time Minimization for Multi-UAV Information Collection via Trajectory Planning. Sensors 2019, 19, 4032; doi:10.3390/s19184032.

УДК 621.39

МЕТОД ПОБУДОВИ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ ДЛЯ МОНІТОРИНГУ МІСЬКОГО СЕРЕДОВИЩА У РОЗУМНИХ МІСТАХ

Богач Б.І., Суліма С.В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: stivmenstivmen@gmail.com

METHOD FOR BUILDING WIRELESS SENSOR NETWORKS FOR MONITORING THE URBAN ENVIROMENT IN SMART CITIES

The paper explores methods for constructing wireless sensor networks (WSNs) for urban environment monitoring. Various approaches to adaptive network management, cluster head selection, and routing optimization are analyzed.

Безпроводові сенсорні мережі (БСМ) є ключовим елементом розумного міста, забезпечуючи автоматизований моніторинг параметрів середовища (якість повітря, шум, освітлення, трафік тощо) у реальному часі [1]. Вони дозволяють оперативно виявляти відхилення та небезпечні ситуації, що сприяє швидкому реагуванню міських служб.

Для підвищення надійності та енергоефективності БСМ застосовуються:

- Ланцюгові структури: протокол PEGASIS мінімізує одночасні передачі, зменшуючи енергоспоживання [2].
- Кластеризація: вузли групуються в кластери, а головний вузол збирає та передає дані. Протокол LEACH передбачає випадковий вибір голови кластера [3].
- Маршрутизація: у БСМ використовується багатохопова передача даних. Протокол Directed Diffusion дозволяє мінімізувати зайвий трафік, використовуючи запити «інтересів» [4].
- Енергозберігаючі алгоритми: MAC-протокол S-MAC вводить цикли «сон-пробудження», продовжуючи час роботи вузлів [5].
- Агрегація даних: об’єднання кількох вимірювань у один пакет зменшує навантаження на мережу.

Для вирішення зазначених проблем запропоновано новий метод побудови БСМ моніторингу міського середовища, який поєднує адаптивну кластеризацію, багатохопову маршрутизацію та енергозберігаючі алгоритми. Основна ідея – динамічно пристосовувати структуру мережі до поточного стану вузлів і умов оточення, щоб досягти балансу між енергоефективністю та надійністю. Алгоритм функціонує циклічно. На початку кожного циклу кожен сенсорний вузол оцінює кілька параметрів:

- власний рівень залишкової енергії,

- якість каналу зв’язку зі сусідами (враховуючи можливі міські перешкоди) та
- щільність сусідніх вузлів.

На основі цих метрик вузли самостійно обчислюють ймовірність стати головою кластера в даному циклі (подібно до LEACH, але з урахуванням додаткових факторів).

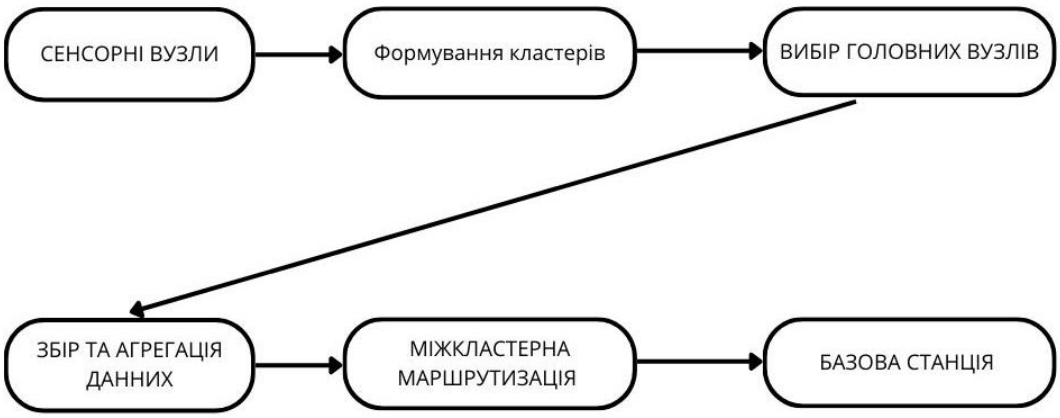


Рис.1. Структурна схема адаптивної кластеризованої БСМ.

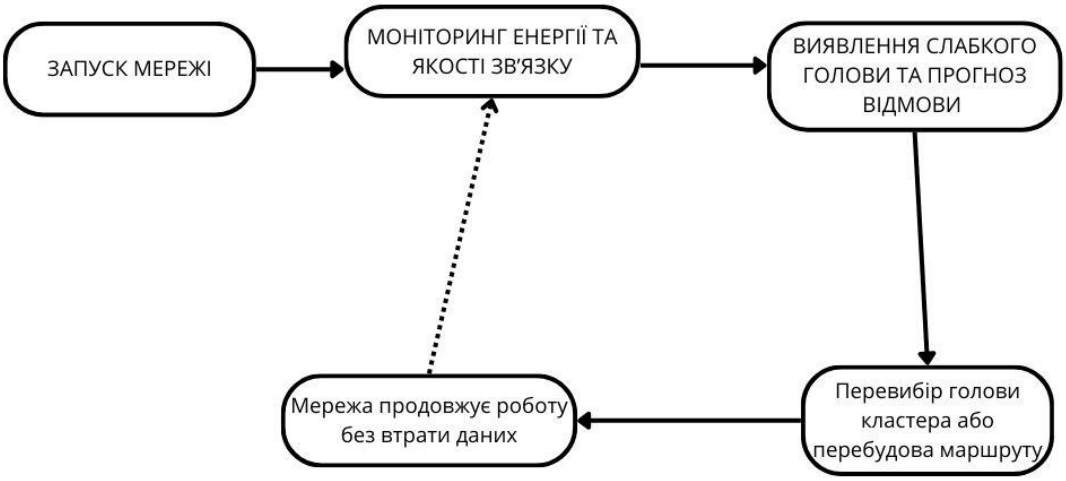


Рис.2. Живучість мережі та стійкість до відмов.

Ймовірність вибору голови кластера розраховується за наступною формулою:

$$P_i = P_o \left(w_E \frac{E_i}{E_{avg}} + w_Q \frac{Q_i}{Q_{avg}} + w_N \frac{N_i}{N_{avg}} \right)$$

де:

- P_i — ймовірність обрання вузлом і головою кластера;
- P_0 — базова ймовірність;
- E_i, Q_i, N_i — залишкова енергія, якість зв'язку та щільність для вузла і;
- $E_{avg}, Q_{avg}, N_{avg}$ — середні значення по мережі;

- w_E, w_Q, w_N — вагові коефіцієнти.

Переваги методу:

- Збільшення часу життя мережі: рівномірний розподіл енергоспоживання та зменшення витрат енергії на кожну передачу.
- Підвищена надійність: мережа функціонує навіть при виході з ладу окремих вузлів.
- Зменшення навантаження на мережу: агрегація даних знижує обсяг переданої інформації.

Для підвищення стійкості мережі вводиться механізм резервування: кожен кластер обирає «заступника» голови – вузол, що матиме роль головного у разі виходу основного з ладу. Крім того, в межах кластера застосовано часовий поділ доступу: вузли передають дані голові у визначені тайм-слоти, залишаючись у сплячому режимі в інший час. Це додатково знижує витрати енергії. Запропонований алгоритм працює в децентралізованому режимі (кожен вузол сам приймає рішення на основі локальної інформації), що важливо для масштабованості в умовах великого міста.

Запропонований метод дозволяє створювати більш ефективні, довговічні та надійні БСМ для моніторингу міського середовища, забезпечуючи стійкість до збоїв та зменшуючи потребу в обслуговуванні. Таким чином, запропонований метод сприяє створенню ефективних БСМ для розумних міст, покращуючи моніторинг середовища та оптимізуючи використання енергоресурсів.

Література

1. Akyildiz I.F., Su W., Sankarasubramaniam Y., Cayirci E. Wireless Sensor Networks: A Survey / I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci // Computer Networks. – 2002. – Vol. 38, No. 4. – P. 393–422.
2. Rashid B., Rehmani M.H. Applications of Wireless Sensor Networks for Urban Areas: A Survey / B. Rashid, M.H. Rehmani // Journal of Network and Computer Applications. – 2016. – Vol. 60. – P. 192–219.
3. Heinzelman W.B., Chandrakasan A.P., Balakrishnan H. An Application-Specific Protocol Architecture for Wireless Microsensor Networks / W.B. Heinzelman, A.P. Chandrakasan, H. Balakrishnan // IEEE Transactions on Wireless Communications. – 2002. – Vol. 1, No. 4. – P. 660–670.
4. Intanagonwiwat C., Govindan R., Estrin D., Heidemann J., Silva F. Directed Diffusion for Wireless Sensor Networking / C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, F. Silva // IEEE/ACM Transactions on Networking. – 2003. 5. – Vol. 11, No. 1. – P. 2–16.

Ye W., Heidemann J., Estrin D. Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks / W. Ye, J. Heidemann, D. Estrin // IEEE/ACM Transactions on Networking. – 2004. – Vol. 12, No. 3. – P. 493–506.

УДК 621.391

АНАЛІЗ ТЕХНОЛОГІЙ ТА ПРОТОКОЛІВ ФІЗИЧНОГО ТА КАНАЛЬНОГО РІВНЯ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ

Семенюк Ю.С., Носков В.І.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: semeniukyulianka333@gmail.com

TECHNOLOGIES AND PROTOCOLS OF PHYSICAL AND DATA LINK LAYERS ANALYSIS FOR INTERNET OF THINGS NETWORKS

The main technologies and protocols of the physical and data link layer of the Internet of Things (IoT) networks are considered. Their features, challenges, and limitations are analyzed, and a comparative analysis is performed to determine the optimal solutions for different application scenarios. The results based on modeling of IoT networks in Cisco Packet Tracer are presented and recommendations for choosing technologies depending on the needs of users are provided.

Розглянуто основні технології та протоколи фізичного та канального рівнів мереж Інтернету речей (IoT). Проаналізовано їх особливості, проблеми та обмеження, проведено порівняльний аналіз для визначення оптимальних рішень для різних сценаріїв застосування. Представлено результати, отримані на основі моделювання мереж IoT в Cisco Packet Tracer, та надано рекомендації щодо вибору технологій в залежності від потреб користувачів.

Зростання популярності IoT стимулює розвиток технологій зв’язку. особливо на фізичному та канальному рівнях. Ефективність IoT-мереж залежить від характеристик обраних стандартів і протоколів. Дослідження цих аспектів дозволяє визначити оптимальні рішення для стійких IoT-систем.

Архітектура IoT-мереж має рівневу модель: фізичний рівень відповідає за передачу сигналів, а канальний — за з’єднання вузлів і контроль доступу. Основні виклики – обмежені ресурси пристроїв, енергоспоживання, безпека та масштабованість.

Фізичний рівень охоплює LPWAN (LoRa, Sigfox, NB-IoT, LTE-M), BLE, Zigbee, Z-Wave, Wi-Fi, 4G, 5G. Канальний рівень включає стандарти IEEE 802.15.4 (Zigbee, Thread, 6LoWPAN), IEEE 802.11 (Wi-Fi), LPWAN-протоколи (LoRaWAN, Sigfox).

Вибір технологій та протоколів залежить від дальності зв’язку, швидкості передачі, енергоспоживання та умов застосування. Наприклад, для розумного міста важлива велика зона покриття та низьке енергоспоживання,

тоді як у промисловості пріоритетом є надійність і швидкість передачі. Нижче наведено порівняльний аналіз технологій та протоколів IoT для різних сценаріїв використання:

Таблиця 1. Порівняльний аналіз технологій IoT.

Технологія/ Протокол	Дальність зв'язку	Швидкість передавання даних	Енергоспоживання	Тип мережі
LoRaWAN	До 15 км	0.3-50 Кбіт/с	Низьке	LPWAN
NB-IoT	До 10 км	20-250 Кбіт/с	Середнє	LPWAN
Sigfox	До 50 км	0.1 Кбіт/с	Низьке	LPWAN
Zigbee	До 100 м	20-250 Кбіт/с	Середнє	PAN (персональна мережа)
Wi-Fi	До 100 м	До 9.6 Гбіт/с	Високе	WLAN (локальна мережа)
5G	До 1 км	До 10 Гбіт/с	Високе	Мобільна мережа

Аналіз технологій показує, що:

1. LoRaWAN та NB-IoT підходять для масштабованих IoT-мереж з низьким енергоспоживанням.

2. Zigbee та BLE використовуються для локальних сенсорних мереж.

3. Wi-Fi та 5G забезпечують високу пропускну здатність, але споживають більше енергії.

Для різних сценаріїв застосування оптимальними є різні рішення: деякі технології краще підходять для розгортання у масштабних мережах із низьким енергоспоживанням, тоді як інші забезпечують високу швидкість передавання даних, що критично для промислових застосувань.

Для оцінки ефективності технологій та протоколів фізичного та канального рівня була досліджена модель IoT-мережі розумного будинку, створеної у Cisco Packet Tracer. У моделі інтегровані розумні лампи, датчики руху, IP-камери, термостат і дверні замки, що взаємодіють через Wi-Fi, Zigbee та MQTT. IoT-контролер керує пристроями та забезпечує їх зв'язок.

Wi-Fi використовується для основних IoT-пристроїв, Zigbee – для малопотужних сенсорів, а MQTT оптимізує обмін даними з хмарним сервером. Моделювання показало, що Zigbee енергоефективний, але має обмежений радіус дії, Wi-Fi забезпечує швидку передачу даних, а MQTT мінімізує затримки.

На рис. 1 представлена схема IoT-мережі, що ілюструє використані технології.

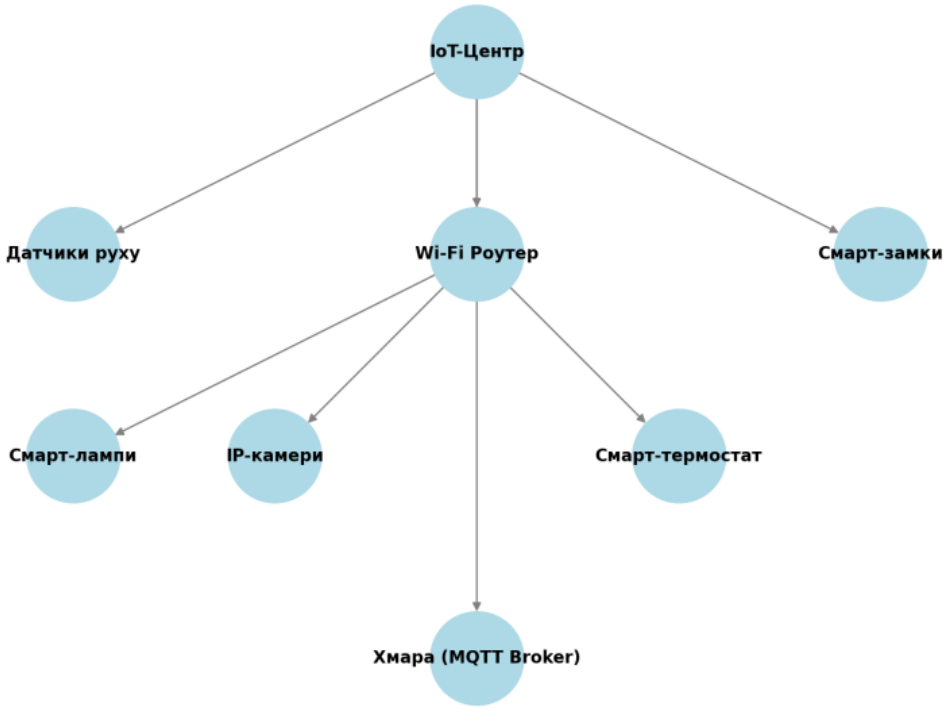


Рис.1. Схема IoT-мережі для розумного будинку.

Результати підтверджують, що комбінація Wi-Fi, Zigbee та MQTT забезпечує баланс між швидкістю, енергоефективністю та стабільністю з’єднання.

Література

1. Harari, Y. N. Homo Deus: A Brief History of Tomorrow / Yuval Noah Harari. – London: Vintage, 2017. – 513 p.
2. Gislason, D. Zigbee Wireless Networking / Drew Gislason. – Burlington: Newnes, 2008. – 344 p.
3. Heydon, R. Bluetooth Low Energy: The Developer's Handbook / Robin Heydon. – Upper Saddle River: Prentice Hall, 2013. – 368 p.
4. Hillar, G. C. MQTT Essentials: A Lightweight IoT Protocol / Gastón C. Hillar. – Birmingham: Packt Publishing, 2017. – 178 p.
5. Hersent, O., Boswarthick, D., Elloumi, O. The Internet of Things: Key Applications and Protocols / Olivier Hersent, David Boswarthick, Omar Elloumi. – Chichester: Wiley, 2012. – 360 p.
6. Cirani, S., Ferrari, G., Picone, M., Veltri, L. Internet of Things: Architectures, Protocols and Standards / Simone Cirani, Gianluigi Ferrari, Marco Picone, Luca Veltri. – Chichester: Wiley, 2018. – 250 p.

УДК 004.9+629.8:004.89

ОБГРУНТУВАННЯ ЕФЕКТИВНОСТІ ПОЄДНАННЯ БСМ ТА БПЛА ДЛЯ ВЕДЕННЯ МОНІТОРИНГУ НА РУХОМІЙ ПЛАТФОРМІ В ЗОНІ БОЙОВИХ ДІЙ

Карпенко М. І., Чумаченко С.М., Мошенський А.О.
Національний університет харчових технологій, Україна
E-mail: sapta@ukr.net

JUSTIFICATION OF THE EFFECTIVENESS OF COMBINING WSN AND UAV FOR MONITORING IN THE COMBAT ZONE

The effectiveness of using WSN and UAVs for the purpose of monitoring CWA and radiation is substantiated. Solutions to the problems of monitoring the combat zone are proposed.

Враховуючи схильність російських військ порушувати домовленості та використовувати заборонені бойові отруйні речовини (БОР), а також обстрілювати цивільні об’єкти, постає актуальність проблеми виявлення небезпечних речовин. Враховуючи воєнний стан, більшість даних про стан РХБ (радіологічної, хімічної та біологічної) розвідки у ЗСУ лишається закритою. З доступної інформації відомо, що більшість зразків техніки представляють собою старі радянські пристрої індивідуальної та стаціонарної дозиметрії та детектування БОР [1]. Наразі відомо про досягнення вітчизняних виробників, що представляють не тільки нові моделі БПЛА, а й високоточну, надійну техніку детектування, наприклад, марки ЕКОТЕСТ. Про використання такої техніки наразі відомо мало. Однак, загалом такі пристрої детектування кріпляться зовні транспортних засобів та сповіщають виключно екіпаж про стан навколишнього середовища. Щодо ДСНС, то служби реагування використовують весь арсенал наявних засобів [2], що може різнитися від підрозділу. Основну частку спорядження детектування ДСНС складають ручні та стаціонарні пристрої, а також сенсори на постах спостереження і об’єктах критичної інфраструктури.

Переважна більшість описаної вище техніки не передбачає надсилання даних, а та, що передбачає, робить це через Bluetooth або Wi-Fi мережу. З огляду на досвід блекаутів, марно покладатися на стабільну роботу стільникової мережі або мережі Internet в зоні повного відключення електроенергії (окрім деяких об’єктів критичної інфраструктури). Черговим обмеженням буде відсутність постійного джерела живлення, що впливатиме на час роботи пристроїв.

Проблеми живлення та відсутності покриття вирішує радіозв’язок. Безпровідні сенсорні мережі (БСМ) на діапазоні ультракоротких хвиль (УКХ) забезпечують комутацію пристроїв на великих дистанціях. Технологія LoRa для БСМ забезпечує низьке енергоживлення для сенсорів та радіомодулів. Протокол LoRaWAN дозволяє створити незалежну архітектуру БСМ, що

передаватиме дані через різні рівні пристроїв до бази даних (БД) на віддаленому або хмарному сервері, де буде проводитись аналітична обробка.

