МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Кваліфікаційна наукова
праця на правах рукопису

КОЗЛОВ ДМИТРО ЄВГЕНОВИЧ

УДК 004.738.5:004.942

ДИСЕРТАЦІЯ

МЕТОД ПОБУДОВИ СЕНСОРНИХ МЕРЕЖ НА БАЗІ САМООРГАНІЗАЦІЇ

123 - Комп’ютерна інженерія

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Д.Є. Козлов

Науковий керівник Сторчак Каміла Павлівна,

доктор технічних наук, професор

Київ - 2025

АНОТАЦІЯ

Козлов Д.Є. Метод побудови сенсорних мереж на базі самоорганізації. - Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія. - Державний університет інформаційно-комунікаційних технологій Міністерства освіти і науки України, Київ, 2025.

Робота присвячена дослідженню проблеми побудови, оптимізації, розгортання та тестування бездротових сенсорних мереж із застосуванням самоорганізації. Особливу увагу приділено розробці методу прийняття рішень щодо вибору оптимальної мережевої технології та її параметрів на етапі впровадження, коли ще відсутня можливість збору емпіричних даних про продуктивність реальної системи.

Актуальність теми дослідження. Сучасні сенсорні мережі демонструють стійку тенденцію до зростання масштабів розгортання, кількості підключених пристроїв та ускладнення топології мереж. Це зумовлює підвищення вимог до характеристик сенсорних мереж як енергоефективність, надійність, масштабованість та стійкість до відмов у складних динамічних умовах. У зв'язку з цим виникає необхідність у створенні нових підходів до вибору конфігурації сенсорних мереж.

Класична архітектура сенсорних мереж є переважно централізованою та має істотні обмеження щодо масштабування, гнучкості маршрутизації та відмовостійкості. Ускладнення мережевої топології та зростання кількості вузлів часто призводить до перевантаження мережі та втрати даних під час передавання повідомлень.

Існуючі методи побудови сенсорних IoT-мереж орієнтовані переважно на окремі аспекти використання, наприклад: енергоефективність або сумісність протоколу та не забезпечують узгодженого врахування прикладних вимог,

особливостей середовища функціонування та параметрів доступних технологій. Особливо недостатньо розроблені підходи, що дозволяють проєктувати сенсорну мережу з урахуванням сценаріїв застосування та зміни умов експлуатації.

Питання ефективності ускладняється тим що більшість протоколів маршрутизації не враховують потенціалу можливості квазіортогонального доступу до мережі та не підтримують багатоперехідну комунікацію, яка могла б істотно підвищити стійкість та покриття, без потреби в використанні додаткових шлюзів. Сучасна практика побудови мережі практично не забезпечує засобів автоматизованої підтримки процесу конфігурації із застосуванням багатокритеріального аналізу та симуляційного моделювання.

Вперше розроблено модель мультипротокольної сенсорної мережі, яка за рахунок використання багатокритеріального аналізу та теорії розподілених систем, дозволяє визначити оптимальну конфігурацію мережі.

Удосконалено метод взаємодії вузлів сенсорної мережі, який за рахунок використання розробленої моделі мультипротокольної сенсорної мережі та комплексного врахування спектральних параметрів сигналу, дозволяє підвищити ефективність передавання повідомлень у сенсорній мережі.

Вперше розроблено метод визначення маршруту передавання даних між вузлами сенсорної мережі, який за рахунок удосконаленого методу взаємодії вузлів сенсорної мережі та врахування параметрів сенсорної мережі на основі теорії зважених графів та самоорганізації дозволяє підвищити коефіцієнт доставки повідомлень.

Експериментально доведено ефективність розробленого методу мережевої взаємодії: кількість пристроїв, які успішно передають повідомлення до центрального додатку зростає у порівнянні з базовим сценарієм передавання даних. Комплексне врахування спектральних параметрів сигналу дозволяє підвищити відсоток успішно переданих повідомлень у сенсорній мережі за рахунок використання службових повідомлень що підтверджують отримання пакету даних, ефект від використання повідомлень що підтверджують отримання

пакету даних особливо помітний у режимі роботи мережі з недостатньою кількістю шлюзів де відсоток успішно переданих повідомлень збільшується в середньому на 40%.

Практичне значення одержаних результатів полягає в розробці програмного комплексу, який дозволяє моделювати і досліджувати функціонування сенсорних мереж в різноманітних режимах роботи. Програмний комплекс підтримує дискретну генерацію подій у мережі, що дозволяє проводити порівняльний аналіз ефективності.

Дисертація виконувалась в Державному університеті інформаційно-комунікаційних технологій. Обраний напрям досліджень відповідає тематиці науково-дослідних робіт комунікаційних технологій.

Ключові слова: Інтернет речей, архітектура, прийняття рішень, алгоритм, саморганізація, оптимізація, автоматизація, сенсорні пристрої, канали зв’язку, моделювання, бездротовий зв’язок, інформаційна система, мережа.

Результати дисертаційного дослідження впроваджено у виробничий процес:

- ТОВ "УКР-ОН";
- ТОВ "КАРНІФЕКС"

Також результати досліджень впроваджені в навчальний процес Державного університету інформаційно-комунікаційних технологій.

Ключові слова: Інтернет речей, архітектура, прийняття рішень, алгоритм, саморганізація, оптимізація, автоматизація, сенсорні пристрої, канали зв’язку, моделювання, бездротовий зв’язок, інформаційна система, мережа, протокол, сервер.

ABSTRACT

Kozlov D.Ye. Method for Constructing Sensor Networks Based on Self-Organization. – Qualification Scientific Work as a Manuscript.

Dissertation for the Degree of Doctor of Philosophy in Specialty 123 – Computer Engineering. – State University of Information and Communication Technologies of the Ministry of Education and Science of Ukraine, Kyiv, 2025.

The dissertation is devoted to the investigation of the construction, optimization, deployment, and testing of wireless sensor networks utilizing self-organization. Special attention is given to the development of a decision-making method for selecting the optimal network technology and its parameters at the deployment stage, when empirical data on the real system's performance are not yet available.

Relevance of the research topic. Modern sensor networks demonstrate a persistent trend toward expanding deployment scales, increasing the number of connected devices, and complicating network topology. This leads to increased requirements for sensor networks in terms of energy efficiency, reliability, scalability, and fault tolerance in complex dynamic conditions. Consequently, there is a growing need for new approaches to the configuration selection of sensor networks.

The classical architecture of sensor networks is predominantly centralized and has significant limitations regarding scalability, routing flexibility, and fault tolerance. The increasing complexity of network topology and the growing number of nodes often lead to network congestion and data loss during message transmission.

Existing methods for constructing sensor IoT networks are mostly focused on specific usage aspects, such as energy efficiency or protocol compatibility, and do not provide for consistent consideration of application requirements, environmental features, and available technology parameters. In particular, approaches that allow for the design of sensor networks with regard to application scenarios and changing operating conditions remain insufficiently developed.

Efficiency issues are further complicated by the fact that most routing protocols do not take into account the potential for quasi-orthogonal network access and do not support multi-hop communication, which could significantly improve resilience and coverage without the need for additional gateways. Current network design practice provides virtually no means of automated configuration support using multicriteria analysis and simulation modeling.

For the first time, a model of a multiprotocol sensor network has been developed, which, by utilizing multicriteria analysis and the theory of distributed systems, enables the determination of the optimal network configuration.

The method of sensor node interaction has been improved. By employing the developed model of a multiprotocol sensor network and comprehensive consideration of the spectral parameters of the signal, it is possible to enhance the efficiency of message transmission within the sensor network.

A method for determining data transmission routes between sensor network nodes has been developed for the first time. Through the improved method of sensor node interaction and consideration of the sensor network parameters based on weighted graph theory and self-organization, the method increases the message delivery ratio.

The effectiveness of the developed method for network interaction has been experimentally demonstrated: the number of devices successfully transmitting messages to the central application increases in comparison with the baseline data transmission scenario. Comprehensive consideration of the spectral parameters of the signal makes it possible to increase the percentage of successfully transmitted messages in the sensor network due to the use of service messages confirming data packet receipt. The effect of such confirmation messages is especially significant under network operation modes with an insufficient number of gateways, where the percentage of successfully delivered messages increases on average by 40%.

The practical significance of the obtained results lies in the development of a software package that allows for modeling and investigating the functioning of sensor

networks in various operating modes. The software package supports discrete event generation in the network, which enables comparative efficiency analysis.

The dissertation was carried out at the State University of Information and Communication Technologies. The chosen research direction is in line with the scientific research topics in communication technologies.

Keywords: Internet of Things, architecture, decision-making, algorithm, self-organization, optimization, automation, sensor devices, communication channels, modeling, wireless communication, information system, network, protocol, server.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

1. Міронов Д. С., Тушич А. М., Козлов Д. Є. Дослідження архітектури API для зв’язку між клієнтом та сервером. Зв’язок. 2024. Т. 167, № 1. С. 26–29.

2. Зуб О. В., Козлов Д. Є. Інтернет речей для розвитку та доступності цифрової освіти. Наукові записки Державного університету інформаційно-комунікаційних технологій. 2024. Т. 6, № 1. С. 145–152.

3. Методика прогнозування мобільності користувачів у 5G-мережах / Д. Козлов та ін. Телекомунікаційні та інформаційні технології. 2024. Т. 85, № 1. С. 136–141.

4. Концевий В. В., Козлов Д. Є. Пошук лідера віртуальної команди в проєктно-орієнтованій організації з використанням моделі FIRO-B. Зв’язок. 2025. Т. 174, № 2. С. 114–121.

5. Лисенко М., Козлов Д. AIOT-система на базі теорії графів для медичної сфери. Телекомунікаційні та інформаційні технології. 2025. Т. 87, № 2. С. 108–112.

6. III Всеукраїнська науково-технічна конференція «Сучасний стан та перспективи розвитку IoT»; Оцінка ефективності штучного інтелекту для вирішення нетипових завдань голосовим помічником; 15 травня 2022р., Державний університет телекомунікацій, м. Київ.

7. IV Всеукраїнська науково-технічна конференція «Сучасний стан та перспективи розвитку IoT». Розробка відмовостійкої інформаційної мережі на базі обладнання MIKROTIK; 7 квітня 2023р., Державний університет телекомунікацій, м. Київ.

8. V Всеукраїнська науково-технічна конференція «Сучасний стан та перспективи розвитку IoT». Створення рекомендацій для автоматизації тестування програмного забезпечення на операційній системі ANDROID, 18 квітня 2024р., Державний університет інформаційно-комунікаційних технологій, м. Київ.

9. Всеукраїнська науково-технічна конференція «Сучасний стан та перспективи розвитку IoT». Підвищення ефективності та безпеки дорожнього руху шляхом інтеграції IoT, 15 квітня 2025р., Державний університет інформаційно-комунікаційних технологій, м. Київ.

ЗМІСТ

ВСТУП……... 18
1 АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ ТА ДОСЛІДЖЕНЬ У СФЕРІ ЗВ’ЯЗКУ СЕНСОРНИХ МЕРЕЖ……..... 24
1.1 Огляд та класифікація сучасних технологій бездротового зв'язку для IoT…… 26
1.1.1 LoRa в контексті сенсорних мереж: технічний аналіз і практичні аспекти……. 34
1.1.2 Принципи роботи та обмеження технологій зв’язку сенсорних мереж……. 39
1.2 Огляд досліджень і практичних підходів до застосування LoRa в бездротових сенсорних мережах……. 46
1.2.1 Багатоперехідні рішення в архітектурі сенсорної мережі…… 47
1.2.2 Багатоперехідні та mesh-мережі для децентралізованих систем ……...……. 52
1.2.3 Програмні бібліотеки та інструменти моделювання……. 65
1.2.4 Комерційні продукти та пристрої……... 68
1.2.5 Виявлення множинних значень фактору розширення модуляції…… 69
1.3 Дослідження існуючих методів оцінки та вибору конфігурації для побудови бездротових сенсорних мереж…… 71
1.3.1. Проблематика вибору конфігурації бездротових сенсорних мереж……. 72
1.3.2. Роль симуляцій та методик підтримки прийняття рішень у проєктуванні конфігурацій сенсорних мереж……... 75
1.3.3 Аналіз можливих методів оптимізації сенсорних мереж з урахуванням продуктивності та масштабованості…… 76
Висновки до розділу 1……. 80
2 РОЗРОБКА МАТЕМАТИЧНОГО МЕТОДУ ВИБОРУ ОПТИМАЛЬНОЇ КОНФІГУРАЦІЇ СЕНСОРНОЇ МЕРЕЖІ…… 82
2.1 Визначення проблеми вибору оптимальної технології та конфігурації сенсорної мережі…… 82
2.1.1 Формування абстракції для сенсорної мережі та визначення ключових параметрів для аналізу мережевої ефективності……. 84
2.1.2 Визначення ключових показників ефективності для оцінки сенсорних мереж …….. 87

2.1.3 Моделювання ключових мережевих параметрів для подальшого вибору оптимальної конфігурації сенсорної мережі..… 88
2.2 Загальний огляд запропонованого методу прийняття рішень…..…. 91
2.2.1 Моделювання вимог до сенсорних мереж…… 93
2.2.2 Попередній відбір мережевих технологій……. 95
2.2.3 Проєктування сценаріїв використання, оцінювання масштабованості та проведення симуляційної оцінки роботи сенсорної мережі……... 95
2.2.4 Оцінювання сценаріїв розгортання та вплив топології на продуктивність сенсорної мережі……....… 97
Висновки до розділу 2…….. 115
3 АРХІТЕКТУРА ТА АНАЛІЗ ЕФЕКТИВНОСТІ ДЕЦЕНТРАЛІЗОВАНОЇ СЕНСОРНОЇ МЕРЕЖІ……. 117
3.1 Передумови для розробки сенсорної мережі екстреного реагування……. 117
3.1.1 Проблема втрати зв’язку у надзвичайних ситуаціях…… 120
3.2 Розробка сенсорної мережі із застосуванням LoRa……. 123
3.2.1 Технічні вимоги до сенсорної мережі…… 124
3.2.2 Базова та розширена архітектура сенсорної мережі……. 126
3.3 Моделювання роботи сенсорної мережі в реальних умовах…….. 137
3.3.1 Визначення основних параметрів роботи мережі……...…. 139
3.3.2 Використання програмного фреймворку OMNet++ для моделювання роботи сенсорної мережі……. 144
3.4 Оцінювання впливу змін параметрів роботи для базової та удосконаленої сенсорної мережі……. 147
3.4.1 Дослідження роботи базової сенсорної мережі…… 148
3.4.2 Дослідження роботи удосконаленої сенсорної мережі з використанням механізму ACK…….. 160
Висновки до розділу 3…….. 178
4 РОЗРОБКА ПРОТОКОЛУ САМООРГАНІЗАЦІЇ З МНОЖИННИМ ВИКОРИСТАННЯМ ФАКТОРУ РОЗШИРЕННЯ МОДУЛЯЦІЇ…… 180
4.1 Попередні дослідження автоматичного визначення та застосування множинного фактору розширення модуляції……. 181
4.1.1 Розробка та впровадження механізму визначення множинного фактору розширення модуляції……... 184
4.1.2 Оцінювання ефективності методу автоматичного визначення множинного фактору модуляції……. 186

4.2 Векторний протокол для самоорганізації в сенсорних мережах….. 189
4.2.1 Мережева топологія та адресація……... 190
4.2.2 Структура мережевих пакетів…… 192
4.2.3 Маршрутизація…… 193
4.2.4 Обмін маршрутами між сусідніми мережевими вузлами…… 198
4.2.5 Використання мережевих метрик для маршрутизації……. 200
4.2.6 Механізми запобігання утворенню мережевих петель…… 204
4.3 Налаштування програмного середовища для тестування протоколу самоорганізації…….. 206
4.3.1 Опис тестової топології сенсорної мережі…… 207
4.3.2 Характеристики мережевих вузлів та налаштування трафіку…. 211
4.3.3 Порівняльний аналіз між продуктивністю реального обладнання та програмної симуляції…….. 212
4.4 Експериментальне дослідження протоколу самоорганізації…….. 214
4.4.1 Масштабованість сенсорної мережі за площею розгортання…. 214
4.4.2 Вплив щільності розміщення вузлів на роботу сенсорної мережі…… 221
4.4.3 Пропускна здатність сенсорної мережі……. 224
4.4.4 Затримки передавання мережевих пакетів у сенсорній мережі…… 230
Висновки до розділу 4…….. 233
ВИСНОВКИ……... 235
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……. 238
ДОДАТОК А…….. 250
ДОДАТОК Б…….. 251
ДОДАТОК В…….. 252

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IoT (Internet of Things) - концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані давачі, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами, за допомогою використання стандартних протоколів зв'язку;

BLE (Bluetooth Low Energy) – енергоефективна версія стандарту Bluetooth, призначена для забезпечення бездротового зв’язку між пристроями з низьким енергоспоживанням;

LPWAN (Low Power Wide Area Network) – клас бездротових мереж, розроблених для забезпечення зв’язку на великі відстані з мінімальним енергоспоживанням;

6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) – протокол, який дозволяє передавати IPv6-пакети через мережі з низьким енергоспоживанням і обмеженою пропускною здатністю, зокрема на основі стандарту IEEE 802.15.4, забезпечуючи інтеграцію пристроїв IoT у глобальну IP-мережу;

Wi-Fi (Wireless Fidelity) – технологія бездротового зв’язку, що забезпечує високошвидкісну передачу даних у локальних мережах на основі стандартів IEEE 802.11, широко використовується для підключення пристроїв до Інтернету в побутових, комерційних і промислових умовах;

NB-IoT (Narrowband Internet of Things) – стандарт стільникового зв’язку, розроблений для енергоефективного передавання невеликих обсягів даних пристроями IoT у мережах з широким покриттям, що забезпечує високу проникність сигналу в приміщеннях та тривалий термін автономної роботи.

BPSK (Binary Phase Shift Keying) – метод цифрової модуляції, у якому фаза несучої хвилі змінюється відповідно до двійкових значень передаваного

сигналу; є одним із найпростіших і найстійкіших до шумів способів фазової маніпуляції, що застосовується в бездротових комунікаційних системах;

ISM (Industrial, Scientific and Medical) – міжнародно зарезервовані частотні діапазони радіочастотного спектра, призначені для використання в промислових, наукових і медичних цілях, а також у безліцензійних бездротових технологіях, таких як Wi-Fi, LoRa та Bluetooth;

3GPP (3rd Generation Partnership Project) – міжнародне співробітництво організацій зі стандартизації, що займається розробкою технічних специфікацій для мобільних телекомунікаційних систем;

GSM (Global System for Mobile Communications) – стандарт цифрового стільникового зв'язку другого покоління (2G), який забезпечує голосовий зв'язок, обмін текстовими повідомленнями (SMS) та передавання даних, широко використовується в мобільних мережах у всьому світі;

LTE (Long Term Evolution) – стандарт бездротового широкосмугового зв'язку четвертого покоління (4G), розроблений для підвищення швидкості та ефективності передачі даних у мобільних мережах, підтримує низькі затримки, високу пропускну здатність і покращену мобільність користувачів;

QPSK (Quadrature Phase Shift Keying) – метод цифрової модуляції, в якому фаза несучого сигналу може набувати одного з чотирьох значень, що дозволяє передавати два біти інформації на кожен символ; забезпечує вищу спектральну ефективність порівняно з BPSK, зберігаючи при цьому стійкість до шумів;

FDMA (Frequency Division Multiple Access) – метод множинного доступу, при якому доступ до каналу здійснюється шляхом розділення частотного спектра на окремі піддіапазони, кожен із яких призначається окремому користувачеві; використовується в аналогових та цифрових системах зв'язку для паралельної передачі даних;

OFDMA (Orthogonal Frequency Division Multiple Access) – технологія множинного доступу, що базується на ортогональному частотному розділенні,

при якій спектр передавання поділяється на піднесучі, динамічно призначені різним користувачам; забезпечує високу ефективність спектра, гнучкість розподілу ресурсів і стійкість до інтерференції, широко застосовується в LTE та 5G мережах;

M-Bus (Wireless Meter-Bus) – стандарт бездротового зв'язку, призначений для дистанційного зчитування показників лічильників води, газу, електроенергії та тепла; забезпечує енергоефективну передачу даних у системах автоматизованого збору інформації (AMI), зокрема в межах інтелектуальних енергомереж;

GFSK (Gaussian Frequency Shift Keying) – метод частотної маніпуляції, при якому цифрові дані модулюються шляхом зміни частоти несучого сигналу, а форма імпульсу фільтрується за допомогою гаусового фільтра для зменшення спектральної ширини;

Weightless SIG (Weightless Special Interest Group) – галузева організація, яка розробляє відкриті стандарти бездротового зв'язку для IoT, зосереджуючись на створенні енергоефективних, масштабованих і надійних LPWAN-технологій із підтримкою двостороннього зв'язку та роботи в неспарених ISM-діапазонах;

DPSK (Differential Phase Shift Keying) – метод фазової маніпуляції, в якому інформація кодується як зміна фази між послідовними символами сигналу, а не як абсолютне значення фази;

TDMA (Time Division Multiple Access) – метод множинного доступу, при якому різним користувачам виділяються окремі часові інтервали в межах одного частотного каналу; використовується для ефективного розподілу ресурсу каналу в стільникових мережах (наприклад, GSM) і бездротових сенсорних системах;

CSS (Chirp Spread Spectrum) – метод модуляції, в якому інформація передається за допомогою частотних "чірпів" сигналів із лінійною зміною частоти протягом часу;

MAC (Media Access Control) – підрівень канального рівня в моделі OSI, відповідальний за контроль доступу до фізичного середовища передавання,

організацію черговості передачі, уникнення колізій і адресацію кадрів у бездротових та проводних мережах;

FEC (Forward Error Correction) – метод корекції помилок, при якому передавач додає до повідомлення надлишкову інформацію, що дозволяє приймачу виявляти та виправляти помилки без потреби в повторному запиті;

SF (Spreading Factor) – коефіцієнт розширення спектра в модуляції Chirp Spread Spectrum (CSS), який визначає тривалість символу та впливає на швидкість передавання даних і стійкість сигналу до шумів, у технології LoRa використовується для адаптації зв'язку до умов навколишнього середовища, де вищі значення SF забезпечують більшу дальність і надійність, але знижують швидкість;

MCU (Microcontroller Unit) – вбудований мікропроцесорний пристрій, що поєднує центральний процесор (CPU), пам'ять і периферійні інтерфейси на одному чипі;.

SoC (System on Chip) – інтегрована мікросхема, що містить усі основні компоненти комп'ютерної системи: центральний процесор (CPU), пам'ять, периферійні контролери, інтерфейси зв'язку та інші модулі;

CAD (Channel Activity Detection) – механізм виявлення активності в радіоканалі;

LBT (Listen Before Talk) – протокол доступу до середовища передавання, що передбачає прослуховування радіоканалу перед початком передачі для визначення його зайнятості;

TRL (Technology Readiness Level) – шкала оцінювання рівня технологічної готовності, що використовується для визначення стадії зрілості технології;

DSDV (Destination-Sequenced Distance Vector) – протокол маршрутизації з періодичним оновленням таблиць, призначений для мобільних ad hoc мереж (MANET), який забезпечує уникнення петель маршрутизації шляхом використання нумерації маршрутів;

AODV (Ad-Hoc On-Demand Distance Vector) – адаптивний протокол маршрутизації для бездротових ad hoc мереж, що створює маршрути до вузлів лише за запитом, зберігаючи таблиці маршрутів лише для активних з'єднань;

ACK (Acknowledgement) – механізм підтвердження доставки в телекомунікаційних протоколах, при якому приймач надсилає відправнику сигнал про успішне отримання даних;

GPS (Global Positioning System) – глобальна навігаційна супутникова система, що забезпечує визначення місцеположення, швидкості та часу з високою точністю в будь-якій точці земної кулі;

PDR (Packet Delivery Ratio) – коефіцієнт доставки пакетів, що характеризує відсоткове співвідношення кількості успішно доставлених пакетів до загальної кількості надісланих;

ASFS (Adaptive Spreading Factor Selection) – метод адаптивного вибору фактора розширення (SF) у мережах LoRa, який дозволяє динамічно змінювати параметри модуляції залежно від умов навколишнього середовища, рівня сигналу або навантаження мережі;

CFO (Carrier Frequency Offset) – зсув частоти несучої, що виникає внаслідок невідповідності генераторів частоти передавача і приймача або через ефекти Доплера;

PRR (Packet Reception Ratio) – коефіцієнт прийому пакетів, що визначає відношення кількості пакетів, успішно отриманих приймачем, до загальної кількості надісланих пакетів;

QoS (Quality of Service) – рівень якості обслуговування, який характеризує здатність мережі забезпечувати гарантовану продуктивність передавання даних за такими параметрами, як затримка, втрата пакетів, пропускна здатність і варіативність затримок;

MBAN (Multiple-Building Area Networks) – мережі, що охоплюють кілька будівель або споруд і забезпечують бездротову передачу даних між пристроями в межах великої інфраструктури;

TCO (Total Cost of Ownership) – загальна вартість володіння, яка охоплює всі прямі та непрямі витрати, пов’язані з придбанням, впровадженням, експлуатацією та обслуговуванням системи або технології протягом усього її життєвого циклу;

KPIs (Key Performance Indicators) – ключові показники ефективності, що використовуються для кількісного оцінювання досягнення цілей системи або процесу;

API (Application Programming Interface) – програмні інтерфейси, які забезпечують стандартизований спосіб взаємодії між програмними компонентами або системами.

ВСТУП

Актуальність теми – Сучасний етап розвитку цифрових технологій характеризується інтенсивним впровадженням концепції Інтернету речей у критично важливі сфери від промислових і транспортних систем до міської інфраструктури, агросектору та енергетики. Однією з ключових технологічних передумов стало широке розгортання бездротових сенсорних мереж, здатних забезпечити збір, передачу й обробку даних у реальному часі навіть у складних, динамічних або ізольованих середовищах передавання даних. У цьому контексті зростає потреба у створенні енергоефективних, масштабованих та автономних рішень, що здатні працювати в умовах обмежених обчислювальних ресурсів, нестабільного зв'язку та високої щільності пристроїв.

Технології зв'язку Інтернету речей зазвичай забезпечують довготривалу автономну роботу кінцевих пристроїв та значну зону покриття при мінімальному енергоспоживанні. Класична топологія «зірка-зірка» у цих мережах передбачає централізовану маршрутизацію через шлюзи, що обмежує гнучкість у розгортанні в умовах, де неможливо або недоцільно створювати інфраструктуру з фіксованими точками доступу. Це особливо актуально в сценаріях зі складною або динамічно змінною топологією середовища, де втрата шлюзу може критично вплинути на функціонування всієї мережі.

Застосування підходів до самоорганізації у сенсорних мережах дозволяє реалізувати більш стійкі та гнучкі рішення, зокрема за рахунок реалізації mesh архітектури або гібридних топологій. Такі мережі здатні динамічно адаптуватися до змін конфігурації, втрати вузлів або змін навколишнього середовища, підвищуючи рівень надійності, ефективності використання частотного ресурсу та живлення. Водночас розширюється потенціал до обчислень на краю мережі, що знижує навантаження на центральні сервери та затримки у прийнятті рішень.

Разом з тим, стрімке зростання кількості альтернативних IoT технологій, топологій і конфігурацій створює багатокритеріальну проблему вибору,

ускладнену високою міжтехнологічною залежністю параметрів та неможливістю отримати емпіричні дані на ранніх етапах проєктування. Відсутність методів, які б дозволяли мережевим архітекторам здійснювати обґрунтований вибір мережевої конфігурації з урахуванням вимог застосування, обмежень середовища та перспектив масштабування, призводить до низької успішності впровадження рішень Інтеренту речей.

Гіпотеза дослідження: «Якщо при проєктуванні бездротової сенсорної мережі застосувати підхід, що поєднує: симуляційне моделювання характеристик мережевих технологій, багатоаспектний аналіз вимог цільового застосування, а також запровадити принципи самоорганізації. Таке поєднання дозволить вибирати оптимальну конфігурацію мережі, яка забезпечить кращу енергоефективність, масштабованість, надійність та дозволить суттєво підвищити ефективність функціонування сенсорної мережі у реальних умовах експлуатації».

Таким чином, у роботі ставиться актуальне та важливе наукове завдання, суть якого полягає в розробці методу вибору конфігурації бездротової сенсорної мережі та використання принципів мережевої самоорганізації.

Метою роботи є підвищення ефективності сенсорних мереж, на основі побудови сенсорних мереж на базі самоорганізації**.**

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Провести аналіз сучасних технологій та протоколів передачі даних для сенсорних IoT-мереж, з метою виявлення їх переваг, обмежень і потенціалу до інтеграції в мультипротокольні мережеві структури.

2. Розробити модель побудови мультипротокольної сенсорної мережі з оптимальною конфігурацією.

3. Удосконалити метод взаємодії вузлів сенсорної мережі для підвищення ефективності передавання повідомлень.

4. Розробити метод визначення маршруту передавання даних між вузлами сенсорної мережі для підвищення коефіцієнту доставки повідомлень.

5. Провести імітаційне моделювання запропонованих рішень маршрутизації у програмному середовищі з метою оцінки ефективності доставки повідомлень.

Об'єктом дослідження є процеси проектування та тестування сенсорних мереж.

Предметом дослідження є моделі, методи проектування сенсорних мереж

Методи дослідження. Дослідження проведено на основі системного підходу із застосуванням: положень теорії передачі сигналів, методів комп'ютерного моделювання, теорії розподілених систем, теорії планування експериментів, теорії графів. методів оптимізації.

Наукова новизна одержаних результатів полягає в наступному:

Вперше розроблено модель мультипротокольної сенсорної мережі, яка за рахунок використання багатокритеріального аналізу та теорії розподілених систем, дозволяє визначити оптимальну конфігурацію мережі.

Удосконалено метод взаємодії вузлів сенсорної мережі, який за рахунок використання розробленої моделі мультипротокольної сенсорної мережі та комплексного врахування спектральних параметрів сигналу, дозволяє підвищити ефективність передавання повідомлень у сенсорній мережі.

Вперше розроблено метод визначення маршруту передавання даних між вузлами сенсорної мережі, який за рахунок удосконаленого методу взаємодії вузлів сенсорної мережі та врахування параметрів сенсорної мережі на основі теорії зважених графів та самоорганізації дозволяє підвищити коефіцієнт доставки повідомлень.

Практичне значення одержаних результатів.

Результати дисертаційного дослідження впроваджено у виробничий процес:

- ТОВ "УКР-ОН";
- ТОВ "КАРНІФЕКС"

Також результати досліджень впроваджені в навчальний процес Державного університету інформаційно-комунікаційних технологій.

Експериментально доведено ефективність розробленого методу мережевої взаємодії: кількість пристроїв, які успішно передають повідомлення до центрального додатку зростає у порівнянні з базовим сценарієм передавання даних. Комплексне врахування спектральних параметрів сигналу дозволяє підвищити відсоток успішно переданих повідомлень у сенсорній мережі за рахунок використання службових повідомлень що підтверджують отримання пакету даних, ефект від використання повідомлень що підтверджують отримання пакету даних особливо помітний у режимі роботи мережі з недостатньою кількістю шлюзів де відсоток успішно переданих повідомлень збільшується в середньому на 40%.

Достовірність наукових результатів і практичних рекомендацій дисертації підтверджується коректним використанням методів симуляційного моделювання, обґрунтованими теоретичними положеннями щодо побудови сенсорних мереж із використанням принципів самоорганізації, а також узгодженістю теоретичних висновків із результатами експериментальних досліджень, проведених із застосуванням розробленого спеціалізованого програмного середовища для оцінювання конфігурацій мереж.

Особистий внесок здобувача. Дисертація є самостійною науковою працею, в якій висвітлені власні ідеї і розробки автора, що дозволили вирішити поставлені завдання. Робота містить теоретичні та методичні положення і висновки, сформульовані дисертантом особисто. Використані в дисертації ідеї, положення чи гіпотези інших авторів мають відповідні посилання і використані лише для підкріплення ідей здобувача.