Ефективність такого способу доводить компанії на кшталт Actility чи Abeeway, DXC Technology, Elbit Systems, Hanwha Group, L3Harris і Leonardo [3], тощо, що представили ідею LoRaWAN трекерів для військових потреб, а саме забезпечення додаткового каналу зв'язку (персональних та групових SMS), відстеження координат військовослужбовця, тощо. IoT (Internet of things) мережі активно застосовуються в інших країнах, наприклад, у Франції та США [4].

Впровадження системи моніторингу на основі БСМ IoT вирішить проблему енергоефективності та відсутності покриття стільникових мереж. Однак БСМ зазвичай є заздалегідь розміщеними стаціонарними об'єктами. Використання різного роду БПЛА (в основному коптерного типу) забезпечить рухомість блоку детектування та, водночас, безпеку для оператора, адже до цього небезпечні дози речовин чи випромінення виявляють ручними детекторами або зафіксованими на наземному транспорті приладами індикації. Топологія LoRaWAN сприяє створенню стійкої мережі, в якій БПЛА з блоками виявлення БОР та дозиметрами будуть водночас ретрансляторами і покриватимуть широкі території. БПЛА типу гібридний дрон (літак-мультикоптер) здатні розвідувати важкодоступні для людини та наземного транспорту місця, а також оперативно повертатися в разі потреби за рахунок високої швидкості, малої ваги та невеликих габаритів.

При всіх перевагах використання БПЛА та БСМ виникає проблема мобільності та передачі даних в хмарне середовище. Існує можливість збирати дані локально і обробляти їх на місці, однак для надсилання даних до оперативного штабу потрібна оперативна закрита мережа типу military Internet.

Для вирішення цієї проблеми пропонується ідея мобільної платформи, що використовуватиме переваги БПЛА та БСМ і буде ефективною у використанні як цивільними службами (ДСНС), так і військовими ЗСУ. Ідея полягає у встановленні на транспортний засіб супутникової інтернет-системи. Starlink не є єдиним представником такої системи, але він найбільш відомий, широко розповсюджений і легкий для налаштування серед аналогів. Супутникова мережа буде розгорнута всередині фургону з відкидним дахом. Супутниковий маршрутизатор автоматично налаштується на найближчі супутники що є на орбіті і через точку доступу будуть надсилатися дані з БПЛА, що надійшли через радіоканал ретрансляторе.

Постає нова проблема у вигляді ворожої розвідки, яка легко фіксує мережу Starlink і наводить артилерію чи ударні дрони в її сектор. Для вирішення цієї проблеми варто звернутися до радіотехніки. Wi-Fi працює на частотах 2,4 ГГц та 5 ГГц, що відповідає довжинам хвиль приблизно 12,5 см та 6 см відповідно. Для обмеження поширення Wi-Fi сигналу в межах конкретного простору, наприклад, фургона, можна застосувати методи екранування. Екранування передбачає використання матеріалів, які блокують або поглинають радіохвилі, запобігаючи їх виходу за межі бажаної зони. Для

блокування поширення хвиль Wi-Fi умовною кліткою Фарадея, нам знадобиться формула глибини проникнення skin-depth: $\delta = \frac{\sqrt{2}}{\omega\mu\sigma}$, де $\omega=2\pi f$ – кутова частота, μ – магнітна проникність матеріалу (для немагнітних матеріалів близько $\mu 0=4\pi\times10-7$ Гн/м), σ–електропровідність. Для екранування підійдуть матеріали: мідь, алюміній, фольга, тощо. У випадку міді лист товщиною 4–7 мікрон забезпечить повне екранування сигналу Wi-Fi. Для забезпечення високої ступені заглушення сигналу зазвичай застосовують матеріал із товщиною приблизно у 3–5 разів більшу за δ. Оскільки частота f_1 = 2.4ГГц та f_2 = 5ГГц відповідно, то для f_1 $\omega \approx 2\pi * 2.4 * 10^9 \approx 15{,}08 * 10^9$ рад/с, $\delta \approx$ 1,35 мікрон; для f_2 $\omega \approx 2\pi * 5 * 10^9 \approx 31{,}42 * 10^9$ рад/с , $\delta \approx$ 0,93 мікрон.

Оскільки радіо модулі працюють на УКХ діапазоні, то їхня довжина хвилі більша порівняно з Wi-Fi, через що вони здатні краще проникати через перешкоди (в т.ч. металеві) і зазнавати меншого послаблення сигналу. Саме тому ретранслятор IoT може спокійно знаходитись як зовні, так і всередині транспортного засобу.

Висновки: Було обґрунтовано використання БСМ та БПЛА з метою моніторингу БОР та радіації. Розглянуто проблеми зони бойових дій, а саме відсутність стабільного електроживлення, відсутності покриття стільникових мереж та інтернету, небезпеку виявлення сигналу точки доступу ворожою радіорозвідкою. Запропоновано рішення у вигляді екранованого транспортного засобу, який прибуватиме на місце проведення моніторингу, розгортатиме мережу супутникового інтернету і збиратиме дані за допомогою БПЛА гібридного типу з блоками детектування через УКХ радіоканал. Потребує подальшого дослідження проблема втрати радіосигналу через гіпотетичне потрапляння в зону дії станції активних перешкод (постановника завад «глушилки»).

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. Коваль М. С. Дії підрозділів ДСНС України в умовах воєнного стану. Львів : ЛДУ БЖД, 2023. 306 с. URL: https://dsns.gov.ua/upload/1/9/2/4/3/5/9/diyi-dsns-objednana-kniga-compressed.pdf.
3. IoT Army Companies, Service Providers & Solutions | IoT Military. Army Technology. URL: https://www.army-technology.com/buyers-guide/leading-iot-companies-military/ (date of access: 20.03.2025).
4. IoT Transforming Defence Systems and Military Operations. Product Engineering Company | IoT App Development Company | HashStudioz Technologies. URL: https://www.hashstudioz.com/blog/iot-defence/ (date of access: 20.03.2025).

УДК 621.39

ПОБУДОВА СИСТЕМИ РЕТРАНСЛЯЦІЇ З ВИКОРИСТАННЯМ ВИСОКОЕФЕКТИВНИХ АНТЕН ДЛЯ ЗВ'ЯЗКУ В УМОВАХ НАДЗВИЧАЙНОГО СТАНУ

Сергієнко М.І., Федотов К.Ю., Кирпич М.С., Кононов А.О.
Радіотехнічний клуб «ПОЛІТЕХНІК» UT7UZA,
КПІ ім. Ігоря Сікорського, Україна
E-mail: ut3upy@gmail.com

CONSTRUCTION OF A RETRANSMISSION SYSTEM USING HIGH-EFFICIENCY ANTENNAS FOR COMMUNICATION IN EMERGENCY CONDITIONS

The paper presents a model of an autonomous branched relay system with the integration of base stations using an analog radio bridge for use in conditions of lack of power supply and other

За основу було взято принцип ретрансляції ультракороткохвильового сигналу з дуплексним розносом частот. Створено дуплексний ретранслятор на основі стаціонарних радіостанцій Motorola, використано дуплексний фільтр, антенну решітку на основі петлевих вібраторів з високим коефіцієнтом підсилення та обладнання для забезпечення безперебійного електроживлення.

Після випробувань роботи одиночного ретранслятора, розташованого в центральній частині міста, дійшли до висновку, що ми отримали недостатній радіус покриття. Беручи до уваги гірський рельєф та багатоповерхову забудову столиці, було прийнято рішення побудови розгалуженої системи, яка буде складатися з двох ретрансляторів. Також було проведено порівняння теоретичного розрахунку зони покриття одиночного ретранслятора і спільної зони покриття розгалуженої системи з використанням ПЗ Radioplanner 3.0.

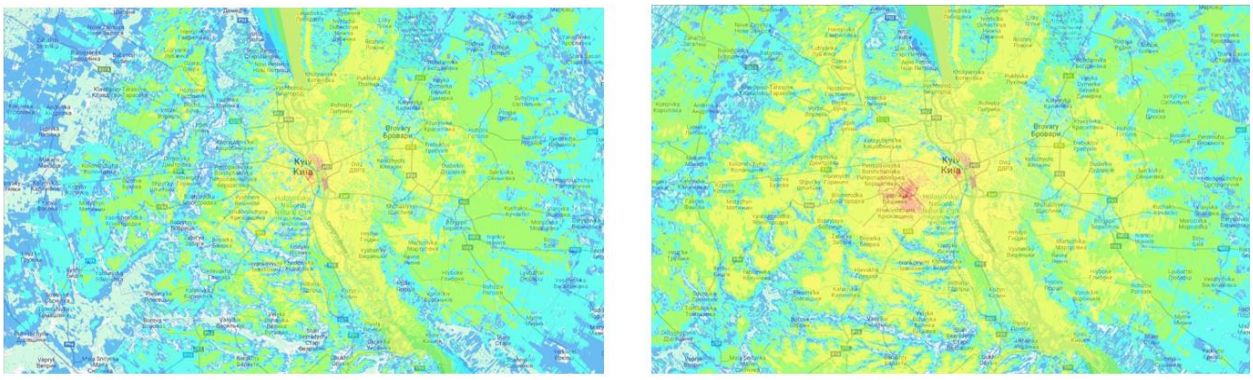


Рис.1. Порівняння зон покриття одиничного ретранслятора та розгалуженої мережі.

Отримано наступні дані, що вказані на мапі (жовта зона – впевнений прийом з рівнем сигналу не менше -105 dBm, синя зона – невпевнений прийом з рівнем сигналу менше-105 dBm). У розрахунок було закладено модель зв'язку з ретранслятором на портативну радіостанцію з висоти людського росту 1.75 м від рівня землі.

Оскільки основним завданням було створення автономної системи, яка може працювати під час довготривалих відключень електроенергії, було прийнято рішення налагодити зв'язок між базовими станціями через окремий радіоканал. Також цей технологічний канал не мав би створювати радіозавад основним приймачам базових станцій, оскільки передавач технологічного каналу має працювати одночасно з основним обладнанням.

Для цього було вжито наступних заходів: у тракти приймачів ретрансляторів було включено смугопропускаючі фільтри на основі об’ємних резонаторів, потужність передавача технологічного каналу була встановлена на рівні 3 Вт.

Головним чинником для забезпечення електромагнітної сумісності було створення антен технологічного «радіомосту» спрямованої дії з досить вузькою діаграмою спрямованості. За основу було взято конструкцію антени Уда – Ягі.

Ключовою задачею було сконцентрувати малу потужність передавача у певному напрямку, щоб якісно передати сигнал від одного ретранслятора до іншого, при цьому не створивши перешкод для роботи основного приймального тракту базової станції. Для моделювання антен радіомосту було використано ПЗ MMANA-GAL.

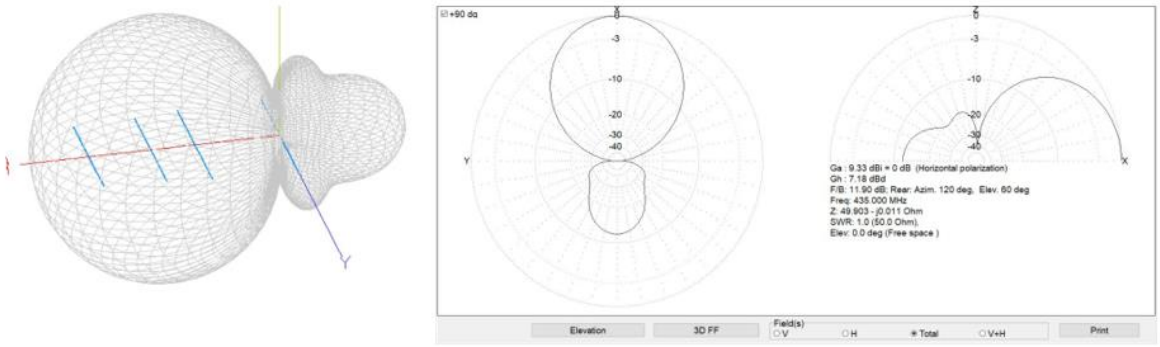


Рис.2. Моделювання діаграми спрямованості антени.

Антени було виготовлено і встановлено на об’єктах розміщення ретрансляторів з віднесенням їх на достатню відстань від основних антен базових станцій, а саме: 14λ по горизонталі та 10λ по вертикалі.

Рис.3. Виготовлення і встановлення антен радіомосту.

Основне антено-фідерне обладнання ретрансляторів було встановлено на двох точках:

1. В центрі міста на висоті 55 м від рівня землі та загальній висоті 260 м над рівнем моря;

2. На південно-західній околиці міста на висоті 50 м від рівня землі та загальній висоті 220 м над рівнем моря.

Для забезпечення каналу зв’язку між ретрансляторами у їх конструкцію було додано ще одну радіостанцію, котра була приєднана до основного обладнання.

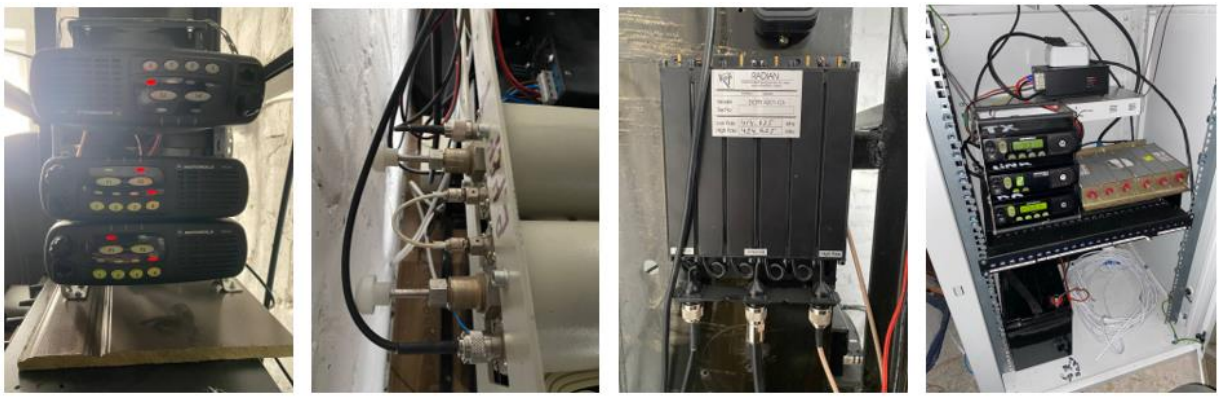


Рис.4. Обладнання розгалуженої системи ретрансляції.

Після встановлення та налагодження системи було розпочато натурні випробування: вимірювання рівня сигналу технологічної лінії зв’язку за допомогою вбудованого в портативну радіостанцію Motorola DP-4800 індикатора, підключаючи її до спрямованої антени зв’язку між базовими станціями. Було зафіксовано рівень сигналу – 88,7 dBm при рівні шуму – 118,5 dBm, що є достатнім для якісного зв’язку між ретрансляторами.

Таким чином, за допомогою впровадження аналогового радіомосту направленої дії нам вдалося побудувати автономну систему ретрансляції, здатну працювати в умовах перебоїв електропостачання та відсутності іншої інфраструктури. Відмічено високу ефективність використання розгалуженої мережі в порівнянні з одиночним ретранслятором. Якість зв’язку та радіус покриття збільшено майже вдвічі. Силами радіотехнічного клубу «Політехнік» UT7UZA розроблено і впроваджено дану систему в реальних умовах, введено необхідні технічні рішення для забезпечення її коректної роботи.

Література

1. Repeater Builder® https://www.repeater-builder.com/rbtip/index.html
2. К.Ротхаммель. «Антени», Том 1 (Видання 11, виправлене). Видавництво «ЛАЙТ Лтд», - с. 91-94.
3. В.Г.Шолудько, М.Ю.Єсаулов, О.В.Вакуленко, Т.Г.Гурський, М.М.Фомін «Організація військового зв’язку» Навчальний посібник, Київ - 2017, - с. 46-48.

УДК 621.39

ДОСЛІДЖЕННЯ ГОРИЗОНТАЛЬНОЇ АНТЕНИ ІЗ ЗМІЩЕНИМ ВІД ЦЕНТРУ ЖИВЛЕННЯМ

Єпіхін Д.О., Ятченко М.А.
Радіотехнічний факультет КПІ ім. Ігоря Сікорського, Україна
Радіоклуб «Політехнік» КПІ ім. Ігоря Сікорського, Україна
E-mail: epihin80@gmail.com

INVESTIGATION OF A HORIZONTAL OFF-CENTER-FED ANTENNA

The research is devoted to analyzing the design of a horizontal off-center-fed antenna (OCF) intended to ensure stable operation on several amateur radio bands. This topic has both historical significance, as the design was first published in QST magazine in 1925, and modern relevance for providing a simple multi-band solution for field or stationary conditions.

У цій роботі представлено результати дослідження конструкції горизонтальної антени зі зміщеним від центру живлення (off-center-fed, OCF), яка призначена для стабільної експлуатації на кількох аматорських діапазонах. Актуальність теми зумовлена як історичною значущістю первинної публікації у журналі QST (1925 р.), так і сучасним запитом на багато діапазонні антени зі спрощеними узгоджувальними характеристиками для стаціонарних або польових умов.

Мета дослідження полягає у визначенні особливостей роботи OCF-антен із урахуванням різних висот підвісу та параметрів ґрунту, а також у розробленні конструкції, придатної для ефективного функціонування на діапазоні 80 м і його гармоніках (40, 20, 15, 12, 10 м). Додатково проаналізовано поширені у літературі та комерційних джерелах варіанти OCF-антен з метою виявлення їхніх переваг і недоліків.

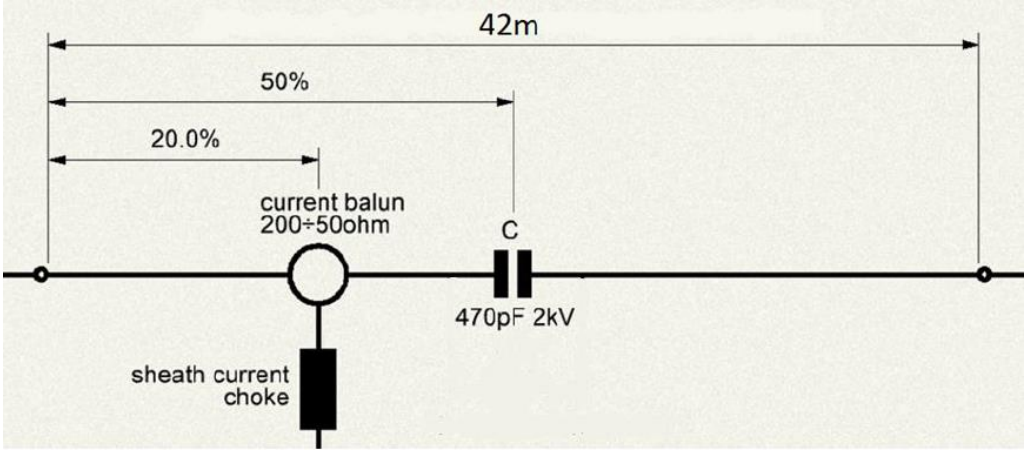


Рис.1. Схематичне зображення моделі антени зі зміщеним від центру живленням.

Антени моделювалися за допомогою програмного забезпечення 4nec2, що реалізує метод моментів із урахуванням реальних параметрів землі. Усього було змодельовано 36 антено-фідерних систем, розрахованих на резонансні частоти 3,5 та 3,55 МГц і різні висоти підвісу (10, 12, 15, 18, 20 м) над ґрунтом із трьома типами діелектричних властивостей (good, average, poor). Як матеріал випромінювача використовувався мідний дріт діаметром 2 мм з автосегментацією не менше ніж 41 сегмент, що забезпечувало необхідну точність. Для кожної моделі визначали оптимальну точку підключення фідера (опція Sweep) та розраховували коефіцієнт стоячої хвилі (КСХ) на діапазонах 80, 40, 20, 15 і 10 м за обраними еталонними частотами.