Основні наукові та прикладні результати дисертаційної роботи, що виносяться на захист, отримані автором особисто. В роботах, які опубліковані в співавторстві, особисто здобувачу належать: в [1] - розроблено модель мультипртокольної сенсорної мережі, яка за рахунок використання

багатокритеріального аналізу та теорії розподілених систем, дозволяє визначити оптимальну конфігурацію мереж; в [2] запропоновано удосконалення методу взаємодії вузлів сенсорної мережі, який за рахунок використання розробленої моделі мультипртокольної сенсорної мережі та комплексного врахування спектральних параметрів сигналу, дозволяє знизити загальне навантаження на сенсорну мережу ; в [3] розроблено метод визначення маршруту передавання даних між вузлами сенсорної мережі.

Апробація результатів дослідження.

Результати дослідження, представлені у дисертаційній роботі, доповідались на міжнародних та всеукраїнських конференціях:

1. III Всеукраїнська науково-технічна конференція «Сучасний стан та перспективи розвитку IoT»; Оцінка ефективності штучного інтелекту для вирішення нетипових завдань голосовим помічником; 15 травня 2022р., Державний університет телекомунікацій, м. Київ.

2. IV Всеукраїнська науково-технічна конференція «Сучасний стан та перспективи розвитку IoT». Розробка відмовостійкої інформаційної мережі на базі обладнання MIKROTIK; 7 квітня 2023р., Державний університет телекомунікацій, м. Київ.

3. V Всеукраїнська науково-технічна конференція «Сучасний стан та перспективи розвитку IoT». Створення рекомендацій для автоматизації тестування програмного забезпечення на операційній системі ANDROID, 18 квітня 2024р., Державний університет інформаційно-комунікаційних технологій, м. Київ.

4. VI Всеукраїнська науково-технічна конференція «Сучасний стан та перспективи розвитку IoT». Підвищення ефективності та безпеки дорожнього руху шляхом інтеграції IoT, 15 квітня 2025р., Державний університет інформаційно-комунікаційних технологій, м. Київ.

Публікації. За результатами досліджень опубліковано в 5 праць у фахових наукових виданнях. Авторський внесок у роботах, написаних у співавторстві, здобувачем розкрито у списку опублікованих праць за темою дисертації.

Обсяг та структура дисертації. Дисертаційна робота складається із вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 253 сторінки тексту, 79 рисунків, 16 таблиць, список літератури із 95 найменувань

1 АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ ТА ДОСЛІДЖЕНЬ У СФЕРІ ЗВ'ЯЗКУ СЕНСОРНИХ МЕРЕЖ

Загальна тенденція до цифровізації, автоматизації та розвитку розподілених систем керування зумовила стрімке зростання зацікавленості до технологій Інтернету речей. Однією з ключових складових архітектури IoT є сенсорні мережі, що базуються на бездротовому з'єднанні великої кількості автономних пристроїв для збору, обробки та передачі інформації. Забезпечення ефективного, надійного і масштабованого зв'язку між вузлами такої мережі в умовах обмежених енергетичних та обчислювальних ресурсів є складним завданням, яке значною мірою залежить від вибору технології бездротової передачі даних.

У сучасних умовах функціонування сенсорних IoT-мереж відзначається значне різноманіття технологій зв'язку, кожна з яких має власну специфіку застосування, переваги та обмеження. Ці технології різняться між собою за низкою ключових характеристик, зокрема: діапазоном дії, швидкістю передачі даних, енергоспоживанням, частотним спектром, архітектурною складністю та потребами в інфраструктурі. Саме тому класифікація і системний аналіз наявних рішень дозволяє оцінити їх придатність до використання в конкретних сценаріях побудови сенсорних мереж з механізмами самоорганізації.

Технології бездротового зв'язку, що використовуються в IoT-системах, умовно поділяються на три основні категорії залежно від дальності дії [1]:

1. Короткого радіуса дії (до 100 м): RFID, Bluetooth Low Energy , ZigBee, 6LoWPAN;

2. Середнього радіуса дії (100 м – 1 км): Wi-Fi, стільникові мережі (2G/3G/4G/5G);

3. Великого радіуса дії (понад 1 км): LPWAN-рішення (LoRa, Sigfox, NB-IoT, Wize, DASH7 тощо).

Найбільший інтерес для побудови сенсорних мереж з автономними вузлами становлять саме технології класу LPWAN, оскільки вони дозволяють забезпечити енергоощадний режим роботи з високим радіусом покриття, що є критично важливим для сценаріїв масштабного розгортання. Серед таких технологій особливої уваги заслуговує LoRa - відкрита, гнучка та доступна до реалізації радіотехнологія, яка підтримується широким спектром апаратного забезпечення і має потужну спільноту розробників.

Метою цього підрозділу є здійснення систематизованого огляду сучасних технологій бездротового зв’язку для IoT, їх порівняння за ключовими параметрами, а також виділення LoRa як технології, що поєднує в собі простоту реалізації, енергоефективність та масштабованість, і є доцільною платформою для реалізації самоорганізованих сенсорних мереж.

1.1. Огляд та класифікація сучасних технологій бездротового зв'язку для IoT

З моменту виникнення сенсорних мереж Інтернету речей та їх широкого впровадження було розроблено низку технологій бездротового зв’язку, здатних забезпечувати з’єднання на відстанях від кількох метрів до кількох кілометрів, переважно в субгігагерцових діапазонах частот [2]. Особливе місце серед них займають протоколи класу LPWAN, які орієнтовані на забезпечення зв’язку між пристроями, що працюють від джерел живлення з обмеженим енергетичним ресурсом, і передають дані між собою або в мережу Інтернет через проміжний шлюз. Для проведення узагальненого порівняльного аналізу існуючих технологій передачі даних доцільно використовувати такі параметри, як частотний діапазон роботи та швидкість передавання інформації. На рисунку (рис. 1.1) подано графічну класифікацію технологій бездротової передачі цифрових даних відповідно до зазначених характеристик. У межах цієї візуалізації виділено три основні категорії: технології ближнього радіуса дії (до

100 м), середнього радіуса дії (від 100 м до 1 км) та великого радіуса дії (понад 1 км). Додатково на рис. 1.1 позначено орієнтовні показники швидкості передавання даних, які можуть бути досягнуті кожною з технологій у контексті побудови сенсорних IoT-мереж.

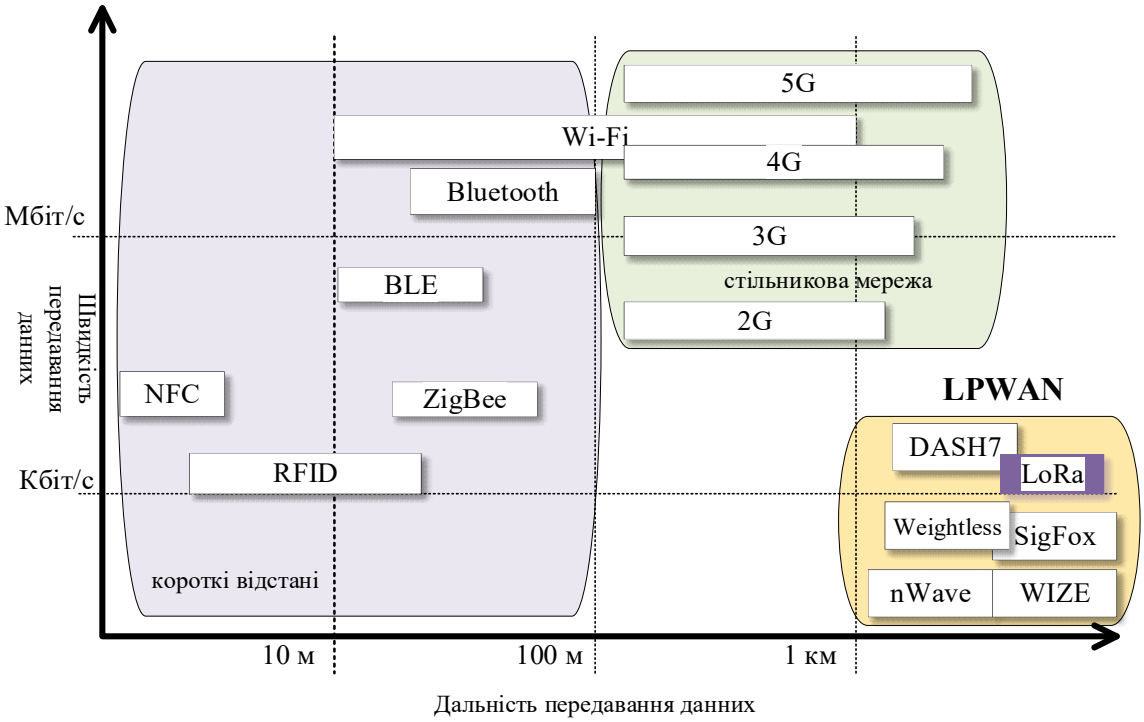

Рис. 1.1. - Класифікація технологій бездротового зв'язку для IoT за дальністю передачі та швидкістю обміну даними

Серед технологій бездротового зв'язку, що забезпечують передавання даних на короткі відстані (від кількох сантиметрів до 100 метрів), слід відзначити RFID, ZigBee, Bluetooth Low Energy, а також їх сучасні варіації з підтримкою IPv6 у рамках малопотужних бездротових персональних мереж 6LoWPAN. Зазначені протоколи функціонують у діапазоні швидкостей передавання даних від кількох кілобітів за секунду до мегабітів за секунду, що робить їх ефективними для локального обміну інформацією між IoT-пристроями з мінімальним енергоспоживанням.

Особливе місце посідає Wi-Fi, який завдяки різноманітності апаратної реалізації (зокрема параметрам антен, вихідної потужності передавачів, типам

модуляції тощо), може бути віднесений як до категорії технологій ближнього радіуса дії, так і до середнього. Водночас до категорії середньої дальності (від 100 метрів до 1 км) традиційно належать і стільникові мережі на основі технологій GSM різних поколінь (2G, 3G, 4G, 5G), які забезпечують значно вищу швидкість передавання даних - у межах десятків, а то й сотень мегабіт на секунду.

Технології класу LPWAN, такі як Sigfox, Wize, DASH7, LoRa, nWave, NB-IoT та Weightless, демонструють інший підхід: вони призначені для передавання невеликих обсягів даних на великі відстані (понад 1 км) з мінімальним енергоспоживанням. Досягнення великої дальності забезпечується шляхом зниження швидкості передавання даних, яка зазвичай обмежується кілобітами за секунду або нижче. Такий компроміс є прийнятним для багатьох типових сценаріїв використання IoT, особливо там, де необхідна передача періодичних вимірювань або подієвих повідомлень, а основним пріоритетом виступає енергоефективність. Завдяки цьому значно знижуються витрати на обслуговування пристроїв, що працюють на автономних джерелах живлення (наприклад, батареях малої ємності), які можуть функціонувати роками без заміни живлення.

Sigfox є прикладом технології, яка поєднує у собі функціональність протоколу класу LPWAN та інфраструктуру оператора зв’язку, що надає повноцінне глобальне рішення для підключення сенсорних мереж IoT. Технологія функціонує на базі власної мережевої архітектури [1], що включає розгорнуті базові станції, які забезпечують покриття національного та міжнародного рівнів.

Протокол Sigfox використовує двійкову фазову модуляцію BPSK у надзвичайно вузькому спектрі - шириною всього 100 Гц, що дозволяє ефективно передавати сигнали в умовах обмеженого енергоспоживання. Передача здійснюється в неліцензованих діапазонах ISM у субгігагерцовому спектрі, що робить використання технології доступним у більшості країн.

Функціональні обмеження протоколу зумовлені його архітектурою та принципами енергоефективності: пристрій може надсилати не більше 140 повідомлень на день, кожне з яких має максимальний розмір 12 байтів. Зворотний зв'язок (від базової станції до пристрою) ще більш обмежений - дозволено лише до 4 повідомлень на день, розмір яких не перевищує 8 байтів. Для забезпечення надійності доставки Sigfox [3] використовує такі методи, як часова диверсифікація, частотне перемикання, а також множинна передача одного і того ж повідомлення, що підвищує ймовірність коректного приймання даних на мережевій стороні.

Технологія NB-IoT була стандартизована в межах проєкту 3rd Generation Partnership Project [4] як спеціалізоване рішення для забезпечення зв'язку пристроїв Інтернету речей у ліцензованих частотних діапазонах. Вона була розроблена як доповнення до існуючих стільникових технологій - зокрема GSM та LTE - з метою ефективної інтеграції IoT-пристроїв у мобільну інфраструктуру зв'язку [5].

NB-IoT функціонує в частотному діапазоні шириною 200 кГц і може бути розгорнута в одному з трьох режимів: автономно, у межах захисного спектра існуючих мереж LTE, або у вигляді частотної вставки у ресурси самого LTE. Архітектурно вона побудована на базі протоколу LTE, який був суттєво спрощений та адаптований для потреб IoT-середовища, що передбачає низьке енергоспоживання, обмежене передавання даних та тривалий час автономної роботи пристроїв [1].

Передавання даних у NB-IoT здійснюється із застосуванням модуляції з квадратурним фазовим зсувом QPSK, а також частотного поділу з множинним доступом FDMA у висхідному каналі та ортогонального частотного поділу OFDMA - у низхідному. Технологія забезпечує швидкість передавання даних у межах від 20 кбіт/с до 200 кбіт/с в обох напрямках, з максимально допустимим обсягом корисного навантаження до 1600 байт, що робить NB-IoT придатною

для широкого спектра застосувань у сфері розумної інфраструктури, агрегації даних зі станів пристроїв і моніторингу середовища.

Wize є однією з технологій класу LPWAN, що спочатку була орієнтована на застосування в галузі промислового Інтернету речей [6 - 7]. Її розробку ініціювали у Франції для реалізації телеметричних систем збору даних з газових та водяних лічильників у межах муніципальної інфраструктури. Технологія базується на стандарті бездротового M-Bus та функціонує у діапазоні 169 МГц, що історично був зарезервований для комунального використання. Це дозволяє забезпечити стабільний, захищений канал зв'язку, придатний для передачі даних з важкодоступних ділянок - таких як підвали, технічні приміщення або промислові об'єкти, - де інші технології можуть бути менш ефективними.

Wize використовує шість частотних каналів по 12,5 кГц кожен, забезпечуючи швидкість передавання даних до 6,4 кбіт/с, що є прийнятним для телеметричних застосувань, які не потребують високої пропускної здатності. Завдяки роботі в низькочастотному діапазоні у порівнянні з іншими LPWAN-протоколами, Wize демонструє вищу здатність проникнення радіосигналу крізь будівельні конструкції та кращий радіус покриття при однакових умовах навколишнього середовища.

Завдяки своїй архітектурі та стабільності передачі на фізичному рівні, Wize також може бути застосована як фізичний рівень моделі OSI для інших технологій, зокрема LoRaWAN, що розширює її інтеграційні можливості у мультипротокольних сенсорних мережах.

DASH7 є однією з найбільш технічно розвинених технологій класу LPWAN, розробленою ініціативною групою DASH7 Alliance як відкритий бездротовий протокол для сенсорних та автоматизованих мереж [8]. Технологія функціонує у субгігагерцовому частотному діапазоні та базується на міжнародному стандарті ISO/IEC 18000-7 [9], який визначає параметри активного радіоінтерфейсу зв'язку на частоті 433 МГц. Стандарт охоплює повну мережеву архітектуру - від фізичного рівня до рівня застосування, що робить

DASH7 комплексним рішенням для побудови розподілених мереж з низьким енергоспоживанням.

У процесі передавання даних у DASH7 використовується подвійна гауссівська частотна модуляція GFSK, яка забезпечує максимальну швидкість до 200 кбіт/с залежно від кількості використовуваних частотних каналів. Завдяки цьому досягається великий радіус дії - до 2 км, що у поєднанні з низькою затримкою зв'язку робить технологію особливо ефективною для сценаріїв, де передача даних відбувається від мобільних або динамічних об'єктів.

Мережева топологія DASH7 базується на ієрархічній (деревоподібній) структурі, яка підтримує двокрокову маршрутизацію, спрощуючи реалізацію маршрутизованих рішень і забезпечуючи достатню гнучкість для побудови середніх та великих мереж зі збереженням ефективного використання енергоресурсів.

Weightless - це відкритий стандарт бездротового зв'язку класу LPWAN, розроблений інженерною групою SIG як гнучке рішення для побудови енергоефективних IoT-мереж [10]. В рамках цього проєкту було представлено три окремі технології: Weightless-W, Weightless-N та Weightless-P [2], кожна з яких має свої особливості та орієнтована на різні сценарії застосування.

Weightless-W [11] була першою розробкою в межах стандарту й орієнтувалася на використання вільних телевізійних частотних діапазонів, що дозволяло забезпечити передачу на великі відстані з урахуванням властивостей поширення сигналу в цьому спектрі. У свою чергу, Weightless-N та Weightless-P працюють у субгігагерцових частотних діапазонах, що є типовим для більшості LPWAN-рішень.

Технологія Weightless-N зосереджена на мінімізації енергоспоживання та реалізує односторонній зв'язок (тільки висхідні повідомлення). Вона використовує вузькосмугову модуляцію, зокрема диференціальну фазову

модуляцію DPSK, що дає змогу ефективно передавати невеликі обсяги даних у пристроях з обмеженими ресурсами.

Натомість Weightless-P забезпечує дуплексний (двосторонній) зв'язок і підтримує підтвердження отримання даних, що робить її придатною для більш вимогливих застосувань. У цій реалізації використовується множинний доступ з частотним поділом каналів FDMA у поєднанні з множинним доступом з часовим поділом TDMA, що дозволяє досягти гнучкого розподілу ресурсів у мережі при збереженні енергоефективності.

Окрім широковідомих рішень, на ринку LPWAN також представлено низку менш поширених технологій, які, як правило, мають вузьке прикладне призначення або є закритими пропрієтарними розробками. Їхня обмежена популярність пояснюється або орієнтацією на специфічні задачі, або недостатньою відкритістю протоколів, що ускладнює інтеграцію та подальший розвиток рішень.

Однією з таких технологій є nWave - ультравузькосмуговий протокол бездротового зв'язку, спеціалізований на забезпеченні зв'язку для паркувальної інфраструктури в межах концепції розумного міста [12]. Основною перевагою цієї технології є низьке енергоспоживання та тривалий час автономної роботи, однак її застосування обмежене переважно транспортною сферою.

Ще одне рішення представлено компанією Ingenu [13, 14], яка розробила закриту LPWAN-технологію, що функціонує у неліцензованому ISM-діапазоні 2,4 ГГц. Хоча заявлені характеристики передбачають високу енергоефективність та добру проникну здатність сигналу, закритість протоколу суттєво обмежує його адаптацію сторонніми розробниками.

Компанія Telensa [15] пропонує вертикально інтегровані LPWAN-рішення, які включають повністю сформований мережевий стек, оптимізований під ультравузькосмугову передачу даних у субгігагерцовому ISM-діапазоні. Такі рішення використовуються у нішевих сферах, як-от інтелектуальне освітлення та міський моніторинг.

Ще одним прикладом є Qowisio [16], що реалізує гібридні LPWAN-мережі, які поєднують технології LoRa з ультравузькосмуговими протоколами, створюючи архітектури з комбінованими підходами до передавання даних [2]. Це дозволяє адаптувати мережу до вимог конкретного середовища або сценарію використання, проте також зумовлює складність впровадження та залежність від інфраструктури постачальник

Серед усіх розглянутих технологій бездротового зв’язку класу LPWAN, особливе значення має LoRa, яка зарекомендувала себе як технологічно зріле, глобально прийняте, економічно ефективне та широко доступне рішення для побудови мереж передачі даних на великі відстані. Її ключова перевага полягає в тому, що вона функціонує у неліцензованих частотних діапазонах ISM, що істотно спрощує процес впровадження і дозволяє зменшити витрати на розгортання інфраструктури.

На фізичному рівні LoRa використовує модуляцію з розширенням спектра за допомогою частотних зсувів CSS. Такий підхід забезпечує стійкість до завад, високу дальність передавання сигналу та енергоефективність, що є критично важливими параметрами для IoT-систем із великою кількістю автономних пристроїв.

На вищому рівні протоколу функціонує архітектура LoRaWAN, яка додає рівень управління доступом до середовища MAC та реалізує повноцінний LPWAN-протокол для забезпечення безпечного двостороннього зв’язку між кінцевими пристроями та серверними додатками. Відкрита специфікація LoRaWAN дає змогу створювати гнучкі рішення з можливістю адаптації до конкретних прикладних сценаріїв — від моніторингу навколишнього середовища та «розумного міста» до промислових IoT-систем і приватних мереж.

Завдяки поєднанню відкритої архітектури, доступності апаратної бази та простоти реалізації, технології LoRa і LoRaWAN сьогодні вважаються одними з

найбільш універсальних і перспективних для побудови масштабованих сенсорних мереж із можливістю реалізації механізмів самоорганізації.

На відміну від окремих розглянутих вище технологій, LoRa хоча і є технологією з закритим вихідним кодом (протокол розроблено компанією Semtech), проте завдяки високому рівню поширеності, економічній доступності та відкритості специфікацій LoRaWAN вона зберігає виняткову привабливість для реалізації приватних мереж без прив'язки до сторонніх операторів інфраструктури. Це дозволяє організаціям, дослідникам та розробникам самостійно розгортати повноцінні IoT-системи, повністю контролюючи усі рівні мережевого стека - від фізичного до прикладного, та адаптувати архітектуру відповідно до власних потреб.

У порівнянні з такими технологіями, як Sigfox або NB-IoT, які передбачають щільну інтеграцію з базовими станціями операторів або шлюзами мобільного зв'язку, LoRa забезпечує значно більшу гнучкість та автономність. У випадках із Sigfox або NB-IoT реалізація додаткових функцій - таких як маршрутизація або управління доступом до середовища (MAC-рівень) - часто є обмеженою або взагалі недоступною для сторонніх розробників через централізовану архітектуру та закритість інтерфейсів.

Серед LPWAN-технологій, які дозволяють вільне використання та розширення функціональності (Wize, DASH7 та LoRa), саме остання вирізняється найкращим поєднанням гнучкості, підтримки з боку спільноти та наявності широкого спектра готових апаратних рішень - як у вигляді плат розробки, так і вбудованих модулів. Це робить LoRa особливо зручною платформою для наукових досліджень, швидкого прототипування та реалізації інноваційних підходів, зокрема в контексті побудови самоорганізованих сенсорних мереж IoT.

1.1.1. LoRa в контексті сенсорних мереж: технічний аналіз і практичні аспекти

LoRa, що розшифровується як long range (велика дальність дії), є технологією бездротового зв’язку, розробленою компанією Semtech. Вона працює у субгігагерцовому частотному діапазоні та призначена для створення енергоефективних бездротових мереж з великою зоною покриття [2]. LoRa реалізує фізичний рівень моделі OSI, а саме - передачу сигналу в радіоефірі, тоді як функціональне управління мережею реалізується через протокол LoRaWAN, що діє на рівні MAC.

Ключовою особливістю LoRa є застосування модуляції CSS - запатентованої технології розширення спектра на основі лінійно змінної частоти , що забезпечує стійкість до завад, мультипроменевого згасання та дозволяє досягати високої дальності передавання сигналу з відносно низьким енергоспоживанням. На відкритій місцевості за сприятливих умов LoRa забезпечує зв’язок на відстані понад 10 км, зберігаючи стабільність сигналу навіть у середовищах з високим рівнем радіоінтерференції.

CSS модуляція також дозволяє досягти високого співвідношення сигнал/шум, що робить LoRa придатною для роботи в умовах глибокого покриття — зокрема у міських районах, сільській місцевості або промислових об’єктах. У зв’язку з цим LoRa здобула широке визнання в науковій та інженерній спільноті, і її характеристики було всебічно проаналізовано в роботах [12, 17].

Параметри фізичного рівня технології LoRa можуть бути гнучко налаштовані відповідно до вимог конкретного сценарію застосування, що дозволяє досягати балансу між дальністю зв’язку, швидкістю передачі даних і енерговитратами. Кожен пристрій, що працює на базі LoRa, може бути індивідуально сконфігурований за такими параметрами, як частотний діапазон,

ширина каналу, потужність передавання, коефіцієнт корекції помилок FEC, а також фактор розширення SF.

Реальні розгортання IoT-мереж із використанням LoRa зазвичай виконуються у неліцензованих ISM-діапазонах, які відрізняються залежно від регіону: 868 МГц для Європи, 915 МГц для США, 433 МГц у деяких країнах Азії тощо. В межах кожного з цих діапазонів доступно декілька каналів зв'язку, які можуть бути налаштовані для дуплексної роботи (передавання й приймання), із вибором відповідної ширини каналу (від вузькосмугових до широкосмугових конфігурацій) та допустимими рівнями потужності передавання відповідно до місцевого регулювання.

Окрім високої завадостійкості модуляції CSS, додатковий захист каналів від впливу шумів і втрат забезпечується завдяки використанню прямого виправлення помилок FEC, що покращує якість зв'язку без збільшення потужності передавача.

Основні конфігуровані параметри передавачів LoRa, що визначають їх роботу в різних умовах експлуатації, узагальнено в таблиці 1.1. Наведені значення можуть варіюватися залежно від регіональних регуляторних обмежень і обраної архітектури мережі.

Таблиця 1.1 – Основні конфігуровані параметри в передавачах LoRa

Параметр:	**Типові значення:**
Радіодіапазон і частота	169, 433, 868, 915 МГц
Ширина каналу	62.5, 125, 250, 500 кГц
Потужність передачі	14 дБм (ЄС), 27 дБм (США)
Фактор розширення	6 до 12
Коефіцієнт корекції помилок (FEC)	4/5, 4/6, 4/7, 4/8
Орієнтовна швидкість передачі	0.3 – 27 кбіт/с

Мікросхеми LoRa доступні у двох основних варіантах: одноканальні передавачі для кінцевих пристроїв і багатоканальні цифрові мікросхеми для шлюзів, які зазвичай використовуються в архітектурі LoRaWAN. Одноканальні модулі виконують функції простих трансиверів, що можуть передавати або приймати дані лише на одному каналі й з фіксованим коефіцієнтом (фактором) розширення SF. Такі пристрої, як правило, використовуються в автономних датчиках та інших енергоефективних IoT-вузлах, де простота реалізації та мінімальне енергоспоживання є ключовими пріоритетами.

На відміну від них, багатоканальні мікросхеми шлюзів мають суттєво вищу обчислювальну потужність і функціонують як приймачі, що обслуговують десятки одночасних передавань. Вони здатні приймати сигнали з різних каналів і різними значеннями SF, що дозволяє шлюзу одночасно обробляти кілька незалежних передавань. Наприклад, пристрій може одночасно декодувати сигнали на каналах CH1-SF7, CH1-SF8, CH2-SF7 і CH2-SF8 без конфліктів - завдяки властивості квазіортогональності між різними коефіцієнтами розширення.

Це дає змогу досягати високої пропускної здатності навіть за умови використання низькошвидкісної технології, зберігаючи при цьому гнучкість у розподілі мережевого навантаження між пристроями з різними характеристиками зв’язку. Подібна архітектура є особливо ефективною в розподілених IoT-системах з великою кількістю кінцевих вузлів, що працюють у різних радіоумовах.

Однією з найважливіших характеристик фізичного рівня LoRa є фактор розширення SF, який визначає прямий компроміс між швидкістю передачі даних та діапазоном зв’язку і безпосередньо впливає на швидкість передачі даних та дальність зв’язку. Вищі значення SF (наприклад SF12) забезпечують більшу стійкість до завад і дозволяють досягати більшого радіуса покриття, проте зменшують швидкість обміну даними та збільшують час передачі. Натомість

нижчі значення (SF6–SF7) забезпечують вищу швидкість при меншій дальності зв’язку.

Цей компроміс є критично важливим у розподілених мережах IoT, оскільки дозволяє динамічно адаптувати параметри передачі залежно від умов середовища, відстані до шлюзу або рівня завад. Гнучкість у виборі SF дає можливість більш ефективного використання ресурсу мережі, як у простих сценаріях прямого зв’язку, так і в більш складних топологіях із самоорганізацією.

Додатково, унікальна властивість LoRa - це квазіортогональність передач із різними значеннями SF на одному частотному каналі, що дозволяє приймачам одночасно декодувати кілька сигналів без взаємних перешкод. Ця особливість використовується як у шлюзах, так і потенційно в розумних кінцевих вузлах, які здатні здійснювати розмежування прийнятих сигналів за допомогою алгоритмів демодуляції.

Таким чином, коефіцієнт розширення SF є не лише базовим параметром фізичного рівня, а й інструментом адаптивного управління мережею, що відкриває перспективи для реалізації більш складних протоколів маршрутизації, кластеризації та динамічної оптимізації енергоспоживання в сенсорних мережах.

На сьогодні LoRa-технологія підтримується широким спектром апаратних платформ, що робить її надзвичайно привабливою як для промислових рішень, так і для експериментальних розробок у дослідницькому середовищі. Доступні мікросхеми реалізуються як у вигляді дискретних трансиверів, так і у вигляді модулів, вбудованих у плати розробки, які легко інтегруються з популярними мікроконтролерами (MCU) або системами на кристалі (SoC).

Серед найбільш поширених платформ варто відзначити Arduino, його численні модифікації та клони, а також ESP8266 і ESP32 які поєднують низьку вартість із широкими комунікаційними можливостями. Завдяки активній спільноті розробників і наявності бібліотек з відкритим кодом, ці пристрої стали

де-факто стандартом для швидкого прототипування IoT-рішень з використанням LoRa.

На рис. 1.2 представлено приклади популярних апаратних платформ, які поєднують LoRa-модулі з різними мікроконтролерами. Такі пристрої дозволяють реалізовувати як прості кінцеві вузли, так і повноцінні шлюзи з багатоканальним приймачем.

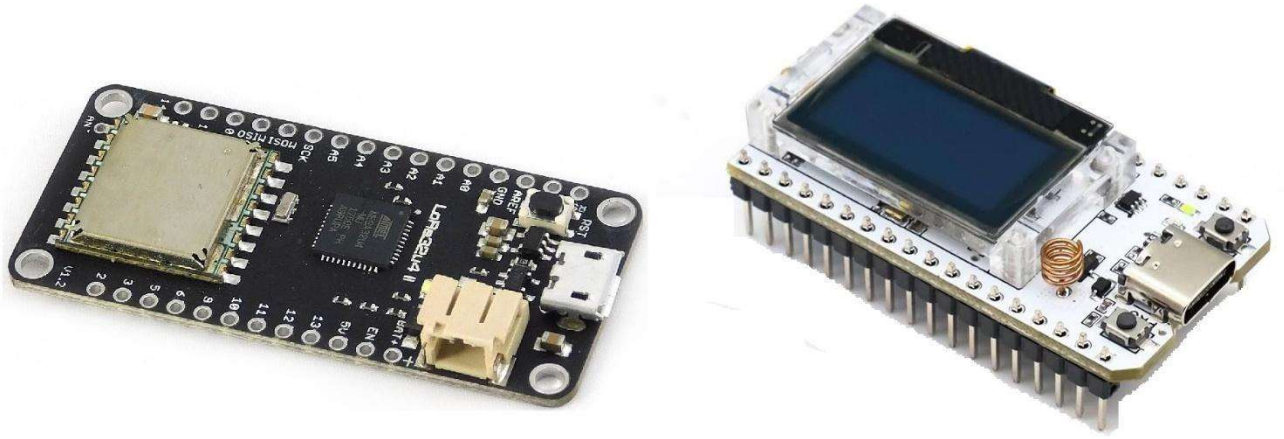

Рис. 1.2 – Приклади апаратних платформ з підтримкою LoRa на базі ESP32

На рисунку 1.2 зображено приклади популярних LoRa-сумісних плат, які активно використовуються для прототипування IoT-пристроїв. Обидва пристрої побудовані на основі мікроконтролера ESP32, що поєднує Wi-Fi, Bluetooth та LoRa-трансивер, і є ідеальними для побудови автономних вузлів у сенсорних мережах.

Наявність великої кількості недорогих комерційно доступних пристроїв, що інтегрують у собі як датчики, так і LoRa-радіомодулі, значно спрощує процес розробки, пришвидшує впровадження прототипів та знижує вхідний бар’єр для реалізації прикладних та експериментальних IoT-систем. Це є особливо важливим у контексті академічних досліджень, де гнучкість платформи та контроль над усіма рівнями мережі дозволяють вивчати складні мережеві процеси, включно із самоорганізацією.

Попри численні технічні переваги, технологія LoRa - як і всі бездротові рішення, що працюють у неліцензованих ISM-діапазонах, - підпадає під дію регіональних нормативних обмежень, які регулюють допустимі режими радіопередачі. Зокрема, однією з ключових вимог є обмеження робочого циклу - тобто частки часу, протягом якого пристрій може активно передавати дані на певному каналі. У багатьох країнах Європи цей показник не перевищує 1% для деяких піддіапазонів, що суттєво обмежує інтенсивність передавання даних.

Ці обмеження варіюються залежно від географічного регіону. Наприклад, в Іспанії або Німеччині пристрій може передавати не більше 36 секунд на годину на кожному каналі. Водночас у США діють інші регуляторні акти (FCC Part 15 [18]), які замість робочого циклу можуть вимагати наявності механізмів уникнення колізій, зокрема CAD або LBT.

Впровадження таких механізмів дозволяє частково обійти жорсткі обмеження шляхом адаптивного моніторингу ефіру, однак це потребує додаткових обчислювальних ресурсів і може вплинути на загальну затримку в мережі. Таким чином, при проєктуванні мережі LoRa важливо враховувати регуляторні вимоги тієї країни чи регіону, де планується її розгортання, оскільки вони мають безпосередній вплив на архітектуру мережі, інтервали передачі, енергоспоживання та навіть вибір класу пристроїв (A, B або C у LoRaWAN).

Усе вищезазначене підкреслює необхідність не лише технічної, а й обґрунтованої побудови мережі LoRa, що є передумовою для подальшого впровадження більш складних мережевих функцій, зокрема таких як самоорганізація вузлів, адаптивна маршрутизація та кластеризація.

1.1.2. Принципи роботи та обмеження технологій зв’язку сенсорних мереж

LoRaWAN є відкритим стандартом, розробленим організацією LoRa Alliance, яка займається розвитком і уніфікацією технологій LPWAN на

глобальному рівні [19]. Цей стандарт визначає специфікацію рівня доступу MAC та рівня застосування в моделі OSI, функціонуючи поверх фізичного рівня, який реалізується за допомогою технології LoRa. Основною метою LoRaWAN є забезпечення енергоефективного, захищеного і масштабованого бездротового зв'язку між кінцевими пристроями IoT (такими як сенсори, лічильники, контролери) та віддаленими додатками для обробки даних, що розгортаються локально або в хмарному середовищі.

Стандарт орієнтований на мінімізацію енергоспоживання пристроями, що живляться від батарей, і забезпечення двостороннього зв'язку в умовах обмежених ресурсів. Саме тому LoRaWAN отримав широке поширення у сфері розумних міст, аграрних технологій, систем моніторингу довкілля та логістики. Його типова архітектура, що базується на однохоповій передачі даних через шлюз, виявилась ефективною для більшості класичних задач побудови сенсорних IoT-мереж [16].

Архітектура мережі LoRaWAN базується на топології типу «зірка-зірок» [20].

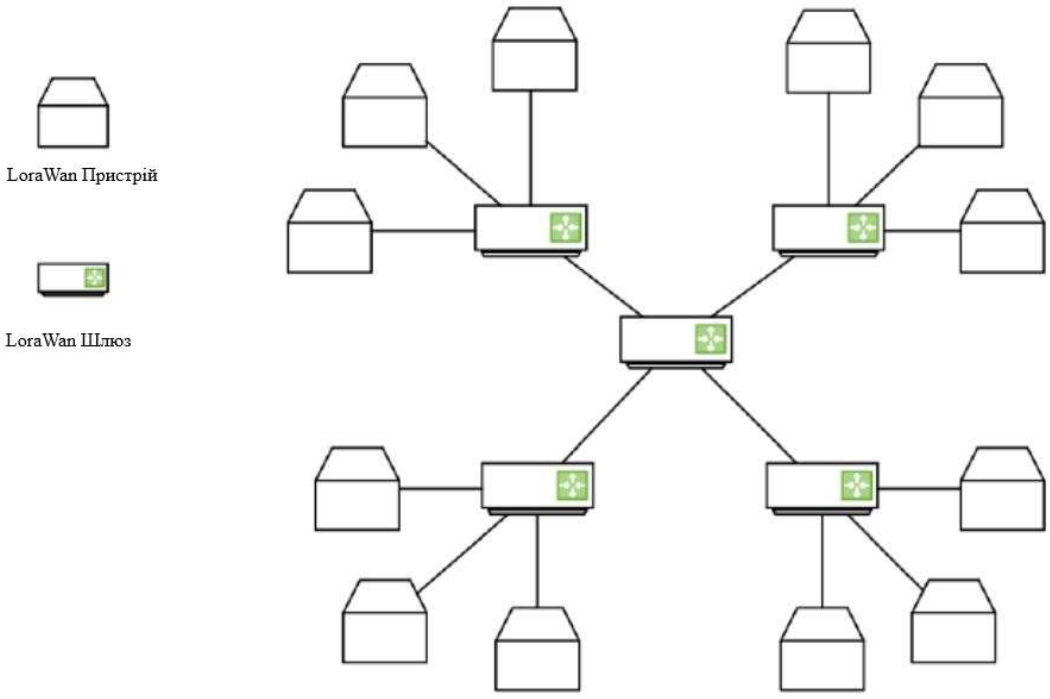

Рис. 1.3 – Топологія «зірка-зірок»

У топології (рис. 1.3) кінцеві пристрої (сенсори, контролери тощо) безпосередньо передають дані до одного або кількох шлюзів. Ці шлюзи, у свою чергу, не виконують попередню обробку, а лише виступають у ролі ретрансляторів, які пересилають прийняті повідомлення через IP-мережу (Ethernet, Wi-Fi або стільниковий зв'язок 3G/4G/5G) до мережевого сервера. На цьому рівні відбувається логічна обробка трафіку, включаючи фільтрацію дублікатів, шифрування, автентифікацію та маршрутизацію до сервера додатків, який обробляє і зберігає дані в межах прикладної IoT-інфраструктури. Архітектурну модель LoRaWAN із прикладами сенсорних застосувань і візуалізацією потоку даних наведено на рис. 1.4.

Така архітектура передбачає, що весь трафік передається у вигляді однохопових повідомлень, тобто без участі проміжних вузлів або маршрутизаторів. У типовому сценарії більшість трафіку здійснюється у висхідному напрямку (від кінцевих вузлів до мережі), що відповідає характеру роботи більшості IoT-систем збору даних. Низхідні-пакети, тобто повідомлення від мережі до вузлів, надсилаються рідше та зазвичай виконують роль команд управління або підтверджень.

Завдяки такій структурі LoRaWAN забезпечує простоту масштабування, оскільки кожен вузол може бути досягнутий без складної маршрутизації. Проте це також зумовлює залежність від інфраструктури шлюзів, які потребують стабільного підключення до IP-мережі. Тому реальне покриття мережі значною мірою визначається фізичним розташуванням шлюзів, їх потужністю та щільністю розміщення в межах обслуговуваної території.

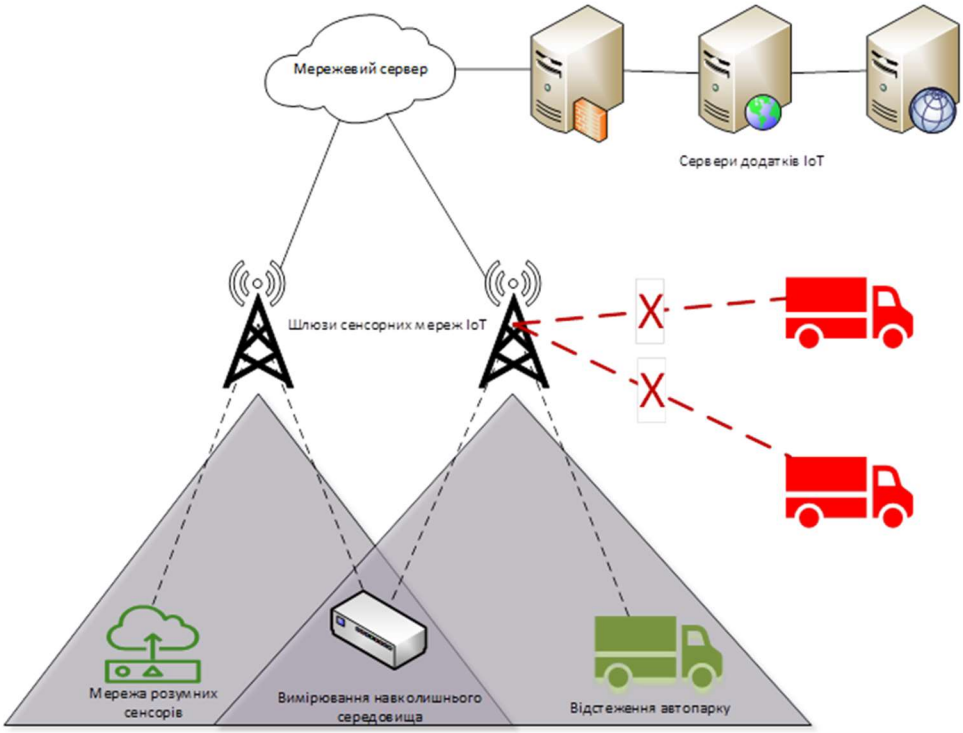

Рис. 1.4 - Архітектура мережі LoRaWAN з прикладами застосувань сенсорних пристроїв і вузлів збору даних

Схематичне зображення на рис. 1.4 демонструє структуру типової мережі LoRaWAN: збір даних з різних сенсорів, передача через шлюзи до мережевого сервера, а також обробка та зберігання інформації в додатках. Водночас на схемі візуалізовано і характерні обмеження downlink-зв'язку, коли кінцеві пристрої можуть не отримати відповідь через обмеження тривалості передачі або затримки каналу.

Хоча LoRaWAN підтримує двосторонній обмін даними, архітектура мережі суттєво відрізняється від традиційних бездротових технологій тим, що основний обсяг трафіку припадає на uplink - тобто на передачу даних від кінцевих вузлів до шлюзів. Передача у зворотному нисхідному напрямку, тобто надсилання повідомлень з мережевого сервера до вузлів, має функціональні обмеження, що обумовлені архітектурною специфікою протоколу та нормативними обмеженнями щодо частоти передач у субгігагерцовому діапазоні.

Кінцеві пристрої LoRaWAN поділяються на три класи: A, B і C, кожен з яких має свої особливості у роботі з низхідною-комунікацією. Пристрої класу A, які є найпоширенішими та найбільш енергоефективними, ініціюють передачу даних лише у напрямку вивантаження, після чого автоматично відкривають два короткі вікна прийому. Якщо під час цих інтервалів сервер надсилає низхідне-повідомлення - вузол його приймає; інакше - повідомлення втрачається, оскільки пристрій переходить у режим сну. Такий режим забезпечує мінімальне енергоспоживання, але суттєво обмежує можливість зворотного зв’язку в реальному часі.

Для пристроїв класу B передбачена періодична синхронізація з мережею за допомогою маячкових сигналів, що дозволяє відкривати вікна прийому згідно з розкладом. Це забезпечує баланс між енергоспоживанням і доступністю прийому. Клас C натомість постійно тримає радіомодуль увімкненим, очікуючи на вхідні повідомлення у будь-який момент. Такий підхід вимагає постійного джерела живлення, але забезпечує максимальну доступність для нисхідної передачі, що критично важливо для шлюзів або пристроїв з потребою у керуванні в режимі реального часу.

Шлюзи LoRaWAN відіграють ключову роль у функціонуванні мережі, оскільки саме вони виступають проміжною ланкою між радіоінтерфейсом LoRa та IP-мережею, що з’єднує пристрої з мережевим сервером. На відміну від кінцевих вузлів, шлюзи базуються на потужніших апаратних платформах, здатних до багатоканального прийому, обробки великого обсягу трафіку та забезпечення стабільного інтернет-з’єднання. Типова апаратна реалізація шлюзу включає вбудовану обчислювальну систему, як-от ARM-платформи, WiSoC-процесори або одноплатні комп’ютери на зразок Raspberry Pi, BeagleBone чи x86-міні-ПК, доповнені модулями LoRa-концентраторів на базі чипів Semtech SX1301/1302/1303.

Головною перевагою шлюзів є можливість одночасної обробки численних передач від різних вузлів, що працюють на різних частотах і з різними факторами

розширення SF. Це досягається завдяки багатоканальним демодуляторам, вбудованим у LoRa-концентратори, які дозволяють приймати десятки незалежних повідомлень паралельно без втрат. Така архітектура суттєво розширює пропускну здатність мережі та дозволяє одному шлюзу обслуговувати від кількох сотень до кількох тисяч кінцевих пристроїв, залежно від частоти передачі, типу даних і конфігурації мережі.

Однак така потужність та гнучкість мають і свою ціну: вартість шлюзу у кілька разів перевищує вартість звичайного вузла, а також вимагає стабільного енергоживлення та постійного зв’язку з IP-мережею. Незважаючи на це, розгортання навіть обмеженої кількості шлюзів дозволяє охопити великі території та суттєво знизити кількість необхідних кінцевих пристроїв для досягнення покриття.

Рис. 1.5 - Приклад компактного шлюзу LoRaWAN для промислових та дослідницьких застосувань

Як приклад, на рис. 1.5 зображено типовий LoRaWAN-шлюз у промисловому виконанні. Такі пристрої можуть бути інтегровані в інфраструктуру «розумного міста», аграрні або екологічні IoT-системи, забезпечуючи надійне приймання сигналів від сотень вузлів. Завдяки компактним розмірам та автономності, вони часто застосовуються у віддалених

регіонах або польових умовах, де необхідно мінімізувати витрати на обслуговування та підключення.

Ефективність роботи мережі LoRaWAN підтверджується численними дослідженнями, проведеними як у лабораторних умовах, так і в рамках польових випробувань. Зокрема, у роботах [20] на основі емпіричних даних і моделювання показано, що для забезпечення стабільного зв'язку у щільно забудованій міській зоні може бути достатньо лише трьох багатоканальних шлюзів для обслуговування мережі зі 10^5 активними вузлами. Такі результати свідчать про високу масштабованість архітектури LoRaWAN, особливо в умовах, де переважає трафік у висхідному напрямку.

Ключовим чинником, що дозволяє зменшити кількість необхідних шлюзів, є висока чутливість приймачів LoRa, здатних коректно декодувати сигнали навіть за дуже низького рівня потужності, а також квазіортогональність різних факторів розширення SF, яка знижує ймовірність колізій при одночасній передачі кількох вузлів. Крім того, можливість використання надвеликих радіусів покриття (до 10 км у сільських умовах) дає змогу ефективно охоплювати великі площі без потреби у щільному розміщенні інфраструктури.

Однак важливо враховувати, що реальні показники продуктивності залежать від розміщення вузлів, умов середовища передавання, щільності житлової забудови, радіочастотних перешкод та інших факторів. Тому при плануванні мережі LoRaWAN доцільно використовувати інструменти симуляції або проводити попередні радіотехнічні обстеження, аби адаптувати топологію до конкретного середовища розгортання.

Таким чином, LoRaWAN надає ефективну платформу для побудови сенсорних IoT-мереж завдяки енергоефективності, простій архітектурі та підтримці двостороннього зв'язку. Проте її централізована топологія типу «зірка-зірка» та відсутність нативної підтримки мультихопових маршрутизуючих механізмів обмежують гнучкість розгортання в умовах великої територіальної протяжності або відсутності доступу до шлюзової

інфраструктури. Це особливо критично для застосувань у віддалених регіонах, підземних об’єктах чи розподілених промислових системах, де централізоване управління втрачає свою ефективність.

Ці обмеження стимулювали появу низки дослідницьких і прикладних ініціатив, спрямованих на впровадження мультихопової передачі, побудову mesh топологій, а також децентралізованих підходів до маршрутизації даних на основі LoRa. У наступному розділі ми розглянемо наукові й практичні реалізації таких підходів, проаналізуємо їхні архітектурні особливості, переваги та недоліки, а також визначимо, якими принципами повинна керуватись ефективна IoT-система, здатна до самостійної організації топології та маршрутування в умовах обмежених ресурсів і відсутності централізованої інфраструктури.

1.2.Огляд досліджень і практичних підходів до застосування LoRa в бездротових сенсорних мережах

Останні роки відзначились зростанням наукового інтересу до впровадження механізмів мультихопової передачі, mesh топологій і динамічної маршрутизації у бездротових мережах на основі технологій LoRa та LoRaWAN. Дослідниками запропоновано низку рішень, що суттєво відрізняються за рівнем складності, функціональним призначенням та ступенем технологічної зрілості TRL - від теоретичних концепцій до експериментально підтверджених прототипів, розгорнутих у лабораторних умовах або в реальних середовищах. Варто зазначити, що лише обмежена кількість із цих рішень представлена у вигляді готових до використання комерційних продуктів.

У цьому підрозділі здійснюється аналіз найбільш релевантних розробок, класифікованих відповідно до їх прикладного призначення, типових сценаріїв використання та функціональних можливостей, які вони надають для побудови гнучких, масштабованих та самоорганізованих мереж. Частина з цих підходів уже була досліджена в попередніх оглядах з різних точок зору: з урахуванням

конкретних прикладних сценаріїв [21], в контексті архітектурних обмежень LoRaWAN [22], а також у рамках аналізу топологій і протоколів маршрутизації [23]. У цьому розділі ми систематизуємо ці підходи, а також виокремлюємо нерозв’язані проблеми, що залишаються відкритими для подальших досліджень

1.2.1. Багатоперехідні рішення в архітектурі сенсорної мережі

Класична топологія типу «зірка-зірка», що лежить в основі архітектури LoRaWAN, є однією з найбільш поширених у бездротових сенсорних мережах завдяки своїй простоті реалізації та енергоефективності. Вона демонструє ефективну роботу в багатьох сферах, де можливе пряме з’єднання кінцевих пристроїв зі шлюзами. Однак така топологія не завжди забезпечує оптимальні маршрути для передавання даних між IoT-вузлами та шлюзами, особливо у випадках складної географії, урбанізованих середовищ або віддалених регіонів [24]. Однією з головних проблем залишається той факт, що покриття мережі LoRaWAN обмежується зоною дії її шлюзів, яка, хоча й може сягати кількох кілометрів завдяки радіотехнології LoRa, все ж виявляється недостатньою для масштабних або розгалужених інфраструктурних об’єктів.

Намір розширити покриття мережі LoRaWAN часто стикається з низкою практичних обмежень, пов’язаних як з технічними, так і з економічними чинниками. Установлення додаткових шлюзів може виявитися неможливим через відсутність придатних монтажних точок, недостатню інфраструктуру живлення або відсутність доступу до IP-мережі. До цього додаються організаційні та юридичні складнощі, оскільки власники інфраструктури та кінцеві користувачі часто є різними суб’єктами з відмінними комерційними інтересами та технічними обмеженнями.

У відповідь на ці виклики дослідники запропонували низку альтернатив, зокрема розширення архітектури LoRaWAN за рахунок впровадження мультихопової передачі. Такий підхід дозволяє даним пересилатися через

послідовність IoT-вузлів або допоміжних елементів мережі до шлюзу призначення, минаючи потребу в прямому підключенні кожного вузла до інфраструктури. В рамках цієї концепції сформувалися три ключові стратегії реалізації:

1. Додавання функції ретрансляції до самих шлюзів;
2. Розширення функціональності кінцевих пристроїв мережі;
3. Інтеграція проміжних ретрансляційних вузлів, які виступають у ролі проксі-компонентів між вузлами та шлюзом.

У рамках подолання зазначених обмежень, Хосе Діас і Антоніо Грило запропонували й реалізували механізм мультихопової ретрансляції, спрямований на розширення покриття шлюзів у LoRaWAN-мережах [25]. Автори підкреслюють, що в ряді практичних випадків установлення додаткових шлюзів не є прийнятним рішенням - зокрема, коли кінцеві користувачі не мають контролю над базовою інфраструктурою. Як альтернативу вони пропонують використання проміжних вузлів ретрансляції, які передають пакети від кінцевих пристроїв до шлюзів. Концептуальна схема такої архітектури представлена на рис. 1.6.

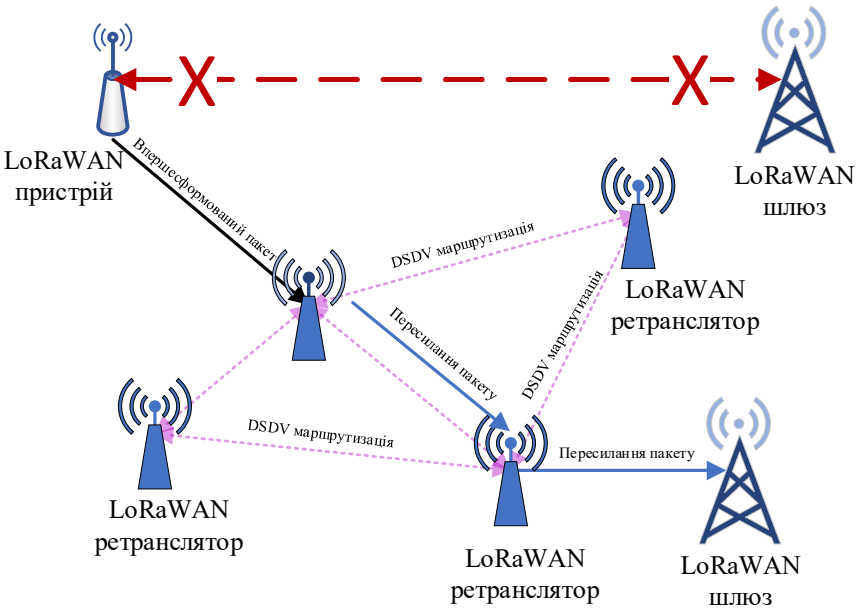

Рис. 1.6 - Схематичне представлення рішення Хосе Діаса і Антоніо Грило щодо мультихопової ретрансляції у висхідному напрямку.

Запропоноване рішення ґрунтується на спрощеному протоколі маршрутизації, реалізованому на основі класичного алгоритму Беллмана-Форда - а саме, його варіанту послідовно дистанційно-векторної маршрутизації DSDV [26]. Цей протокол працює на проміжних вузлах, які координуються між собою для ретрансляції пакетів до найближчого та найнадійнішого доступного шлюзу. Такий підхід не лише дозволяє обійти обмеження класичної топології, але й забезпечує більшу відмовостійкість, оскільки трафік може бути автоматично перенаправлений через інші вузли у разі виходу шлюзу з ладу або перевантаження.

Запропоноване рішення було експериментально протестоване у двох типах мережевої топології:

1. Топології загальної шини;

2. Конфігурації вузького місця, яка моделює сценарії з обмеженою пропускною здатністю між окремими ділянками мережі.

У своїй реалізації автори використали елементи гібридного протоколу безпровідних мереж HWMP [27] та протокол динамічної маршрутизації для мобільних ad-hoc мереж AODV [28], які були адаптовані до особливостей роботи LoRa-технології. Ключовою інновацією став механізм тунелювання пакетів між шлюзами, що дозволяє забезпечити зв’язок навіть у випадках, коли кінцевий вузол підключений лише до «віддаленого» шлюзу без інтернет-доступу.

Запропонований протокол був реалізований на практиці та перевірений як у лабораторних умовах, так і під час польових випробувань, де підтверджено можливість успішної передачі висхідних повідомлень через мережу з чотирма переходами. При цьому низхідні передачі (від сервера до вузлів) були розглянуті концептуально, але не пройшли практичного тестування в межах представленої роботи.

Бруно Ван де Вельде запропонував підхід до реалізації багатохопової комунікації в мережах LoRaWAN шляхом впровадження проміжного ретрансляційного пристрою, призначеного для розширення зони покриття та

покращення якісних характеристик зв'язку [29]. За своєю архітектурою цей пристрій поєднує функціональність повноцінного шлюзу LoRaWAN і мережевого сервера, а також виконує роль активного ретранслятора даних.

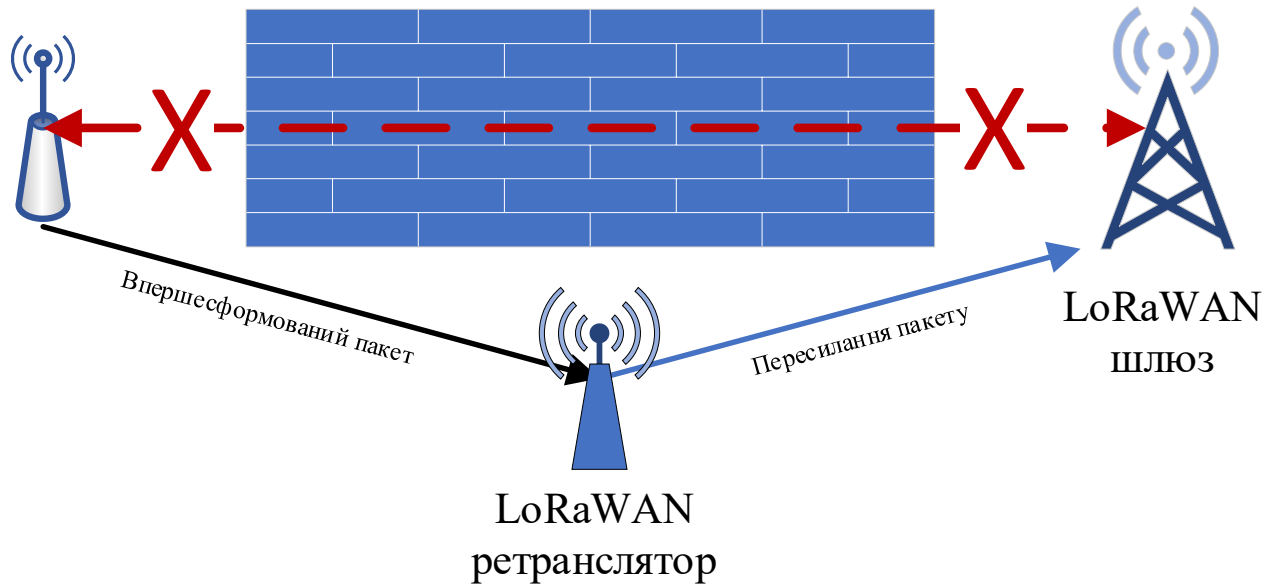

Рис. 1.7 - Схематичне зображення ретрансляційного вузла Бруно Ван де Вельде.

На рис. 1.7 представлено архітектурну схему цієї системи, в якій ретранслятор розташований у центрі процесу комунікації. В основі ідеї лежить зменшення енергоспоживання кінцевих пристроїв: завдяки скороченню відстані передачі знижується необхідна потужність сигналу та тривалість перебування в ефірі. Сам ретранслятор функціонує як комплексний вузол, що поєднує в собі роль шлюзу LoRaWAN та мережевого сервера, включаючи всі компоненти, притаманні класичному шлюзу.

Крім того, пристрій запускає додаткову програму, яка відповідає за повторну трансляцію пакетів даних, отриманих від кінцевих пристроїв, безпосередньо до шлюзу. Перша реалізація підтримувала лише висхідну передачу даних, але виявилася непридатною для коректної роботи з низхідними пакетами, зокрема із підтвердженнями доставки ACK. У другій, більш досконалій версії, було реалізовано покращене управління низхідним потоком,

однак залишилась невирішеною проблема асиметрії швидкостей передачі між кінцевим вузлом та ретранслятором і між ретранслятором і шлюзом.

Рішення пройшло тестування у лабораторних умовах, де пристрої були розміщені на невеликих відстанях один від одного, з фізичними перешкодами між ними. Результати експериментів показали, що використання ретрансляційного пристрою дозволило зменшити час перебування в ефірі на дві третини, що позитивно вплинуло на енергоспоживання. Водночас було зафіксовано збільшення втрат пакетів, причини чого автор не зміг повністю з'ясувати. Крім того, затримка передачі також зросла щонайменше на одну секунду, що було обумовлено додатковими обчисленнями та обробкою на рівні ретранслятора.

Крістіан Ебі та співавтори дослідження представили реалізацію синхронного протоколу LoRa mesh, спрямованого на розширення мережі LoRaWAN у специфічних умовах підземної інфраструктури, зокрема для моніторингу важкодоступних кінцевих вузлів [30]. Запропоноване ними рішення передбачає використання вузлів-ретрансляторів, які з'єднують сегмент синхронної LoRa mesh-мережі з типовим LoRaWAN шлюзом, що дозволяє значно покращити зв'язок у середовищах із високим рівнем радіоізоляції, як-от тунелі, підземні об'єкти або сховища.

Згідно з результатами досліджень, запропонована архітектура переважає класичну LoRaWAN за надійністю доставки пакетів при передачі даних з критичних ділянок. Така модель підвищує ефективність і гнучкість мережі, дозволяючи реалізувати більш стабільний і прогнозований зв'язок у складних умовах розгортання. Проте система вимагає жорсткої синхронізації вузлів, що забезпечується завдяки зовнішньому часовому еталону, наприклад за допомогою супутникової синхронізації (GPS) або сигналів радіочасу DCF77.

1.2.2. Багатоперехідні та mesh-мережі для децентралізованих систем

Другим етапом у прагненні до побудови більш гнучких топологій мереж, ніж традиційна «зірка-зірка», є розробка мультихопових протоколів для формування mesh мереж, у яких вузли взаємодіють децентралізовано. У таких мережах ієрархічна структура між шлюзами та кінцевими пристроями нівелюється, що дозволяє реалізувати горизонтальні розгортання, де всі вузли мають рівні функціональні обов’язки щодо організації мережі, пересилання трафіку та обміну інформацією.

Цей підхід відкриває можливість відмови від централізованих шлюзів і хмарних серверів на користь локальних, самокерованих систем, які використовують обчислювальні потужності на периферійних пристроях для обслуговування розподілених IoT-додатків. Такі мережі не лише забезпечують автономність, а й дозволяють скоротити затримки, уникнути перевантаження центрального вузла, а також вбудовувати керовану логіку безпосередньо в кінцеві пристрої, що є важливим для застосувань з високими вимогами до інтеграції в замкнене кероване середовище.

Серед причин, що стимулюють розвиток подібних архітектур, слід виділити як технічні чинники, так і потреби у збереженні конфіденційності даних, кібербезпеки та технологічної незалежності. У багатьох випадках автономність у розгортанні й керуванні мережею дозволяє уникнути залежності від сторонніх провайдерів або власників інфраструктури, що є особливо актуальним у критичних або віддалених сценаріях застосування.