За результатами моделювання виявлено, що традиційні конструкції OCF-антен, роз-раховані на резонанс у діапазоні 80 м, мають недостатній рівень ефективності на вищих частотах унаслідок розбіжностей у резонансних довжинах. У середньому для 80 м необхідно ~40,2 м, тоді як для гармонік оптимальним виявився розмір ~42 м. Через цю різницю (~1,8 м) неможливо досягнути прийнятного компромісу, що задовольняв би усі цільові діапазони одночасно.

Для розв’язання виявленої проблеми запропоновано інженерне рішення, що полягає у збереженні довжини антени на рівні 42 м, оптимальної для вищих частот, та застосуванні електричного укорочення для 80-метрового діапазону за допомогою конденсатора, уведе-ного в центральну частину полотна. На частоті 3,6 МГц цей конденсатор компенсує надмірну індуктивність, не погіршуючи роботу антени на гармоніках, адже у центральній точці на високих частотах струм є мінімальним, і вплив конденсатора стає незначним.

Важливим етапом дослідження було також визначення оптимальної точки живлення відносно центру. Чисельний аналіз показав, що стабільне узгодження для різних висот і типів ґрунту досягається за зміщенням живлення на 20% від загальної довжини антени (тобто на 1/5 від кінця).

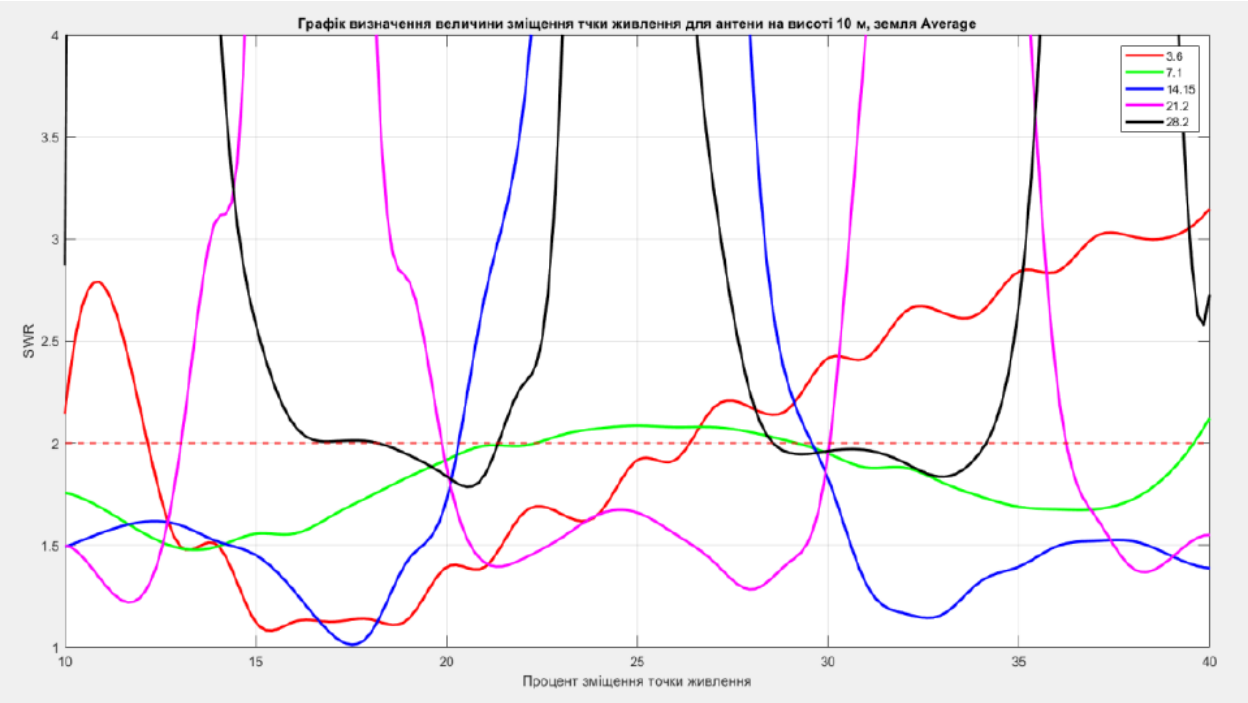


Рис.2. Графік визначення величини зміщення точки живлення для антени на висоті 10м.

На прикінцевому етапі побудовано вісім моделей антени завдовжки 42 м, зі зміщенням точки живлення 20% та різними значеннями конденсатора. Усі моделі було протестовано у середовищі 4nec2, отримані значення КСХ засвідчили стабільну роботоздатність антени на аматорських діапазонах 80, 40, 20, 15, 12 та 10 м.

Експериментальна перевірка здійснювалася на прототипі з конденсатором 560 пФ, встановленому на даху між корпусами № 22 та № 23 НТУУ «КПІ імені Ігоря Сікорського», з середньою висотою підвісу ~16 м. Значення КСХ, виміряні антенним аналізатором, не перевищували 2 на всіх цільових діапазонах, що підтвердило релевантність теоретичних результатів.

Таким чином, проведене дослідження засвідчило доцільність і ефективність застосування удосконаленої OCF-антени для багатодіапазонного використання без додаткових узгоджувальних пристроїв. Запропонована конструкція відзначається відносною просто-тою виготовлення, зручністю під час експлуатації та може бути рекомендована радіоаматорам як універсальне рішення для стаціонарних або польових умов.

Література

1. Howard M. Williams, "The Hertz Antenna at 20 and 40 Meters", QST. – 1925. – № 7. – С. 24-25.
2. Loren G. Windom, "Notes on Ethereal Adornments", QST. – 1929. – № 9. – С. 19–21.
3. Fritz Spillner, DJ2KY, "Windom Antenna Modification", 1971.

УДК 621.382

АНАЛІЗ АРХІТЕКТУРИ, ТЕХНОЛОГІЙ І ВИКЛИКІВ ЛІТАЛЬНИХ AD HOC МЕРЕЖ

Валуйський С.В., Пономаренко О.М.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: ponomarenko.alexandra@lll.kpi.ua, valuiskyi.stanislav@lll.kpi.ua

ANALYSIS OF THE ARCHITECTURE, TECHNOLOGIES AND FUTURE CHALLENGES OF FLYING AD HOC NETWORKS

This work is focused on analyzing the architecture, technologies, and challenges of Flying Ad Hoc Networks (FANETs). The study involves a detailed examination of the network structure, routing protocols, wireless communication technologies, and the main technical and security challenges faced by FANETs. The research also explores potential solutions to improve the efficiency and reliability of these networks.

Літальні Ad Hoc мережі (FANETs) є динамічними мережами, що складаються з безпілотних літальних апаратів (БПЛА), які можуть самоорганізовуватися для виконання різноманітних завдань. Вони знаходять застосування у військовій, цивільній та комерційній сферах, зокрема для моніторингу, пошуково-рятувальних операцій, доставки вантажів та інших задач. Основною перевагою FANETs є їхня здатність працювати в умовах, де традиційні мережі недоступні або неефективні.

Мета роботи. Основна мета роботи полягає в аналізі архітектури, технологій та викликів літальних Ad Hoc мереж. Для цього використовуються дослідження архітектурних рішень, протоколів маршрутизації, технологій бездротового зв'язку та основних проблем, пов'язаних із функціонуванням FANETs.

Огляд архітектури, технологій та викликів FANETs [1-6].

1. Архітектура FANETs. FANETs можуть мати різні типи архітектур, включаючи централізовану, децентралізовану та гібридну. Централізована архітектура передбачає наявність головного вузла, який керує всіма іншими БПЛА. Децентралізована архітектура дозволяє кожному вузлу приймати самостійні рішення, що підвищує гнучкість мережі. Гібридна архітектура поєднує переваги обох підходів.

2. Технології бездротового зв'язку. Для зв’язку між БПЛА використовуються Wi-Fi, Bluetooth, Zigbee, LTE/5G, LoRaWAN та спеціалізовані радіопротоколи. LPWAN (Low Power Wide Area Network) є перспективним варіантом для енергоефективного зв’язку дронів, особливо у

віддалених районах, оскільки забезпечує зв’язок на великі відстані з низьким енергоспоживанням.

3. Протоколи маршрутизації. Ефективна маршрутизація є ключовим аспектом функціонування FANETs. Використовуються:

- Проактивні протоколи (OLSR, DSDV) – швидке реагування, але високе використання смуги пропускання через постійне оновлення таблиць маршрутів.
- Реактивні протоколи (AODV, DSR) – економія ресурсів, оскільки маршрути встановлюються лише за потреби, однак може збільшуватися затримка через необхідність їхнього пошуку.
- Гібридні протоколи (ZRP, HWMP) – поєднують переваги обох підходів, наприклад, використовують проактивний метод для локальних вузлів і реактивний – для віддалених.

4. Технічні виклики. FANETs стикаються з низкою технічних викликів, таких як обмежена енергоємність БПЛА, висока мобільність вузлів та нестабільність зв'язку. Для подолання цих проблем використовуються методи оптимізації енергоспоживання, динамічного маршрутизації та покращення якості зв'язку.

5. Забезпечення безпеки. Оскільки FANETs часто використовуються для передачі конфіденційних даних, питання безпеки є критичним. Методи шифрування, аутентифікація вузлів і захист від атак відіграють ключову роль у надійності мережі. Зокрема, розглядається використання блокчейн-технологій (Aerial Blockchain) для захисту зв’язку між дронами, що дозволяє створювати децентралізовану та стійку до атак систему автентифікації та перевірки цілісності даних.

6. Інтеграція з іншими мережами. FANETs можуть бути інтегровані з іншими типами мереж, такими як IoT (Internet of Things) та VANETs (Vehicular Ad Hoc Networks). Це дозволяє створювати комплексні системи, здатні вирішувати складніші завдання, такі як моніторинг великих територій або управління транспортними потоками. Інтеграція з IoT дозволяє використовувати дані з різних джерел для покращення ефективності роботи мережі.

Висновок. Робота спрямована на аналіз архітектури, технологій та викликів літальних Ad Hoc мереж. Дослідження показало, що FANETs мають великий потенціал для використання у різних сферах, однак їх ефективне функціонування вимагає подолання низки технічних та організаційних проблем.

Аналіз показав, що гібридна архітектура є оптимальним варіантом, оскільки вона поєднує централізоване управління та автономність вузлів, що підвищує гнучкість та масштабованість FANETs. Гібридні протоколи маршрутизації демонструють найкращу ефективність в умовах динамічної топології мережі.

Для забезпечення стабільного зв'язку в умовах високої мобільності FANETs найбільш перспективними є LTE/5G та спеціалізовані радіопротоколи. Додатково, використання Wi-Fi, Bluetooth 5 та LPWAN дозволяє покращити ефективність енергоспоживання.

Важливим напрямком є безпека FANETs, де сучасні криптографічні методи, аутентифікація вузлів та технологія Aerial Blockchain дозволяють підвищити рівень захищеності переданих даних.

Перспективи подальших досліджень включають:

- Інтеграцію FANETs з IoT та VANETs для створення більш комплексних систем.
- Використання штучного інтелекту для автономного управління мережею.
- Впровадження квантових технологій шифрування для підвищення рівня безпеки.

Література

1. İlker Bekmezci, Ozgur Koray Sahingoz, Şamil Temel. Flying Ad-Hoc Networks (FANETs): A survey. Ad Hoc Networks. 11(3):1254-1270, 2013.
2. Jennifer S. Raj. A Novel Hybrid Secure Routing for Flying Ad-hoc Networks. Journal of Trends in Computer Science and Smart Technology (TCSST), Vol. 02, No. 03, 155-164, 2020.
3. Sunil Kr Maakar, Yudhvir Singh, Rajeshwar Singh. Considerations and Open Issues in Flying Ad Hoc Network. International Journal of Scientific Engineering and Research (IJSER), Vol. 5, Issue 7, 2017.
4. Yixin He, Xiao Tang, Ruonan Zhang, Xiaojiang Du, Deyun Zhou, Mohsen Guizani. A Course-Aware Opportunistic Routing Protocol for FANETs. IEEE Access, 7, 144303-144312, 2019.
5. Macaw Publications. Blockchain-Enhanced Secure Routing in FANETs: Integrating ABC Algorithms and Neural Networks for Attack Mitigation. Smart Mobile Review Journal, 2022. URL: https://www.macawpublications.com/Journals/index.php/SMRJ/article/view/55

УДК 621.382

ПОТЕНЦІАЛ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В РАДІО ТА ТЕЛЕКОМУНІКАЦІЙНИХ ПРИСТРОЯХ ДЛЯ МЕДИЧНОЇ ДІАГНОСТИКИ ТА МОНІТОРИНГУ ЗДОРОВ'Я

Валуйський С.В., Забожко А.В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: valuiskyi.stanislav@lll.kpi.ua

THE POTENTIAL OF APPLYING ARTIFICIAL INTELLIGENCE IN RADIO AND TELECOMMUNICATIONS DEVICES FOR MEDICAL DIAGNOSTICS AND HEALTH MONITORING

Radio and telecommunication devices play a key role in the collection of medical data, and the application of AI opens up new possibilities for their analysis and interpretation. This paper explores the latest innovations in the application of AI for medical diagnostics and monitoring, emphasizing accuracy, speed, personalization, accessibility, and integration with existing systems. By addressing these factors, modern AI methods aim to improve the quality of medical services, optimize treatment, and ensure reliable monitoring of patient conditions. This review provides valuable information for researchers and practitioners in the field of medical diagnostics and telemedicine.

Застосування штучного інтелекту в радіо- та телекомунікаційних пристроях для медичної діагностики та моніторингу здоров'я є важливим завданням для оптимізації роботи таких систем. Основна мета застосування ШІ полягає в аналізі медичних даних, отриманих з таких пристроїв, з метою підвищення ефективності діагностики, зменшення часу обробки даних та підвищення точності моніторингу стану пацієнтів. Наступне покоління медичних пристроїв може використовувати різноманітні методи ШІ, включаючи класичні підходи, такі як алгоритми машинного навчання та глибокого навчання, а також спеціалізовані методи, розроблені спеціально для медичної діагностики та моніторингу.

Деякі з основних методів ШІ, що застосовуються в радіо- та телекомунікаційних пристроях для медичної діагностики та моніторингу, включають:

1. CNN (Convolutional Neural Networks): Це один з найпопулярніших методів для аналізу медичних зображень, таких як рентгенівські знімки, КТ та МРТ. CNN розроблені для виявлення складних патернів та аномалій у зображеннях.

2. RNN (Recurrent Neural Networks): Цей метод використовується для аналізу часових рядів медичних даних, таких як ЕКГ та ЕЕГ. RNN

допомагають виявляти зміни в сигналах та прогнозувати ризики захворювань.

3. SVM (Support Vector Machines): Цей метод застосовується для класифікації медичних даних, таких як дані з носимих пристроїв. SVM допомагають розділяти пацієнтів на групи ризику та персоналізувати лікування.

4. Глибоке навчання з підкріпленням: Цей метод використовується для розробки алгоритмів автоматичного введення інсуліну для діабетиків. Він допомагає оптимізувати дозування інсуліну на основі даних з носимих пристроїв.

5. NLP (Natural Language Processing): Цей метод застосовується для аналізу медичних текстів, таких як історії хвороби та медичні звіти. NLP допомагає виявляти ключову інформацію та покращувати документування медичних даних.

Звичайні завдання застосування ШІ в медичній діагностиці та моніторингу включають аналіз медичних зображень, аналіз електрофізіологічних сигналів, аналіз даних з пристроїв носіїв, прогнозування ризиків захворювань, персоналізацію лікування, дистанційний моніторинг пацієнтів тощо.

Однією з ключових проблем, які вирішуються в цьому контексті, є забезпечення надійності та безпеки ШІ-систем, а також інтеграція ШІ в існуючі системи медичного обслуговування. Також важливо враховувати етичні та правові аспекти, такі як конфіденційність даних, відповідальність за помилки ШІ та доступність ШІ-технологій.

Основні напрямки застосування AI у цій сфері включають:

1. Телеметрія та віддалений моніторинг пацієнтів – використання радіо- та телекомунікаційних пристроїв для збору, передачі та аналізу медичних даних, що дозволяє віддалено контролювати стан пацієнта та реагувати на критичні зміни.

2. Розпізнавання патологій на основі аналізу сигналів – алгоритми машинного навчання здатні аналізувати радіосигнали та виявляти ознаки серцево-судинних захворювань, дихальних розладів, неврологічних станів тощо.

3. Оптимізація передачі даних – AI може використовуватися для покращення роботи безпроводових мереж, забезпечуючи швидку та надійну передачу медичних даних без затримок.

4. Автоматичне оброблення та аналіз даних – системи AI можуть самостійно аналізувати велику кількість медичних показників, виявляючи аномалії та прогнозуючи можливі ризики для здоров’я пацієнта.

5. Персоналізована медицина – використання AI дозволяє створювати індивідуальні плани лікування, ґрунтуючись на аналізі історії хвороби, генетичних факторів та поточних медичних показників.

Однак, незважаючи на значний потенціал, впровадження AI у радіо- та телекомунікаційні пристрої для медичної діагностики стикається з низкою викликів. До них належать забезпечення конфіденційності та безпеки медичних даних, стандартизація алгоритмів, необхідність високої точності AI-моделей та інтеграція з існуючими медичними системами.

Одним із ключових питань є ефективність оброблення великих обсягів даних у режимі реального часу. Для цього використовуються технології, такі як хмарні обчислення та периферійні обчислення (edge computing), які дозволяють зменшити затримки при передачі даних та підвищити швидкість їх аналізу.

Також важливим аспектом є адаптивність AI-систем до різних умов використання. Наприклад, в умовах обмеженого доступу до інтернету AI-алгоритми повинні забезпечувати автономну роботу та прийняття рішень на основі локальних даних.

Майбутнє впровадження AI у радіо- та телекомунікаційні системи для медичних цілей залежить від подальших досліджень та розробки нових алгоритмів, що зможуть працювати з високою точністю та ефективністю.

Важливим напрямком розвитку є також розробка етичних стандартів використання AI у медицині та створення регуляторної бази для забезпечення безпечного та відповідального застосування новітніх технологій.

Література

1. **Bohr, A., & Memarzadeh, K. (Eds.). (2020).** *Artificial Intelligence in Healthcare*. Academic Press. ISBN: 978-0128184387. 1-16. URL: https://doi.org/10.1016/C2018-0-04097-9
2. "Deep Learning for Healthcare Decision Making" / Vishal Jain, Jyotir Moy Chatterjee, Ishaani Priyadarshini, Fadi Al-Turjman. – Boca Raton: CRC Press, 2023. – ISBN: 978-1003373261.
4-16. URL: https://doi.org/10.1201/9781003373261
3. **Biomedical Informatics: Computer Applications in Health Care and Biomedicine** / Editors: Edward H. Shortliffe, James J. Cimino. – 4th ed. – London: Springer, 2014. – ISBN: 978-1447144731. 6-14. URL: https://doi.org/10.1007/0-387-36278-9
4. **Xing, L., Giger, M., & Min, J. K. (Eds.). (2020).** *Artificial Intelligence in Medicine: Technical Basis and Clinical Applications*. Academic Press. ISBN: 978-0128212592.

УДК 007.5:004.72:004.8

УПРАВЛІННЯ РОБОТАМИ-ДОСТАВНИКАМИ ІЗ ЗАСТОСУВАННЯМ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

Конотопова Ю.В., Курдеча В.В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: konotopova.julia@lll.kpi.ua

MANAGEMENT OF DELIVERY ROBOTS BASED ON INTERNET OF THINGS TECHNOLOGY

In recent years, the rapid development of the Internet of Things (IoT) technology has led to its implementation in various areas of human activity. This paper analyzes the management processes of IoT mobile nodes in the delivery sector. The structure of the IoT mobile node — the delivery robot — is presented, along with the identification of key management procedures and their application features.

Останні роки характеризуються стрімким розвитком технології Інтернету речей, що сприяло її впровадженню в різні сфери людської діяльності. У цій роботі проведено аналіз процесів управління мобільними вузлами Інтернету речей у сфері доставки. Представлено структуру мобільного IoT-вузла - робота-доставника, а також визначено ключові процедури управління та особливості їх застосування.