Хуан-Чен Лі, Кай-Сян Ке та співдослідники розробили та впровадили систему mesh мережі на базі технології LoRa, орієнтовану на потреби IoT-додатків [25 - 26]. На їхню думку, розгортання у міських середовищах потребує високої щільності LoRaWAN-шлюзів, щоб гарантувати надійний зв’язок для кінцевих пристроїв, зокрема розташованих у приміщеннях. Щоб уникнути необхідності встановлення додаткових шлюзів, вони запропонували

альтернативну архітектуру сітчастої мережі, яка мінімізує інфраструктурні витрати. На рис. 1.8 вузли мережі динамічно формують деревоподібну топологію шляхом встановлення ролей "батьківських" і "дочірніх" пристроїв для досягнення точки збору даних (шлюзу), який періодично опитує вузли для отримання показників сенсорі

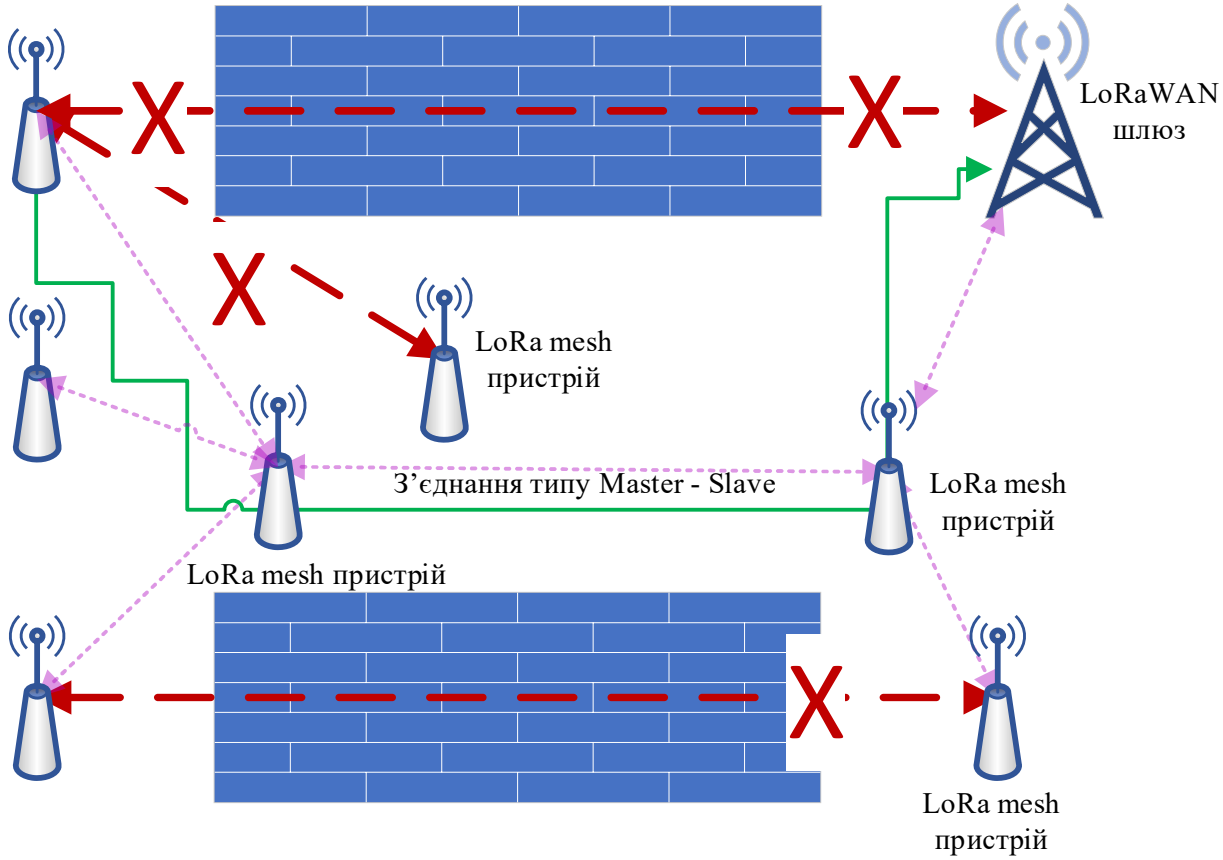

Рис. 1.8 - Mesh мережа LoRa розроблена Хуаном-Чен Лі, Кай-Сяном Ке та ін.

На рисунку 1.8 представлено загальну архітектуру мережі, сформовану з пристроїв LoRa, що реалізують деревоподібну топологію з можливістю масштабування й адаптації до змін середовища розгортання.

Запропонована система базується на центральному пристрої-збірнику даних, який автори умовно називають "шлюзом" - не через апаратну реалізацію, а через його логічну роль у мережі. На початковому етапі роботи цей пристрій транслює маячкові сигнали, запрошуючи кінцеві вузли приєднатися до мережі.

Вузли, які отримують ці сигнали, фіксують передавач як "батьківський" вузол і встановлюють з ним логічне з’єднання.

Після цього передача даних відбувається за допомогою опитування: "шлюз" ініціює запит до кожного з дочірніх вузлів. Нові вузли, які перебувають у зоні досяжності сигналів від шлюзу або інших вузлів, також можуть приєднатися до мережі, обираючи оптимальний батьківській вузол за кількома критеріями: RSSI та кількість переходів до "шлюзу". Централізоване збереження топології в "шлюзі" дає змогу оптимізувати маршрутизацію, динамічно змінюючи ієрархію вузлів відповідно до змін у мережі.

Систему було експериментально протестовано шляхом розгортання 19 вузлів на площі 900×700 м² на території університетського кампусу протягом 8 днів. Отримані результати показали динамічні зміни в топології мережі, а також вплив запропонованої структури на коефіцієнт доставки пакетів PDR для кожного вузла. Встановлено, що мережа покращила показники PDR для всіх вузлів, зокрема для тих, що знаходилися на межі або поза прямим радіусом дії умовного шлюзу. Водночас автори підкреслюють, що хоча запропоноване рішення дозволяє уникнути встановлення додаткових шлюзів, така архітектура обмежує максимальну кількість підтримуваних вузлів. Це пов’язано з послідовним пересиланням даних, що спричиняє збільшення часу доставки повідомлень у мережі.

Серед низки сучасних підходів до побудови гнучких багатохопових мереж на базі LoRa, Бенджамін Сарторі та колеги запропонували рішення для розширення покриття бездротових мереж шляхом поєднання протоколу маршрутизації RPL із MAC-рівнем, специфічно адаптованим під LoRa - так званий протокол RPL+LoRa MAC (RLMAC) [31]. Дослідники наголошують, що хоча зіркова топологія зручна для швидкого розгортання і приваблива з точки зору бізнес-моделей, мультихопова структура має значні переваги у випадках перевантаження мережі або необхідності покриття великих територій, де розміщення численних базових станцій є складним або неекономічним.

Зокрема, мультихопова передача може не лише покращити покриття, але й збільшити загальну пропускну здатність, зменшуючи час передачі шляхом використання вищих значень фактору розширення SF. У своїй реалізації автори зосередилися на мережах, побудованих на одночастотних пристроях LoRa, тоді як шлюзи у такій архітектурі, як правило, оснащені більш продуктивними радіочіпами з підтримкою багатоканального прийому.

Архітектура RLMAC базується на поєднанні повільного циклу прийому з більш частими циклами передачі, що дозволяє вузлам приймати повідомлення від будь-якого сусіднього пристрою, незалежно від використовуваного ними SF. На рис. 1.9 схематично зображено реалізацію запропонованої мережі з кореневим вузлом протоколу RPL. Вузли слухають ефір у циклі на кожному факторі розширення SF та формують топологію з мінімальною вартістю шляху.

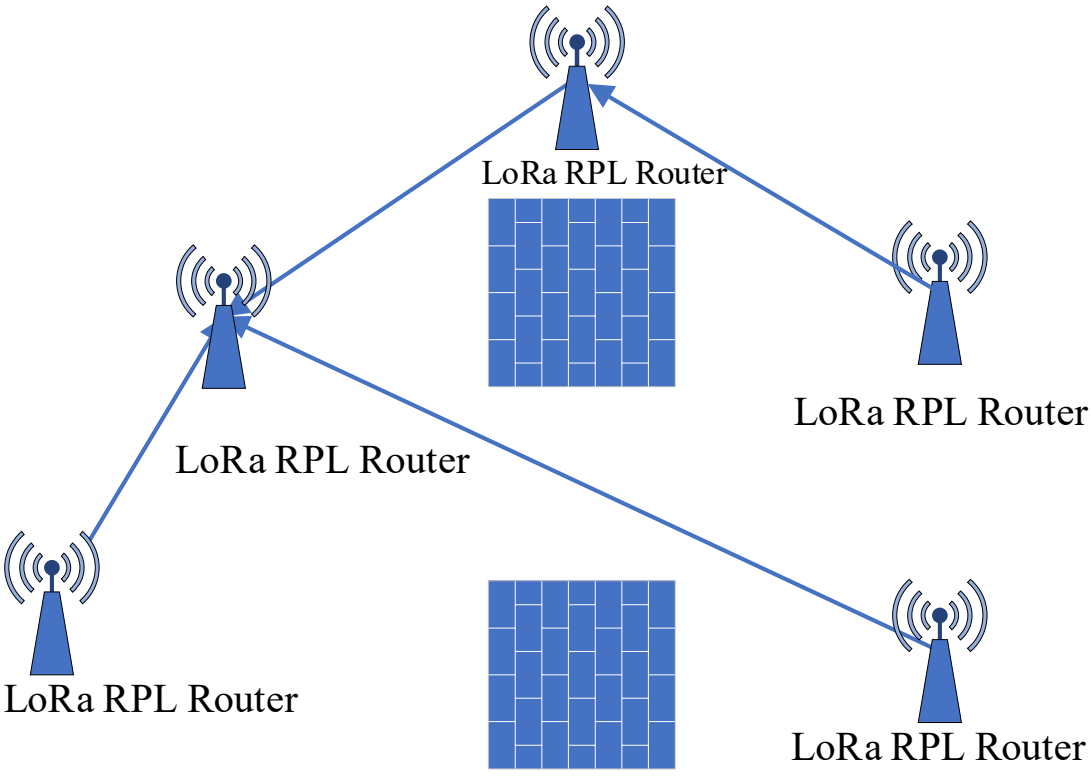

Рис.1.9 – Mesh LoRa-мережа на основі RPL, запропонована Бенджаміном Сарторі та ін.

У ході початкових експериментальних перевірок було виявлено, що коли декілька вузлів одночасно обирають однаковий SF для передачі даних до одного

приймача, виникають часті колізії. Для розв'язання цієї проблеми дослідники ввели механізм випадкових затримок, що базуються на оцінках рівня RSSI. Автори відзначають, що надалі їхнє рішення буде додатково перевірене з використанням симуляційних інструментів з метою глибшого аналізу енергоспоживання та продуктивності в умовах масштабного розгортання.

Сунуку Кім та ін. запропонували схему адаптивного вибору фактора розширення ASFS для побудови mesh мереж LoRa з використанням одночастотних трансиверів, з метою підвищення пропускної здатності та зниження витрат [32]. Запропоноване рішення ґрунтується на використанні можливостей детекції активності на каналі CAD, що підтримуються модемами LoRa, у поєднанні з ітеративним алгоритмом перевірки та вибору оптимального фактора розширення SF. Такий підхід дозволяє кожному вузлу працювати на різних швидкостях передачі даних незалежно один від одного, досягаючи майже 100% точності у виявленні колізій.

Ідея ASFS була раніше реалізована в одночастотних шлюзах, однак не адаптована до мультихопової архітектури. У своїх дослідженнях автори експериментально оцінили ефективність підходу із залученням до 10 вузлів і протестували три мережеві топології: зірка, деревоподібна та сітчаста (mesh). Для експериментів використовувались як одночастотні LoRa-трансивери Semtech SX1272, так і багатоканальні SX1301. Виявилося, що завдяки ASFS вузли могли обирати швидші SF, що дозволяло досягати швидкостей передачі даних у 4–6 разів вищих порівняно з мережами, де всі вузли використовували повільні, загальноприйняті значення SF.

Чунь-Хао Ляо та співавтори здійснили спробу побудови багатохопової мережі на основі LoRa, поєднаної з концепцією одночасної передачі CT [33]. Вони підтвердили, що технологія LoRa є сумісною з механізмами CT, і що продуктивність приймача може бути суттєво підвищена шляхом введення часових зсувів між ретрансляційними пакетами, що передаються в мережі. Для цього було запропоновано метод "зсуву-CT", який полягає у випадковому

внесенні затримок у передачу сигналу, що водночас дозволяє уникнути накопичення зсуву протягом багатохопового передавання.

У першій частині дослідження автори оцінили, як саме одночасна передача впливає на LoRa, зокрема з урахуванням тривалого часу передачі символу, особливо за умов використання високих значень фактора розширення SF. Результати показали, що CT з великою ймовірністю не призводить до повного згасання символів LoRa, навіть за умов їх перекриття.

У другій частині вони дослідили потенційну несумісність модуляції LoRa -M-ary FSK (частотна маніпуляція з багатьма рівнями) та зсуву частоти несучої (CFO) з механізмом CT. Проте аналіз виявив, що дві властивості Сефекту захоплення" - у частотній та часовій областях, притаманні модуляції FSK, навпаки, сприяють ефективному функціонуванню LoRa в умовах одночасної передачі.

Таким чином, поєднання LoRa та CT видається особливо перспективним для щільних IoT-середовищ, де потрібна висока надійність прийому за умов багатохопової маршрутизації. На рис. 1.10 наведено запропоновану топологію мережі, в якій пакети передаються між вузлами один за одним, використовуючи переваги CT.

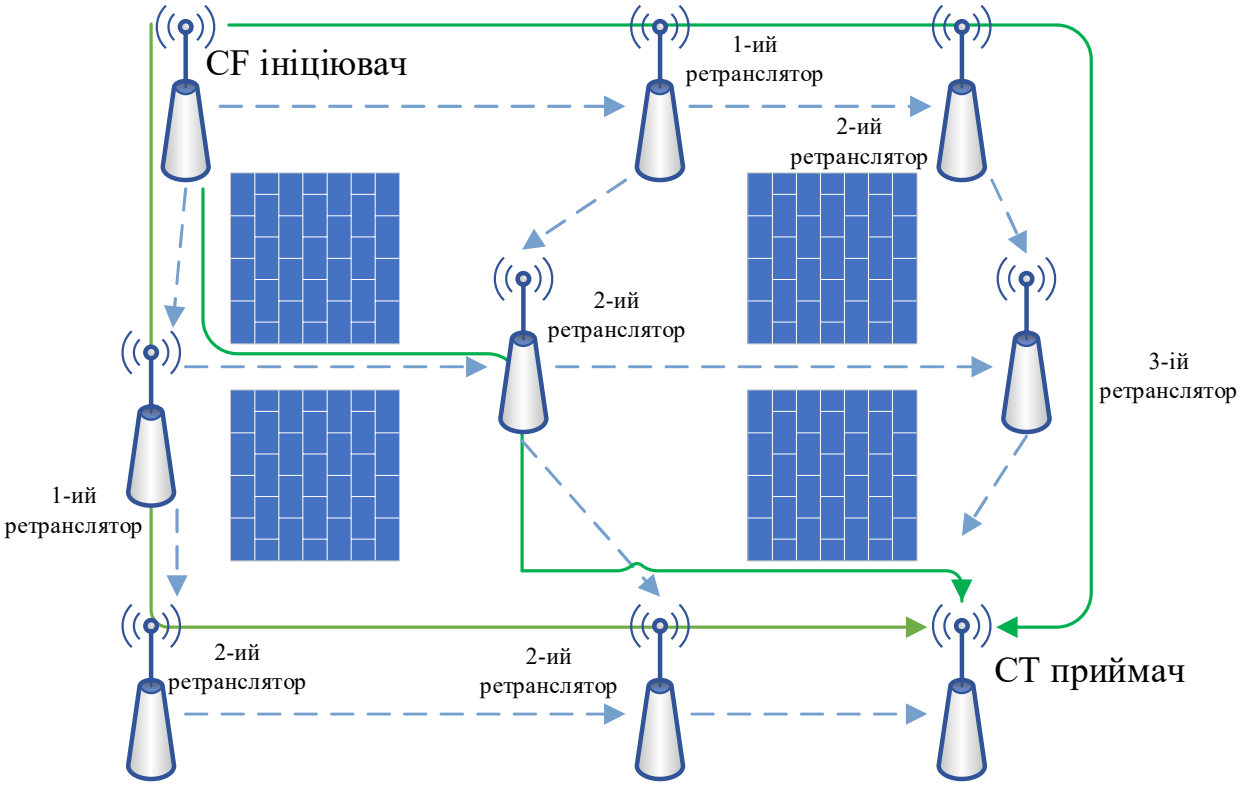

Рис. 1.10 - СТ-орієнтована LoRa mesh-мережа, запропонована Чунь-Хао Ляо та ін.

На рис 1.10 представлено схематичне зображення сітчастої мережі, запропонованої Чунь-Хао Ляо та колегами, у якій використовується механізм одночасної передачі СТ. Цей підхід забезпечує послідовне багатохопове розповсюдження пакета, поки той не досягне вузла-призначення. Така стратегія суттєво покращує ефективність ретрансляції в щільних мережах і відкриває нові перспективи для гнучких IoT-інфраструктур, особливо у складних умовах зв'язку.

Для підтвердження отриманих аналітичних результатів, автори спочатку змоделювали продуктивність приймача LoRa в умовах одночасної передачі СТ, а згодом провели практичні експерименти з використанням реальних радіомодулів Semtech LoRa SX1272. Результати засвідчили, що приймачі LoRa здатні функціонувати в умовах СТ без потреби у додаткових захисних

механізмах - на рівні, не гіршому за інші стандарти, сумісні з CT, зокрема IEEE 802.15.4 [34].

Крім того, у дослідженні було оцінено ефективність запропонованого підходу "зсуву-CT", який базується на введенні випадкових часових зсувів між ретрансляційними передачами. Цей підхід дозволяє уникати накладання символів у мультихопових сценаріях. Дослідники дійшли висновку, що швидкість прийняття пакетів PRR суттєво покращується, коли ці затримки не збігаються з кратними значеннями часу символу модуляції.

Для демонстрації життєздатності підходу, було проведено експерименти концептуального рівня (PoC) у рамках сценарію багатобудинкових мереж MBAN. У тестовій мережі, що складалася з 18 вузлів з радіомодулями SX1272, проводились вимірювання у середовищах як з низькою, так і з високою щільністю розміщення пристроїв. Встановлено, що навіть без оптимізації, CT-LoRa демонструє високий рівень прийому, який суттєво покращується із застосуванням методики offset-CT, особливо в умовах щільного розміщення вузлів.

Мойзес Нуньєс Очоа та співавтори дослідники [35] здійснили детальний аналіз ключових радіопараметрів технології LoRa - зокрема, фактору розширення SF, ширини смуги каналу та потужності передавання - з метою оцінки енергоспоживання передавачів у мережах з топологіями типу "зірка" та mesh. У ході дослідження було підкреслено високу гнучкість LoRa щодо налаштування фізичних параметрів для різних сценаріїв розгортання мережі, а також оцінено їхній вплив на споживання енергії при передаванні та прийомі даних.

У випадку топології "зірка" встановлено, що збільшення значення SF має значно більший вплив на енергоспоживання порівняно з підвищенням потужності передавання. У зв’язку з цим, дослідники рекомендують спочатку адаптувати потужність передавача, а лише потім збільшувати фактор

розширення SF - що дозволить ефективно знижувати загальне споживання енергії.

Для мереж типу mesh, навпаки, енергоспоживання оптимізується шляхом підбору індивідуальних радіоконфігурацій залежно від макета розгортання, при цьому щільність розміщення вузлів відіграє ключову роль у досяжному радіусі зв'язку та кількості необхідних хопів (пересилань).

На основі отриманих результатів автори формують висновок, що гібридна стратегія, яка комбінує обидві топології - як "зірка", так і mesh - може забезпечити ефективний компроміс між енергоощадженням та покриттям мережі. Загальна продуктивність такої системи істотно залежатиме від географічної площі розгортання та щільності вузлів. Схематичне зображення відповідної мережевої конфігурації наведено на рис. 1.11.

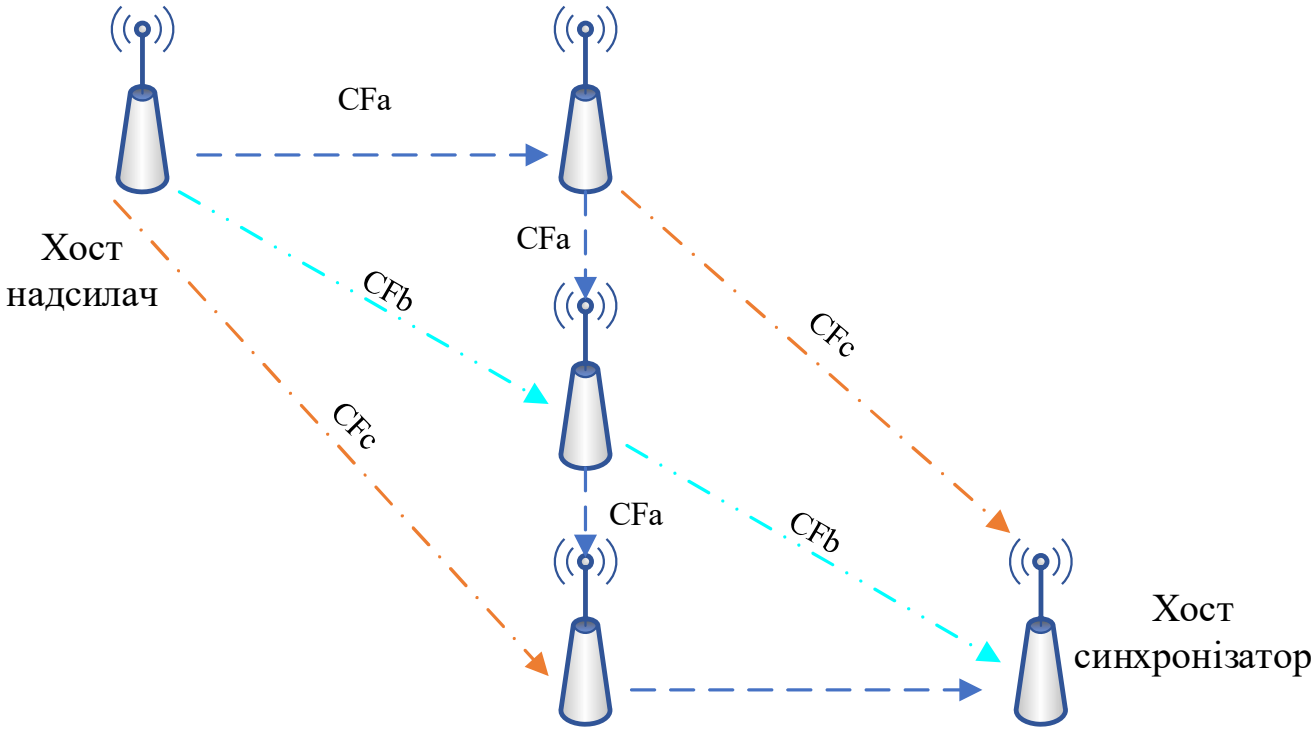

Рис. 1.11 - Енергоефективна mesh-мережа LoRa за версією дослідження Нуньєса Очоа та ін.

Використання різних факторів розширення (SFa, SFb, SFc) дозволяє пристроям адаптувати дальність передачі, забезпечуючи так звані "ступені свободи" і впливаючи на загальний рівень енергоспоживання.

Багатоперехідні лінійні сенсорні мережі. Системи моніторингу лінійних об'єктів інфраструктури, таких як лінії електропередач, водні канали, трубопроводи, транспортні коридори або підземні тунелі, становлять важливий клас розгортань у сфері Інтернету речей. Схожі проблеми покриття також виникають у підземних розгортаннях, зокрема в шахтах або каналізаційних системах. Попри те, що технологія LoRa забезпечує велику дальність передачі сигналу та характеризується низьким енергоспоживанням, у випадку надвеликих протяжностей - понад сотні кілометрів - її можливостей може виявитися недостатньо. Встановлення великої кількості шлюзів уздовж таких об'єктів часто є недоцільним або неможливим через обмеження щодо доступу, живлення або вартості.

У цьому контексті мультихопові рішення для лінійних мереж виступають як окрема підкатегорія серед загальних реалізацій мультихопової або mesh-топології на основі LoRa. Їх характерною особливістю є передбачувана, строго послідовна схема передавання даних, що відкриває можливості для високоефективної синхронізації роботи вузлів. Дослідники пропонують рішення, в яких кожен вузол більшість часу перебуває в енергоощадному "сплячому" режимі, активуючись лише на короткий період для прийому пакета, додавання локального вимірювання (за наявності) та подальшої пересилки пакета вздовж лінії до кінцевого вузла або шлюзу. Такий підхід значно знижує загальне енергоспоживання і дозволяє ефективно розгортати мережі на великій території з мінімальним використанням інфраструктури.

Андреа Абардо та Алессандро Поцебон розробили мультихопову лінійну мережу на базі технології LoRa, орієнтовану на застосування в підземних середовищах, з акцентом на оптимізацію циклів сну та пробудження вузлів для зменшення споживання енергії батарейними пристроями [36]. Після проведення натурного експериментального вимірювання в умовах реального середовища, автори виявили, що ефективна відстань передачі LoRa обмежується приблизно 200 метрами. Це унеможливлює використання класичної топології "зірка" для

безперервного моніторингу довгих об'єктів інфраструктури, таких як акведуки або підземні комунікації, які часто мають вигини або інші перешкоди, що перекривають пряму видимість між передавачами.

Для подолання цієї проблеми дослідники реалізували модель передачі даних, у якій сенсорні вузли формують ланцюг послідовної ретрансляції - від початкового вузла до центрального шлюзу, як показано на рис. 1.12. Такий підхід дозволяє підтримувати передачу навіть у випадках, коли пряме з'єднання між вузлами та шлюзом неможливе через особливості фізичної структури середовища.

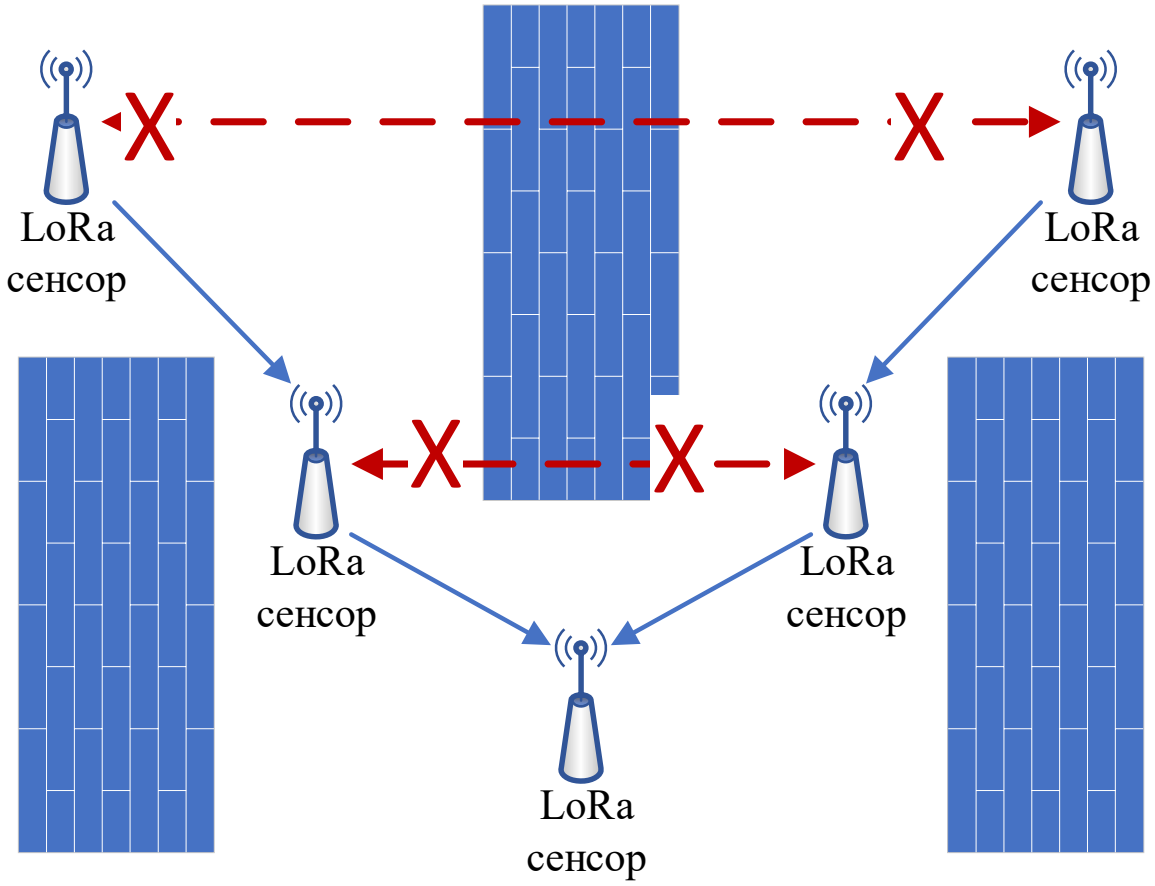

Рис. 1.12 - Мультихопова лінійна мережа LoRa за Абрардо і Поцебоном

З огляду на складність доступу до підземної інфраструктури та необхідність мінімального втручання після встановлення, система була спроєктована з фокусом на максимальне зниження енергоспоживання. Вузли

залишаються в режимі сну більшу частину часу та активуються лише під час вибірки або передачі даних - як власних, так і ретрансльованих.

Прототип системи було побудовано з використанням мікроконтролерних плат Arduino UNO як сенсорних вузлів, а також шлюзу на базі пристрою Waspmote USB GW, який виступав як пункт збору даних. Під час експлуатації виявилося, що внутрішній годинник Arduino має недостатню точність для гарантованого пробудження пристрою у заданий момент після тривалих циклів сну (тобто понад 120 секунд). Для розв'язання цієї проблеми дослідники розробили оптимізований механізм синхронізації, який забезпечує узгоджене прокидання вузлів і послідовну передачу даних від одного до іншого. Це дозволило збільшити інтервали сну та зменшити загальне споживання енергії більш ніж на 50% у порівнянні з початковим рішенням.

Конг Тан Дуонг та Мен Кюн Кім запропонували та реалізували протокол багатохопової комунікації, орієнтований на лінійні розгортання мереж LoRa, які охоплюють значні відстані [37]. Рішення було спеціально розроблене для інфраструктурних сценаріїв моніторингу, де вузли розташовуються вздовж протяжних об’єктів - таких як газопроводи, лінії електропередач або залізничні колії. У таких конфігураціях класична топологія "зірка" виявляється малопридатною через обмеження дальності покриття окремих шлюзів.

Запропонована система функціонує у два основні етапи: ініціалізаційний та експлуатаційний. На першому етапі формується лінійна топологія мережі - вузли послідовно передають ініціалізаційне повідомлення від пристрою збору даних (шлюзу) до найвіддаленішого вузла. У процесі цієї передачі забезпечується правильне позиціювання та синхронізація кожного вузла. На другому етапі мережа переходить до регулярної роботи: вузли періодично прокидаються відповідно до заздалегідь узгодженого графіка, отримують пакети від сусідів, об’єднують їх із власними даними й передають далі по лінії до шлюзу.

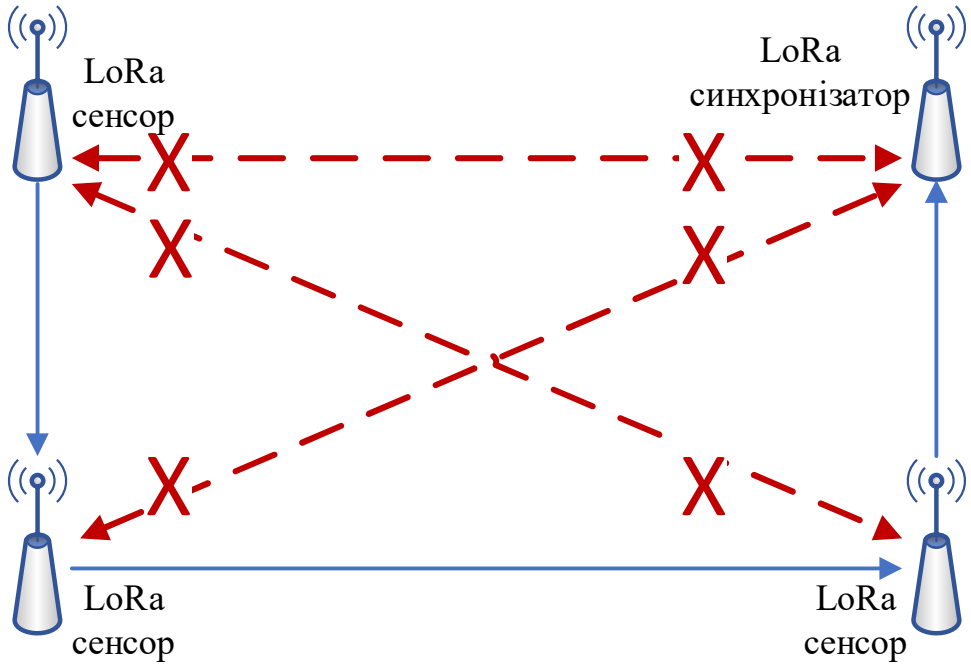

Рис. 1.13 – Лінійна багатохопова мережа LoRa за Дуонгом і Кімом.