Рухомі об'єкти в системах доставки на основі технології IoT можна класифікувати за наступними категоріями:

- за середовищем функціонування: наземні роботи-доставщики (автономні колісні платформи). повітряні дрони-доставники, водні автономні системи доставки
- за радіусом дії: системи локальної доставки (в межах будівлі або комплексу), системи міської доставки (в межах окремих районів міста), системи регіональної доставки (між населеними пунктами)
- за типом вантажу: системи доставки їжі та продуктів, системи доставки медикаментів, системи доставки поштових відправлень, універсальні системи доставки

Прикладом успішного впровадження наземних роботів-доставщиків є автономні шестиколісні платформи, що використовуються для доставки їжі та товарів у міських умовах. Ці роботи оснащені набором датчиків для навігації, системами машинного зору для розпізнавання перешкод та GPS-модулями для точного позиціонування. Вони здатні автономно переміщатися тротуарами, перетинати пішохідні переходи та доставляти товари безпосередньо до дверей замовника.

Повітряні системи доставки представлені мультироторними дронами, що можуть швидко доставляти невеликі вантажі в складних міських умовах, обминаючи наземні перешкоди. Такі системи особливо ефективні для термінової доставки медикаментів або критично важливих компонентів.

Система управління роботами-доставщиками на основі технології IoT складається з кількох взаємопов'язаних компонентів(рис.1), що забезпечують ефективне функціонування всього комплексу. Нижче представлена блок-схема такої системи:

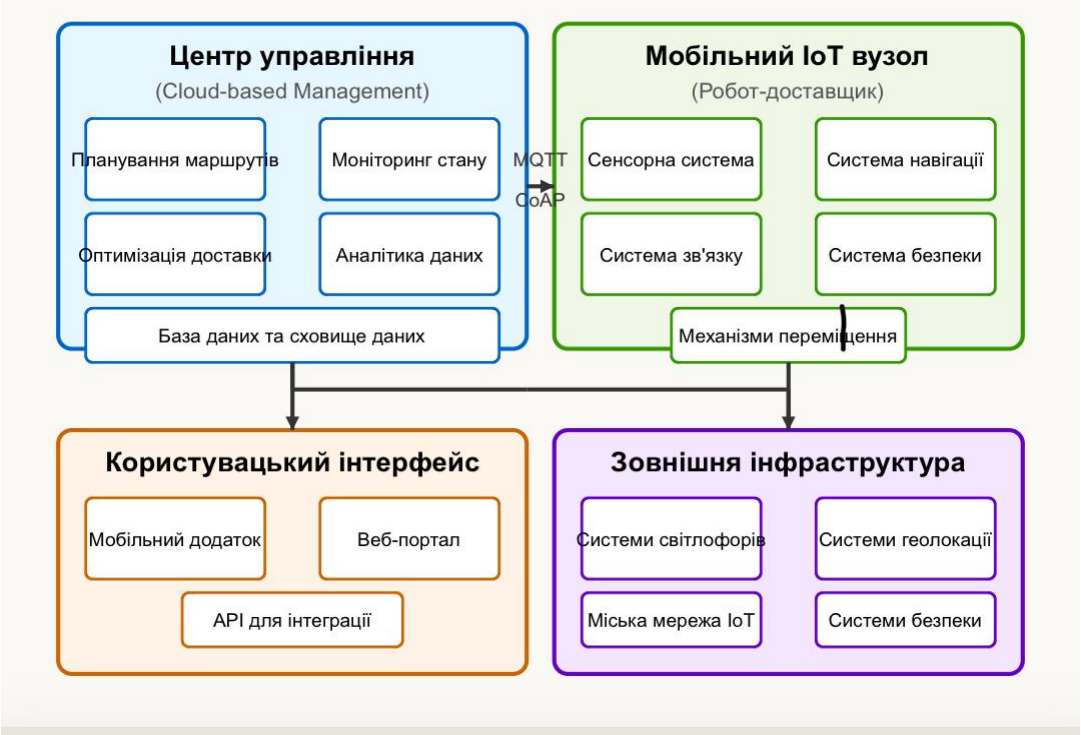


Рис.1. Система управління робота на основі Інтернету речей.

Перерахуємо основні компоненти системи.

1. Центр управління (Cloud-based Management);

- Модуль планування маршрутів - визначає оптимальний шлях доставки;
- Модуль моніторингу стану - відстежує поточне розташування та стан;
- Модуль оптимізації доставки - аналізує ефективність маршрутів;
- Модуль аналітики даних - обробляє інформацію;
- База даних та сховище даних - зберігає історію операцій, маршрути.

2. Мобільний IoT вузол - Робот-доставщик(рис.2):

- Сенсорна система - набір датчиків для орієнтації в просторі;
- Система навігації - обробляє дані з сенсорів та визначає шлях руху;
- Система зв'язку - забезпечує взаємодію з центром управління;
- Система безпеки - відповідає за захист вантажу та самого робота;
- Механізми переміщення - двигуни, колеса тощо.

3. Користувацький інтерфейс:

- Мобільний додаток - для замовлення та відстеження доставки;
- Веб-портал - для управління замовленнями та аналізу статистики;
- API для інтеграції - дозволяє підключати систему до інших сервісів.

4. Зовнішня інфраструктура:

- Системи світлофорів - для безпечного перетину доріг;
- Системи геолокації - GPS, ГЛОНАСС для точного позиціонування;
- Міська мережа IoT - взаємодія з іншими розумними пристроями міста;
- Системи безпеки - камери спостереження та інші елементи міської інфраструктури.

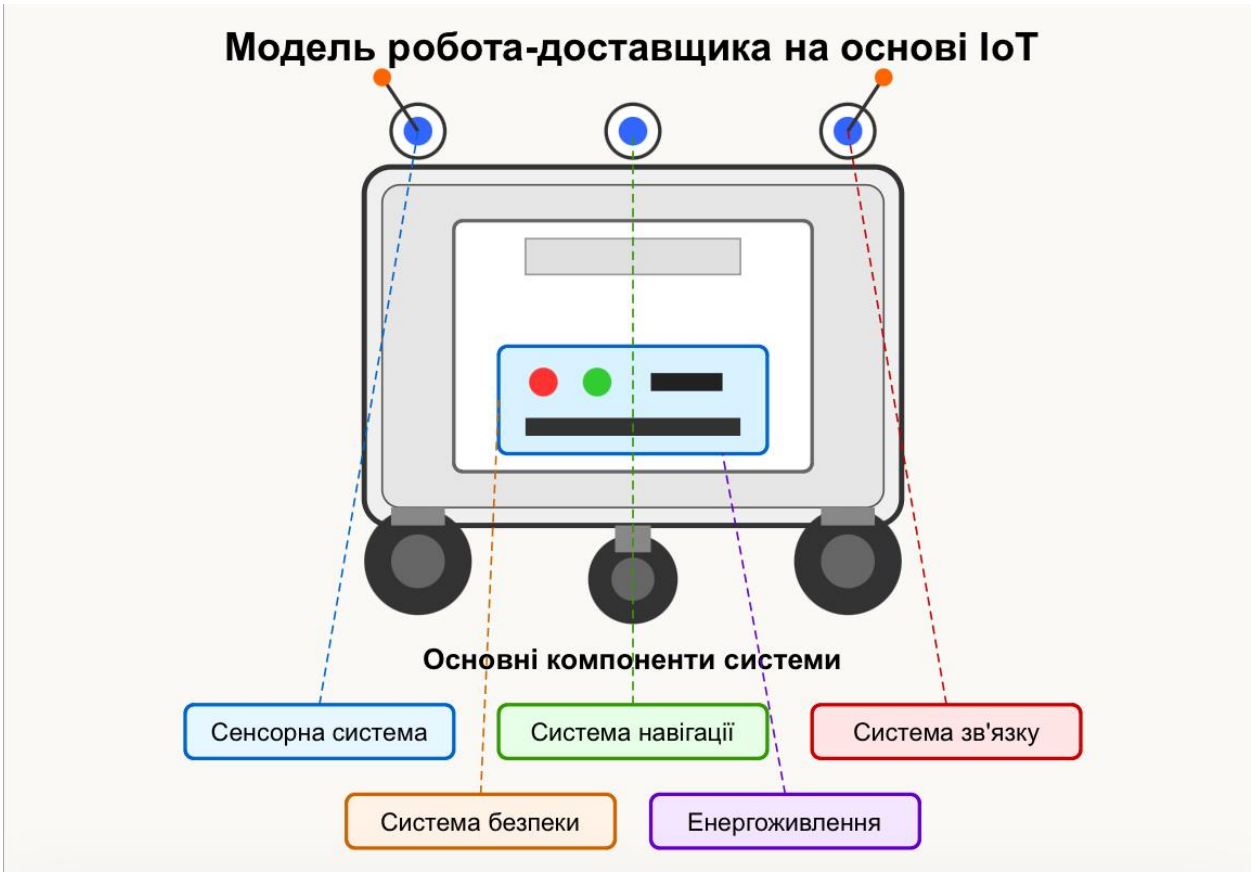


Рис.2. Модель робота-доставщика на основі Інтернету речей.

Запропонована система управління, що відрізняється набором функціоналу та реалізована в моделі робота-доставщика, дозволить підвищити ефективність процесу доставки, розширить можливості та сфери застосування робота-доставщика. Даний робот-доставщик на відміну від існуючих зразків показує високу ефективність навіть за короткочасної втрати зв’язку зі сервісами хмарного середовища та системою навігації GPS

Література

1. S. Ushakov, L. Globa and V. Kurdecha, "EVOLVING INDUSTRY 4.0: A METHODICAL APPROACH TO OPTIMIZING IOT ONTOLOGIES FOR ENHANCED AUTOMATION," 2024 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Tbilisi, Georgia, 2024, pp. 131-134, doi: 10.1109/BlackSeaCom61746.2024.10646225.
2. Ushakov Serhii and Kurdecha 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.
3. Eduard Siemens, Vasyl Kurdecha, Serhii Ushakov, "INTERNET OF THINGS DATA TRANSFER METHOD USING NEURAL NETWORK AUTOENCODER" Information and Telecommunication Sciences, 2023, #1, DOI: 10.20535/2411-2976.12023.9-15
4. Globa, L., Kurdecha, V., Popenko, D., Bezvuhliak, M., Porolo, Y. (2022). Data Collection and Processing Method in the Networks of Industrial IOT. In: Perakovic, D., Knapcikova, L. (eds) Future Access Enablers for Ubiquitous and Intelligent Infrastructures. FABULOUS 2022. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 445. Springer, Cham. https://doi.org/10.1007/978-3-031-15101-9_11

УДК 004.7

СИСТЕМА ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ ВИЯВЛЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Юсин І. С.,Курдеча В.В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: IvanYusinS@gmail.com

INTERNET OF THINGS SYSTEM FOR EMERGENCY DETECTION

The study focuses on the use of modern technologies for monitoring and responding to emergencies. The approach is based on a combination of automated data collection systems, sensor networks and intelligent information analysis.

Надзвичайні ситуації, такі як пожежі, повені, землетруси та інші, постійно ставлять під загрозу безпеку та благополуччя нашого суспільства. Відповідно до звітів організацій з надзвичайних ситуацій, частота та інтенсивність цих подій зростають через різні фактори, включаючи зміни клімату, техногенні ризики та інші.

Подолання цих викликів потребує розробки та впровадження ефективних систем виявлення надзвичайних ситуацій, що дозволять оперативно реагувати на них та мінімізувати їхні наслідки. Одним із перспективних напрямків в цьому відношенні є використання технологій Інтернету речей (IoT), які дозволяють підключати різні сенсори, пристрої та системи моніторингу до мережі Інтернет з метою збору та аналізу даних в реальному часі.

Пожежі можуть завдати колосальних збитків природі, тому, щоб уникнути їх наслідків, здійснюють моніторинг лісових пожеж. Серед існуючих способи: є перевірені часом візуальні огляди, також практикують спостереження за допомогою супутників і сучасної техніки. Ефективно використовувати способу моніторингу лісових пожеж у комплексі. У багатьох країнах діють профільні служби та установи зі збирання, аналізу і структурування даних для подальшого узагальнення. Розглянуто існуючі види та типи моніторингу пожеж.

Серед перспективних є:

- супутниковий моніторинг,
- система відеоспостереження,
- системи інших датчиків (температури, диму та ін.),
- дрони і БПЛА літакового типу,
- штучний інтелект.

Усі вище перераховані є ефективними і корисними засобами у виявленні пожеж, які є ефективними на різних площах і розмірах лісу. Ідея використання багатьох методів моніторингу даних, у вигляді певної автоматизованої системи полягає у створенні максимально ефективної системи реагування, в якій усі елементи будуть поєднані за допомогою

інтернету речей, і виконувати різні функції однієї системи сенсорів нагляду. Вона включає в себе супутники, БПЛА, відеокамери та інші датчики.

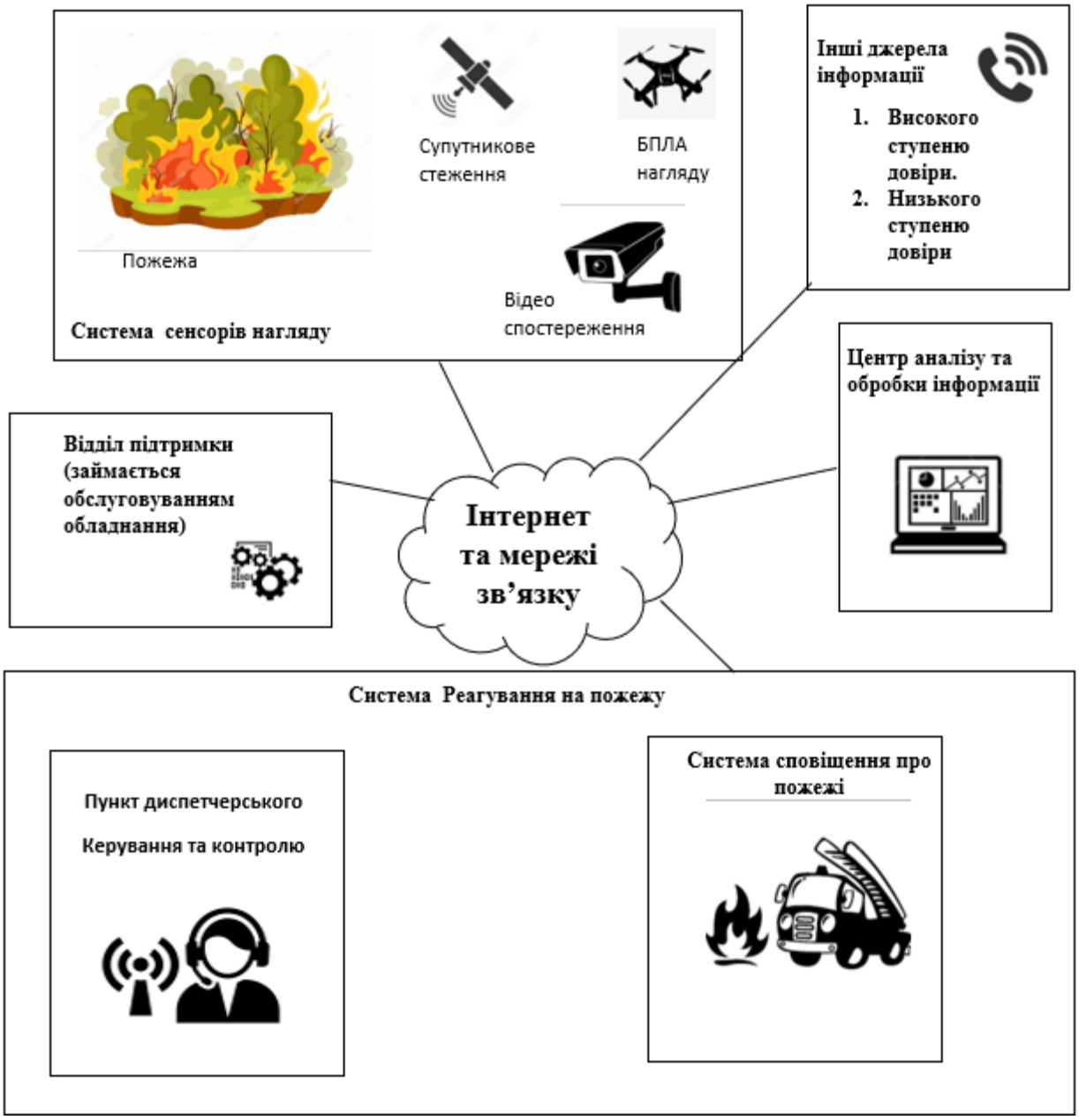


Рис.1. Система Інтернету речей для виявлення надзвичайних ситуацій.

Робота складається з трьох етапів:

1. Етап моніторингу, виявлення зародку пожежі.
2. Етап отримання сигналу та обробки інформації.
3. Етап прийняття рішення та повідомлення відповідних служб.

По всій площі лісу встановлені спеціальні високі вишки на яких встановлені камери з тепловізійними на інфрачервоними датчиками. Супутники будуть цілодобового надавати на оновлювати інформацію про можливі області загоряння, за допомогою космічного зондування. Яка буде зберігатися у Центрі аналізу та обробки інформації, та автоматично оброблятися штучним інтелектом. При виявленні ознак пожежі за допомогою супутникового спостереження, Диспетчер отримує відповідний сигнал. І

надалі має сповістити відповідні служби безпеки. Якщо повідомлення про пожежі не точне, або важко точно побачити на зображенні з супутника, диспетчер має право на команду про формування маршрутів БПЛА, які в екстреному порядку вирушають за координатами наданими Супутником, для оцінки обсягів пожежі, та її підтвердження у випадку не точного сигналу.

За результатами теоретичного рішення було проведено моделювання, що показало - запропонована система IoT забезпечує високу точність та швидкість виявлення пожеж. Порівняння з традиційними методами виявлення пожеж підтвердило значну перевагу системи IoT у зменшенні часу реагування та підвищенні ймовірності виявлення пожежі. Це робить запропоновану систему ефективним рішенням для моніторингу лісових пожеж, що може бути впроваджене для забезпечення екологічної безпеки та збереження природних ресурсів.

Отже, аналіз традиційних методів моніторингу, таких як візуальний моніторинг та ручне патрулювання, показав що вони мають значні обмеження в ефективності. Сучасні технології, зокрема використання сенсорів, відеокамер, супутників та БПЛА, забезпечують значно вищий рівень точності та швидкості виявлення пожеж. Розроблена структура системи IoT для моніторингу лісових пожеж, яка відрізняється інтеграцією різних типів сенсорів, відеокамер, супутників та БПЛА дозволяє підвищити імовірність виявлення та швидкість реагування на надзвичайні ситуації.

Література

1. Лаврівський М. З., Тур Н. Е. Використання безпілотних літальних апаратів для моніторингу надзвичайних ситуацій у лісовій місцевості. 149 Збірник науково-технічних праць. Науковий вісник НЛТУ України. 2015. Вип. 25.8. С. 353–359.
2. Гусак О. М. Інформаційна технологія раннього виявлення лісових пожеж за допомогою безпілотних літальних апаратів : Дисертація : 126. Львів, 2018. 187 с.
3. S. Ushakov, L. Globa and V. Kurdecha, "EVOLVING INDUSTRY 4.0: A METHODICAL APPROACH TO OPTIMIZING IOT ONTOLOGIES FOR ENHANCED AUTOMATION," 2024 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Tbilisi, Georgia, 2024, pp. 131-134, doi: 10.1109/BlackSeaCom61746.2024.10646225.
4. Ushakov Serhii and Kurdecha 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.
5. 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 2022. Lecture Notes in Networks and Systems, vol 809. Springer, Cham. https://doi.org/10.1007/978-3-031-46880-3_13
6. Eduard Siemens, Vasyl Kurdecha, Serhii Ushakov, "INTERNET OF THINGS DATA TRANSFER METHOD USING NEURAL NETWORK AUTOENCODER" Information and Telecommunication Sciences, 2023, #1, DOI: 10.20535/2411-2976.12023.9-15
7. Види та класифікація лісових пожеж – Сталий розвиток для України. Сталий розвиток для України – Сталий розвиток для України. URL: https://sd4ua.org/vydy-ta-klasyfikatsiya-lisovyh-pozhezh/ (дата звернення: 04.06.2024).

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

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ
НДІ ТЕЛЕКОМУНІКАЦІЙ

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

14-18 квітня 2025 року

Тези конференції

м. Київ

ПРОГРАМНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ ПРІТС-2025

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., в.о. директора НН ІТС КПІ ім. І. 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:

Авдєєнко Г.Л., к.т.н., 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.

ДОСЛІДЖЕННЯ МЕТОДІВ СТЕГАНОГРАФІЇ В ТЕКСТОВИХ ФАЙЛАХ

Хусам Абдулсахіб Альклкаві
Науковий керівник: **Агеєв Д.В.**
Харківський національний університет радіоелектроніки, Україна
E-mail: husam.abdulsahib.abdulazzaq.alklkawi@nure.ua

Захист конфіденційної інформації є критично важливим у сучасних умовах кіберзагроз. Текстова стеганографія дозволяє передавати дані непомітно, приховуючи їх у звичайних текстових документах.

У цьому дослідженні розглядаються основні методи текстової стеганографії: зміна пробілів і табуляцій, заміна символів на аналогічні Unicode-коди та генерація псевдонімних текстів. Аналіз включав приховану ємність (бит/символ), стійкість до виявлення та збереження читаємості.

Результати показали, що метод маніпуляції пробілами забезпечує приховану ємність до 0,5 біт/символ, але легко виявляється статистичними методами. Найефективнішими виявилися комбіновані підходи, що дозволяють досягати 0,4 біт/символ зі збереженням природності тексту.

Запропоновані рекомендації щодо вибору методу залежно від рівня безпеки та вимог до прихованості інформації.

STUDY OF STEGANOGRAPHY METHODS IN TEXT FILES

Husam Abdulsahib Alklkawi
Scientific adviser: **Ageyev D.V.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: husam.abdulsahib.abdulazzaq.alklkawi@nure.ua

Protecting confidential information is critically important in today's cyberthreat environment. Text steganography allows data to be transmitted invisibly, hiding it in plain text documents.

This study examines the main methods of text steganography: changing spaces and tabs, replacing characters with similar Unicode codes, and generating pseudonymous texts. The analysis included hidden capacity (bits/character), resistance to detection, and preservation of readability.

The results showed that the whitespace manipulation method provides a hidden capacity of up to 0.5 bits/character, but is easily detected by statistical methods. The most effective were combined approaches that allow reaching 0.4 bits/character while preserving the naturalness of the text.

Recommendations for choosing a method depending on the level of security and requirements for information secrecy are proposed.

ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ З ВИКОРИСТАННЯМ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Герраб Азхар
Науковий керівник: **Агеєв Д.В.**
Харківський національний університет радіоелектроніки, Україна
E-mail: azkhar.herrab@nure.ua

Розвиток Інтернету речей (IoT) сприяє підвищенню ефективності в різних сферах, проте безпека таких мереж залишається критичною проблемою через велику кількість підключених пристроїв і їхню вразливість до кібератак. Метою цього дослідження є оцінка рівня захищеності IoT-мереж і розробка методів виявлення загроз із застосуванням машинного навчання. Гіпотеза дослідження полягає в тому, що алгоритми машинного навчання можуть ефективно ідентифікувати аномалії в мережевому трафіку IoT. Для аналізу було використано набір даних із реальних IoT-мереж

Дослідження показало, що запропоновані методи дозволяють досягти високої точності у виявленні аномального трафіку, що підтверджує їхню ефективність. Отримані результати мають практичне значення для покращення кібербезпеки IoT-систем, знижуючи ризики несанкціонованого доступу та атак.

RESEARCH ON THE SECURITY OF INTERNET OF THINGS NETWORKS USING MACHINE LEARNING METHODS

Herrab Azkhar
Scientific adviser: **Ageyev D.V.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: azkhar.herrab@nure.ua

The development of the Internet of Things (IoT) contributes to increased efficiency in various areas, but the security of such networks remains a critical issue due to the large number of connected devices and their vulnerability to cyberattacks. The purpose of this study is to assess the level of security of IoT networks and develop methods for detecting threats using machine learning. The hypothesis of the study is that machine learning algorithms can effectively identify anomalies in IoT network traffic. A dataset from real IoT networks was used for the analysis.

The study showed that the proposed methods allow achieving high accuracy in detecting anomalous traffic, which confirms their effectiveness. The results obtained have practical significance for improving the cybersecurity of IoT systems, reducing the risks of unauthorized access and attacks.

АНАЛІЗ МЕТОДІВ СТЕГАНОГРАФІЇ НА ОСНОВІ ЗОБРАЖЕНЬ ДЛЯ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Алі Мохаммед Алаві Ахмед
Науковий керівник: **Агеєв Д.В.**
Харківський національний університет радіоелектроніки, Україна
E-mail: mohammed.alawi.ahmed.ali@nure.ua

Захист конфіденційної інформації є актуальною проблемою у цифрову епоху. Стеганографія на основі зображень забезпечує приховану передачу даних, що ускладнює несанкціонований доступ.

У цьому дослідженні аналізуються сучасні методи стеганографії, такі як метод найменш значущих бітів (LSB), дискретне косинусне перетворення (DCT) та хвильове перетворення (DWT). Проведено порівняльний аналіз ефективності методів за параметрами прихованості, стійкості до атак та збереження якості зображень.

Результати показали, що методи на основі DWT забезпечують кращу стійкість до спотворень, тоді як LSB має вищу ємність приховання. Запропоновані рекомендації щодо вибору методу залежно від вимог безпеки.

Дослідження сприяє вдосконаленню методів захисту даних та їх використанню в безпечних системах комунікації.

ANALYSIS OF IMAGE-BASED STEGANOGRAPHY METHODS FOR CONFIDENTIAL INFORMATION PROTECTION

Ali Mohammed Alawi Ahmed
Scientific adviser: **Ageyev D.V.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: mohammed.alawi.ahmed.ali@nure.ua

Protecting confidential information is a crucial challenge in the digital era. Image-based steganography enables covert data transmission, making unauthorized access more difficult.

This study analyzes modern steganography methods, including the Least Significant Bit (LSB) method, Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). A comparative analysis was conducted based on concealment capacity, resistance to attacks, and image quality preservation.

The results show that DWT-based methods offer higher resistance to distortions, while LSB provides greater embedding capacity. Recommendations are proposed for selecting the appropriate method based on security requirements.

This research contributes to the improvement of data protection methods and their application in secure communication systems.

АНАЛІЗ ТА МОДЕЛЮВАННЯ ТРАФІКУ IoT

Сидоренко В.С.
Науковий керівник: **Агеєв Д.В.**
Харківський національний університет радіоелектроніки, Україна
E-mail: vladyslav.sydorenko.cpe@nure.ua

Швидке зростання Інтернету речей (IoT) призводить до збільшення обсягу мережевого трафіку, проте його вплив на продуктивність мережі досліджено недостатньо. Пристрої IoT, через обмежені ресурси, вразливі до кіберзагроз, що робить аналіз трафіку необхідним для забезпечення безпеки.

У цьому дослідженні вивчаються характеристики IoT-трафіку за допомогою тестового стенда розумного дому, визначення його параметрів та створення генератора трафіку з аналогічними характеристиками. Використано ентропійний аналіз для класифікації пристроїв та виявлення аномалій. Запропонований підхід досяг точності до 94% у ідентифікації пристроїв, що підтверджує його ефективність.

Отримані результати сприяють покращенню ефективності IoT-мереж, забезпечуючи моделювання трафіку для майбутніх IoT-середовищ.

IoT TRAFFIC ANALYSIS AND MODELING

Sydorenko V.S.
Scientific adviser: **Ageyev D.V.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: yevhen.svitlychnyi.cpe@nure.ua

The rapid growth of the Internet of Things (IoT) has led to an increasing volume of network traffic, yet its impact on network performance remains insufficiently studied. IoT devices, due to resource constraints, are vulnerable to cyber threats, making traffic analysis essential for security.

This study investigates IoT traffic characteristics using a smart-home testbed and a traffic generator. Entropy-based analysis were applied to classify IoT devices and detect anomalies. The proposed approach achieved up to 94% accuracy in device identification, demonstrating its robustness.

These findings contribute to improving IoT network, enabling efficient raffic modeling for future IoT environments.

ДОСЛІДЖЕННЯ МЕРЕЖ З ВИКОРИСТАННЯМ VPN ТЕХНОЛОГІЙ

Світличний Є.Ю.
Науковий керівник: **Агеєв Д.В.**
Харківський національний університет радіоелектроніки, Україна
E-mail: yevhen.svitlychnyi.cpe@nure.ua

Віртуальні приватні мережі (VPN) широко використовуються для безпечного з'єднання за низькими витратами. Проте їхня продуктивність варіюється, що ускладнює вибір оптимального рішення.

Метою дослідження є порівняння VPN-рішень на основі Linux з відкритим кодом (OSLV). Аналіз охоплює продуктивність (накладні витрати, пропускну здатність, затримку) та безпеку.

Результати показали, що VPN із UDP-тунелями мають на 50% менше накладних витрат, на 80% вищу пропускну здатність та на 40–60% нижчі затримки, ніж TCP-аналоги. Оптимальний вибір залежить від потреб користувача.

Отримані дані можуть допомогти у виборі ефективних VPN-рішень та їх подальшій оптимізації.

RESEARCH OF NETWORKS USING VPN TECHNOLOGIES

Svitlychny E.Yu.
Scientific adviser: **Ageyev D.V.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: yevhen.svitlychnyi.cpe@nure.ua

Virtual private networks (VPNs) are widely used for secure connectivity at low costs. However, their performance varies, making it challenging to choose the optimal solution.

This study aims to compare open-source Linux-based VPN solutions (OSLVs). The analysis covers performance (overhead, bandwidth utilization, latency) and security aspects.

Results show that VPNs using UDP tunnels have 50% lower overhead, 80% higher bandwidth utilization, and 40–60% lower latency compared to TCP-based alternatives. The optimal choice depends on user needs.

The findings can assist in selecting efficient VPN solutions and further optimizing their performance.

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ МОДЕЛЕЙ І ПРОТОКОЛІВ IOT

Дідковська Н.А.
Науковий керівник: **Григоренко О.Г.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: didkovska.natalia@lll.kpi.ua

Проаналізовані особливості побудови та використання моделей та протоколів технології Інтернету речей, що є актуальним для розробників, адміністраторів та користувачів IoT-систем та мереж, оскільки сприяє вдосконаленню методів передачі та обробки даних, підвищенню рівня безпеки та ефективності функціонування сучасних IoT-екосистем.

ANALYSIS OF APPLICATION LAYER PROTOCOLS IN INTERNET OF THINGS NETWORKS

Didkovska N.A.
Scientific adviser: **Grygorenko O.G.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: didkovska.natalia@lll.kpi.ua

The features of the construction and use of models and protocols of the Internet of Things technology were analyzed, which is relevant for developers, administrators and users of IoT systems and networks, as it contributes to the improvement of data transmission and processing methods, increasing the level of security and efficiency of the functioning of modern IoT ecosystems.

АНАЛІЗ ПРОТОКОЛІВ РІВНЯ ЗАСТОСУВАНЬ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ

Зазимкін Я.В.
Науковий керівник: **Григоренко О.Г.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: yarusya.yar@gmail.com

Проаналізовано основні протоколи рівня застосувань в мережах Інтернету речей, що забезпечують ефективну та безпечну передачу даних між пристроями IoT.

ANALYSIS OF APPLICATION LAYER PROTOCOLS IN INTERNET OF THINGS NETWORKS

Zazymkin YA.V.
Scientific adviser: **Grygorenko O.G.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: yarusya.yar@gmail.com

The main application-layer protocols in Internet of Things networks that ensure efficient and secure data transmission between IoT devices are analyzed.

ЗАБЕЗПЕЧЕННЯ ЕЛЕКТРОМАГНІТНОЇ СУМІСНОСТІ В АВТОНОМНИХ NPN МЕРЕЖАХ 5G З ЧАСОВИМ ДУПЛЕКСОМ

Долженков І.С.
Науковий керівник: **Якорнов Є.А.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: dolzhenkov.ivan@lll.kpi.uat

Автономні мережі NPN є однією з ефективних бізнес-моделей для розвитку мереж 5G завдяки здатності максимізувати реалізацію майже всіх технологічних переваг 5G, особливо нарізки або «розшарування» роботи системи для окремих додатків. Водночас існують наступні труднощі у розвитку таких мереж: вторинна основа використання, обмежений частотний ресурс, обмежені параметри випромінювання, необхідність забезпечення сумісності обладнання як усередині мереж, так і з обладнанням у сусідніх зонах інших автономних мереж NPN, а також з іншими системами зв'язку в суміжних діапазонах частот. У доповіді представлено результати оцінки вимог щодо забезпечення сумісності обладнання в автономній мережі NPN.

PROVIDING ELECTROMAGNETIC COMPATIBILITY IN AUTONOMOUS NPN 5G NETWORKS WITH TIME DUPLEX

Dolzhenkov I.S.
Scientific supervisor: **Yakornov E.A.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: dolzhenkov.ivan@lll.kpi.ua

Autonomous NPN networks are one of the effective business models for the development of 5G networks due to the ability to maximize the implementation of almost all technological advantages of 5G, especially slicing or "layering" of the system operation for individual applications. At the same time, there are following difficulties in the development of such networks: secondary usage basis, limited frequency resource, limited radiation parameters, the need to ensure compatibility of equipment both within networks and with equipment in neighboring areas of other autonomous NPN networks as far as other communication systems in adjacent frequency bands. Report presents the results of assessment the requirements for ensuring compatibility of equipment within an autonomous NPN network.

РОЗПІЗНАВАННЯ ТА ЗАХИСТ ТЕКСТОВИХ ПРИВАТНИХ АТРИБУТІВ КОРИСТУВАЧІВ МОБІЛЬНИХ ПРИСТРОЇВ В МЕДІАДАНИХ

Солоденко М.А.
Науковий керівник: **Педан С.І.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: mushenok.mariia@lll.kpi.ua

У цифрову епоху актуальною проблемою є витік конфіденційної інформації через мультимедійні дані, зокрема відео, що передаються з мобільних пристроїв. Проведено аналіз технологій обробки відеопотоку з мобільних пристроїв з метою виявлення текстових приватних атрибутів – таких як паспортні дані, адреса, номер телефону, номер банківської картки тощо. Запропоновано методи захисту виявлених приватних атрибутів для забезпечення вимог сучасних законодавчих норм обробки даних.

RECOGNITION AND PROTECTION OF TEXTUAL PRIVATE ATTRIBUTES OF MOBILE DEVICE USERS IN MEDIA DATA

Solodenko M.A.
Scientific adviser: **Pedan S.I.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: mushenok.mariia@lll.kpi.ua

In the digital age, a pressing problem is the leakage of confidential information through multimedia data, in particular videos transmitted from mobile devices. An analysis of video stream processing technologies from mobile devices was conducted to detect textual private attributes – such as passport data, address, phone number, bank card number, etc. Methods for protecting detected private attributes were proposed to ensure the requirements of modern legislative data processing standards.

МОНІТОРИНГ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ

Дубінко А.Д.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: dubinko.andrii@lll.kpi.ua

Розвиток інфокомунікацій забезпечується технологічним зростанням та розвитком технологій, зокрема розвитком пакетних мереж. При цьому особливо актуальною постає задача моніторингу мережі зв'язку – саме цьому питанню присвячена дана робота. Серед показників, які розглядаються в даній публікації з точки зору моніторингу можна виділити: доступність вузлів, пропускна спроможність, швидкість передачі тощо.

INFOCOMMUNICATION NETWORKS MONITORING

Dubinko A.D.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: dubinko.andrii@lll.kpi.ua

The development of infocommunications is ensured by technological growth and development of technologies, in particular the development of packet networks. At the same time, the task of monitoring the communication network becomes particularly relevant - this is the issue to which this work is devoted. Among the indicators considered in this publication from the point of view of monitoring, we can distinguish: availability of nodes, bandwidth, transmission speed, etc.

ОСОБЛИВОСТІ МОНІТОРИНГУ СТАНУ БАЗОВИХ СТАНЦІЙ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ

Радуга Н. С.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: raduganazar@gmai.com

Ця робота присвячена дослідженню актуальної проблеми моніторингу стану базових станцій стільникового зв'язку. В умовах стрімкого розвитку телекомунікаційних технологій та зростання вимог до якості зв'язку, ефективний моніторинг стає ключовим фактором забезпечення надійності та безперебійності роботи мережі.

Робота спрямована на виявлення потенційних напрямків для вдосконалення існуючих методів та розробки нових підходів до моніторингу, що дозволять підвищити ефективність та точність діагностики стану базових станцій.

FEATURES OF MONITORING THE STATE OF CELLULAR COMMUNICATION BASE STATIONS

Raduga N. S.
Scientific adviser: **KurdechaV.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: raduganazar@gmail.com

This work is devoted to the study of the current problem of monitoring the condition of cellular base stations. In the conditions of rapid development of telecommunication technologies and increasing requirements for communication quality, effective monitoring becomes a key factor in ensuring the reliability and uninterrupted operation of the network.

The work is aimed at identifying potential areas for improving existing methods and developing new approaches to monitoring, which will increase the efficiency and accuracy of diagnostics of the condition of base stations.

СИСТЕМА ОПОВІЩЕННЯ РОБІТНИКІВ З ВИКОРИСТАННЯМ IOT

Щербина Н.Є.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: shcherbina.nikita@lll.kpi.ua

Розвиток системи Інтернету речей сприяє впровадженню даної технології в усі сфери людської діяльності. В публікації досліджено особливості розробки IoT системи оповіщення із застосуванням сенсорів. На основі IoT системи оповіщення запропоновано метод комунікації та режим роботи спеціалізованого IoT пристрою.

EMPLOYEES ALERT SYSTEM USING IOT

Shcherbyna N.Y.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: shcherbina.nikita@lll.kpi.ua

Development of the Internet of Things system to promote the implementation of this technology in the entire field of human activity. The publication explores the peculiarities of the development of an IoT notification system using sensors. Based on the IoT notification system, the communication method and operation mode of the specialized IoT device are proposed.

ОСОБЛИВОСТІ АРХІТЕКТУРИ СИСТЕМИ ЗВ'ЯЗКУ РУХОМИХ ВУЗЛІВ ІНТЕРНЕТУ РЕЧЕЙ

Кушнір О.О.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: kushnir.oleg@lll.kpi.ua

Розвиток мережі Інтернету речей призвів до застосування цієї технології в різних сферах життя, в тому числі вигляді рухомих об'єктів. Це в свою чергу призвело до необхідності забезпечення зв'язку для таких вузлів. В даній роботі розглядається особливості архітектури системи зв'язку рухомих вузлів інтернету речей, зокрема враховано необхідність забезпечення зв'язності такої мережі Інтернету речей.

FEATURES OF THE ARCHITECTURE OF THE COMMUNICATION SYSTEM FOR MOBILE NODES OF THE INTERNET OF THINGS

Kushnir O.O.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: kushnir.oleg@lll.kpi.ua

The development of the Internet of Things network has led to the application of this technology in various spheres of life, including in the form of moving objects. This, in turn, has led to the need to ensure communication for such nodes. This paper examines the features of the architecture of the communication system of mobile nodes of the Internet of Things, in particular, the need to ensure connectivity of such an Internet of Things network is taken into account.