Як зображено на рис 1.13, вузли в мережі організовані вздовж напівкола, утворюючи лінійну багатохопову топологію. Така структура дозволяє ефективно передавати дані від кожного вузла до центрального вузла-збирача, поєднуючи їх з власними вимірюваннями на кожному етапі пересилання.

Дослідники реалізували тестову мережу, яка складалася з чотирьох моніторингових вузлів, встановлених вздовж прямої ділянки на території університету, з інтервалами 150–200 метрів, та одного пристрою збору даних. У ході експерименту були протестовані різні значення фактора розширення SF для оптимізації зв’язку. Результати демонструють високий рівень ефективності - коефіцієнт доставки пакетів PDR варіювався від 92% до 98%, тоді як пропускна здатність змінювалась у межах від 28 до 185 біт/с залежно від обраного SF.

Система продемонструвала високу надійність для односпрямованого висхідного потоку даних, а також ефективно реалізувала цикли сну та пробудження вузлів, що дозволяє суттєво скоротити енергоспоживання. Проте слід зазначити, що архітектура не підтримує напівдуплексну або

повнодуплексну передачу даних у зворотному (низхідному) напрямку, що обмежує її застосування у випадках, коли необхідна двостороння комунікація.

1.2.3. Програмні бібліотеки та інструменти моделювання

Майк Макколі розробив бібліотеку RadioHead - програмне забезпечення для пакетного радіозв'язку, призначене для використання у вбудованих мікропроцесорних системах. Воно надає об'єктноорієнтовану бібліотеку для надсилання та отримання повідомлень за допомогою різних технологій радіозв’язку, зокрема LoRa [38]. Особливий інтерес становить підклас RHMesh, який дозволяє здійснювати адресовану, за необхідності підтверджену, передачу дейтаграм у мережах з багатохоповою маршрутизацією. RHMesh забезпечує автоматичне виявлення маршрутів і обмін маршрутною інформацією між вузлами, що знаходяться у безпосередній радіодоступності один до одного, утворюючи mesh топологію.

Цей підхід особливо корисний для динамічних мереж, де топологія часто змінюється, а вузли можуть переміщуватися або ставати недоступними. RHMesh підтримує надійну доставку повідомлень між окремими хопами, хоча підтвердження на рівні "кінець-кінець" не передбачено. На рис. 1.14 зображено умовну сітчасту мережу, де така бібліотека може бути ефективно застосована.

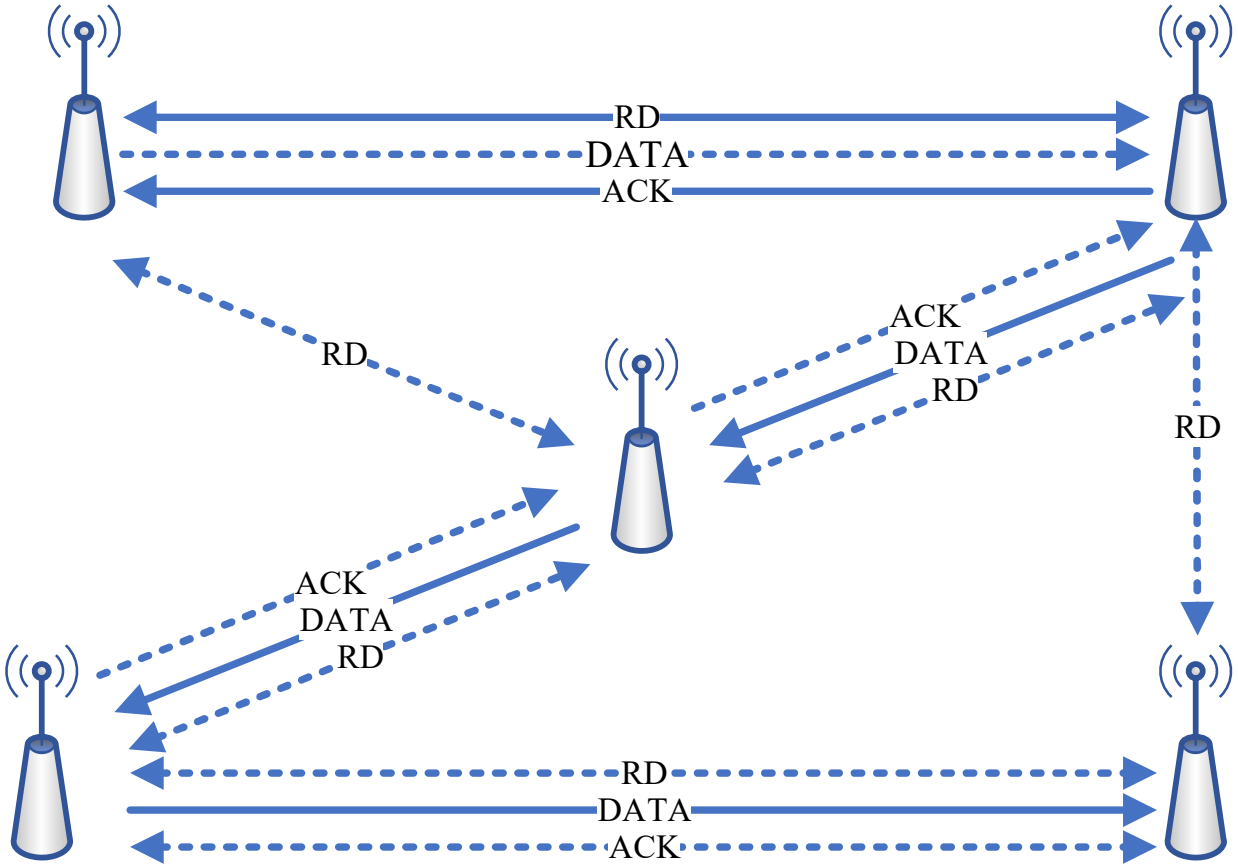

Рис. 1.14 - Схематичне зображення сітчастої мережі, що працює з бібліотекою RadioHead RHMesh..

На рис. 1.14 зображена теоретична mesh мережа, де це рішення може бути використане. Воно може бути використане в мережах, де топологія мережі є динамічною, а вузли переміщуються або стають недоступними. RHMesh використовує надійну доставку повідомлень від вузла до вузла, але без підтверджень на кінцевих точках зв'язку. Автор звертає увагу на обмеження цієї бібліотеки: для її функціонування необхідно близько 2 кБ оперативної пам’яті SRAM, що перевищує ресурси деяких пристроїв Arduino. Крім того, клас RHMesh не підтримує черги повідомлень, тому може обробляти лише одне повідомлення одночасно, що обмежує його продуктивність у сценаріях з високою інтенсивністю трафіку.

Волонтери з ініціатив Sudo Mesh та Secure Scuttlebutt розробляють автономну, сонячну, далекобійну mesh-мережу, орієнтовану на забезпечення

зв’язку у надзвичайних ситуаціях [39]. Метою цього проєкту є створення відкритої апаратно-програмної платформи, здатної підтримувати критичну інфраструктуру громад у випадках природних катастроф або тривалих відключень електроенергії та зв'язку. Розробка базується на використанні популярного Wi-Fi мікроконтролера ESP8266, що забезпечує повний стек TCP/IP, у поєднанні з LoRa-трансивером Semtech SX1276, який виконує функції довготривалої бездротової передачі даних між вузлами мережі.

Такий гібридний підхід дозволяє кожному вузлу одночасно підтримувати локальне з'єднання через Wi-Fi для доступу кінцевих користувачів і далекобійне з'єднання через LoRa для ретрансляції повідомлень між вузлами в мережі. Це дає змогу організувати незалежну від зовнішньої інфраструктури сітку, яка може функціонувати навіть в умовах повної відсутності Інтернет-з’єднання. Розгортання особливо актуальне для громад, які прагнуть підвищити свою стійкість до криз і зберегти комунікаційну доступність у складних обставинах.

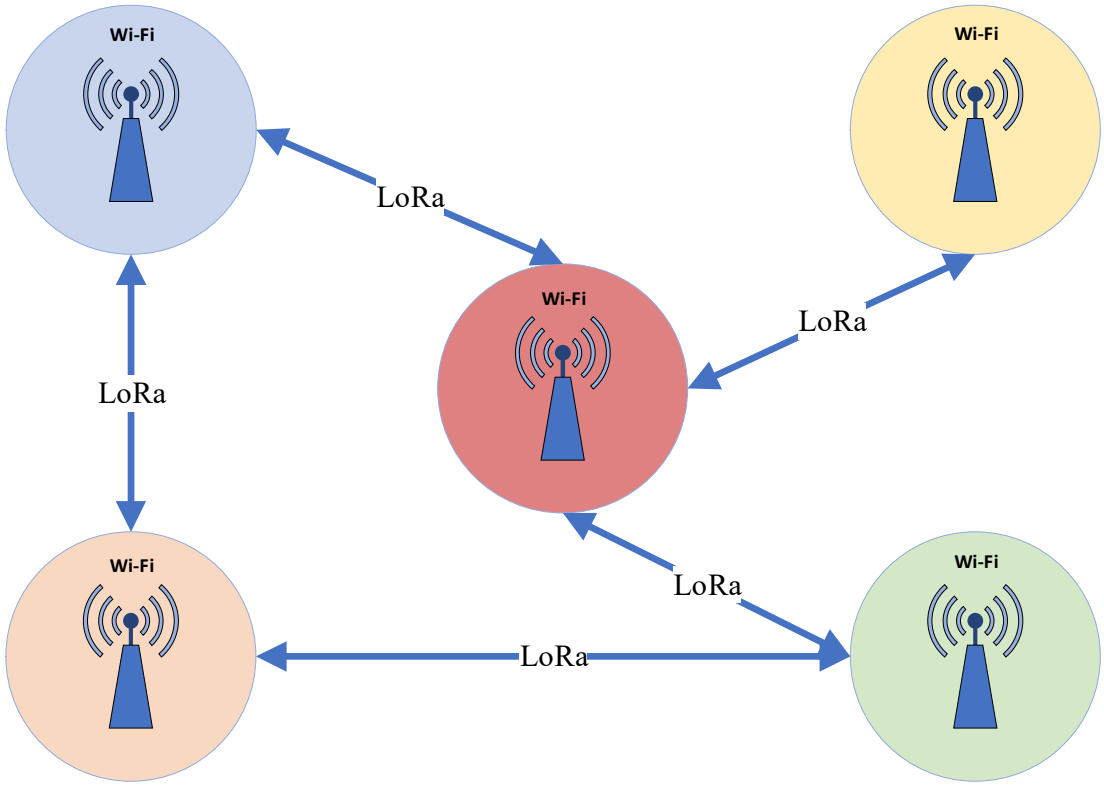

Рис. 1.15 - Mesh-мережа LoRa, розроблена ініціативами Sudo Mesh та Secure Scuttlebutt

Вузли використовують Wi-Fi-модуль для створення точки доступу короткого радіуса дії для кінцевих користувачів (смартфонів, ноутбуків тощо) і LoRa-модуль для побудови міжвузлової mesh-мережі, яка забезпечує обмін даними, зокрема текстовими повідомленнями.

Розроблюване програмне забезпечення, яке наразі перебуває у стадії активної розробки, передбачає створення низки прикладних сервісів для кінцевих користувачів, які будуть доступні через Wi-Fi-інтерфейс мікроконтролера ESP8266. Крім того, система має включати реалізацію протоколу векторної маршрутизації для сітчастих мереж, натхненного принципами роботи протоколу SRAM. У межах цієї ініціативи також запропоновано концепцію мереж зони катастроф DAN - гетерогенної бездротової mesh-мережі, яка використовує LoRa для реалізації точкових або багатоточкових з’єднань між вузлами.

1.2.4. Комерційні продукти та пристрої

Кевін Гестер та низка інших дослідників працюють над проєктом Meshtastic [40], що передбачає використання недорогих плат розробки, обладнаних GPS, акумулятором і LoRa-чіпом, як захищених mesh комунікаторів.

Ця система орієнтована на використання під час активностей на відкритому повітрі або в інших ситуаціях, коли доступ до Інтернету є обмеженим або повністю відсутнім. Користувачі можуть створювати приватну mesh-мережу для обміну даними про своє місцезнаходження та надсилання текстових повідомлень у групових чатах. Передача повідомлень у мережі здійснюється за допомогою алгоритму затоплення, який дозволяє доставляти пакети даних до найвіддаленіших вузлів. Апаратною основою пристроїв є мікроконтролер ESP32 з підтримкою Wi-Fi/BLE, доповнений LoRa-трансивером і за потреби, GPS-приймачем.

Компанія Pycom пропонує комерційні плати розробки та OEM-продукти, орієнтовані на розробку IoT-рішень з використанням мови програмування Python. Ці пристрої підтримують прошивку Pymesh - інструмент для побудови гнучких LoRa mesh-мереж [41]. Pymesh забезпечує зашифровану ad-hoc комунікацію через LoRa (у режимі raw), реалізує прослуховування перед передачею LBT MAC і підтримує декілька ролей для вузлів, зокрема: лідер, маршрутизатор, кінцевий пристрій та прикордонний маршрутизатор. Прошивка також включає базові функції маршрутизації, забезпечуючи передачу даних через найефективніші доступні з'єднання. Проте обмеження полягає в тому, що Pymesh працює виключно на пристроях Pycom, що обмежує її застосування з апаратним забезпеченням сторонніх виробників.

Компанія NiceRF [42] комерційно пропонує LoRa-трансивери серій SV-Mesh та LoRaStar, доступні як у вигляді вбудованих плат, так і як повністю зібрані пристрої. Ці продукти забезпечують послідовну передачу даних через інтерфейси TTL, RS232 або RS485 за допомогою LoRa-з'єднань. Апаратна реалізація включає малопотужний мікроконтролер у поєднанні з класичним LoRa-трансивером. Для підтримки функціональності mesh-комунікації виробник розробив пропрієтарний протокол LoRa-Pro, який включає двобайтову систему адресації, підтримку трьох ролей у мережі (вузол, маршрутизатор, комбінований вузол-маршрутизатор), а також практично необмежену кількість маршрутів у мережі.

1.2.5. Виявлення множинних значень фактору розширення модуляції

У традиційній архітектурі LoRa та LoRaWAN, шлюзи здатні приймати пакети, що надходять з різними значеннями фактору розширення SF, завдяки паралельному багатоканальному демодулятору, реалізованому в їхньому радіочіпі. Це дозволяє досягати високої пропускної здатності та ефективного використання спектра. Натомість у багатьох експериментальних або недорогих

рішеннях використовуються одночастотні LoRa-пристрої, які можуть працювати лише з одним значенням SF у заданий момент часу. Це істотно обмежує їхню здатність приймати пакети від різних вузлів, які можуть використовувати різні параметри модуляції.

Щоб подолати це обмеження, дослідники розробили підходи до виявлення SF у реальному часі, що дозволяє одночастотним пристроям адаптуватися до характеристик прийнятого сигналу. Такі методи відкривають нові можливості для побудови більш гнучких мереж на основі LoRa, зокрема для побудови мультихопових топологій або підвищення сумісності у гетерогенних середовищах. У цьому розділі розглянемо найцікавіші роботи, присвячені реалізації механізмів мульти-SF виявлення, їхні принципи роботи та результати оцінювання.

Хоча більшість недорогих одночастотних LoRa-трансиверів спроєктовано для роботи лише на одному каналі з фіксованим фактором розширення SF, існують апаратні й програмні підходи, які дозволяють подолати ці обмеження. Завдяки використанню можливостей детекції активності на каналі CAD, деякі пристрої здатні автоматично ідентифікувати SF, на якому передається вхідний пакет, і коректно його обробити. Це значно розширює функціональність таких пристроїв, даючи змогу приймати сигнали з різними параметрами модуляції, що особливо корисно в гетерогенних багатохопових топологіях.

Зокрема, Мартен Вестенберг реалізував підхід до мульти-SF виявлення, що базується на використанні можливостей CAD для одночасного виявлення кількох значень SF на одночастотному шлюзі LoRaWAN, побудованому на базі мікроконтролерів ESP8266/ESP32 [43]. Його рішення дозволяє перетворити звичайні кінцеві пристрої або плати розробки на повноцінні шлюзи LoRaWAN з підтримкою базових функцій мульти-SF прийому. Згодом Яап Браам переніс реалізацію цього проєкту на мову Lua, що дало змогу запускати одноканальний шлюз LoRaWAN на популярній прошивці NodeMCU для ESP8266 [44], зробивши цю технологію ще більш доступною для спільноти розробників.

Окремої уваги заслуговує також комерційний продукт компанії Heltec - двоканальний шлюз на основі ESP32 SoC з двома LoRa-трансиверами, що забезпечує базову підтримку мульти-SF виявлення для невеликих LoRaWAN-розгортань [45]. Такий підхід дозволяє реалізувати функціональність двох незалежних одночастотних приймачів в одному пристрої, що робить його зручним рішенням для бюджетних експериментальних мереж.

Наостанок, варто згадати й про роботу Конг Тан Дуонг та Мен Кюн Кім в якій було запропоновано схему адаптивного вибору SF (ASFS). Цей метод дозволяє одночастотним пристроям динамічно змінювати SF залежно від умов середовища, забезпечуючи одночасну підтримку різних швидкостей передачі в межах однієї мережі. Порівняльний аналіз цієї роботи та її вплив на побудову багатофакторних систем буде представлено у наступних розділах.

1.3. Дослідження існуючих методів оцінки та вибору конфігурації для побудови бездротових сенсорних мереж

Попередні підрозділи були присвячені детальному аналізу бездротових технологій, зокрема LoRa та архітектури LoRaWAN, які набули широкого поширення у сфері побудови енергоефективних IoT-систем. Однак зростаюча кількість доступних технологій зв’язку, конфігурацій пристроїв та варіантів архітектурних рішень зумовлює потребу у формалізованих підходах до їхньої об’єктивної оцінки, порівняння та обрання найбільш доцільного варіанту згідно з вимогами конкретного сценарію застосування.

У цьому підрозділі розглянуто сучасні методологічні підходи до аналізу, оцінювання та вибору конфігурації бездротових IoT-мереж. Окрему увагу приділено інструментам для моделювання альтернатив, аналізу ключових характеристик та визначення відповідності технічних параметрів запитам прикладного рівня. Використання таких методик дозволяє не лише забезпечити відповідність технічним вимогам, але й знайти фінансово оптимальні

конфігурації мережі, що особливо важливо при масштабних або ресурсно обмежених впровадженнях. Розгляд подібних підходів дає змогу сформувати системне уявлення про процес ухвалення рішень під час проєктування ефективних IoT-інфраструктур.

1.3.1. Проблематика вибору конфігурації бездротових сенсорних мереж

Протягом останніх п’ятнадцяти років Інтернет речей пройшов шлях від дослідницької концепції до повноцінної реальності. Сьогодні IoT-технології інтегровані у виробничі та організаційні процеси, а також у побут і повсякденне життя людини, ставши одночасно невід’ємною і майже невидимою частиною сучасної цифрової інфраструктури. Пристрої IoT зустрічаються всюди: від трекерів активів, що відстежують місцезнаходження відправлень і сповіщають про можливі затримки доставки, до розумних лічильників, які вимірюють споживання енергії, сенсорів, що виявляють витоки води або рівень забруднення повітря, та систем дистанційного керування, які автоматизують роботу промислового обладнання. Ці пристрої забезпечують роботу широкому спектру додатків і сервісів, функціонуючи на основі передачі даних і команд у реальному часі. Така інтеграція фізичного та цифрового середовищ не лише підвищує ефективність операційної діяльності організацій, але й сприяє забезпеченню сталого розвитку та збереженню здоров’я населення.

Щодня на ринку з’являються десятки нових IoT-продуктів - як універсальних, так і адаптованих під конкретні прикладні сценарії - у вигляді готових рішень або платформ, що налаштовуються. Відповідно до аналітичних прогнозів, до 2030 року глобальна економічна цінність, яку створює IoT, може сягати від 5,5 до 12,6 трильйона доларів США, включаючи як вартість, створену безпосередньо в бізнес-процесах, так і ту, що отримують споживачі та кінцеві користувачі [46]. Ця тенденція підтверджується швидкими темпами впровадження IoT-пристроїв у таких сферах, як логістика, енергетика,

агропромисловість, охорона здоров’я та міська інфраструктура. Наприклад, згідно з оцінками, постачання трекерів активів зростатимуть більш ніж на 50% щорічно до 2024 року [47], що свідчить про високий попит на сервіси моніторингу в реальному часі та автоматизоване управління мобільними об’єктами.

Технології, необхідні для побудови наскрізних IoT-рішень, сьогодні є широко доступними та стрімко розвиваються. З архітектурної точки зору, ключову роль у такій системі відіграє мережевий рівень, як це визначено в моделі ISO/OSI, який забезпечує взаємозв’язок між підсистемами, що формують повноцінне IoT-рішення. На периферії цієї взаємодії знаходиться фізична IoT-мережа - критичний компонент, що безпосередньо відповідає за з’єднання кінцевих пристроїв з Інтернетом. Саме ця частина системи забезпечує передачу даних між сенсорами, шлюзами та хмарними або локальними сервісами, формуючи інфраструктурну основу цифрового середовища.

Мережеві технології IoT постійно вдосконалюються для того, щоб відповідати різноманітним та дедалі жорсткішим вимогам щодо зв’язку і передачі даних, які висуваються сучасними IoT-додатками.

Серед таких технологій:

1. бездротові протоколи ближнього радіуса дії, як Wi-Fi, BLE;

2. технології середньої та великої дальності, як-от Wi-Fi HaLow та 6LoWPAN;

3. низькопотужні широкосмугові мережі (LPWAN), зокрема LoRaWAN, Sigfox, NB-IoT і LTE-M.

Крім того, активно розробляються архітектури IoT на основі mesh-топологій, як-от Wirepas а також використовуються рішення на основі 5G для підтримки сценаріїв, що потребують високої пропускної здатності та низької затримки. Таке різноманіття технологічних підходів покликане вирішити завдання сумісності з гетерогенними вимогами IoT-додатків.

Однак швидке зростання кількості технологій, їх взаємозалежність та специфічність параметрів налаштування, а також багатокритеріальний характер вибору ускладнюють процес проєктування та конфігурування бездротових IoT-мереж. На практиці IoT є складною технічною системою, функціонування якої значною мірою залежить від параметрів комунікаційного рівня - таких як пропускна здатність, надійність передавання даних, затримки та енергоефективність. У різних прикладних сценаріях, перевага надається високій надійності та мінімальній затримці, тоді як для розумних будівель більш вагомими стають масштабованість і гнучкість мережі.

Автори дослідження [48] визначили ключові властивості, якими повинна володіти IoT-система: еволюційність та інтероперабельність, доступність та стійкість, довіра, безпека і конфіденційність, продуктивність та масштабованість. На етапі проєктування [49 - 50] критично важливим є вибір бездротової технології, яка б відповідала не лише технічним і вартісним вимогам конкретного застосування, а й враховувала стратегічні амбіції власника продукту щодо розширення або еволюції IoT-рішення у майбутньому. У фазі розгортання вирішальне значення має точне налаштування параметрів трафіку та мережі — саме вони визначають рівень якості обслуговування QoS та енергоефективність усього рішення.

Під час експлуатації розгорнутої IoT-системи обсяги трафіку можуть змінюватися: зокрема, розробник може оновити логіку застосунку або додати нові функції, що підвищить навантаження на мережу. Такі зміни істотно впливають на продуктивність системи в цілому та можуть скоротити час автономної роботи пристроїв. Через наявність численних технологій і конфігурацій, що потенційно можуть відповідати певному застосуванню, архітекторам IoT-рішень вкрай необхідно мати можливість порівняльного тестування, що дозволить вибрати найбільш придатну технологію та оптимально налаштувати мережу під потреби конкретного завдання.

Вибір найбільш придатної мережевої технології, її топології та параметрів конфігурації є критичним чинником успішності IoT-рішення. Актуальні дослідження [51] свідчать про те, що майже 75% проєктів у сфері Інтернету речей - незалежно від країни реалізації, чи то США, Велика Британія чи Індія - були визнані невдалими, а близько 30% так і не змогли подолати етап перевірки концепції PoC. Хоча кінцеві користувачі та замовники бачать реальну цінність у впровадженні IoT-рішень, значна частина промислових компаній стикається з труднощами при переході до масштабної реалізації: згідно з оцінками, до 70% проєктів перебувають у так званому стані «пілотного застою», не досягаючи повного виробничого розгортання.

До основних бар'єрів належать нестача висококваліфікованих фахівців, складність орієнтування у великому технологічному різноманітті, а також відсутність ефективних методів обґрунтованого прийняття рішень. Надмірна кількість можливих комбінацій технологій та їх параметрів часто призводить до зволікань, субоптимального вибору або ж невиправданих витрат на експлуатацію та підтримку мережі. У результаті це підвищує загальну вартість володіння TCO та значно підвищує ризик провалу проєкту. Наприклад, невдале рішення щодо вибору мережевої технології або неправильна оцінка бюджету можуть стати критичними помилками, які зведуть нанівець потенційні переваги IoT-впровадження.

1.3.2. Роль симуляцій та методик підтримки прийняття рішень у проєктуванні конфігурацій сенсорних мереж

У межах цього дослідження особлива увага зосереджується на двох ключових характеристиках мережевої інфраструктури IoT - продуктивності та масштабованості [48], які відіграють вирішальну роль у здатності IoT-рішення стабільно працювати відповідно до заданих параметрів та ефективно обробляти зростаючі обсяги даних у разі масштабування. У роботі формалізовано задачу

оптимізації проєктування - з метою вибору та налаштування мережевої технології підключення IoT-пристроїв, яка б відповідала не лише поточним вимогам, а й мала потенціал до адаптації в майбутньому.

Щоб подолати складність, пов'язану з багаторівневою абстракцією цієї задачі, запропоновано чітко розмежувати сферу відповідальності проєктувальників IoT-систем та фахівців з мереж. Для досягнення балансу між точністю оцінки та обчислювальною складністю пропонується методологічний підхід, що поєднує: формалізацію вимог додатка, постановку цілей, моделювання IoT-мережі, імітаційне моделювання з дискретними подіями та методи багатокритеріального прийняття рішень. Основним із майбутніх наукових внесків цієї роботи є розробка першого формального підходу та алгоритмів для автоматичної оптимізації проєктування IoT мережі, адаптованої до конкретного прикладного сценарію.

1.3.3. Аналіз можливих методів оптимізації сенсорних мереж з урахуванням продуктивності та масштабованості

Проблема вибору мережевої технології у найширшому сенсі викликає значний інтерес з моменту стрімкого розгортання бездротових мереж. Особливої актуальності вона набуває в контексті проєктування IoT-рішень, де необхідно визначити найбільш відповідну технологію зв'язку для конкретного прикладного сценарію. В цьому процесі корисним джерелом є численні оглядові дослідження, що містять дані щодо використовуваних модуляцій, ширини каналу, максимального розміру переданих повідомлень, а також засобів автентифікації та шифрування. Такі огляди охоплюють як загальні аспекти IoT-комунікацій [52 - 53], так і окремо розглядають технології класу LPWAN, включаючи LoRaWAN, NB-IoT, Sigfox тощо.

Втім, ці дослідження мають суттєві обмеження. Зокрема, вони часто подають лише узагальнені оцінки ключових показників ефективності KPI, які

відображають продуктивність мережевих технологій, але не враховують специфіку конкретних IoT-додатків. Крім того, ці показники зазвичай обмежуються граничними (найкращими та найгіршими) значеннями й не відображають залежності від таких критичних чинників, як топологія мережі, середовище розгортання, обчислювальні ресурси кінцевих пристроїв тощо.

Як приклад, теоретична пропускна здатність мережевої технології не завжди відповідає реальним умовам. У практичному застосуванні ця здатність може суттєво знижуватися через вплив перешкод, помилок каналу та конкуренції за доступ до радіоканалу між великою кількістю пристроїв, що працюють одночасно.

У низці наукових робіт було проведено дослідження ефективності з метою порівняння двох або більше мережевих технологій для підтримки конкретних IoT-застосунків. Як правило, такі дослідження розглядають окремі сценарії розгортання й оцінюють відповідну продуктивність за допомогою симуляцій або експериментальних випробувань [54 - 55]. У роботі [55] автори досліджують відносні переваги технологій NB-IoT, SigFox та LoRaWAN для потреб інтелектуальних водопровідних систем, використовуючи симулятор ns-3 [56]. Висновком дослідження стало визнання NB-IoT найефективнішою технологією у цьому контексті, однак воно не враховує важливі показники ефективності, такі як затримка передавання, фінансові витрати, радіус дії та енергоспоживання.

У роботі [57] проведено симуляційне порівняння Wi-Fi HaLow, LoRaWAN і NB-IoT у контексті розумного міста. У свою чергу, дослідження [54] порівнює охоплення та пропускну здатність технологій SigFox, LoRaWAN, GPRS і NB-IoT для великомасштабних IoT-розгортань. Незважаючи на те, що всі досліджувані технології продемонстрували здатність забезпечити покриття для зовнішніх умов, результати вказують на перевагу NB-IoT, а частково також SigFox для внутрішніх середовищ. Водночас, як і попередні дослідження, ця робота не враховує такі критичні KPI, як енергоспоживання та затримка.

Загальним недоліком згаданих досліджень є відсутність універсального інструментарію для вибору та конфігурації мережевих технологій. Для подолання цієї прогалини необхідним є впровадження додаткових етапів, зокрема моделювання цільового IoT-застосунку та можливих мережевих альтернатив, використання оцінювальної методики для розрахунку KPI кожної технології та застосування методу порівняння для ранжування альтернатив і визначення оптимального варіанту.

У роботі [58] запропоновано фреймворк для оцінки технологій IoT-мережі, що зосереджує увагу на ефективності енергоспоживання, проте не передбачає механізмів порівняння або прийняття рішень.

У роботі було розроблено [59] дворівневу методику, яка допомагає користувачам IoT визначити відповідну мережеву технологію: на першому етапі за допомогою анкетування відсіюються несумісні технології, а на другому — оцінюються основні компоненти вартості для визначення найбільш економічного варіанту. Незважаючи на прогресивність такого підходу, варто зауважити що у досліджені використовуються фіксовані значення KPI, які не враховують контекст застосування, а порівняння здійснюється виключно на основі фінансових параметрів.

Тестові стенди IoT, які базуються на використанні реальних IoT-пристроїв, є потужним інструментом для оцінювання застосунків у реальних умовах експлуатації. Такі платформи зазвичай надають програмні інтерфейси API, що спрощують процес розробки експериментів, а також обробку зібраних даних. До таких прикладів відкритих дослідницьких стендів можна віднести FIT IoT-LAB [60], SmartSantander [61], COPELABS IoT [62] та FIESTA-IoT [63].

Незважаючи на свою практичну цінність, відкриті IoT стенди мають низку обмежень. Зокрема, їхня інструментальна база може виявитися недостатньою у випадках, коли потрібні точні вимірювання затримок або енергоспоживання пристроїв. Використання стендів передбачає певні обмеження щодо доступної топології мережі та масштабу експерименту. Це може стосуватися, наприклад,

відстані між кінцевими пристроями та шлюзами, максимальної кількості доступних пристроїв, а також типового середовища розгортання - яке здебільшого є внутрішнім і не піддається повному контролю з боку дослідників, що проводять випробування.

Що стосується методів підтримки прийняття рішень, більшість досліджень зосереджені на виборі динамічного інтерфейсу, також відомого як вертикальне рукостискання VHO, з метою оптимізації продуктивності для кінцевих користувачів [64 - 66]. Такі дослідження природно призводять до формулювання задач динамічного багатокритеріального прийняття рішень, де необхідно ретельно формувати функцію корисності. Для цього застосовуються алгоритми на зразок простого адитивного зважування SAW, методу зваженого добутку WPM і методу подібності до ідеального розв’язку TOPSIS [67].