ОСОБЛИВОСТІ АРХІТЕКТУРИ МОБІЛЬНОЇ СЕНСОРНОЇ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

Короїд Б.О.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: koroid.bohdan@lll.kpi.ua

Розвиток систем Інтернету речей призвів до застосування даної технології в сенсорних мережах. Особливістю таких мереж є зберігання і подальша обробка інформації в хмарному середовищі. Але таке рішення призвело до появи проблемних питань пов’язаних з енергоефективністю, безпекою, тощо. Дана робота присвячена аналізу особливостей архітектури мобільної сенсорної мережі з метою зменшення впливу зазначених проблемних питань.

FEATURES OF THE ARCHITECTURE OF THE MOBILE SENSOR NETWORK OF THE INTERNET OF THINGS

Koroid B.O.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: koroid.bohdan@lll.kpi.ua

The development of Internet of Things systems has led to the use of this technology in sensor networks. A feature of such networks is the storage and further processing of information in the cloud environment. But such a solution has led to the emergence of problematic issues related to energy efficiency, security, etc. This work is devoted to the analysis of the features of the architecture of a mobile sensor network in order to reduce the impact of these problematic issues.

ОСОБЛИВОСТІ СТРУКТУРНО-ПАРАМЕТРИЧНОГО СИНТЕЗУ СУЧАСНИХ КОМУНІКАЦІЙНИХ МЕРЕЖ

Куренко В.О.
Науковий керівник: **Лемешко О.В.**
Харківський національний університет радіоелектроніки, Україна
E-mail: vladyslav.kurenko@nure.ua

Досліджено процес структурно-параметричного синтезу комунікаційних мереж, який відіграє важливу роль у забезпеченні виконання низки вимог, що висуваються до сучасних мереж. Проведено аналіз підходів до вирішення задачі оптимізації комунікаційних мереж, і визначено вимоги до них. Розглянуто особливості трафіку, що передається, та вплив на структуру і параметри комунікаційної мережі. Визначено ряд показників, що мають бути враховані в ході структурно-параметричного синтезу сучасних комунікаційних мереж. Обґрунтовано доцільність врахування показників мережної безпеки в ході синтезу.

FEATURES OF STRUCTURAL-PARAMETRIC SYNTHESIS OF MODERN COMMUNICATION NETWORKS

Kurenko V.O.
Scientific supervisor: **Lemeshko O.V.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: vladyslav.kurenko@nure.ua

The process of structural-parametric synthesis of communication networks, which plays an important role in ensuring the fulfillment of a number of requirements imposed on modern networks, has been studied. An analysis of approaches to solving the problem of optimizing communication networks has been conducted, and requirements for them have been determined. The features of the transmitted traffic and the impact on the structure and parameters of the communication network have been considered. A number of indicators have been determined that should be taken into account during the structural-parametric synthesis of modern communication networks. The feasibility of taking into account network security indicators during the synthesis has been substantiated.

ОПТИМІЗАЦІЯ ІНВЕСТИЦІЙ У СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ ТЕОРІЇ ІГОР

Фукс М.А.
Науковий керівник: **Лемешко О.В.**
Харківський національний університет радіоелектроніки, Україна
E-mail: maksymillian.fuks@nure.ua

Досліджено економічну модель Гордона-Лоєба для визначення оптимальних інвестицій у системи захисту інформації. Проаналізовано наявні підходи до оптимізації вибору стратегій інвестування адміністратором безпеки за допомогою теорії ігор. Виявлено, що більшість моделей орієнтовані лише на адміністратора безпеки, ігноруючи цілі зловмисника. Запропоновано моделювання конфлікту на основі біматричної гри, де функції виграшів формуються для обох гравців з урахуванням економічних показників, що дозволяє оптимізувати стратегії захисту інформаційних активів та приймати більш збалансовані рішення щодо інвестицій у контрзаходи.

THE OPTIMIZATION OF INVESTMENTS IN INFORMATION SECURITY SYSTEMS USING THE CAPABILITIES OF GAME THEORY

Fuks M.A.
Scientific adviser: **Lemeshko O.V.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: maksymillian.fuks@nure.ua

The economic model of Gordon-Loeb for determining optimal investments in information security systems has been studied. Existing approaches to optimizing investment strategies by the security administrator using game theory have been analyzed. It was found that most models focus only on the security administrator, ignoring the aims of attacker. A methodology for modeling the conflict based on a bimatrix game is proposed, where the payoff functions for both players are formed considering economic indicators, allowing for the optimization of information asset protection strategies and making more balanced decisions regarding investments in countermeasures.

ПОРІВНЯННЯ МЕТОДІВ ЗБОРУ ТА ОБРОБКИ ІНФОРМАЦІЇ ДЛЯ СОЦІАЛЬНИХ МЕДІА

Пінчук Ю.М.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail pinchuk.yulia@lll.kpi.ua

Метою роботи є підвищення ефективності процесів збору та обробки інформації в соціальних медіа за рахунок порівняння та вибору існуючих рішень. Проаналізовано їх вплив на користувачів та ризики, такі як порушення конфіденційності і маніпуляція свідомістю. Було розглянуто канали збору даних (персональні, текстові, зображення, відео) і алгоритми, що використовуються для персоналізації контенту. В роботі також було запропоновано рекомендації та покращення існуючих рішень щодо безпечного використання соцмереж і захисту даних.

COMPARISON OF METHODS OF COLLECTING AND PROCESSING INFORMATION FOR SOCIAL MEDIA

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@lll.kpi.ua

The aim of the paper is to improve the efficiency of information collection and processing in social media by comparing and selecting existing solutions. The author analyzes their impact on users and risks, such as privacy violations and mind manipulation. Data collection channels (personal, text, image, video) and algorithms used to personalize content were considered. The paper also offers recommendations and improvements to existing solutions for the safe use of social media and data protection.

ПОРІВНЯННЯ МЕТОДІВ ОБРОБКИ ГРАФІЧНОЇ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

Голуб А.С.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: holub.anna@lll.kpi.ua

Розвиток систем Інтернету речей призводить до зростання об’ємів графічної інформації, що генерується та передається в таких мережах. В роботі досліджено існуючі методи обробки графічної інформації в мережі Інтернету речей, зокрема Edge Computing та Cloud Computing. Результатом є рекомендації по застосуванню методів в залежності від особливостей та характеристик мережі Інтернету речей.

COMPARISON OF GRAPHIC INFORMATION PROCESSING METHODS IN THE INTERNET OF THINGS NETWORK

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@lll.kpi.ua

The development of Internet of Things systems leads to an increase in the volume of graphic information generated and transmitted in such networks. The paper examines the existing methods of processing graphical information in the Internet of Things network, in particular Edge Computing and Cloud Computing. The result is recommendations for the application of methods depending on the features and characteristics of the Internet of Things network.

ЗАСТОСУВАННЯ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ШІ ДЛЯ БЕЗПЕКИ IOT

Кузнецов Я.В.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: kyiv12@bigmir.net

Інтернет речей забезпечує взаємодію різноманітних пристроїв для автоматизації та надання інтелектуальних послуг, проте є вразливим до кіберзагроз. Використання великих мовних моделей (LLM) відкриває нові можливості для підвищення рівня безпеки IoT. Досліджено основні загрози для IoT-систем та розглянуто методи їх нейтралізації за допомогою LLM. Визначено особливості впровадження LLM моделей у частині конфіденційності та відповідності задачам кібербезпеки.

APPLYING AI LARGE LANGUAGE MODELS TO IOT SECURITY

Kuznetsov Y.V.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: kyiv12@bigmir.net

The Internet of Things enables the interaction of various devices to automate and provide intelligent services, but is vulnerable to cyber threats. The use of large language models (LLMs) opens up new opportunities for improving the security of IoT. The main threats to IoT systems are investigated and methods of their neutralization using LLM are considered. The peculiarities of implementing LLM models in terms of confidentiality and compliance with cybersecurity tasks are determined.

АНАЛІЗ СТАНДАРТІВ ЗВ'ЯЗКУ ДЛЯ КОМУНІКАЦІЇ МОБІЛЬНИХ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

Прокопчук Я.В.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: prokopchuk.yaroslav@lll.kpi.ua

Розвиток Інтернету речей призводить до застосування даної технології для рухомих об’єктів. Це в свою чергу вимагає специфічних методів управління та комунікації даними пристроями. В зв’язку з цим задачею даної роботи є аналіз стандартів зв’язку для комунікації та передачі даних мобільних пристроїв Інтернету речей. В публікації визначено особливості застосування способів комунікації в процесі управління рухомими пристроями Інтернету речей.

ANALYSIS OF COMMUNICATION STANDARDS FOR THE COMMUNICATION OF MOBILE DEVICES OF THE INTERNET OF THINGS

Prokopchuk Y.V.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: prokopchuk.yaroslav@lll.kpi.ua

The development of the Internet of Things leads to the application of this technology to mobile objects. This in turn requires specific methods of control and communication with these devices. In this regard, the task of this work is to analyze communication standards for communication and data transmission of mobile Internet of Things devices. The publication identifies the features of the application of communication methods in the process of controlling mobile Internet of Things devices.

ЗАСТОСУВАННЯ UNREAL ENGINE В ІНФОКОМУНІКАЦІЯХ

Дядюра К.О.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: diadiura.kirill@lll.kpi.ua

Досліджено особливості застосування рушія Unreal engine в інфокомунікаційних системах – зокрема для створення візуальних матеріалів. Для цього показано принципи візуалізації інформації та створення контенту. Обґрунтовано вибір Unreal Engine як інструменту для створення навчальних і демонстраційних медіаматеріалів завдяки його можливостям візуалізації та інтерактивності .

APPLICATION OF UNREAL ENGINE IN INFORMATION COMMUNICATIONS

Diadiura K.O.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: diadiura.kirill@lll.kpi.ua

The features of the Unreal Engine application in infocommunication systems are investigated - in particular, for creating visual materials. For this purpose, the principles of information visualization and content creation are shown. The choice of Unreal Engine as a tool for creating educational and demonstration media materials is justified due to its visualization, interactivity, and cross-platform capabilities.

ОСОБЛИВОСТІ РОЗМІЩЕННЯ МОБІЛЬНИХ СТАНЦІЙ ЗВ'ЯЗКУ НА ОСНОВІ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

Кривенко Ю.В.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: kryvenko.yura@lll.kpi.ua

Досліджено особливості розміщення мобільних станцій зв'язку із застосуванням технології Інтернету речей (IoT). Актуальність теми зумовлена зростанням потреби у стабільному зв'язку та ефективному використанні ресурсів мережі. Проаналізовано можливість збору та обробки даних у реальному часі за допомогою IoT для динамічного розташування станцій. Розглянуто вплив змін трафіку, умов середовища та мобільності користувачів на ефективність мережі. Запропонований підхід сприяє покращенню якості зв'язку, зниженню витрат і підвищенню адаптивності телекомунікаційної інфраструктури.

FEATURES OF DEPLOYING MOBILE COMMUNICATION STATIONS BASED ON THE INTERNET OF THINGS TECHNOLOGY

Kryvenko Y.V.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: kryvenko.yura@lll.kpi.ua

Features of deploying mobile communication stations using the Internet of Things (IoT) technology has been studied. The relevance of the topic is driven by the growing demand for stable communication and efficient network resource utilization. The possibility of collecting and processing real-time data using IoT for dynamic station location was analyzed. The impact of traffic fluctuations, environmental conditions, and user mobility on network efficiency is examined. The proposed approach enhances communication quality, reduces costs, and increases the adaptability of telecommunication infrastructure.

МОДИФІКОВАНА АРХІТЕКТУРА ІНФОКОМУНІКАЦІЙНОЇ СИСТЕМИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ОПЕРАЦІЙНОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА РОЗДРІБНОЇ ТОРГІВЛІ

Бачук М. І.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: bachuk.maxym@lll.kpi.ua

Розглянуто сучасні інформаційно комунікаційні системи, які використовуються для автоматизації процесів роздрібної торгівлі, такі як CRM, POS, ERP, WMS та інші. Проведено аналіз існуючих інфокомунікаційних рішень для ринків США та Китаю, розглянутих на прикладі платформ Amazon та AliExpress. Досліджено основні проблеми функціонування систем та запропоновано модифіковану архітектуру для оптимізації операційної діяльності підприємств роздрібної торгівлі.

MODIFIED ARCHITECTURE OF THE INFOCOMMUNICATION SYSTEM FOR ENSURING THE OPERATIONAL ACTIVITIES OF A RETAIL TRADE ENTERPRISE

Bachuk M.I.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: bachuk.maxym@lll.kpi.ua

Modern information and communication systems used to automate retail processes, such as CRM, POS, ERP, WMS, and others, are considered. An analysis of existing information and communication solutions for the US and Chinese markets, considered on the example of the Amazon and AliExpress platforms, is conducted. The main problems of the systems' functioning are investigated and a modified architecture is proposed to optimize the operational activities of retail enterprises.

МЕТОД УПРАВЛІННЯ ОБІГОМ ТОВАРУ ЗА РАХУНОК АВТОМАТИАЦІЇ ПРОЦЕСІВ НА ОСНОВІ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

Журба І. О.
Науковий керівник: **Курдеча В. В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: izhurba321@gmail.com

За останні роки технології Інтернету речей набули стрімкого розвитку. Це, в свою чергу, призвело до застосування таких рішень в усіх сферах людського життя, зокрема в сфері комерційної торгівлі. В даній роботі запропоновано модифікований метод управління обігом товару за рахунок Інтернету речей. Результатом такої модифікації є підвищення ефективності та зручності комерційної торгівлі.

METHOD OF MANAGING GOODS CIRCULATION THROUGH PROCESS AUTOMATION BASED ON INTERNET OF THINGS TECHNOLOGY

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

In recent years, Internet of Things technologies have developed rapidly. This, in turn, has led to the application of such solutions in all spheres of human life, in particular in the field of commercial trade. This work proposes a modified method of managing the circulation of goods using the Internet of Things. The result of such a modification is an increase in the efficiency and convenience of commercial trade.

ОСОБЛИВОСТІ ІНФОКОМУНІКАЦІЙНОГО АУДИТУ

Ковальська Д.Д.
Науковий керівник: **Ільченко М.Ю.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: zashkvar.youtuba01@gmail.com

Досліджено особливості та вразливі аспекти проведення інфокомунікаційного аудиту із застосуванням натурного експерименту. Основною проблемою аудиту великих мереж є необхідність комплексного аналізу всієї інфраструктури для виявлення потенційних загроз, ризиків і слабких місць. Запропоновано новий метод аудиту, що базується на модифікації стандартних підходів шляхом інтеграції спеціалізованого програмного забезпечення. Такий підхід підвищує точність оцінки, мінімізує вплив людського фактору та забезпечує більш глибоке дослідження стану мережевої інфраструктури.

FEATURES OF INFORMATION COMMUNICATION AUDIT

Kovalaska D.D.
Scientific adviser: **Ilchenko M.Y.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: zashkvar.youtuba01@gmail.com

The features and vulnerabilities of conducting an infocommunication audit using a natural experiment have been studied. The main challenge of auditing large networks is the need for a comprehensive analysis of the entire infrastructure to identify potential threats, risks, and weaknesses. A new audit method has been proposed, based on modifying standard approaches by integrating specialized software. This approach enhances assessment accuracy, minimizes the impact of human factors, and ensures a more in-depth examination of the network infrastructure.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ЗАСОБІВ IPERF ТА D-ITG У ТЕСТУВАННІ ПРОДУКТИВНОСТІ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ

Шестопалов С.С.
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: serhii.shestopalov@nure.ua

Досліджено особливості використання засобів iPerf та Distributed Internet Traffic Generator (D-ITG) під час моделювання та навантажувального тестування програмно-конфігурованих мереж (Software-Defined Network, SDN). Розглянуто можливості iPerf для тестування пропускної здатності та D-ITG для генерації реалістичного трафіку з детальним аналізом затримки. Експерименти виконано в середовищі Mininet із контролером Ryu та комутатором Open vSwitch. Проаналізовано вплив мережного навантаження на пропускну здатність, затримку та втрати пакетів. Визначено переваги та обмеження кожного інструменту, що дозволяє обґрунтовано обирати методи навантажувального тестування для SDN залежно від поставлених завдань.

APPLICATION OF IPERF AND D-ITG TOOLS IN PERFORMANCE TESTING OF SOFTWARE-DEFINED NETWORKS

Shestopalov S.S.
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: serhii.shestopalov@nure.ua

The features of applying iPerf and Distributed Internet Traffic Generator (D-ITG) tools for modeling and load testing of Software-Defined Networks (SDN) are investigated. The capabilities of iPerf for throughput testing and D-ITG for generating realistic traffic with detailed delay analysis are considered. The experiments were performed in a Mininet environment with a Ryu controller and an Open vSwitch switch. The impact of network load on throughput, delay, and packet loss is analyzed. The advantages and limitations of each tool are determined, which allows a reasonable choice of load testing methods for SDN, depending on the tasks.

ПОТЕНЦІЙНІ ЗАГРОЗИ ВИКОРИСТАННЯ ДІПФЕЙК-ТЕХНОЛОГІЙ У КІБЕРАТАКАХ

Капуста Р.Д.
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: roman.kapusta@nure.ua

Проведено аналіз існуючих ризиків, що виникають унаслідок використання діпфейк-технологій для створення шкідливого контенту під час кібератак. Виявлено зростання можливостей зловмисників завдяки застосуванню інструментів генерації діпфейк-контенту. Встановлено, що діпфейк-технології сприяють створенню більш правдоподібних оманливих матеріалів, що ускладнює їхнє виявлення. Розкриття такого контенту неможливе без спеціалізованого програмного забезпечення, заснованого на нейромережах. Зроблено висновок, що протидія сучасним атакам із використанням діпфейків потребує високого рівня підготовки та навичок роботи з інструментами штучного інтелекту.

POTENTIAL THREATS OF USING DEEPFAKE TECHNOLOGIES IN CYBERATTACKS

Kapusta R.D.
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: roman.kapusta@nure.ua

The analysis of the existing risks arising from exploiting deepfake technologies to create malicious content during cyberattacks is carried out. An increase in the attackers' capabilities due to using tools for generating deepfake content is revealed. It is established that deepfake technologies contribute to the creation of more plausible misleading materials, which makes them difficult to detect. Disclosure of such content is impossible without specialized software based on neural networks. It is concluded that countering modern attacks using deepfakes requires a high level of expertise and skills in working with artificial intelligence tools.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ПРОТОКОЛІВ OSPF ТА EIGRP В ГІБРИДНИХ МЕРЕЖАХ

Горяінова К.О.
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: karyna.horiainova@nure.ua

Проаналізовано особливості використання протоколів маршрутизації OSPF (Open Shortest Path First) та EIGRP (Enhanced Interior Gateway Routing Protocol) у гібридних мережах. Встановлено, що протокол OSPF є ефективним для розмірних ієрархічних мереж, проте потребує значних обчислювальних ресурсів. Водночас пропрієтарний протокол EIGRP характеризується швидкою конвергенцією та механізмом балансування навантаження, але його застосування обмежене через несумісність із обладнанням сторонніх виробників. Оптимальним підходом може бути використання OSPF для глобальної маршрутизації та EIGRP для локальних сегментів, що сприятиме підвищенню ефективності інфраструктури, хоча ускладнить управління мережею.

FEATURES OF USING OSPF AND EIGRP PROTOCOLS IN HYBRID NETWORKS

Horiainova K.O.
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: karyna.horiainova@nure.ua

The features of using the OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol) routing protocols in hybrid networks are analyzed. It is established that the OSPF protocol is effective for large hierarchical networks but requires significant computing resources. At the same time, the proprietary EIGRP protocol is characterized by rapid convergence and a load-balancing mechanism, but its application is limited due to incompatibility with third-party equipment. The optimal approach would be to use OSPF for global routing and EIGRP for local segments, increasing infrastructure efficiency, although it would complicate network management.

ВИКОРИСТАННЯ АВТОКОРЕЛЯЦІЇ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Пастушенко М.О.
Науковий консультант: Самойленко І.В.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Україна
E-mail: pastushenko.maksym@lll.kpi.ua

Розглядається завдання підвищення безпеки телекомунікаційних систем за рахунок удосконалення системи автентифікації, в яких зараз широко використовуються біометричні ознаки користувача. З точки зору критерію ефективність/вартість найперспективнішими є системи голосової автентифікації (СГА). Для зниження помилок 1 та 2 роду в СГА та якісного розрахунку формантних даних голосового сигналу користувача запропоновано використовувати автокореляційну функцію. На прикладі обробки голосового сигналу користувача показано ефективність використання автокореляції для оцінки формантних даних, у тому числі, і за наявності сигналів, що заважають.

THE USAGE OF AUTOCORRELATION FOR ENHANCING SECURITY IN TELECOMMUNICATION NETWORKS

Pastushenko M.O.
Scientific consultant: Samoilenko I.V.
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Ukraine
E-mail: pastushenko.maksym@lll.kpi.ua

The goal is to improve the security of telecommunication systems by enhancing authentication methods, which often rely on biometric features. From the efficiency/cost criterion perspective, voice authentication systems are the most promising. To reduce Type I and Type II errors in such systems and to accurately calculate the formant data of the user's voice signal, the use of the autocorrelation function is proposed. The effectiveness of using autocorrelation for formant data estimation, including in the presence of interfering signals, is demonstrated using an example of user voice signal processing.

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ВІРТУАЛІЗАЦІЇ МЕРЕЖНИХ ФУНКЦІЙ У ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ

Линник Є.О.
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: yehor.lynnyk@nure.ua

Досліджено використання віртуалізації мережних функцій (Network Functions Virtualization, NFV) у програмно-конфігурованих мережах (Software-Defined Networks, SDN). Визначено основні переваги NFV як зниження витрат на апаратне забезпечення, підвищення гнучкості під час розгортання мережних сервісів, покращення масштабованості та ефективності використання ресурсів завдяки динамічному керуванню мережними функціями, а також інтеграція з технологіями 5G та інтернету речей. Серед недоліків виділено зростання вимог до обчислювальних ресурсів через потребу віртуалізації та безпекові ризики. Окреслено проблемне питання для подальших досліджень щодо розробки методів оптимізації продуктивності NFV.

FEATURES OF NETWORK FUNCTION VIRTUALIZATION IN SOFTWARE-DEFINED NETWORKS

Lynnyk Y.O.
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
mail: yehor.lynnyk@nure.ua

The application of Network Functions Virtualization (NFV) in Software-Defined Networks (SDN) is investigated. The main advantages of NFV are identified as reducing hardware costs, increasing flexibility in the deployment of network services, improving scalability and resource efficiency through dynamic management of network functions, as well as integration with 5G and Internet of Things technologies. Among the disadvantages are the growing demands on computing resources due to the need for virtualization and security risks. The problematic area for further research on developing optimization methods for NFV performance is outlined.

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ МУЛЬТИКОНТРОЛЕРНИХ ПРОГРАМНО-КОНФІГУРОВАНИХ АРХІТЕКТУР

Бондаренко І.М.
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: illia.bondarenko@nure.ua

Досліджено особливості реалізації мультиконтролерних програмно-конфігурованих архітектур. Проаналізовано підходи до взаємодії контролерів, механізми розподілу навантаження та забезпечення відмовостійкості. Розглянуто ключові аспекти масштабованості та узгодженості даних, що передаються між контролерами в централізованих і децентралізованих моделях управління. Оцінено вплив мультиконтролерної архітектури на продуктивність і стабільність програмно-конфігурованих мереж. Отримані результати можуть бути використані для вибору та впровадження ефективних підходів до побудови розподілених систем управління трафіком.

IMPLEMENTATION FEATURES OF MULTI-CONTROLLER SOFTWARE-DEFINED ARCHITECTURES

Bondarenko I.M.
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: illia.bondarenko@nure.ua

The implementation features of multi-controller software-defined architectures are examined. Approaches to controller interaction, mechanisms of load distribution, and fault tolerance are analyzed. The key aspects of scalability and consistency of data transmitted between controllers in centralized and decentralized control models are considered. The impact of the multi-controller architecture on the performance and stability of software-defined networks is evaluated. The obtained results can be used to select and implement effective approaches to building distributed traffic control systems.

ПОРІВНЯННЯ КОНТРОЛЕРІВ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ

Бондаренко І.М.
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: illia.bondarenko@nure.ua

Досліджено особливості роботи та ефективність різних контролерів програмно-конфігурованих мереж. Виконано порівняльний аналіз популярних рішень, як-от ONOS, OpenDaylight, Ryu та Floodlight, за показниками продуктивності, масштабованості та зручності інтеграції. Розглянуто особливості використання контролерів у розподілених архітектурах. На основі проведеного аналізу для подальшої роботи обрано контролер Ryu, який продемонстрував оптимальний баланс продуктивності та гнучкості. Отримані результати можуть бути використані для вибору перспективного рішення залежно від вимог конкретного сценарію застосування.

COMPARISON OF SOFTWARE-DEFINED NETWORK CONTROLLERS

Bondarenko I.M.
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: illia.bondarenko@nure.ua

The features and efficiency of various controllers of software-defined networks are investigated. A comparative analysis of popular solutions, such as ONOS, OpenDaylight, Ryu, and Floodlight, is conducted regarding performance, scalability, and integration convenience. The features of using controllers in distributed architectures are considered. Based on the analysis, the Ryu controller was chosen for further work, as it demonstrated the optimal balance of performance and flexibility. The results obtained can be used to select a promising solution depending on the requirements of a particular application scenario.

ПОРІВНЯННЯ КЛЮЧОВИХ ВІДМІННОСТЕЙ І ПЕРСПЕКТИВ РОЗВИТКУ ТРАДИЦІЙНИХ І ПРОГРАМОВАНИХ МЕРЕЖ

Бондаренко І.М.
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: illia.bondarenko@nure.ua

Проведено порівняння традиційних і програмованих мереж з акцентом на їх ключові відмінності та переваги в різних умовах експлуатації. Обґрунтовано роль програмно-конфігурованих мереж у підвищенні гнучкості та ефективності управління мережними ресурсами. Виконано аналіз архітектури традиційних мереж і порівняння з інноваційними підходами програмованих мереж, зокрема у контексті управління трафіком, масштабованості та адаптивності. Оцінено можливості інтеграції програмованих мереж з існуючими мережами та переваги, що виникають при використанні централізованого контролю та автоматизації порівняно з традиційними підходами.

COMPARISON OF KEY DIFFERENCES AND PROSPECTS FOR THE DEVELOPMENT OF TRADITIONAL AND PROGRAMMABLE NETWORKS

Bondarenko I.M.
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: illia.bondarenko@nure.ua

A comparison of traditional and programmable networks is conducted to emphasize their key differences and advantages in different operating conditions. The role of software-defined networks in increasing the flexibility and efficiency of network resource management is substantiated. The architecture of traditional networks is analyzed and compared with innovative approaches of programmable networks, particularly in traffic management, scalability, and adaptability. The possibilities of integrating programmable networks with existing networks and the advantages arising from the use of centralized control and automation compared to traditional approaches are evaluated.

МЕТОД УПРАВЛІННЯ РУХОМИМИ ОБ'ЄКТАМИ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

Прокопчук Я.В.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: prokopchuk.yaroslav@lll.kpi.ua

Розвиток технологій Інтернету речей (IoT) забезпечує швидке зростання кількості рухомих об’єктів, які потребують ефективного управління. При цьому особливої актуальності набуває завдання розробки методів управління такими об’єктами в динамічному мережевому середовищі. Метою даної роботи є підвищення ефективності управління рухомими об’єктами в мережі IoT шляхом розробки методу, що враховує особливості їх функціонування та забезпечує надійний контроль і координацію.

METHOD FOR CONTROLLING MOVING OBJECTS IN THE INTERNET OF THINGS NETWORK

Prokopchuk Y.V.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: prokopchuk.yaroslav@lll.kpi.ua

The development of Internet of Things (IoT) technologies is ensuring a rapid growth in the number of moving objects that require effective management. At the same time, the task of developing methods for managing such objects in a dynamic network environment becomes particularly relevant. The aim of this work is to increase the efficiency of managing moving objects in the IoT network by developing a method that takes into account the peculiarities of their functioning and provides reliable control and coordination.

СИСТЕМА ЗВ'ЯЗКУ НАЗЕМНОГО ТРАНСПОРТУ ПАСАЖИРСЬКИХ ПЕРЕВЕЗЕНЬ

Богдан А. С.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: bogdan.anastasia@lll.kpi.ua

Розвиток пасажирських перевезень неможливий без забезпечення постійно наявного та надійного зв'язку. При цьому, не звачаючи на постійний розвиток систем зв'язку, в сфері наземного транспорту є ряд невирішених питань, таких як наявність зон «без покриття», вибір рішення в залежності від місця застосування транспорту тощо. В даній роботі розглядаються питання підвищення якості зв'язку за рахунок сумісного застосування кількох систем, окремо сформовано та запропоновано рекомендації по створенню та модифікації таких систем.

PASSENGER TRANSPORT GROUND TRANSPORT COMMUNICATION SYSTEM

Bogdan A.S.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: bogdan.anastasia@lll.kpi.ua

The development of passenger transportation is impossible without ensuring constantly available and reliable communication. At the same time, despite the constant development of communication systems, there are a number of unresolved issues in the field of ground transport, such as the presence of "no coverage" zones, the choice of a solution depending on the place of use of transport, etc. This work considers the issues of improving the quality of communication through the joint use of several systems, and separately formulated and proposed recommendations for the creation and modification of such systems.

IOT СИСТЕМА ІНФОРМУВАННЯ

Ковальчук С.С.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: serghkoval1337@ukr.net

Розглянуто особливості систем інформування. Показано можливість підвищення ефективності таких систем за рахунок застосування IoT-технологій. Для підтвердження ефективності в роботі пропонується вибрати в якості критеріїв енергоефективність, затримку передачі інформації та складність реалізації системи.

IOT INFORMATION SYSTEM

Kovalchuk S.S.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: serghkoval1337@ukr.net

The features of information systems are considered. The possibility of increasing the efficiency of such systems through the use of IoT technologies is shown. To confirm the efficiency in the work, it is proposed to choose energy efficiency, information transmission delay and complexity of system implementation as criteria.

ОСОБЛИВОСТІ МОНІТОРИНГУ АВТОБУСНОГО ПАРКУ

Богдан А. С.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: bogdan.anastasia@lll.kpi.ua

Забезпечити ефективне управління автобусним парком та надання високоякісного сервісу пасажирам можливо лише при наявності ефективного моніторингу. В даній роботі розглянуто як особливості моніторингу так і вимоги систем контролю руху. Метою є підвищення безпеки пасажирів, оптимізація маршрутів і зниженню експлуатаційних витрат. В роботі показано можливі варіанти комплектування засобами моніторингу автобусів, сформовано переваги та недоліки кожного з них.

FEATURES OF BUS FLEET MONITORING

Bogdan A.S.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: bogdan.anastasia@lll.kpi.ua

Ensuring effective management of the bus fleet and providing high-quality service to passengers is possible only with effective monitoring. This work considers both the features of monitoring and the requirements of traffic control systems. The goal is to increase passenger safety, optimize routes and reduce operating costs. The work shows possible options for equipping buses with monitoring means, and the advantages and disadvantages of each of them are formed.

МЕТОД ЗБОРУ ТА ЗБЕРІГАННЯ ІНФОРМАЦІЇ СЕНСОРНОЇ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

Мальченко Д.С.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: malchenko.diana@lll.kpi.ua

Стрімкий розвиток систем зв'язку призвів до широкого застосування систем Інтернету речей, у тому числі сенсорних мереж. Це в свою чергу сформувало проблемне питання збору та зберігання інформації. Саме це і є предметом дослідження даної роботи. В роботі проаналізовано існуючі рішення та запропоновано рекомендації по їх застосуванню.

METHOD OF COLLECTING AND STORAGE OF INFORMATION AT THE SENSOR NETWORK OF THE INTERNET OF THINGS

Malchenko D.S.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: malchenko.diana@lll.kpi.ua

The rapid development of communication systems has led to the widespread use of Internet of Things systems, including sensor networks. This, in turn, has created a problematic issue of information collection and storage. This is the subject of this work. The work analyzes existing solutions and offers recommendations for their application.

DEVICE OF THE INTERNET OF FOR CARGO SUPPORT

Petrov N.E.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: petrov.nikita@lll.kpi.ua

The development of Internet of Things systems has made it possible to use this technology in many applied areas of human activity. Of particular interest is the application in cargo delivery. In this work, an Internet of Things device is proposed, which will allow monitoring the condition of the cargo and informing interested parties.

ПРИСТРІЙ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ СУПРОВОДУ ВАНТАЖУ

Петров Н.Є.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: petrov.nikita@lll.kpi.ua

Розвиток систем Інтернету речей дозволив застосовувати цю технологію в багатьох прикладних сферах людської діяльності. Особливий інтерес становить застосування в доставці вантажів. В даній роботі запропоновано пристрій Інтернету речей, що дозволить відслідковувати стан вантажу та інформувати зацікавлених осіб.

ПРОЦЕС УПРАВЛІННЯ РУХОМИМИ РОБОТАМИ

Конотопова Ю.В.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: konotopova.julia@lll.kpi.ua

Розвиток робототехніки забезпечується тенденціями розвитку дронів, штучного інтелекту, мікроелектроніки тощо. При цьому ці пристрої зустрічаються не лише в виробництві і спеціалізованих сферах, але й в побутовій сфері, що було забезпечено здешевінням подібних рішень. Однак управління роботами на «побутовому» рівні все ще має досить багато проблем. В даній роботі проведено аналіз процесів управління рухомими роботами, показано типову структуру мобільного робота.

MOBILE ROBOT CONTROL PROCESS

Konotopova Y.V.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: konotopova.julia@lll.kpi.ua

The development of robotics is provided by the trends in the development of drones, artificial intelligence, microelectronics, etc. At the same time, these devices are found not only in production and specialized areas, but also in the household sector, which was ensured by the reduction in the cost of such solutions. However, robot control at the "household" level still has quite a few problems. This paper analyzes the processes of controlling mobile robots, shows a typical structure of a mobile robot.

СПЕЦИФІКА 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

Визначено ключові фактори, що впливають на успішність оновлення програмного забезпечення в розподілених IoT-системах. Дослідження показало, що швидкість передачі даних, енергоспоживання пристрою, тип мережевого з'єднання та рівень відмов мають значний вплив на результат оновлення. Особливу увагу приділено стабільності з'єднання, оскільки переривання процесу оновлення може призвести до пошкодження файлової системи пристрою або його повної непрацездатності. Запропоновано використовувати адаптивні алгоритми завантаження оновлень, які враховують поточний рівень сигналу та залишковий заряд акумулятора пристрою.

SPECIFICITIES OF SOFTWARE UPDATES 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

Key factors influencing the success of software updates in distributed IoT systems have been identified. The study showed that data transfer rate, device power consumption, network connection type, and failure rate have a significant impact on the update result. Particular attention is paid to connection stability, since interruption of the update process can lead to damage to the device's file system or its complete inoperability. It is proposed to use adaptive update download algorithms that take into account the current signal level and the remaining battery charge of the device.

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ ІНТЕРНЕТУ РЕЧЕЙ

Прудкий В. С.
Науковий керівник: **Курдеча В. В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: reker166@gmail.com

Дослідження існуючих методів підвищення енергоефективності IoT. Аналіз найбільш поширених протоколів зв’язку, алгоритмів управління живленням та механізмів збору енергії з навколишнього середовища. Аналіз підходів для зменшення навантаження на мережу та мінімізаії зайвого трафіку.

FEATURES OF ENSURING ENERGY EFFICIENCY OF THE INTERNET OF THINGS

Prudkiy V. S.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: reker166@gmail.com

Research on existing methods for improving IoT energy efficiency. Analysis of the most common communication protocols, power management algorithms, and mechanisms for harvesting energy from the environment. Analysis of approaches to reducing network load and minimizing unnecessary traffic.

ВИКОРИСТАННЯ CISCO MODELING LABS ДЛЯ ТЕСТУВАННЯ ТА МОДЕЛЮВАННЯ МЕРЕЖНИХ ІНФРАСТРУКТУР

Савченко Р.О.
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: roman.savchenko1@nure.ua

Досліджено використання Cisco Modeling Labs (CML) для тестування та моделювання мережних інфраструктур. Обґрунтовано важливість використання віртуалізації для створення реалістичних мережних середовищ без необхідності фізичного обладнання. Проаналізовано переваги CML для емуляції різних типів пристроїв та створенні віртуальних складних топологій мереж, що забезпечують можливість швидкої адаптації до нових технологій, тестування та моніторингу продуктивності мереж у реальному часі. Виконано порівняння ефективності CML з традиційним тестуванням на фізичному обладнанні та іншими середовищами (EVE-NG, Containerlab). Розроблено тестові сценарії для перевірки стабільності, продуктивності та безпеки мережі.

USING CISCO MODELING LABS TO TEST AND MODEL NETWORK INFRASTRUCTURES

Savchenko R.O.
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: roman.savchenko1@nure.ua

The use of Cisco Modeling Labs (CML) for testing and modeling network infrastructures is investigated. The importance of using virtualization to create realistic network environments without the need for physical equipment is substantiated. The advantages of CML for emulating various types of devices and creating virtual complex network topologies that provide the ability to quickly adapt to new technologies and test and monitor network performance in real time are analyzed. CML performance was compared with traditional testing on physical hardware and other environments (EVE-NG, Containerlab). Test scenarios were developed to check network consistency, performance, and security.

РЕАЛІЗАЦІЯ ПРОТОКОЛІВ VRRP ТА GLBP В СУЧАСНИХ МЕРЕЖАХ З ТЕСТУВАННЯМ У ВІРТУАЛЬНИХ СЕРЕДОВИЩАХ

Савченко Р.О.
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: roman.savchenko1@nure.ua

Досліджено реалізацію рішень захисту шлюзу на основі протоколів VRRP (Virtual Router Redundancy Protocol) та GLBP (Gateway Load Balancing Protocol) у сучасних мережах. Обґрунтовано важливість їх використання для забезпечення надійності та відмовостійкості. Виконано аналіз функціональних можливостей VRRP та GLBP для забезпечення резервування та балансування навантаження між шлюзами у разі виникнення збоїв. Розглянуто процес налаштування протоколів у локальній мережі та хмарній платформі, а також проведено тестування їх ефективності під час збоїв (переривання зв'язку, перевантаження мережі та DDoS атак). Використано інструменти, як-от CML, EVE-NG, Containerlab і Mininet, для відтворення тестових сценаріїв.

IMPLEMENTATION OF VRRP AND GLBP PROTOCOLS IN MODERN NETWORKS WITH TESTING IN VIRTUAL ENVIRONMENTS

Savchenko R.O.
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: roman.savchenko1@nure.ua

Implementing gateway protection solutions based on the VRRP (Virtual Router Redundancy Protocol) and GLBP (Gateway Load Balancing Protocol) protocols in modern networks is investigated. The importance of their application to ensure reliability and fault tolerance is justified. The functionality of VRRP and GLBP is analyzed to provide redundancy and load balancing between gateways in the event of failures. The process of configuring protocols in the local network and cloud platform is considered, and their effectiveness is tested during failures (communication interruption, network congestion, and DDoS attacks). Tools including CML, EVE-NG, Containerlab, and Mininet are used to reproduce test scenarios.

ДОСЛІДЖЕННЯ МЕТОДІВ КЛАСТЕРИЗАЦІЇ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

Соколов О.К.
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: oleksandr.sokolov1@nure.ua

Досліджено застосування методів кластеризації для аналізу кіберзагроз і виявлення аномальної активності в інформаційних системах. Проаналізовано ефективність алгоритмів K-means, DBSCAN та агломеративної кластеризації для сегментації мережного трафіку з метою ідентифікації підозрілих патернів. Розглянуто використання кластеризації для автоматичного виявлення ботнетів, атак DDoS і шкідливих IP-адрес. Оцінено роль машинного навчання (МН) у формуванні адаптивних моделей поведінкового аналізу загроз. Обґрунтовано необхідність подальшого розвитку МН і методів кластеризації та запропоновано підхід до їх інтеграції у системи виявлення вторгнень для покращення точності та швидкості реагування на атаки.