Для подолання дилеми між дослідженням нових можливостей і експлуатацією вже відомих, дослідники вдаються до різноманітних математичних підходів, таких як комбінаторна оптимізація [68, 69], нечітка логіка [70, 71], процеси прийняття рішень на основі Марковських моделей MDP [72, 73], теорія ігор [74, 75] та методи машинного навчання як наприклад фреймворк "багаторукого бандита" [76, 77].

Варто зазначити, що всі ці дослідження передбачають вже розгорнуту і налаштовану гетерогенну бездротову мережу, в якій можливе проведення тестів продуктивності перед остаточним вибором найбільш відповідного мережевого інтерфейсу для кожного кінцевого пристрою. Це суттєво відрізняється від підходу, який розглядається у нашому дослідженні, де вибір технології бездротової мережі здійснюється на етапі проєктування - ще до її фізичного впровадження. Відтак, можливість збору емпіричних даних про продуктивність на цьому етапі відсутня.

У підсумку можемо зазначити що наразі відсутній універсальний метод підтримки прийняття рішень щодо вибору технології бездротової мережі для IoT, який охоплював би усі фази життєвого циклу IoT-рішення - проєктування,

конфігурування та експлуатацію - та враховував би ключові аспекти як самої мережі, так і цільового застосування в контексті ключових показників ефективності KPI.

Висновки до розділу 1

У першому розділі дисертаційної роботи проаналізовано сучасний стан та тенденції розвитку технологій бездротових сенсорних IoT мереж з акцентом на перспективи їх використання у складних середовищах з обмеженими ресурсами. Проведено дослідження архітектур, топологій та методів конфігурації сенсорних мереж із підтримкою самоорганізації.

Досліджено архітектурні особливості технологій, а також принципи функціонування скнсорних мереж із фіксованою та динамічною топологією. Проаналізовано ключові вимоги до таких мереж з боку прикладних сценаріїв розгортання мереж Інтернету речей, включаючи вимоги до масштабованості, енергоефективності, надійності та стійкості до змін середовища.

Проведено порівняльний аналіз існуючих підходів до оцінювання та вибору конфігурацій бездротових мереж з позиції задоволення специфічних вимог, а також моделей прийняття рішень щодо впровадження конфігурацій.

При проведеному аналізі виявлені недоліки існуючих рішень, а саме:

обмеження щодо масштабованості, енергоефективності та здатності до самоадаптації в гетерогенних умовах експлуатації.

Визначено актуальні наукові виклики що пов’язані з необхідністю розвитку методів адаптації мережі до динамічних умов роботи та впровадження багатоперехідної передачі пакетів даних, навідміну від класичних топологій типу «зірка».

Запропоновано та обґрунтовано доцільність використання самоорганізованих підходів як методу підвищення гнучкості, адаптивності та надійності сенсорних мереж. Визначено, що наявна література лише частково

відповідає на ключові питання щодо продуктивності та ефективності таких мереж у реальних умовах, що підтверджує наукову новизну та практичну значущість обраного напряму досліджень.

Спираючись на проведений комплексний аналіз сучасного стану розвитку бездротових сенсорних мереж формується постановка задачі дисертаційного дослідження. Основна мета дослідження полягає у розробці нового методу побудови сенсорної мережі із застосуванням самоорганізації, що дозволить оптимізувати інформаційну взаємодію та підвищити ефективність передавання даних в мережах Інтернету речей. Майбутній метод побудови сенсорних мереж має включати в себе механізми: багатокритеріального вибору конфігурацій мережі, самоорганізації та оптимізації передавання даних у мережі.

У наступному розділі на основі проведеного аналізу буде розроблено математичну модель прийняття рішень щодо вибору оптимальної сенсорної мережі з урахуванням вимог прикладного застосування та потенційних сценаріїв масштабування.

2 РОЗРОБКА МАТЕМАТИЧНОГО МЕТОДУ ВИБОРУ ОПТИМАЛЬНОЇ КОНФІГУРАЦІЇ СЕНСОРНОЇ МЕРЕЖІ

У попередньому розділі було здійснено всебічний огляд існуючих бездротових IoT-технологій, підходів до побудови топологій, а також методів вибору та оцінки конфігурацій мереж. Було виявлено, що в умовах значного розмаїття доступних мережевих рішень, їх параметричної складності, різної масштабованості та залежності від прикладного сценарію, вибір оптимального варіанту потребує не лише досвіду, а й формалізованого методичного підходу.

Перед тим як перейти до практичних етапів, зокрема, до проєктування власного прикладного рішення, розробки протоколу маршрутизації та його порівняльного аналізу з іншими технологіями та методами маршрутизації - доцільно мати інструмент, що дозволяє об'єктивно оцінити мережеві конфігурації ще на етапі проєктування. Такий інструмент має враховувати ключові вимоги до продуктивності, масштабованості, енергоефективності, а також здатність до адаптації під змінні умови середовища або експлуатаційні сценарії.

Цей розділ присвячено розробці методики прийняття рішень щодо вибору оптимальної конфігурації сенсорної IoT-мережі. В її основі - поетапна процедура, яка включає опис вимог прикладного рівня, моделювання IoT-мережі, оцінку продуктивності з використанням засобів імітаційного моделювання, а також застосування багатоатрибутних методів прийняття рішень для обрання найкращого варіанту.

2.1. Визначення проблеми вибору оптимальної технології та конфігурації сенсорної мережі

У загальному вигляді розробники IoT-систем мають справу з нефункціональними вимогами, такими як продуктивність, масштабованість чи

енергоефективність, які повинні бути враховані під час проєктування. У цьому випадку, фокус дослідження зосереджено на параметрах продуктивності та масштабованості фізичної IoT-мережі. Ці параметри відображають здатність системи забезпечувати гарантований рівень продуктивності при поточному навантаженні, а також її потенціал для обробки зростаючих обсягів даних у майбутньому.

Для формального опису задачі оптимального проєктування розглядаються такі компоненти:

1. A - цільовий IoT-додаток з множиною характеристик і комунікаційних вимог R;

2. T - множина доступних технологій бездротового зв'язку;

3. C_i - набір можливих конфігурацій для кожної технології T_i з T;

4. K - набір ключових показників ефективності (KPI), що характеризують роботу IoT-додатку A при використанні технології T_i з конфігурацією C_i;

5. G - цільові значення KPI, які задаються проєктувальниками системи.

Таким чином, задача полягає у знаходженні технології T_d в T асоційованої з мережевою конфігурацією C_d^k (технологія та кількість відповідних конфігурацій) разом, які найкраще задовольняють вимоги до додатка R та досягають заданих цілей G щодо продуктивності, враховуючи KPI K.

Першим етапом запропонованої методики є абстрагування та формалізація вимог до комунікації, що висуваються цільовим застосуванням, а також характеристик мережевих технологій, які розглядаються як потенційні кандидати для впровадження. Після цього необхідно здійснити якісну оцінку відповідності конкретної технології та її конфігурації до визначених вимог і умов застосування. Для цього передбачається проведення систематичного аналізу поведінки застосунку A при функціонуванні на різних типах мережевих технологій.

Ті варіанти, які демонструють невідповідність ключовим критеріям або обмеженням, мають бути виключені на ранніх етапах аналізу. Решта кандидатів підлягає детальному порівнянню, що дозволяє сформувати обґрунтовані висновки щодо остаточного вибору.

Для ефективного дослідження впливу основних параметрів на продуктивність застосування необхідно чітко визначити ключові характеристики як IoT-додатка, так і мережевої технології. Такий підхід дозволяє суттєво зменшити складність моделювання сценаріїв роботи IoT-системи, не втрачаючи при цьому релевантності результатів. Водночас у процесі моделювання слід враховувати потенційну еволюцію застосунку, зокрема зміну навантаження на мережу в майбутньому, а також масштабованість розгортання з урахуванням зростання кількості підключених пристроїв.

Деякі аспекти, які мають другорядне значення з точки зору прийняття стратегічного рішення на етапі проєктування, можуть бути навмисно опущені або спрощені задля зменшення обчислювальної складності моделі

2.1.1 Формування абстракції для сенсорної мережі та визначення ключових параметрів для аналізу мережевої ефективності

Першим етапом у побудові методики прийняття рішень щодо вибору конфігурації бездротової IoT-мережі є моделювання IoT системи. Сенс такої абстракції полягає в кількісному описі навантаження. Це навантаження розглядається як функція кількості кінцевих пристроїв та обсягу трафіку, що генерується кожним з них. У даній роботі розглядаються лише статичні сценарії розгортання. Для оцінки масштабованості та здатності рішення до еволюції необхідно попередньо визначити очікувані мінімальні та максимальні значення ключових параметрів.

Додатково враховуються фактори, що описують умови фізичного середовища, оскільки вони мають суттєвий вплив на якість бездротової передачі.

Комунікаційні вимоги конкретного IoT-застосування визначаються типами кінцевих пристроїв, навантаженням, яке вони створюють, а також характеристиками фізичного середовища їхнього функціонування.

Щодо кінцевих пристроїв, до уваги беруться такі характеристики:

1. мінімальна кількість кінцевих пристроїв, які планується під'єднати до мережі;

2. максимальна кількість пристроїв, які потенційно можуть бути підключені в ході масштабування системи;

3. ємність батареї кінцевих пристроїв, що безпосередньо впливає на тривалість їх автономної роботи.

У частині, що стосується навантаження на мережу, виділяються наступні параметри:

1. напрямок трафіку - тобто чи здійснюється передача даних у висхідному (uplink), низхідному (downlink) напрямку або в обох;

2. розмір повідомлень, які передаються між пристроями;

3. мінімальна частота надсилання повідомлень;

4. максимальна частота повідомлень, яка може бути досягнута в ході експлуатації.

Також необхідно враховувати характеристики фізичного середовища та розгортання:

1. масштаб розгортання, що визначається максимальною очікуваною відстанню між двома кінцевими пристроями;

2. тип середовища, в якому функціонує IoT-застосування (наприклад, приміщення або відкрита місцевість: сільська, передмістя, міська зона), оскільки це впливає на поширення радіосигналу;

3. очікуваний строк експлуатації розгорнутого IoT-рішення, який також повинен бути визначений на етапі проєктування.

Щодо фізичного середовища, розглядаються два основні випадки: внутрішнє середовище та зовнішнє середовище. У другому випадку середовище може бути додатково класифіковане як:

1. сільське
2. передміське
3. міське

Відповідно до підходу, запропонованого в [78], для кожного з цих типів середовищ доцільно асоціювати відповідну модель поширення втрат сигналу, яка дозволяє коректно відобразити радіоумови середовища при моделюванні або симуляції. Відповідні параметри моделей наведено в таблиці 2.1.

Таблиця 2.1 – Відповідність типів середовищ і моделей поширення сигналу

Тип середовища:	**Модель поширення сигналу:**
Внутрішнє середовище	Гібридна модель будівель враховує умови поширення сигналу всередині та поблизу будівель.
Відкрите сільське середовище	Емпірична модель для оцінки втрат у сільських зонах.
Відкрите міське середовище	Модифікована модель для щільної міської забудови
Відкрите передмістя	Модель яка базується на логарифмічній залежності загасання сигналу від відстані

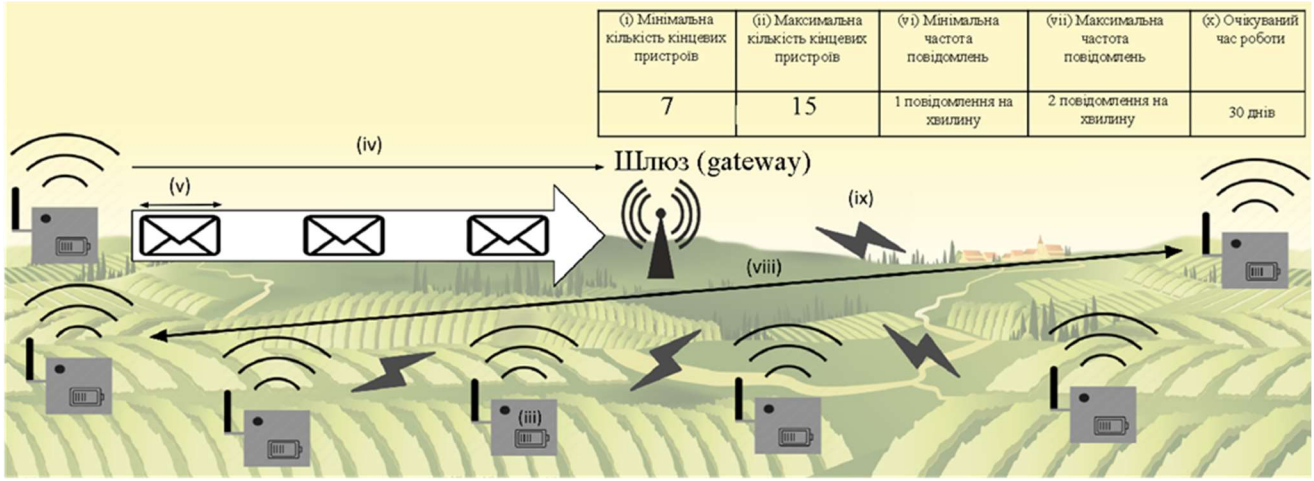

Рис. 2.1 - Абстрактне представлення мережі IoT

На Рис. 2.1 зображено абстрактну модель IoT-додатку, яка дозволяє формалізувати його ключові характеристики з метою подальшої оцінки відповідності мережевих технологій. До основних параметрів моделі належать: мінімальна та максимальна кількість кінцевих пристроїв, які можуть бути підключені; ємність батареї кінцевих пристроїв; напрямок передачі даних (висхідний, низхідний або двосторонній); розмір повідомлень; мінімальна та максимальна частота передачі; максимальна відстань між пристроями в межах розгортання; тип середовища (внутрішнє чи зовнішнє, з уточненням умов поширення сигналу); а також очікуваний термін експлуатації рішення.

Така абстракція забезпечує можливість узагальненого, але при цьому інформативного представлення вимог до зв’язку, характерних для цільового сценарію використання IoT-додатку.

2.1.2 Визначення ключових показників ефективності для оцінки сенсорних мереж

У контексті IoT-систем існує велика кількість метрик, які можуть відображати ефективність роботи комунікаційного рішення. Проте для цілей оцінки та оптимізації конфігурації сенсорної IoT-мережі доцільно виокремити п’ять ключових показників ефективності (KPI), що мають визначальний вплив на продуктивність і доцільність вибору тієї чи іншої мережевої технології.

Нижче наведено основні з них:

1. Коефіцієнт доставки повідомлень - показник, що відображає відношення кількості успішно отриманих повідомлень до загальної кількості надісланих. Він є критичним для забезпечення надійності передачі даних у системі.

2. Споживання енергії - загальний обсяг енергії, витраченої кінцевими пристроями на обмін повідомленнями протягом усього строку експлуатації проєкту. У цьому дослідженні не враховується енергоспоживання, пов’язане із сенсорною або виконавчою активністю, оскільки воно, як правило, є набагато

меншим порівняно з витратами на передачу даних в IoT-системах [79]. У разі необхідності, методику можна адаптувати для врахування цих витрат.

3. Тривалість роботи від батареї - час, протягом якого батарея кінцевого пристрою залишається працездатною до моменту повного розряду. Для цілей оцінки вважається, що загальна тривалість роботи системи обмежується моментом першого розряду будь-якого з пристроїв.

4. Затримка повідомлень - середній час, необхідний для доставки повідомлення від джерела до місця призначення. Цей показник є важливим для додатків, що потребують низької затримки.

5. Вартість - сукупні фінансові витрати, пов’язані з розгортанням та обслуговуванням обраної мережевої технології з урахуванням кількості шлюзів і параметрів конфігурації протягом усього строку реалізації проєкту.

1. Без порогового значення - це такі показники, для яких ціль формулюється як «чим більше (або менше), тим краще». Наприклад, для вартості ціллю зазвичай є її мінімізація;

2. З пороговим значенням - це такі метрики, для яких встановлено конкретний поріг досягнення. У таких випадках немає потреби виходити за межі цього порогу: досягнення мінімально або максимально допустимого значення вважається достатнім.

2.1.3 Моделювання ключових мережевих параметрів для подальшого вибору оптимальної конфігурації сенсорної мережі

Для опису, дослідження та порівняння широкого спектра мережевих технологій необхідно побудувати відповідну модель. Для кожної мережевої технології можна виокремити загальні та специфічні параметри. Загальні параметри, такі як максимальна швидкість передавання даних (або ширина каналу), частотний діапазон, тип топології - характеризують будь-яку мережеву технологію. Специфічні параметри залежать від конкретної реалізації мережі.

Наприклад, у випадку LoRaWAN до специфічних параметрів належать фактор розширення (SF), коефіцієнт корекції помилок (coding rate) та тип передавання (підтверджене або непідтверджене).

Зазначимо, що деякі параметри легко налаштовуються архітекторами або програмними засобами (наприклад, SF у LoRaWAN), тоді як інші - менш доступні для конфігурації або взагалі поза межами контролю архітекторів (наприклад, потужність передавання у LoRaWAN або параметри модуляції MCS у Wi-Fi). У таблиці 2.2 наведено приклад класифікації загальних та специфічних параметрів для мережевої технології LoRaWAN.

Таблиця 2.2 – Модель мережевої технології LoRaWAN

Мережева технологія:	**LoRaWAN**
Перелік загальних параметрів:	•Швидкість передавання даних •Частотний діапазон •Тип топології
Перелік специфічних параметрів:	•Фактор розширення (SF) •Коефіцієнт корекції помилок (Coding Rate) •Контрольна сума (CRC) •Тип передавання (підтверджене / непідтверджене)

Після того як були формалізовані ключові елементи проєктування IoT-рішення - зокрема абстракція прикладного навантаження, перелік ключових показників ефективності (KPI) та модель параметрів бездротових мережевих технологій, постає необхідність у чіткій постановці задачі прийняття рішень. В умовах великої кількості альтернативних технологій, різних сценаріїв використання та обмежених ресурсів, правильна формалізація такої задачі є критично важливою для вибору оптимального варіанту конфігурації мережі.

Формулювання задачі дозволяє поєднати різнорідні характеристики як зі сторони прикладної системи, так і зі сторони технічних можливостей мережевих технологій у єдиний процес прийняття рішень. Такий підхід спрямований на те, щоб підтримати інженера чи архітектора IoT-рішення в аналізі компромісів між

показниками продуктивності, енергоспоживанням, витратами, масштабованістю тощо.

У подальшому на Рис 2.2 представлено узагальнену формальну постановку задачі вибору мережевої технології, її конфігурації та мінімальної кількості необхідних шлюзів, що найкраще відповідають вимогам цільового IoT-застосування:

Вхідні дані:

- **Вимоги до застосунку:** $R = [R_1, \dots, R_k]$, параметри, що описують прикладне навантаження (наприклад, мінімальна та максимальна кількість пристроїв, розмір пакету і частота повідомлень тощо);
- **Ключові показники ефективності (KPI):** $K = [K_1, \dots, K_n]$, обрані метрики (наприклад, рівень доставки повідомлень, тривалість роботи від батареї, затримка, вартість тощо);
- **Цілі значення продуктивності KPI:** $G = [G_1, \dots, G_n]$, $G_i \in R_+$, порогові значення для відповідних KPI (якщо $G_i < 0$ означає, що для відповідного KPI не задано порогового значення);
- **Вага індексу продуктивності KPI:** $W = [W_1, \dots, W_n]$, $W_i \in R_+$, $\sum_{i=1}^{n} W_i = 1$ ваги, що відображають відносну важливість кожного KPI;
- **Набір кандидатів на мережеві технології:** $T = [T_1, \dots, T_m]$, - наприклад, LoRaWAN, NB-IoT, LTE-M, Wi-Fi тощо;
- **Параметри конфігурації мережі:** $C = [C_1, \dots, C_m]$ - параметри налаштування (наприклад, коефіцієнт розширення для LoRaWAN, схема модуляції та кодування для Wi-Fi тощо).

Вихідні дані:

Рішення D_1: Обрати мережеву технологію T_d яка найкраще відповідає цільовим значенням KPI.

Рішення D_2: Обрати конфігурацію мережі для вибраної мережевої технології T_d, яка найкраще відповідає цільовим значенням KPI.

Рішення D_3: Обрати мінімальну кількість шлюзів g_d для вибраної мережевої технології T_d, яка найкраще відповідає цільовим значенням KPI.

Рис. 2.2 – Постановка задачі вибору технології мережі для сенсорної системи

2.2. Загальний огляд запропонованого методу прийняття рішень

Запропонована методика орієнтована на забезпечення простоти, ефективності та зниження ризиків під час вирішення задачі вибору конфігурації бездротової мережі IoT, що була алгоритмічно сформульована на рисунку 2.2.

Для досягнення зазначених цілей метод поділяється на дві основні частини:

1. компоненту моделювання мережевих технологій, яка покликана задовольнити потреби та вимоги мережевих інженерів;

2. компоненту прийняття рішень, орієнтовану на фахівців, що займаються проектуванням IoT-додатків.

Частина, присвячена моделюванню мережевих технологій, передбачає абстрагування та кількісне представлення релевантних параметрів кожної мережевої технології. Цей процес може бути здійснений експертами в галузі на основі технічної документації або результатів експериментальної оцінки. У таблиці 2.3 наведено приклади моделей мережевих технологій, розглянутих у межах даного підходу, зокрема для LoRaWAN, 5G mmWave, Wi-Fi HaLow, Wi-Fi та 6LoWPAN. Ці моделі можуть бути повторно використані спільнотою та застосовані розробниками IoT-рішень для прийняття обґрунтованих рішень, заснованих на даних.

Компонент прийняття рішень, орієнтований на застосування, зображено на рисунку 2.3. Він складається з п’яти послідовних етапів:

1) **Моделювання застосунку**, що включає визначення вимог до IoT-додатку, цільових значень ключових показників ефективності (KPI) та їхніх ваг;

2) **Попередній відбір**, під час якого відсіюються мережеві технології-кандидати, що не відповідають базовим вимогам додатка;

3) **Проєктування сценаріїв**, що охоплює створення гіпотетичних сценаріїв взаємодії між додатком і обраними мережевими технологіями;

4) **Оцінювання**, де змодельовані сценарії запускаються в середовищі моделювання для отримання значень KPI;

5) **Прийняття рішення**, на основі якого здійснюється ранжування сценаріїв і вибір найпридатнішої мережевої технології та її конфігурації за допомогою методу багатокритеріального аналізу.

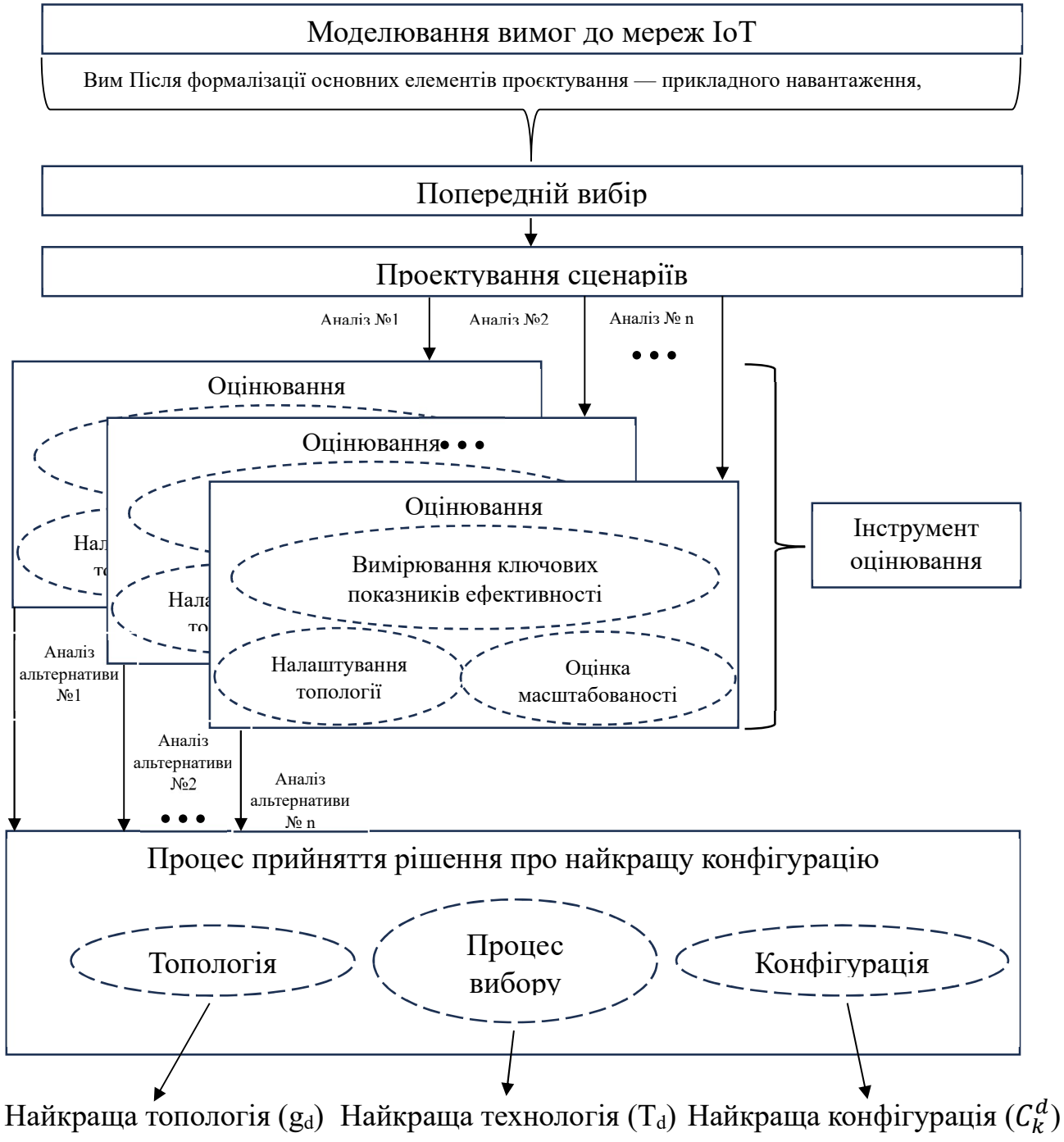

Рис. 2.3 – Загальна структура етапів методики прийняття рішень для вибору конфігурації бездротової IoT-мережі.

2.2.1 Моделювання вимог до сенсорних мереж

На етапі моделювання системи здійснюється:

1. кількісне визначення вимог (R), що пред'являються до IoT-додатку (приклад для кейсу розумного будинку наведено в таблиці 2.4);

2. встановлення цільових показників ефективності (KPI) та визначення цільових значень для кожного з них;

3. присвоєння вагових коефіцієнтів (W) кожному KPI залежно від їхньої важливості для цільового застосування.

Приклад структури KPI, порогових значень і вагових коефіцієнтів для випадку з розумною будівлею наведено в таблиці 2.5. Слід пам'ятати, що значення Gi < 0 означає, що для відповідного показника ефективності не встановлюється порогове обмеження.

Таблиця 2.3 – Перелік специфічних параметрів деяких моделей мережевих технологій

Мережева технологія:	Перелік специфічних параметрів:
LoRaWAN	• Фактор розширення (SF) ∈ [7; 12] • Кодова швидкість (Coding rate) ∈ [1; 4] • Контрольна сума (CRC) ∈ {0, 1} • Тип трафіку ∈ {непідтверджений, підтверджений}
Wi-Fi HaLow	• Індекс модуляції та кодування (MCS) ∈ [0; 9] • Кількість просторових потоків ∈ [1; 3]
Wi-Fi	• Індекс модуляції та кодування (MCS) ∈ [0; 9] • Кількість просторових потоків ∈ [1; 3] • Агрегація пакетів ∈ {0, 1}
6LoWPAN	• Мін. Експонента відстрочки ∈ [0; 7] • Макс. Експонента відстрочки ∈ [3; 8] • Макс. Кількість CSMA відстрочок ∈ [0; 5] • Макс. Кількість повторних передач кадру ∈ [0; 7]

Таблиця 2.4 – Параметри моделі IoT-додатку (приклад для кейсу «розумний будинок»)

Компонент абстракції	Параметр	Значення
Кінцеві пристрої:	Мінімальна кількість пристроїв	50
	Максимальна кількість пристроїв	100
	Ємність батареї (А·год)	2.4
Навантаження:	Напрямок трафіку	Висхідний
	Розмір повідомлення (байт)	100
	Мінімальна частота передачі (пакетів/сек)	1
	Максимальна частота передачі (пакетів/сек)	1
Середовище:	Тип середовища	Внутрішнє
	Дальність розгортання (метрів)	100
	Очікуваний строк служби (днів)	730

Таблиця 2.5 – Цільові показники ефективності (KPI), порогові значення та вагові коефіцієнти для прикладного сценарію

Назва KPI	**Одиниця виміру**	**Цільове значення**	**Вага**
Коефіцієнт доставки повідомлень	Відсотки (%)	90	0,2
Тривалість роботи від батареї	Дні (д)	60	0,2
Споживання енергії	Джоулі (J)	1	0,2
Затримка передачі повідомлення	Мілісекунди (мс)	10	0,2
Вартість мережі	UAH	-1	0,2

Слід зазначити що від’ємне значення цільового показника зазначеного у таблиці 2.5 означає, що мета полягає у мінімізації відповідного параметра

(наприклад, вартості). У випадках, коли для KPI не встановлено конкретного порогового значення, його вважають значенням "без порогу″

2.2.2 Попередній відбір мережевих технологій

Метою етапу попереднього відбору є відсів мережевих технологій, які явно не відповідають вимогам заданого прикладного сценарію. Наприклад, певна мережева технологія може бути виключена з розгляду, якщо її максимальна швидкість передачі даних не здатна забезпечити передбачуване навантаження, яке визначається частотою передачі повідомлень та розміром одного повідомлення. Для реалізації цього процесу у методиці застосовується фільтрація, яка може бути представлена у вигляді дерева прийняття рішень. Значення параметрів прикладного навантаження порівнюються з граничними характеристиками кожної мережевої технології, зокрема максимально допустимим розміром повідомлень та пропускною здатністю. Наприклад, сценарій, в якому загальне навантаження перевищує 1 Мбіт/с, апріорі не може бути реалізованим на базі LoRaWAN. У таких випадках подальша оцінка технології є недоцільною, і вона виключається з наступних етапів аналізу.

2.2.3 Проєктування сценаріїв використання, оцінювання масштабованості та проведення симуляційної оцінки роботи сенсорної мережі

У цьому підрозділі розглядається наступний етап методики - проєктування сценаріїв, який полягає у глибокому дослідженні відібраних на попередньому етапі кандидатів мережевих технологій шляхом варіювання їхніх параметрів конфігурації. Кожен набір параметрів створює окремий сценарій (what-if сценарій), що підлягає моделюванню й оцінці. Таким чином, одна й та сама технологія може бути представлена кількома конфігураціями - наприклад,

LoRaWAN зі значенням фактора розширення SF7 і окремо SF12, які розглядатимуться як окремі сценарії.

Більшість параметрів конфігурації, які враховуються на цьому етапі, мають чітко визначені межі. Це дозволяє створити обмежену, але репрезентативну множину конфігурацій для кожної мережевої технології, придатних для подальшого порівняння за обраними критеріями продуктивності.

Більшість розгортань IoT передбачає поступову еволюцію, зокрема збільшення щільності мережі (тобто кількості кінцевих пристроїв) або зростання навантаження на трафік (частота надсилання повідомлень і розмір повідомлень). У зв'язку з цим необхідно також оцінити майбутню поведінку кожної мережевої технології в умовах таких змін. Методика передбачає створення сценаріїв, що враховують крайні значення цих параметрів.

Для досягнення цієї мети кожен what-if сценарій складається з двох конфігурацій: мінімального розгортання (із найменшою кількістю пристроїв і мінімальною частотою повідомлень) та максимального розгортання (з максимальною кількістю пристроїв і максимальною частотою). Як було зазначено в, саме ці значення визначаються на етапі моделювання застосунку. Такий підхід дозволяє отримати уявлення про масштабованість та еволюційну придатність кожного сценарію, що є критично важливим для вибору найбільш адаптованої конфігурації IoT-мережі.