RESEARCH OF CLUSTERING METHODS FOR DETECTING CYBER THREATS

Sokolov O.K.
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: oleksandr.sokolov1@nure.ua

The application of clustering methods for analyzing cyber threats and detecting abnormal activity in information systems is investigated. The effectiveness of K-means, DBSCAN, and agglomerative clustering algorithms for segmenting network traffic to identify suspicious patterns has been analyzed. Clustering is considered for automatically detecting botnets, DDoS attacks, and malicious IP addresses. The role of machine learning (ML) in the formation of adaptive models of behavioral threat analysis is evaluated. The necessity of further development of ML and clustering methods is substantiated, and an approach to their integration into intrusion detection systems is proposed to improve the accuracy and speed of attack response.

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ БЕЗПРОВОДОВИХ ТОЧОК ДОСТУПУ ТА МЕТОДИ ЇХ ЗАХИСТУ

Подлісний Г.С.
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: hlib.podlisnyi@nure.ua

Досліджено найпоширеніші вразливості бепроводових точок доступу, зокрема атаки типу MITM (людина посередині), несанкціонований доступ до мережі та вразливості протоколів безпеки, таких як WPA2 та WPS. Розглянуто типові атаки, що використовують уразливості цих протоколів, а саме KRACK для WPA2 та методів підбору PIN-кодів для WPS. Обґрунтовано важливість використання сучасних стандартів безпеки, таких як WPA3, який забезпечує покращену криптографію та захист від відомих вразливостей. Запропоновано комплексний підхід до захисту безпроводових мереж, що включає в себе постійне оновлення операційних систем, використання стійких паролів та приховання SSID.

RESEARCH OF VULNERABILITIES OF WIRELESS ACCES POINTS AND METHODS OF THEIR PROTECTION

Podlisnyi H.S.
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: hlib.podlisnyi@nure.ua

The most common vulnerabilities of wireless access points are investigated, including man-in-the-middle (MITM) attacks, unauthorized network access, and vulnerabilities of security protocols such as WPA2 and WPS. Typical attacks that exploit the vulnerabilities of these protocols are considered, namely KRACK for WPA2 and PIN guessing methods for WPS. The importance of using modern security standards, such as WPA3, which provides improved cryptography and protection against known vulnerabilities, is substantiated. An integrated approach to protecting wireless networks is proposed, including the constant updating of operating systems, the use of strong passwords and SSID hiding.

SECOPS І NETOPS ДЛЯ ПІДТРИМКИ КІБЕРСТІЙКОСТІ СИСТЕМ І МЕРЕЖ

Гребенюк Є. А.
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: yelyzaveta.hrebeniuk@nure.ua

Досліджено роль SecOps і NetOps у забезпеченні кіберстійкості сучасних інформаційних систем і мереж. Проаналізовано методи автоматизації безпеки та управління мережею для мінімізації ризиків і оперативного реагування на інциденти. Розглянуто підходи до інтеграції засобів безперервного моніторингу, аналізу загроз і самовідновлення систем. Запропоновано використання штучного інтелекту для адаптивного управління безпекою, аналізу поведінкових аномалій та прогнозування атак. Виконано порівняльний аналіз ефективності сучасних рішень для автоматизації SecOps і NetOps, а також їх вплив на кіберстійкість.

SECOPS AND NETOPS TO SUPPORT CYBER RESILIENCE OF SYSTEMS AND NETWORKS

Hrebeniuk Y. A.
Scientific adviser: **Yeremenko O. S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: yelyzaveta.hrebeniuk@nure.ua

The role of SecOps and NetOps in ensuring the cyber resilience of modern information systems and networks is investigated. Security automation and network management methods are analyzed to minimize risks and respond promptly to incidents. Approaches to integrating continuous monitoring tools, threat analysis, and self-healing systems are considered. The use of artificial intelligence for adaptive security management, behavioral anomaly analysis, and attack prediction is proposed. A comparative analysis of the effectiveness of modern solutions for SecOps and NetOps automation, as well as their impact on cyber resilience, is performed.

ДОСЛІДЖЕННЯ СТІЙКОСТІ КАНАЛІВ УПРАВЛІННЯ ДРОНІВ В УМОВАХ ДІЇ АКТИВНИХ ШУМОВИХ ЗАВАД РІЗНОЇ ПОЛЯРИЗАЦІЇ

Душенков О.В.
Науковий керівник: **Мартинчук О.О.**
Харківський національний університет радіоелектроніки, Україна
E-mail: oleksii.dushenkov@nure.ua

У роботі досліджується вплив активних шумових завад різної поляризації на стабільність каналів зв’язку безпілотних авіаційних систем. Визначено, що завади можуть суттєво знижувати ефективність керування, особливо в умовах радіоелектронного протиборства.

Розглядаються різні підходи до зменшення впливу завад, зокрема використання адаптивних антенних систем і цифрової обробки сигналів. Такі методи дозволяють знизити рівень перешкод і покращити якість прийому сигналів управління.

STUDYING THE STABILITY OF DRONE CONTROL CHANNELS UNDER THE INFLUENCE OF ACTIVE NOISE INTERFERENCE OF DIFFERENT POLARIZATION

Dushenkov O.V.
Scientific adviser: **Martynchuk O.O.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: oleksii.dushenkov@nure.ua

The paper investigates the effect of active noise interference of different polarization on the stability of communication channels of unmanned aerial systems. It is determined that interference can significantly reduce the efficiency of control, especially in conditions of electronic warfare.

Various approaches to reducing the impact of interference are considered, including the use of adaptive antenna systems and digital signal processing. Such methods can reduce the level of interference and improve the quality of control signal reception.

ТИПИ АКТИВНИХ ШУМОВИХ ЗАВАД З ВРАХУВАННЯМ РІЗНОЇ ПОЛЯРИЗАЦІЇ МЕТОДОМ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ

Душенков О.В.
Науковий керівник: **Мартинчук О.О.**
Харківський національний університет радіоелектроніки, Україна
E-mail: oleksii.dushenkov@nure.ua

У роботі досліджуються типи активних шумових завад різної поляризації методом математичного моделювання. Визначено їхній вплив на стійкість каналів зв'язку безпілотних авіаційних систем, особливо в умовах радіоелектронного протиборства.

Розглянуто математичне моделювання завад із лінійною, круговою та еліптичною поляризацією, а також методи їхньої нейтралізації, зокрема адаптивні антени та цифрову обробку сигналів. Це дозволяє знизити рівень перешкод і покращити прийом сигналів управління.

STUDYING THE STABILITY OF DRONE CONTROL CHANNELS UNDER THE INFLUENCE OF ACTIVE NOISE INTERFERENCE OF DIFFERENT POLARIZATION

Dushenkov O.V.
Scientific adviser: **Martynchuk O.O.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: oleksii.dushenkov@nure.ua

The study examines the types of active noise jamming with different polarization using mathematical modeling. Their impact on the stability of communication channels in unmanned aerial systems, especially in electronic warfare conditions, is determined.

The research considers mathematical modeling of jamming with linear, circular, and elliptical polarization, as well as methods for their mitigation, including adaptive antennas and digital signal processing. These approaches help reduce interference levels and improve control signal reception.

ЗАСТОСУВАННЯ CISCO PACKET TRACER ПРИ ПОСТАНОВЦІ ЕКСПЕРИМЕНТУ

Дубінко А.Д.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: dubinko.andrii@lll.kpi.ua

Експеримент є невід'ємною частиною наукового дослідження – в тому числі при розробці нових систем, моделюванні певних ситуацій, для навчальних задач. А тому актуальним завданням є постановка експерименту. В даній роботі розглянуто особливості постановки експерименту в Cisco packet tracer. Показано, що даний засіб доцільно застосовувати для моделювання IP мереж – як проводових так і безпроводових.

USING CISCO PACKET TRACER IN EXPERIMENTAL DESIGN

Dubinko A.D.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: dubinko.andrii@lll.kpi.ua

The experiment is an integral part of scientific research – including when developing new systems, modeling certain situations, for educational purposes. And therefore, the actual task is to set up an experiment. This paper examines the features of setting up an experiment in Cisco packet tracer. It is shown that this tool is appropriate to use for modeling IP networks – both wired and wireless.

ПАРАМЕТРИ РОБОТИ БЕЗПРОВОДОВОЇ БАЗОВОЇ СТАНЦІЇ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ

Радуга Н. С.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: raduganazar@gmai.com

В задачі забезпечення якості послуг входить забезпечення надійної та ефективної роботи елементів мережі. Так для стільникового зв’язку окрему увагу слід приділяти базовій станції зв’язку. Завданням публікації є формування переліку параметрів, які найбільш критично відслідковувати для забезпечення надійної роботи базової станції та виявлення нетипових ситуацій.

WIRELESS CELLULAR BASE STATION OPERATION PARAMETERS

Raduga N. S.
Scientific adviser: **KurdechaV.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: raduganazar@gmail.com

The task of ensuring the quality of services includes ensuring reliable and efficient operation of network elements. For example, for cellular communication, special attention should be paid to the communication base station. The task of the publication is to form a list of parameters that are most critically monitored to ensure reliable operation of the base station and identify atypical situations.

ПОРІВНЯННЯ СЕНСОРНИХ МЕРЕЖ ПЛАСКОЇ ТА ІЄРАРХІЧНОЇ ТОПОЛОГІЇ

Короїд Б.О.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: koroid.bohdan@lll.kpi.ua

Сенсорні мережі дозволяють ефективний збір інформації для задач біологічних досліджень, виробництва, служб надзвичайних ситуацій тощо. При цьому при побудові сенсорної мережі існує необхідність вибору топології майбутньої системи. Саме тому в даній роботі визначено переваги та недоліки сенсорних мереж пласкої та ієрархічної топології, а також сформовано рекомендації по вибору топології системи в залежності від специфіки сенсорних мереж.

COMPARISON OF SENSOR NETWORKS WITH FLAT AND HIERARCHICAL TOPOLOGY

Koroid B.O.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: koroid.bohdan@lll.kpi.ua

Sensor networks allow for effective information collection for tasks in biological research, production, emergency services, etc. At the same time, when building a sensor network, there is a need to choose the topology of the future system. That is why this work identifies the advantages and disadvantages of sensor networks of flat and hierarchical topology, and also formulates recommendations for choosing the topology of the system depending on the specifics of sensor networks.

ПОРІВНЯННЯ ЦЕНТРАЛІЗОВАНОГО ТА РОЗПОДІЛЕНОГО ЗБОРУ ІНФОРМАЦІЇ В СЕНСОРНІЙ МЕРЕЖІ

Мальченко Д.С.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: malchenko.diana@lll.kpi.ua

Збір інформації – одна з основних задач сенсорної мережі. І за останні роки в зв'язку зі стрімким розвитком сенсорних мереж на основі технологій Інтернету речей все актуальнішим завданням є налаштування особливостей даного процесу. Зокрема вибір доволі часто постає поміж централізованим та розподіленим збором інформації. Це питання і розкриває дана публікація. Зокрема в якості критеріїв розглядаються питання енергоефективності, можливостей передачі інформації та її обробки не тільки в хмарному середовищі.

COMPARISON OF CENTRALIZED AND DISTRIBUTED INFORMATION COLLECTION IN A SENSOR NETWORK

Malchenko D.S.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: malchenko.diana@lll.kpi.ua

Information collection is one of the main tasks of a sensor network. And in recent years, due to the rapid development of sensor networks based on Internet of Things technologies, the task of configuring the features of this process has become increasingly relevant. In particular, the choice often arises between centralized and distributed information collection. This issue is addressed in this publication. In particular, the criteria considered include energy efficiency, the ability to transmit information and process it not only in a cloud environment.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ У СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

Прудкий В. С.
Науковий керівник: **Курдеча В. В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: reker166@gmail.com

Стрімке зростання кількості пристроїв Інтернету речей призвело до того, що проблема безпеки систем IoT стала однією з головних. Враховуючі особливості технічних можливостей, територіального розміщення таких пристроїв, фактор безпеки одного пристрою може стати вразливістю всієї системи. В даній публікації розглянуто основні шляхи забезпечення безпеки таких систем.

SECURITY IN INTERNET OF THINGS SYSTEMS

Prudkiy V. S.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: reker166@gmail.com

The rapid growth of the number of Internet of Things devices has led to the fact that the problem of security of IoT systems has become one of the main ones. Taking into account the peculiarities of technical capabilities and the territorial location of such devices, the security factor of one device can become a vulnerability of the entire system. This publication considers the main ways to ensure the security of such systems.

ОСОБЛИВОСТІ СОЦІАЛЬНОГО ІНТЕРНЕТУ РЕЧЕЙ

Пінчук Ю.М.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail pinchuk.yulia@lll.kpi.ua

Соціальний Інтернет речей (SIoT) – це та частина Інтернету речей, яка здатна встановлювати соціальні зв'язки з іншими об'єктами стосовно людей. SIoT намагається пом'якшити проблеми Інтернету речей у сферах масштабованості, довіри та пошуку ресурсів, взявши приклад із соціальних обчислень. В роботі розглядаються деякі з основних компонентів, які забезпечують успішну роботу програм SIoT, такі як метаінформація, особливості безпеки, наявні сервіси таких систем.

FEATURES OF THE SOCIAL INTERNET OF THINGS

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@lll.kpi.ua

The Social Internet of Things (SIoT) is the part of the Internet of Things that is capable of establishing social connections with IoT objects in relation to people. SIoT attempts to mitigate the problems of the Internet of Things in the areas of scalability, trust, and resource search, taking an example from social computing. The paper examines some of the main components that ensure the successful operation of SIoT applications, such as meta-information, security features, and available services of such systems.

МОДИФІКОВАНИЙ МЕТОД ПІДВИЩЕННЯ БЕЗПЕКИ РОЗУМНОГО БУДИНКУ

Кузнецов Я.В.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: kuznetsov.yaroslav@lll.kpi.ua

Безпека Інтернету речей – одне з ключових проблемних питань, особливо, якщо це стосується розумного будинку, тобто напряму має відношення до комфорту, життя та здоров'я людини. В роботі пропонується механізм підвищення безпеки розумного будинку, за рахунок кількох механізмів контролю подій вузлів Інтернету речей.

MODIFIED METHOD OF ENHANCING SMART HOME SECURITY

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@lll.kpi.ua

The security of the Internet of Things is one of the key topics, especially when it comes to a smart home – that is, it is directly related to human comfort, life, and health. The paper proposes a mechanism for increasing the security of a smart home through several mechanisms for controlling events in Internet of Things nodes.

РІШЕННЯ
ДЕВ'ЯТНАДЦЯТОЇ МІЖНАРОДНОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ» ПТ-2025 та ПРІТС-2025

Відповідно наказу **№НОД/14.00/443/25 від 28.01.2025 р**. КПІ ім. Ігоря Сікорського з 14 по 18 квітня 2025 року в м. Києві, на базі Навчально-наукового Інституту телекомунікаційних систем та НДІ телекомунікацій КПІ ім. Ігоря Сікорського, в умовах воєнного стану в Україні, у змішаному форматі (пленарні засідання – очно, секційні засідання - on-line), відбулася XIX Міжнародна науково-технічна конференція «ПТ-2025» та XVII МНТК студентів та аспірантів ПРІТС-2025. На пленарних та 6 секційних засіданнях було заслухано: привітання, 10 пленарних виступів, 3 стендові та 109 доповідей із 155 поданих. Загалом у роботі конференції заявили про участь 192 особи (автори, співавтори, слухачі). Проведено on-line виставку: «Інноваційні розробки у сфері телекомунікацій», на якій представлено 3 стенди.

В організації та проведенні конференції ПТ-2025 взяли участь від КПІ ім. Ігоря Сікорського 10 підрозділів, 21 організацій з 4 міст України – Києва, Житомира, Харкова, Чернівців, Черкас та 4 країн світу: Англії, Швеції, Іраку, Єгипету.

Цього року на конференції зросла кількість доповідей присвячених розвитку мереж 5G та 6G, перспективам супутникового зв'язку, та використанню штучного інтелекту та Інтернету речей в електронних комунікаціях. На цьогорічній конференції були представлені доповіді виконані закордонними науковцями. Зміст цих доповідей відповідав пріоритетним науковим напрямкам, які визначені Всесвітнім мікрохвильовим конгресом 2024 року.

Оцінюючи науковий рівень, практичні результати та перспективи подальшого використання матеріалів, що склали зміст пленарних і секційних засідань, конференція відзначає такі 5 груп доповідей (додаток 1):

1. За сукупністю зазначених критеріїв найбільший інтерес і перспективу пріоритетного використання в навчальному процесі отримали 19 доповідей, з яких 15 у співавторстві зі студентами та аспірантами.
2. Після певного доопрацювання, можливого об'єднання матеріалів з розширенням обсягу статей та акцентування на новизні наукових результатів 16 доповідей можуть бути рекомендовані до включення в черговому випуску монографії видавництва «Springer».

3. Після належного оформлення під вимоги вітчизняних фахових наукових журналів категорії А або Б, зокрема журналу «Information and Telecommunication Sciences», 19 доповідей можуть бути опубліковані в цих журналах.
4. 10 доповідей, в яких представлені новітні розробки, рекомендуються до участі в конкурсах (фестивалях) інноваційних проектів та стартапів, зокрема *Sikorsky* Challenge.
5. 8 доповідей мають потенціальні можливості для подальшого отримання нових науково-практичних результатів і рекомендуються для участі у вітчизняних або міжнародних конкурсах чи грантах.
6. Організаційно-фаховими рекомендаціями конференції є такі:

6.1. Активізація участі в конференції науково-педагогічних працівників і аспірантів в контексті виконання ними їхніх індивідуальних планів роботи та взаємодії із закордонними партнерами.

6.2. Залучення до участі в конференції фахівців телекомунікаційної галузі, установ Мінцифри, Держспецзв'язку, компаній зі сфери ІКТ і підприємств ОПК ґрунтувати на базі спільних інтересів і спільної діяльності з виконання конкретних проектів, надання послуг, підготовки кадрів.

6.3. Активізувати залучання іноземних науковців до виступів на конференції. Науковцям ННІТС, які мають іноземних партнерів в рамках виконання наукових проектів та отримання грантів, примати участь у конференції у співавторстві з іноземними колегами.

6.4. Обмежити можливість подання матеріалів на конференцію від одного автора кількістю 3 тези.

6.5. Провести роз’яснювальну роботу зі студентами ННІТС стосовно академічної доброчесності та плагіату в контексті участі у конференціях.

6.6. Продовжити практику проведення під час конференції виставок інноваційних розробок у сфері інфокомунікацій, в тому числі за участі радіотехнічного клубу «Політехнік» КПІ ім. Ігоря Сікорського UT7UZA.

6.7. Розширити об’єм тез доповідей виконаних на пленарному засіданні до 8 стр.

6.8. За результатами виступу на пленарному засіданні рекомендувати монографію Трубіна О.О. «INTRODUCTION TO THE THEORY OF DIELECTRIC RESONATORS» до участі у конкурсі на кращі видання КПІ ім. Ігоря Сікорського».

6.9. Кращі доповіді пленарного засідання та від секцій відзначати сертифікатами конференції.

7. Інформацію про проведення XIX МНТК ПТ-2025 та ПРІТС-2025 (програму, збірник матеріалів, рішення та фотозвіти, відеозаписи найкращих доповідей) розмістити на сайтах конференції, телеграм каналі конференції та сайті НН ІТС, та на загальноуніверситетських ресурсах й на відеохостінгу YouTube.
8. Відзначити подякою усіх організаторів проведення конференції, а саме Новогрудську Р.Л., Іванову Т.Л., Березовську О.
9. Наступну XX Міжнародну науково-технічну конференцію «Перспективи телекомунікацій-2026» та XVII МНТК студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем», провести у квітні 2026 року.

Рішення схвалено на засіданні Вченої Ради НН ІТС КПІ ім. Ігоря Сікорського 28.04.2025 р. (Протокол № _4_).