Більшість розгортань IoT очікувано змінюються з часом, як у плані щільності мережі (тобто кількості кінцевих пристроїв), так і в плані навантаження на трафік (частота та розмір повідомлень). Відповідно, для прийняття обґрунтованого рішення необхідно передбачити та оцінити поведінку мережевої технології в умовах таких змін. Методика, що розглядається, рекомендує на етапі проєктування створювати сценарії, що включають крайні значення - тобто максимально можливу кількість пристроїв і найінтенсивніше навантаження.

З цією метою кожен what-if сценарій складається з двох конфігурацій:

1. мінімального розгортання, яке передбачає найменшу кількість кінцевих пристроїв і мінімальну частоту повідомлень;

2. максимального розгортання, що відповідає найвищій щільності пристроїв і найбільшому передбаченому трафіку.

Як зазначалося раніше ці параметри задаються ще на етапі моделювання застосунку. Такий підхід дозволяє ефективно оцінити масштабованість та еволюційну стійкість кожної потенційної конфігурації мережі, що є важливим чинником у процесі прийняття остаточного рішення.

2.2.4 Оцінювання сценаріїв розгортання та вплив топології на продуктивність сенсорної мережі

Етап оцінювання полягає в інсталяції та реалізації варіантів сценаріїв типу what-if, сформованих на попередньому етапі проєктування сценаріїв, з метою обчислення відповідних значень ключових показників ефективності (KPI) як для мінімального, так і для максимального навантаження. Для реалізації оцінювання можуть застосовуватись як експериментальні дослідження, так і інструменти симуляційного моделювання. У разі використання експериментального підходу необхідно підготувати та активувати кінцеві пристрої, а також засоби моніторингу для збору відповідних метрик. Після цього здійснюється аналіз зібраних даних і розрахунок показників KPI.

Такий підхід може бути доцільним у випадку невеликих проєктів з обмеженою кількістю технологій та сценаріїв, які можна реалізувати в лабораторних умовах у прийнятні строки. Проте, зі збільшенням кількості сценаріїв або кінцевих пристроїв, експериментальне оцінювання стає складним або навіть неможливим. Крім того, практичне тестування широкого спектра технологій вимагає наявності висококваліфікованих фахівців у всіх відповідних мережевих галузях. У цьому контексті симуляційне моделювання розглядається як більш гнучкий і масштабований підхід для отримання прийнятних оцінок KPI.

Попри те, що симуляційні результати можуть мати певні відхилення від реальних значень, вони забезпечують необхідний рівень масштабованості та налаштовуваності, що є критично важливим для вивчення різних конфігурацій мережевих технологій.

У контексті заданої мережевої технології та її конфігурації, кількість розгорнутих шлюзів, позначена як **g**, у подальшому розглядається як **топологія**. Цей параметр має суттєвий вплив на продуктивність IoT-додатку. Збільшення значення **g** може мати три ключові наслідки для функціонування мережі та показників якості комунікацій:

1. **Зменшення навантаження на кожен шлюз.** Припускається, що кожен шлюз використовує окремий канал зв'язку, тож збільшення кількості шлюзів веде до пропорційного зменшення навантаження на кожен з них. Це припущення є реалістичним для багатьох сучасних технологій, які підтримують множинні ортогональні канали (наприклад, 64 канали у спектрі 868 МГц для LoRaWAN або 24 канали у діапазоні 5 ГГц для Wi-Fi).

2. **Зменшення максимальної відстані між кінцевим пристроєм і його відповідним шлюзом.** У моделі додатка вважається, що максимальна відстань *d* між кінцевим пристроєм та його призначеним шлюзом визначається за формулою:

$$d = \frac{D}{(2 \times g)} \tag{2.1}$$

де *D* - це область розгортання, тобто максимальна відстань між двома кінцевими пристроями . Ця проста залежність відображає загальну закономірність: чим більше шлюзів, тим ближче знаходяться кінцеві пристрої до своїх шлюзів.

3. **Збільшення вартості рішення.** Зі зростанням кількості шлюзів зростають і фінансові витрати, не лише на їх закупівлю, але й на розгортання, налаштування та подальше обслуговування.

Таким чином, для кожного сценарію типу «що, якщо» необхідно визначити оптимальну топологію, тобто ідеальну кількість шлюзів. Запропонований підхід передбачає поетапну оцінку сценарію, починаючи з мінімального значення кількості шлюзів g (зазвичай - 1), з подальшим поетапним збільшенням цього параметра на одиницю. Ітераційний процес триває доти, доки:

1. досягаються задані порогові цілі для всіх KPI з пороговими значеннями (зокрема, доставка повідомлень, час роботи батареї, затримка передачі);

2. покращення цих KPI стає меншим за заданий мінімальний приріст ε.

Для забезпечення надійності розрахунків граничне значення g збільшується ще на одиницю в якості запасу. Загальна кількість досліджених топологій для кожного сценарію визначається як максимальне значення g, яке було протестовано у ході цього процесу.

У межах існуючих методики для оцінки показника ефективності за вартісним критерієм використовується така формула, яка враховує як витрати на розгортання (модулі підключення кінцевих пристроїв та шлюзи), так і витрати на обслуговування (заміна батарей):

$$Cost = (p_{gw} \times n_{gw} + p_{ed} \times n_{ed}) + \left(\frac{l}{b} \times p_{br} \times n_{ed}\right) \quad (2.2)$$

де:

p_{gw} - вартість одного шлюзу;

n_{gw} - кількість шлюзів;

p_{ed} - вартість одного кінцевого пристрою;

n_{ed} - кількість кінцевих пристроїв;

l - очікуваний термін експлуатації рішення (у днях);

b - час роботи одного пристрою від батареї (у днях);

p_{br} - вартість заміни батареї.

Слід зазначити що ліва частина рівняння $(p_{gw} \times n_{gw} + p_{ed} \times n_{ed})$ описує сумарну вартість розгортання, а права частина $(\frac{l}{b} \times p_{br} \times n_{ed})$ описує сумарну вартість експлуатаційних витрат.

Зокрема, частка $\frac{l}{b}$ відображає кількість разів, яку знадобиться замінити батареї кінцевих пристроїв протягом усього життєвого циклу системи. Варто зазначити, що саме значення b (час автономної роботи батареї) визначається на основі результатів симуляції, на відміну від інших параметрів, які задаються безпосередньо.

Оцінювання альтеративних конфігурацій обраних сенсорних мереж

У рамках цього дослідження альтернативою вважається сценарій типу «якщо що», поєднаний з певною топологією (тобто фіксованим значенням g). Цей процес детальніше представлений на рисунку 2.4.

Опис вхідних параметрів для алгоритму зображеного на рисунку 2.4:

$R = [R_1, \dots, R_k]$ - вимоги додатка (наприклад, мінімальна та максимальна кількість пристроїв, розмір та частота повідомлень тощо);

$T = [T_1, \dots, T_m]$ - попередньо відібрані мережеві технології IoT;

$C = [C_1, \dots, C_n]$ - конфігурації мереж для кожної технології;

$G = [G_1, \dots, G_n]$; $G_i \in \mathbb{R}$ - цільові значення KPI (якщо $G_i < 0$, це означає, що для відповідного показника немає порогового значення);

$\epsilon \in \mathbb{R}$ - мінімальне поліпшення значення KPI, яке вважається суттєвим (використовується як критерій зупинки ітерацій).

Опис змінних для алгоритма зображеного на рисунку 2.4:

$q \in \mathbb{N}$ - кількість оцінених альтернативних конфігурацій;

$P = (p_{ij}) \in \mathbb{R}^{q \times 2n}$- матриця значень KPI для альтернатив (для кожної альтернативи зберігаються значення усіх KPI для мінімального та максимального сценаріїв).

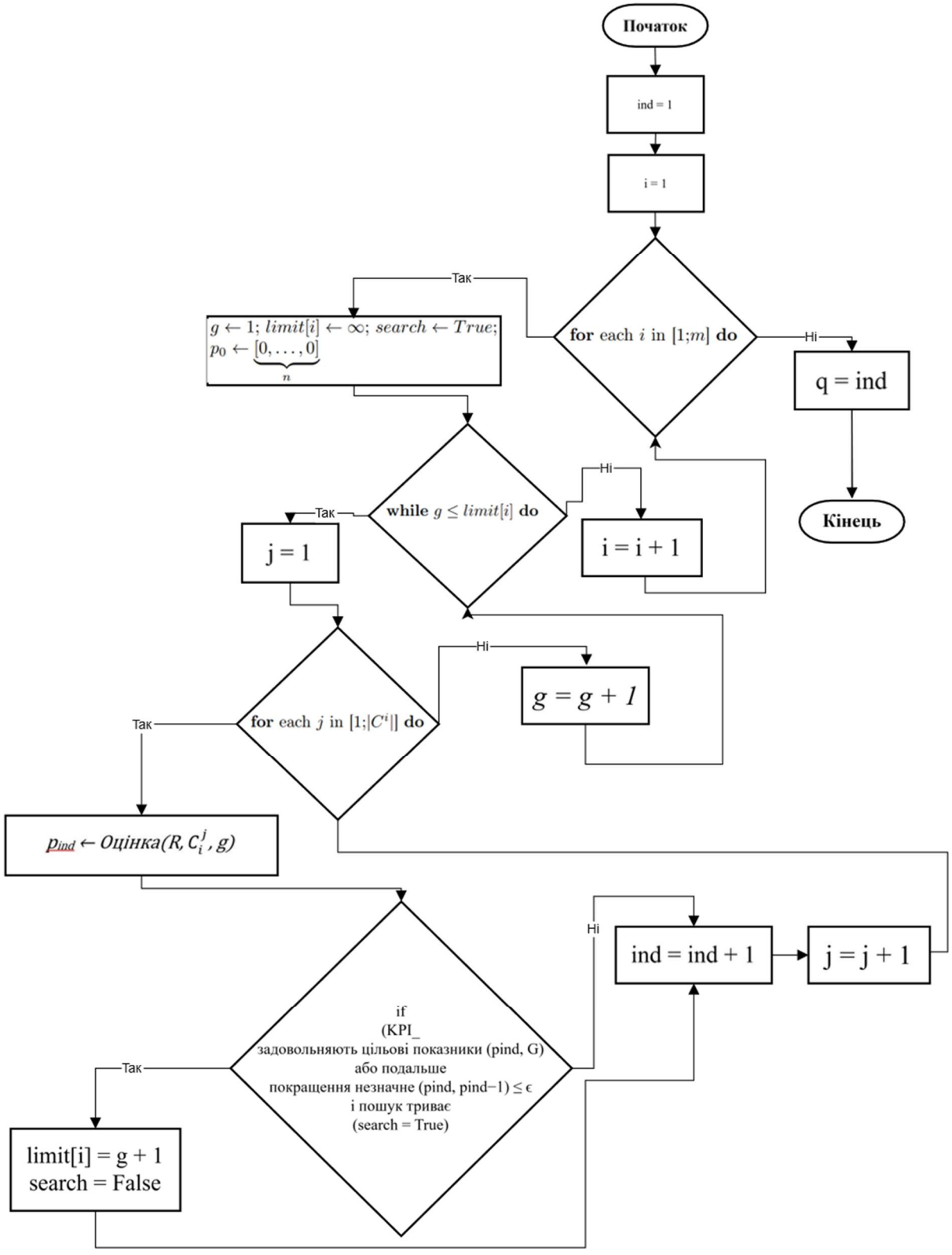

Рис. 2.4 – Процес оцінювання альтернативних конфігурацій IoT-мережі

Логіку роботи процесу оцінювання альтернативних конфігурацій IoT-мережі описати наступними пунктами:

1. Початкова ініціалізація: Індекс *ind* приймає значення 1 (що відображає номер поточної оцінюваної альтернативи).

2. Далі запускається цикл по всім мережевим технологіям *i* від 1 до m і для кожної оцінюваної технології T_i встановлюються наступні змінні:

$g = 1$ - початкова кількість шлюзів;

$limit[i] = \infty$ - верхня межа для перебору кількості шлюзів;

$search = True$ - прапорець що зберігає булеве значення True доки йде пошук оптимальної конфігурації;

p_0 - вектор нульових KPI значень (для першого порівняння).

3. Поки кількість шлюзів g не перевищує $limit[i]$, цикл буде запускатися по всім конфігураціям C_i^j для технології T_i.

4. Для кожної конфігурації C_i^j буде виконуватися цикл у якому буде виконуватися оцінювання конфігурації з врахуванням наступних параметрів: (R - вимог до додатка, C_i^j - вибраного варіанту конфігурації, g - початкової кількості шлюзів). Метою для цієї ітерації є отримання значення KPI що буде записане в матрицю $P[ind] \leftarrow p_ind$.

4.1 Якщо усі KPI задовольняють цільові значення G або покращення порівняно з попереднім кроком ≤ ε (незначне), і булеве значення змінної Search = True, то встановлюється нове значення $limit[i] = g + 1$ (збільшуємо верхню межу) і булеве значення змінної Search = False то пошук для окремої конфігурації C_i^j можна вважати завершеним.

4.2 Якщо усі KPI не задовольняють цільові значення, то індекс альтернатив інкрементується $ind \leftarrow ind + 1$

5. Лічильник кількості шлюзів інкрементується $g \leftarrow g + 1$ і процес переходить тестування конфігурацій з більшою кількістю шлюзів

6. Коли всі конфігурації $C_{1...n}$ оброблено, то зініціюється перехід до оцінки конфігурації наступної технології.

7. Результатом роботи є $q \leftarrow ind$ - кількість унікальних альтернатив, сформованих у процесі перебору.

Результатом роботи є матриця значень KPI (P), що містить оцінки всіх розглянутих альтернативних конфігурацій IoT-мережі з різною кількістю шлюзів. Далі ці результати використовуються для ухвалення фінального рішення щодо вибору оптимальної конфігурації (у наступних алгоритмах).

Запропонований процес оцінки забезпечує систематичний підхід до вибору оптимальної конфігурації бездротової IoT-мережі, орієнтуючись на багатокритеріальне оцінювання ефективності. Його ключова перевага полягає в можливості автоматизованого формування та перевірки великої кількості what-if сценаріїв, які охоплюють як різні мережеві технології, так і варіативність їхніх конфігурацій та топологій (кількості шлюзів).

Цей метод дозволяє адаптивно обмежувати пошук, завдяки застосуванню порогового критерію покращення (ε) та цільових значень KPI, що істотно знижує обчислювальні витрати без втрати якості прийняття рішень. У такий спосіб досягається ефективний компроміс між точністю оцінювання й складністю аналізу. Це робить алгоритм особливо корисним для проєктування IoT-систем, де важливо знайти не лише функціональне, але й енергетично та економічно доцільне рішення.

Відбір альтеративних конфігурацій сенсорних мереж

Метою етапу прийняття рішення є порівняння та ранжування альтернатив, що були оцінені на попередньому етапі. Значення ключових показників ефективності (KPI), отримані в процесі оцінки, зберігаються у вигляді матриці P. Подальша обробка цих значень залежить від класу, до якого належить кожен з KPI. Відповідно до цього, значення або залишаються незмінними, або

обмежуються певним порогом згідно з правилами, наведеними в алгоритмі зображеному на рисунку 2.5.

Опис вхідних параметрів для алгоритму зображеного на рисунку 2.5:

$q \in \mathbb{N}$ - кількість оцінених альтернатив;

$G = [G_1, \dots, G_n]$; $G_i \in \mathbb{R}$ - цільові значення KPI (якщо $G_i < 0$, це означає, що для відповідного показника *i* немає порогового значення);

$P = (p_{ij}) \in \mathbb{R}^{q \times 2n}$- матриця значень KPI для альтернатив (для кожної альтернативи де зберігаються значення усіх KPI для мінімального та максимального сценаріїв).

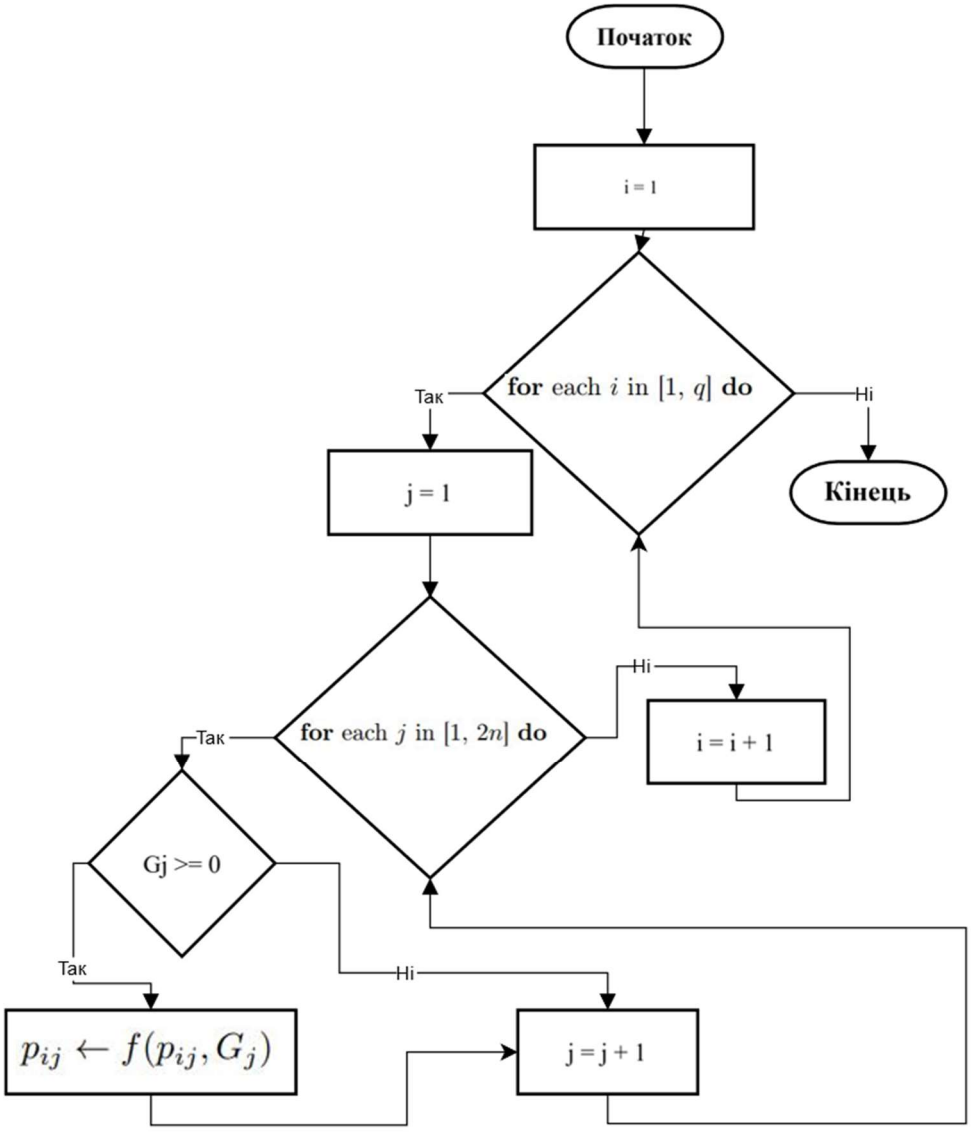

Рис. 2.5 – Застосування порогових значень KPI для відбору допустимих альтернативних конфігурацій

Логіку роботи алгоритму можна описати наступними пунктами:

1. Для кожної з оцінюваних альтернативних конфігурацій застосовується індекс *i* який набуває значень від *1* до *q*

2. Вкладений цикл фільтрації KPI $j \in [1, 2n]$ для кожної множини альтернативної конфігурації *n* (значення 2n застосовується, тому що для кожного KPI з оригінальної множини *n*, можуть бути два значення, наприклад, для мінімального і максимального навантаження) виконує дію:

– Якщо KPI має тип «чим більше - тим краще» (наприклад, коефіцієнт доставки повідомлень), то значення KPI, менші або рівні цільовому порогу G_j встановлюються в 0 (що означає неприйнятність цієї альтернативи) та інші значення залишаються без змін.

$$p_{ij} = \begin{cases} 0, & \text{якщо } p_{ij} \leq G_j \\ p_{ij}, & \text{якщо } p_{ij} > G_j \end{cases} \tag{2.3}$$

– Якщо KPI має тип «чим менше - тим краще» (наприклад, затримка передачі повідомлень), то значення KPI, менші за цільовий поріг G_j приймають значення порогу G_j, та інші значення залишаються без змін.

$$p_{ij} = \begin{cases} G_j, & \text{якщо } p_{ij} < G_j \\ p_{ij}, & \text{якщо } p_{ij} \geq G_j \end{cases} \tag{2.4}$$

3. В результаті цієї операції отримується очищена матриця (P) KPI значень, яка містить лише допустимі альтернативні конфігурації та готова до подальшого процесу нормалізації та фінального багатокритеріального оцінювання.

На виході маємо оновлену **матрицю KPI (P)**, в якій усі показники з порогами приведені до значень, які відповідають політиці прийняття рішення: KPI, що не задовольняє порогу, замінюється нульовим або обмеженим значенням. Це дозволяє уніфікувати всі метрики перед нормалізацією та багатокритеріальним аналізом.

Для KPI з пороговими значеннями (другий клас), у випадку мінімального порогу (наприклад, для коефіцієнта доставки повідомлень або тривалості роботи від акумулятора), використовується наступна функція**:**

$$f(x,\alpha) = \begin{cases} x, & \text{якщо } x > \alpha \\ 0, & \text{в іншому випадку} \end{cases} \quad (2.5)$$

Ця функція означає, що якщо показник перевищує визначений поріг α, то його значення залишається незмінним. Якщо ж показник нижчий за поріг, то він вважається неприйнятним, і для подальшого аналізу встановлюється нульове значення. Це дозволяє виключити з розгляду конфігурації, що не відповідають мінімально допустимому рівню ефективності.

У випадку KPI з максимальним порогом (наприклад, затримка передачі повідомлення), застосовується функція:

$$f(x,\alpha) = \begin{cases} x, & \text{якщо } x < \alpha \\ 0, & \text{в іншому випадку} \end{cases} \quad (2.6)$$

У цьому випадку, якщо значення KPI нижче за визначений максимум - воно приймається без змін. Якщо ж воно перевищує поріг, то вважається таким, що не задовольняє вимогам, і зводиться до порогового значення.

Після обробки порогових значень усі KPI нормалізуються відповідно до встановлених правил, що описуються далі в алгоритмі. Нормалізація необхідна для забезпечення можливості порівняння показників, що мають різні одиниці виміру та діапазони.

Після цього значення ключових показників ефективності (KPI) підлягають нормалізації, як це представлено в алгоритмі зображеному на рисунку 2.6. Нормалізація є важливим кроком для уніфікації шкал вимірювання різних KPI, що дозволяє об'єктивно їх порівнювати, незалежно від одиниць виміру чи діапазонів значень.

Нормалізація відібраних конфігурацій сенсорних мереж

У рамках цієї методики нормалізація виконується з урахуванням того, чи є KPI прямим (тобто «чим більше - тим краще») або зворотним («чим менше - тим краще»). Це забезпечує справедливу оцінку усіх альтернатив і дозволяє провести їх подальше ранжування в багатокритеріальному аналізі. Алгоритм 4 формалізує

цей процес і слугує базою для побудови фінального рішення щодо вибору оптимальної конфігурації мережі.

Вхідні значення для алгоритму

$P = (p_{ij}) \in \mathbb{R}^{q \times 2n}$ матриця KPI де q - кількість альтернатив, 2n - кількість KPI (наприклад, мінімальні та максимальні значення кожного з n показників).

Змінні значення:

$N = (n_{ij}) \in \mathbb{R}^{q \times 2n}$ матриця нормалізованих KPI де кожне n_{ij} - нормалізоване значення KPI для альтернативи i за показником j.

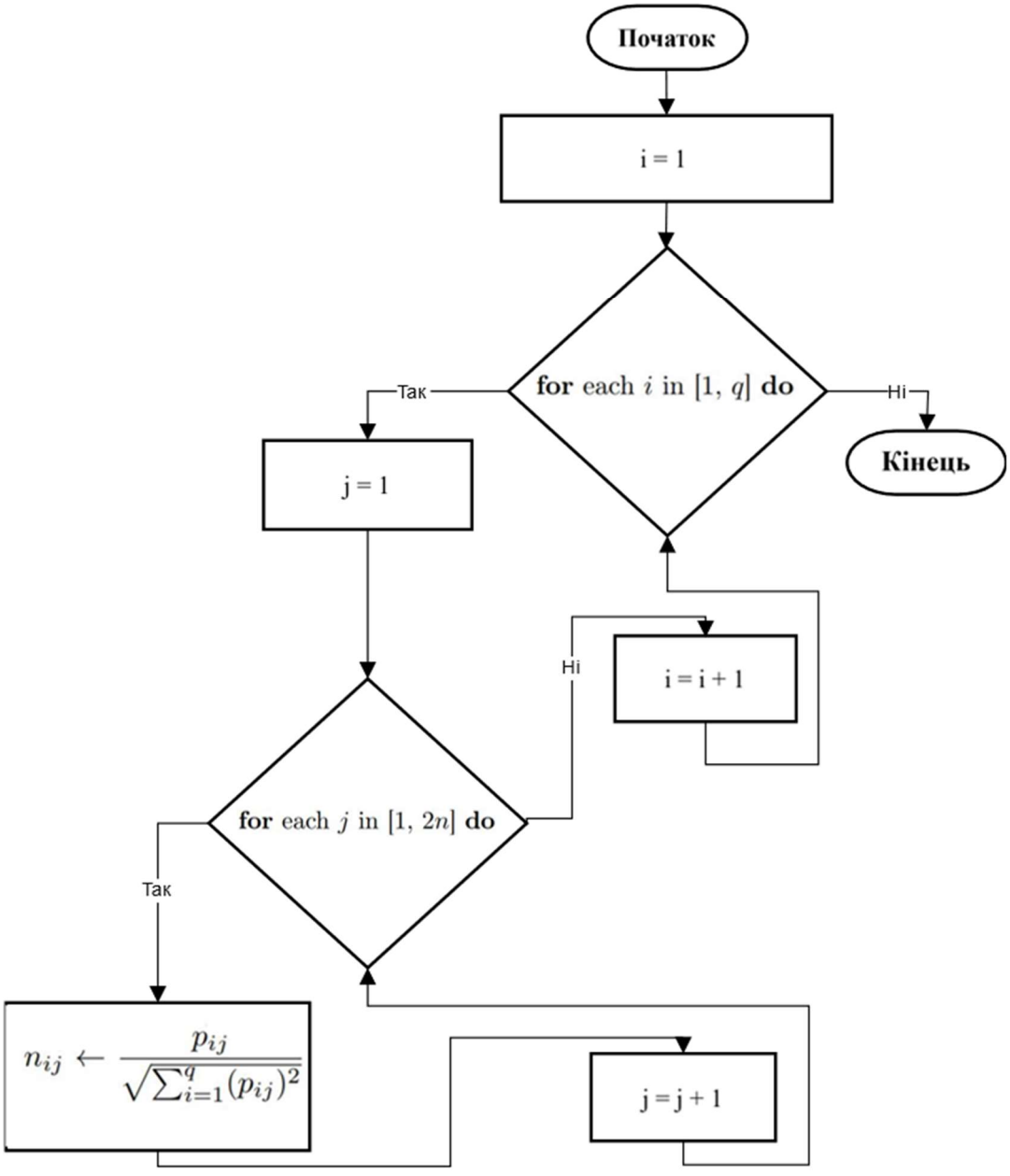

Рис. 2.6 – Нормалізація матриці KPI

Логіку роботи алгоритму можна описати наступними пунктами:

1. Для кожної з оцінюваних конфігурацій застосовується індекс *i* який набуває значень від *1* до q

2. Вкладений цикл з індексом *j* який набуває значень від *1* до q обчислює:

$$\sqrt{\sum_{i=1}^{q}(p_{ij})^2} \tag{2.7}$$

норму (довжину вектора) для кожного стовпця KPI, та наступним кроком для кожної альтернативи $i \in [1; q]$ виконується нормалізація:

$$n_{ij} = \frac{p_{ij}}{\sqrt{\sum_{i=1}^{q}\left(p_{ij}\right)^2}} \tag{2.8}$$

3. Усі значення n_{ij} записуються до нової матриці N.

Алгоритм застосовує нормалізацію за евклідовою нормою (нормалізація векторів ознак), тобто це означає, що кожне значення KPI p_{ij} нормалізується шляхом ділення на корінь квадратний суми квадратів всіх значень p_j для цього стовпця (тобто для всіх альтернатив по одному KPI).

Це дозволяє справедливо порівнювати альтернативи з різними одиницями виміру та впливом на результат.

Алгоритм зображений на рисунку 2.6 виконує нормалізацію матриці KPI P, приводячи всі значення до безрозмірної форми в межах одного діапазону. Це є обов'язковою умовою для застосування методів багатокритеріального аналізу на наступному етапі прийняття рішення.

Зважування відібраних та нормалізованих конфігурацій IoT мереж

Для ранжування отриманих результатів використовується система оцінювання яка базується на одному з методів багатокритеріального прийняття

рішень (MADM) [67]. У запропонованій методології ранжування враховує два ключові аспекти:

1. **Вагові коефіцієнти KPI**, які відображають пріоритетність кожного з критеріїв ефективності.

Кожному KPI призначається вага згідно з вектором уподобань:

$$W = [W_1, W_2, \dots, W_n], \qquad \text{де } W_j \in \mathbb{R}, \quad \sum_{j=1}^{n} W_j = 1 \qquad (2.9)$$

Ці ваги визначають відносну важливість кожного показника у загальній оцінці.

2. **Коефіцієнт масштабованості (β)**, який задається архітекторами IoT-системи на основі їхньої обізнаності з бізнес-контекстом.

Параметр β може приймати значення з множини {0, 1, 2}, що визначає пріоритетність між оцінками, проведеними на мінімальному або максимальному розгортанні систем

- **β=0** - найбільша важливість надається початковому (мінімальному) сценарію розгортання;
- **β=1** - обидва сценарії (мінімальний та максимальний) вважаються однаково важливими;
- **β=2** - фокус зосереджується на поведінці системи при масштабованому навантаженні.

Якщо масштабованість рішення (тобто здатність підтримувати більшу кількість пристроїв або вищу інтенсивність трафіку) є критичною, архітектору рекомендується встановити β = 2.

Вхідні значення для алгоритму:

$W = [W_1, \dots, W_n]$ де $W_i \in R_+, \sum_{i=1}^{n} W_i = 1$ - вектор вагових коефіцієнтів KPI

$N = (n_{ij}) \in \mathbb{R}^{q \times 2n}$ - матриця нормалізованих KPI

$\beta \in \{0, 1, 2\}$ - коефіцієнт масштабованості

Змінні:

$V = (v_{ij}) \in \mathbb{R}^{q \times 2n}$ - зважена нормалізована матриця KPI

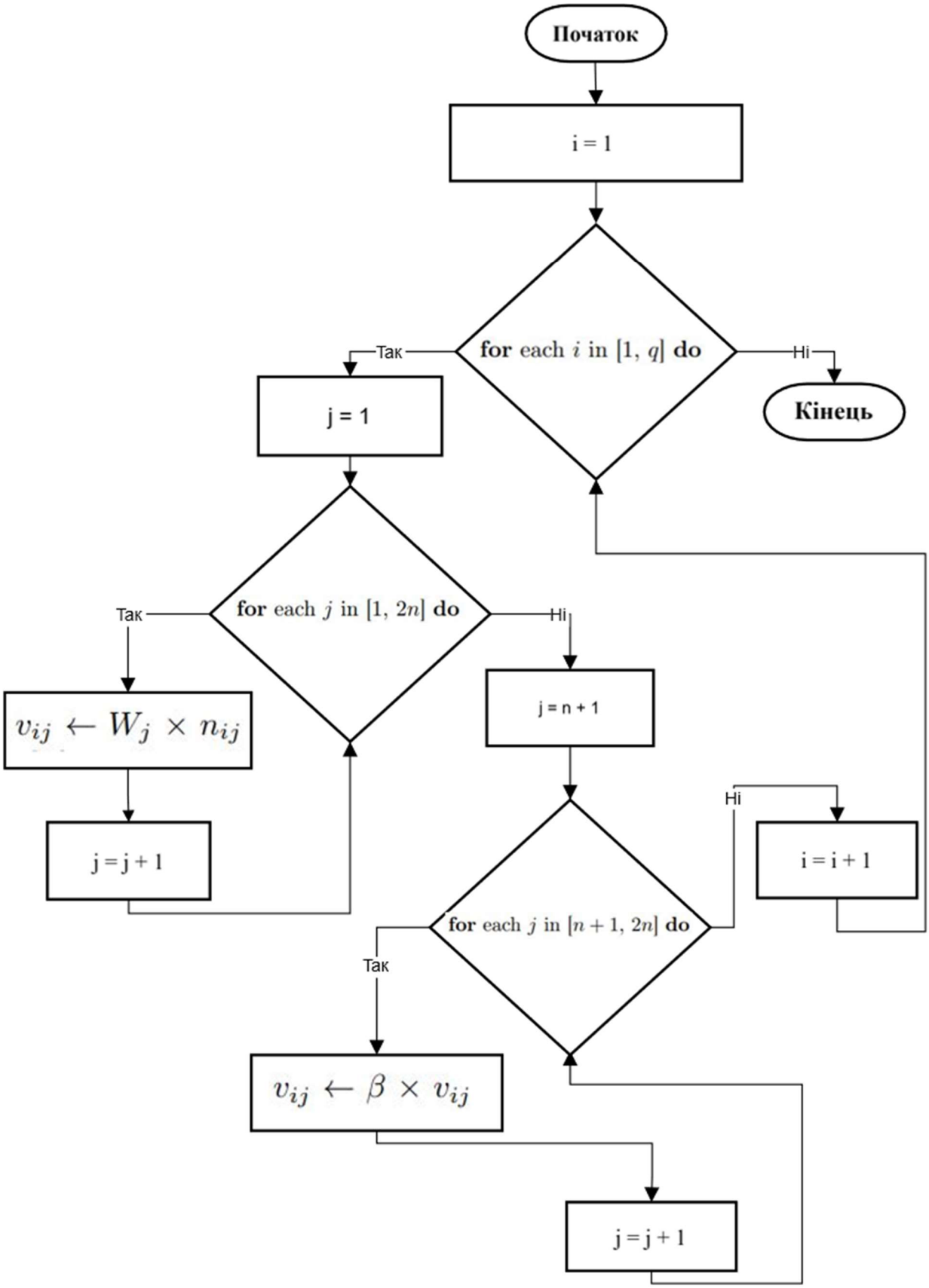

Рис. 2.7 – Зважування нормалізованих значень KPI з урахуванням масштабованості

Логіку роботи алгоритму можна описати наступними пунктами:

1. У зовнішньому циклі алгоритм послідовно перебирає всі оцінені альтернативи конфігурації IoT-мережі, які представлені у нормалізованій матриці KPI $N = (n_{ij}) \in$. Кожна альтернатива характеризується вектором із $2n$ нормалізованих показників, що відповідають мінімальному та максимальному сценаріям експлуатації системи.

2. У другому циклі для кожного показника $j \in \{1, 2n\}$ виконується зважування нормалізованого значення n_{ij} на відповідну вагу W_j. З огляду на те, що ваговий вектор заданий лише для n KPI, вважається, що:

$$W_{j+n} = W_j \text{ де } j \in \{1, n\} \quad (2.10)$$

3. У третьому циклі додатково коригується друга половину стовпців (тобто ті, що відповідають сценарію максимальної конфігурації мережі). Для цих показників значення v_{ij} домножуються на заданий фактор масштабованості $\beta \in \{0, 1,2\}$. Це дозволяє змістити акценти оцінки в бік: мінімальної конфігурації β=0, збалансованого підходу β=1, максимальної конфігурації або масштабованості β=2.

Алгоритм зображений на рисунку 2.7 виконує зважування нормалізованої матриці KPI відповідно до визначених пріоритетів ключових показників ефективності. Це дозволяє інтегрувати експертні уявлення про значущість кожного критерію в оцінку альтернатив. Оскільки кожна альтернатива має дві проєкції KPI (для мінімальної та максимальної конфігурації) додатково застосовується коефіцієнт масштабованості β, що дозволяє адаптувати результати до контексту цільового розгортання системи.

У результаті формується зважена матриця $V = (v_{ij})$, значення якої будуть використані в подальшому етапі

Алгоритм обчислює позитивний ідеальний розв’язок (найкращий можливий варіант) та негативний ідеальний розв’язок (найгірший варіант) на основі діапазону отриманих значень KPI. Далі для кожної альтернативи обчислюється

інтегральна оцінка, що базується на евклідовій відстані між альтернативою та обома ідеальними розв’язками.

Визначення максимального негативного та позитивного розв’язку для кожної із конфігурацій сенсорної мережі

Порядок визначення позитивного й негативного ідеальних розв’язків, а також формули для обчислення рейтингових оцінок наведено в Алгоритмі 6.

Вхідні значення для алгоритму:

$V = (v_{ij}) \in \mathbb{R}^{q \times 2n}$ зважена нормалізована матриця KPI

Змінні:

$V^+ = [v_1^+, \dots, v_{2n}^+], v_1^+ \in \mathbb{R}$ - позитивне ідеальне рішення (найкращі значення для кожного KPI)

$V^- = [v_1^-, \dots, v_{2n}^-], v_1^- \in \mathbb{R}$ - негативне ідеальне рішення (найгірші значення для кожного KPI)

$S^+ = [s_1^+, \dots, s_{2n}^+], s_1^+ \in \mathbb{R}$ - евклідові відстані до негативного ідеалу

$S^- = [s_1^-, \dots, s_{2n}^-], s_1^- \in \mathbb{R}$ - евклідові відстані кожної альтернативи до позитивного ідеалу.

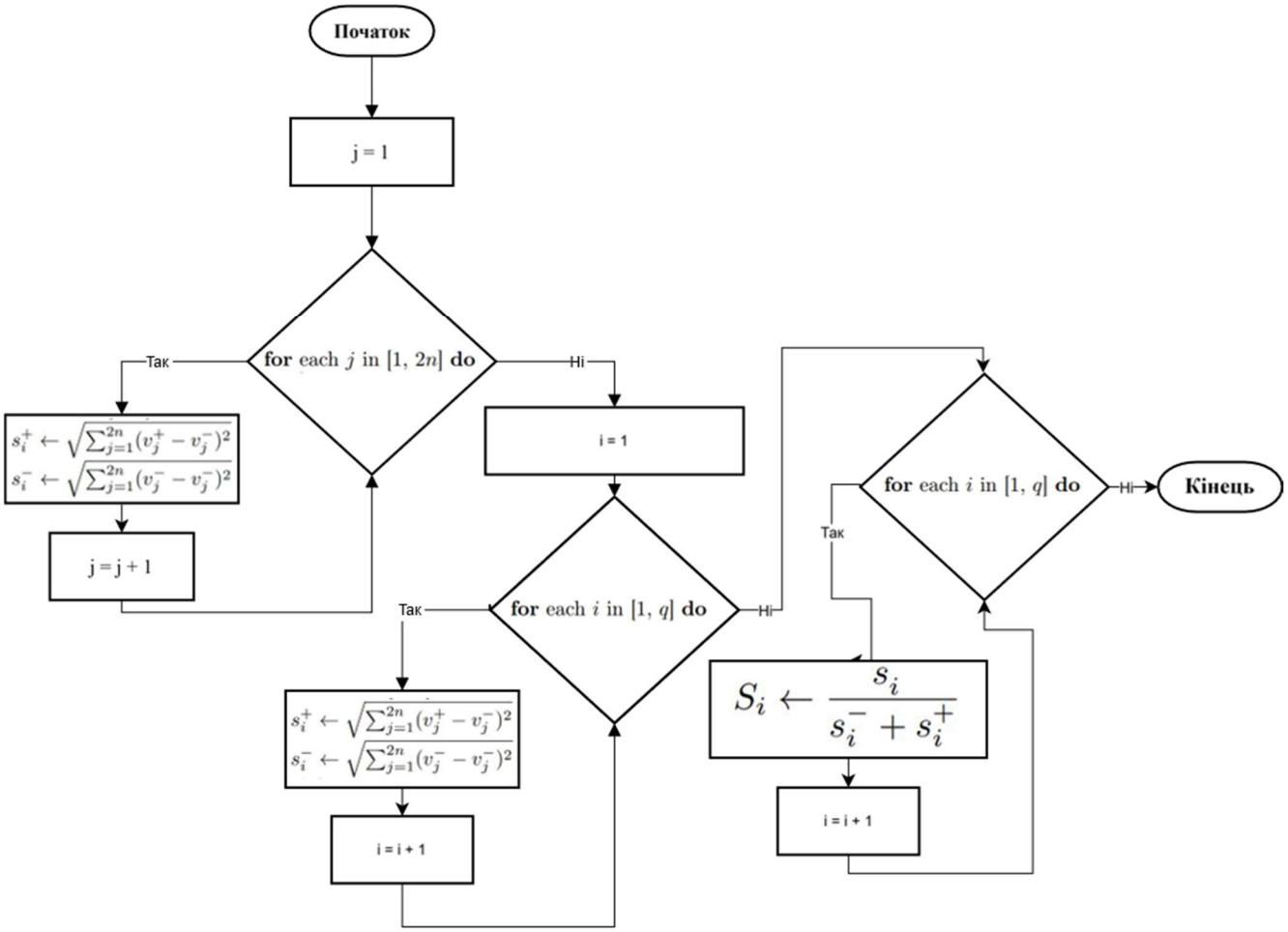

Рис. 2.8 – Ранжування фінальних кофігурацій для IoT мереж

Логіку роботи алгоритму можна описати наступними пунктами:

1. У першому циклі для кожного показника KPI $j \in [1,2n]$ обчислюються:
   - максимальне значення серед усіх альтернатив

$$v_j^+ = max_{i=1}^{q}(v_{ij}) \tag{2.11}$$

   - мінімальне значення серед усіх альтернатив

$$v_j^- = min_{i=1}^{q}(v_{ij}) \tag{2.12}$$

Таким чином формується два умовні вектори - V^+ (еталонно найкраще рішення) та - V^- (еталонно найгірше рішення).

2. У другому циклі для кожної альтернативи $i \in [1, q]$ обчислюються евклідові відстані до позитивного та негативного ідеалів:

- відстань до позитивного ідеалу

$$s_i^+ = \sqrt{\sum_{j=1}^{2n} (v_{ij} - v_j^+)^2} \tag{2.13}$$

- відстань до негативного ідеалу

$$s_i^- = \sqrt{\sum_{j=1}^{2n} (v_{ij} - v_j^-)^2} \tag{2.14}$$

3. Третім циклом виконується обчислення рейтингової оцінки (індексу близькості до ідеалу):

$$S_i = \frac{s_i^-}{s_i^- - s_i^+} \tag{2.15}$$

Ця формула забезпечує **нормовану інтегральну оцінку** в межах від 0 до 1 де:

$S_i \approx 1$ - альтернатива максимально близька до позитивного ідеалу (найкраща);

$S_i \approx 0$ - альтернатива наближена до негативного ідеалу (найгірша).

На завершальному етапі прийняття рішення використовується метод, який дозволяє ранжувати альтернативні конфігурації IoT-мережі за ступенем наближеності до умовно найкращого рішення. Спочатку для кожного показника KPI формується вектор позитивного ідеального рішення V^+, що містить найвищі досягнуті значення KPI серед усіх альтернатив, та негативного ідеального рішення V^-, що містить найнижчі значення. Далі для кожної альтернативи обчислюється евклідова відстань до обох ідеалів.

Після цього визначається рейтинговий індекс близькості S_i для кожної альтернативи/

Отримані значення S_i дозволяють впорядкувати альтернативи за спаданням ефективності. Альтернатива з найбільшим значенням S_i вважається найприйнятнішою для реалізації.

Висновки до розділу 2

У другому розділі «Розробка математичного методу вибору оптимальної конфігурації сенсорної мережі» основну увагу приділено моделі побудови оптимальної сенсорної мережі, застосовуючи метод багатокритеріального аналізу та теорію розподілених систем.

Визначено проблему вибору оптимальної технології та конфігурації сенсорної мережі, у якому для формального проєктування виділені наступні компоненти:

6. A - цільовий IoT-додаток з множиною характеристик і комунікаційних вимог R;

7. T - множина доступних технологій бездротового зв'язку;

8. C_i - набір можливих конфігурацій для кожної технології T_i з T;

9. K - набір ключових показників ефективності, що характеризують роботу додатку A при використанні технології T_i з конфігурацією C_i;

10. G - цільові значення KPI, які задаються проєктувальниками системи.

Головною задачею математичного методу стало знаходження технології T_d в T асоційованої з мережевою конфігурацією C_d^k (технологія та кількість відповідних конфігурацій) разом, які найкраще задовольняють вимоги до додатка R та досягають заданих цілей G щодо продуктивності, враховуючи KPI K.

У математичному методі було сформовано абстракцію та ключові параметри для аналізу мережевої ефективності що забезпечує можливість узагальненого але інформативного представлення вимог до зв'язку, характерних для цільового сценарію розгортання сенсорної мережі.

Для аналізу великого спектру мережевих технологій було побудовано відповідну модель якій виокремлено загальні та специфічні параметри для сенсорних мереж, в умовах наявності великої кількості альтернативних технологій правильна формалізація є критично важливою для вибору оптимального варіанту конфігурації мережі.

Для досягнення зазначених цілей метод поділяється на дві основні частини:

1. компоненту моделювання мережевих технологій, яка покликана задовольнити потреби та вимоги мережевих інженерів;

2. компоненту прийняття рішень, орієнтовану на фахівців, що займаються проектуванням IoT-додатків

Частина, присвячена моделюванню мережевих технологій, передбачає абстрагування та кількісне представлення параметрів кожної мережевої технології.

Компонент прийняття рішень складається з п’яти послідовних етапів: моделювання застосунку, попередній відбір, проєктування сценаріїв, оцінювання, прийняття рішення.

В результаті дослідження був запропонований математичний метод який дозволяє об’єктивно оцінити безліч запропонованих технологій кандидатів для впровадження в сенсорну мережу на етапі проектування, що дозволяє вибрати ту технологію що буде оптимально задовольняти перелік технічних вимог визначених для майбутньої мережі.

Головними перевагами запропонованого підходу є здатність до зваженого прийняття рішень щодо конфігурації, масштабованості, енергоефективності.

3 АРХІТЕКТУРА ТА АНАЛІЗ ЕФЕКТИВНОСТІ ДЕЦЕНТРАЛІЗОВАНОЇ СЕНСОРНОЇ МЕРЕЖІ

Цей розділ присвячений розробці та аналізу архітектури децентралізованої сенсорної мережі для екстреного інформування в умовах надзвичайних ситуацій. В умовах часткової або повної втрати зв’язку, викликаної деструктивними подіями (такими як військові дії чи стихійні лиха), традиційні телекомунікаційні засоби стають недоступними. У таких ситуаціях виникає критична потреба у створенні автономної, стійкої до відмов інфраструктури комунікації. У межах цього розділу описано концептуальні засади, функціональні компоненти, а також результати моделювання системи, заснованої на технології LoRa, яка дозволяє забезпечити базовий інформаційний обмін без залежності від централізованих ресурсів або зовнішніх сервісів.

3.1 Передумови для розробки сенсорної мережі екстреного реагування

Зона роботи мережі LoRaWAN визначається радіусом покриття, який забезпечується інфраструктурою встановлених шлюзів. Така архітектура є оптимальною для застосувань, що базуються на централізованому зборі або обробці даних. Проте існують підстави для використання більш гнучкої топології замість типової однохопової архітектури LoRaWAN за схемою "шлюз - клієнт". Зокрема, це може бути необхідно для розширення покриття мережі без встановлення додаткових шлюзів, подолання наслідків відмови інфраструктури або уникнення передавання даних до хмарних систем через підключення до Інтернету в районах із недостатньою телекомунікаційною інфраструктурою. На Рис 3.1 ілюструються ці обмеження.

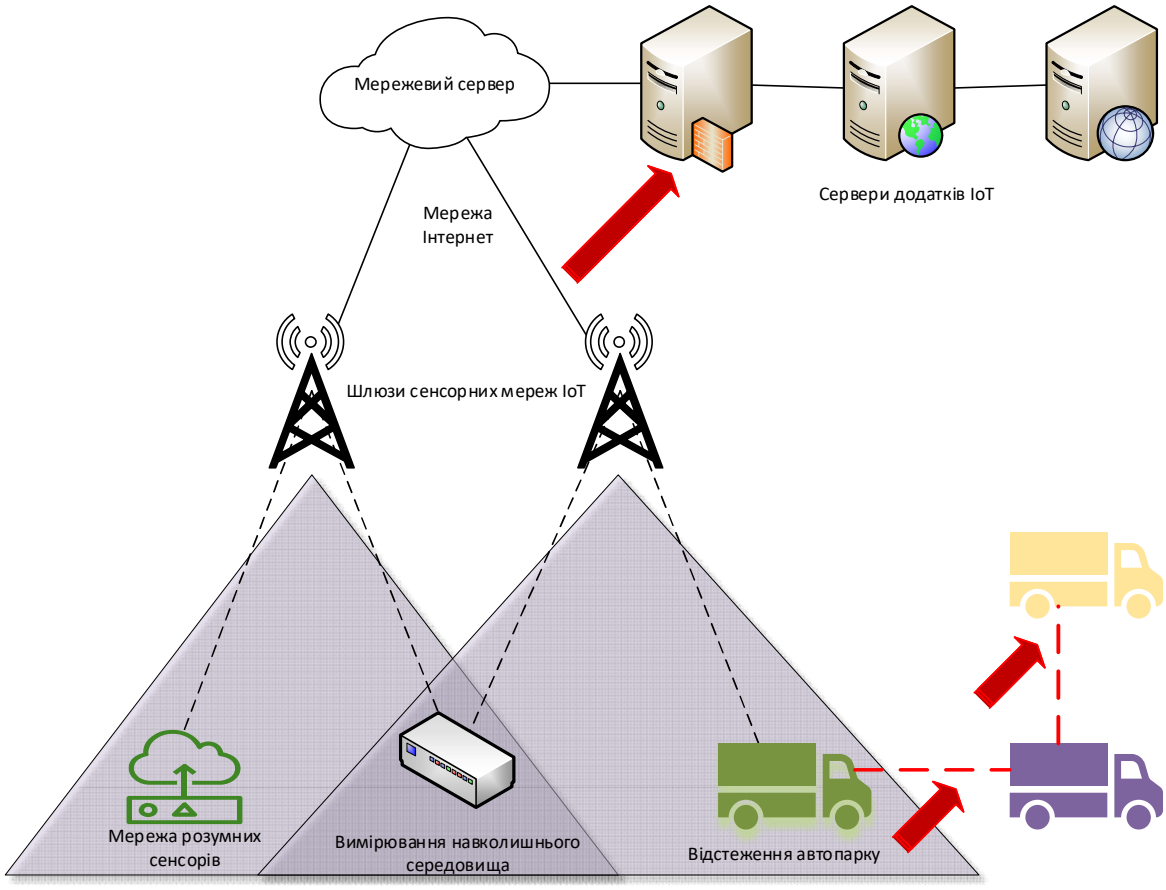

Рис. 3.1 - Архітектура LoRaWAN із позначеними обмеженнями прямої взаємодії між вузлами

У цьому розділі представлено комунікаційну систему, орієнтовану на забезпечення обміну інформацією про безпеку серед цивільного населення в умовах надзвичайних ситуацій. Мотивацією для розробки такої системи стало прагнення підвищити стійкість бездротових мереж у разі часткового руйнування інфраструктури що часто супроводжує подібні події. У процесі розробки було проведено комп'ютерне моделювання функціонування великої мережі LoRaWAN, із врахуванням можливих відмов шлюзів через деструктивні фактори. Додатково було проаналізовано вплив на продуктивність мережі стратегії, за якої кінцевим вузлам надається можливість ретрансляції пакетів сусідніх пристроїв з метою підтримання комунікаційної цілісності у випадку пошкодження інфраструктури.

Запропонована система базується на розширенні архітектури LoRaWAN і використовує радіотехнологію LoRa для обміну інформацією між кінцевими пристроями (тобто користувачами у їхніх домівках або місцях роботи) та додатком, розміщеним у спеціалізованих центрах координації надзвичайних ситуацій. Такий підхід дозволяє уникнути необхідності хмарної інфраструктури та залежності від зовнішніх Інтернет-сервісів. Взаємодія користувачів із системою здійснюється за допомогою компактного пристрою на основі LoRa, встановленого в приміщенні користувача, у поєднанні з програмним забезпеченням, інстальованим на персональному смартфоні. Програмний додаток використовує цей LoRa-пристрій як інтерфейс для обміну повідомленнями із загальною системою.

Щодо вибору базової технології, було обрано LoRa та LoRaWAN завдяки їхній здатності підтримувати спеціалізовані, цільові рішення у сфері Інтернету речей. Такі рішення дозволяють контролювати доступ до мережі та регулювати трафік повідомлень при мінімальному енергоспоживанні. Ці властивості сприяють значному подовженню періоду функціональної роботи системи після виникнення надзвичайних ситуацій, таких як військові дії, у порівнянні зі звичайними мережевими сервісами, що надаються Інтернет-провайдерами.

У розширеній версії запропонованої системи реалізовано протокол керування перевантаженнями, заснований на використанні підтверджувальних повідомлень ACK, який передбачає механізм зворотного зв'язку для підвищення ефективності взаємодії кінцевих користувачів із системою. Крім того, запропоноване рішення виходить за межі традиційної архітектури LoRaWAN, забезпечуючи можливість прямої комунікації між кінцевими пристроями. Така функціональність включає механізм ретрансляції пакетів, що підвищує стійкість мережі у випадку відмови інфраструктури.

Оцінка ефективності та можливостей системи була проведена за допомогою комп'ютерного моделювання з використанням OMNet++. Результати дослідження демонструють переваги запропонованого підходу у порівнянні з

раніше існуючими рішеннями. Система здатна забезпечити комунікацію між громадянами в умовах надзвичайних ситуацій, а також підтримувати інформування служб швидкого реагування та координаційних центрів управління надзвичайними ситуаціями.

3.1.1 Проблема втрати зв’язку у надзвичайних ситуаціях

Надзвичайні ситуації, що виникають раптово в населених пунктах, ставлять перед постраждалими два основні завдання: по-перше, забезпечення власної безпеки та евакуація до безпечного місця, і по-друге, встановлення інформації про стан безпеки своїх близьких. Традиційні заходи безпеки зазвичай орієнтовані переважно на перше завдання - фізичний захист життя та здоров’я. Водночас після початкової фази реагування, коли загроза безпосередньо для життя вже зменшилася, люди стикаються з необхідністю отримання інформації про своїх родичів і друзів.

Ця проблема ускладнюється умовами повного або часткового припинення роботи інфраструктури - таких як мобільний або стаціонарний телефонний зв'язок, а також сервіси обміну повідомленнями через Інтернет. Втрата зв’язку часто є наслідком фізичного руйнування об’єктів інфраструктури, перевантаження комунікаційних систем або знеструмлення через пошкодження електромереж [80]. З міркувань безпеки електропостачання зазвичай відключається одразу після настання надзвичайної події та відновлюється лише після індивідуальної перевірки стану об'єктів, що може тривати кілька днів. Усі ці чинники сприяють виникненню характерного комунікаційного "блекауту", який супроводжує кризові ситуації [81].

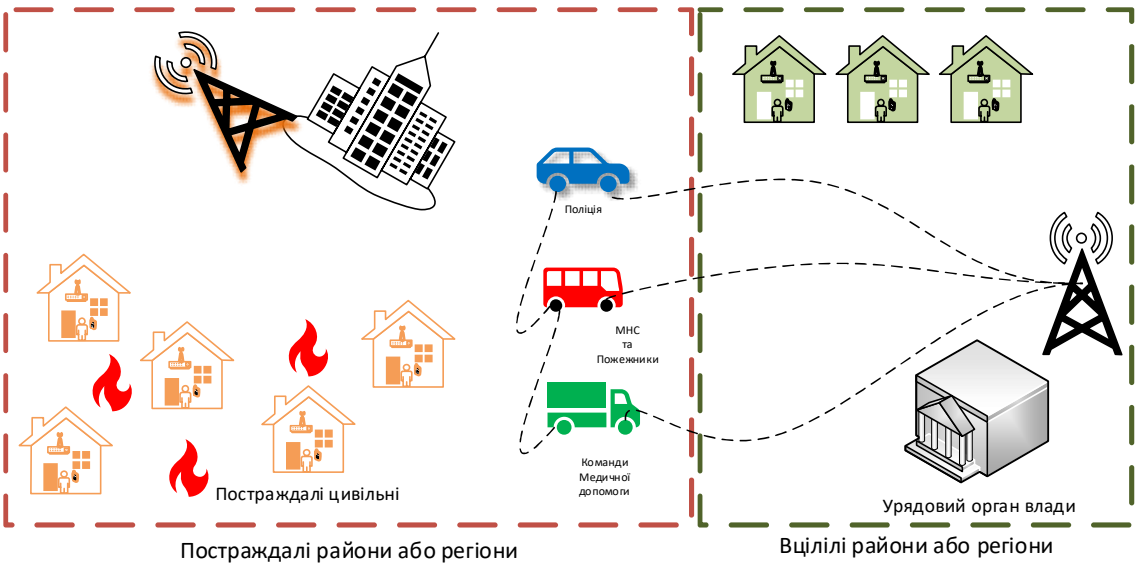

Рис 3.2 - Характерна ситуація з комунікаціями після настання надзвичайної події

На Рис. 3.2 представлено спрощене концептуальне зображення такої комунікаційної ситуації, коли більшість традиційних посередників зв'язку в зоні надзвичайної ситуації (наприклад базові станції стільникового зв’язку) вийшли з ладу або були вимушено вимкнені. У подібних умовах цивільне населення та організації першої допомоги стикаються з нагальною потребою у створенні альтернативних каналів комунікації для забезпечення координації своїх дій.

Зазвичай організації першого реагування - такі як пожежні підрозділи, поліція, служби екстреної медичної допомоги та державні агентства використовують для внутрішніх комунікацій системи радіозв’язку у діапазонах VHF/UHF [82]. Проте така інфраструктура, як правило, не призначена для забезпечення взаємодії цивільного населення між собою або їхньої комунікації з рятувальниками.

За відсутності звичних засобів комунікації у надзвичайних ситуаціях багато людей намагаються дістатися до домівок своїх близьких на власних транспортних засобах, щоб дізнатися про їхній стан. Такі дії не лише створюють

загрозу для особистої безпеки самих постраждалих, але й ускладнюють роботу аварійно-рятувальних служб.

Оскільки системи громадського транспорту зупиняються з міркувань безпеки, можливості цивільного населення для переміщення стають обмеженими. Ті хто не має доступу до транспорту, зазвичай залишаються вдома, дотримуючись стратегії "залишатися на місці", що рекомендується більшістю процедур безпеки. У таких умовах люди очікують, що з ними зв'яжуться інші, що супроводжується зростаючим рівнем тривожності та занепокоєння, які можуть мати негативний вплив на їхній емоційний стан.

Більшість досліджень, присвячених комунікації під час і безпосередньо після надзвичайних ситуацій, зосереджуються на роботі аварійно-рятувальних служб або на взаємодії із цивільним населенням, яке перебуває поза межами зони ураження [83]. Проте останнім часом з'являються наукові роботи, що досліджують потенційну участь цивільних у процесах реагування на надзвичайні ситуації, таких як оцінка пошкоджень, передача запитів про допомогу [], а також виявлення місцеперебування людей у великих міських агломераціях і спрямування їх у безпечні місця [84].

Попри цей прогрес, питання організації ефективної комунікації з цивільними та залучення їх у ролі "людських сенсорів" і споживачів інформації залишаються актуальними. Для цього необхідний комплексний підхід, за якого люди та їхні пристрої стають активними елементами системи реагування, що фактично передбачає еволюцію до парадигми взаємодії Інтернету Людей (IoP) [85].

Для сприяння участі цивільного населення в діяльності з реагування на надзвичайні ситуації пропонується концепція комунікаційної системи, що орієнтована на забезпечення можливості обміну інформацією про стан безпеки між громадянами та їхніми родинами, а також із представниками аварійно-рятувальних служб після виникнення надзвичайної ситуації військового характеру. Оскільки така інформація є геоприв’язаною та закодованою, її можна

агрегувати для подальшого використання у процесах прийняття рішень органами державної влади чи командами першого реагування.

Наприклад, на основі зібраних даних можливо створювати карти щільності постраждалих районів або виявляти ділянки, де допомога є найбільш нагальною. Таким чином, залучення цивільних осіб у ролі "людських сенсорів" є критичним для забезпечення практично реального часу отримання інформації, що підтримує ефективне ухвалення рішень на вищих рівнях управління.

Перші години після виникнення надзвичайної ситуації є критичним періодом, протягом якого цивільне населення, аварійно-рятувальні служби та державні органи потребують актуальної інформації щодо стану безпеки інших осіб для прийняття подальших рішень. У цей час процес ухвалення рішень зазвичай відбувається у розподілений і часто хаотичний спосіб, причому під значним тиском часу, що виступає найбільш обмеженим ресурсом [86]. В умовах такої невизначеності забезпечення надійних каналів комунікації та своєчасного отримання інформації є надзвичайно важливим для прийняття обґрунтованих і оперативних рішень.

3.2 Розробка сенсорної мережі із застосуванням LoRa

3.2.1 Технічні вимоги до сенсорної мережі

У результаті виникнення надзвичайної ситуації звичайна комунікаційна інфраструктура, така як мережі стільникового зв’язку, проводові Інтернет-з’єднання та фіксовані телефонні лінії (на основі волоконно-оптичних або мідних кабелів), має високу ймовірність зазнати серйозних перебоїв у функціонуванні. Надзвичайні події можуть впливати на інфраструктуру різними шляхами: фізичні пошкодження волоконно-оптичних або мідних ліній передачі даних унаслідок надмірних механічних навантажень, руйнування опорних

конструкцій базових станцій мобільного зв'язку, а також зсув або дезорієнтація високочастотних антен, що потребують точного вирівнювання для належної роботи. Окрім безпосереднього руйнування обладнання, критичним чинником стає припинення постачання електроенергії, що виводить з ладу навіть ті елементи інфраструктури, які залишаються фізично непошкодженими.

Варто зазначити, що втрата електроживлення може бути спричинена як прямими руйнуваннями об'єктів енергетичної інфраструктури (наприклад, підстанцій або ліній електропередачі), так і застосуванням запобіжних заходів з боку відповідальних служб для запобігання виникненню пожеж або інших аварійних ситуацій. Таким чином, традиційні канали комунікації стають ненадійними або повністю недоступними саме у той момент, коли критично необхідно забезпечити обмін інформацією для координації рятувальних робіт, взаємодії між цивільним населенням та органами першої допомоги. Це підкреслює важливість створення альтернативних систем комунікації, здатних функціонувати автономно, незалежно від централізованої інфраструктури та наявності електропостачання.

З огляду на вищезазначені міркування, система екстреного зв'язку для цивільного населення у випадку надзвичайної ситуації повинна працювати паралельно та незалежно від традиційних каналів комунікації, не покладаючись на чинні телекомунікаційні служби. Важливо також, щоб така система використовувала бездротові технології замість кабельних з'єднань, що забезпечить стійкість до потенційних фізичних пошкоджень інфраструктури.

Крім того, враховуючи можливі тривалі перебої в електропостачанні, система має бути здатною працювати від автономних джерел енергії, таких як джерела безперебійного живлення (UPS) або батареї, принаймні протягом кількох годин, доки не буде відновлено основне живлення. Зазначені вимоги безпосередньо впливають на архітектуру системи, обумовлюючи вибір ключових параметрів: радіус дії бездротового зв'язку, діапазон робочих частот, рівень потужності передавання сигналу, тип антенних систем, а також

максимально можливу пропускну здатність. Кожен із цих аспектів має бути оптимізований відповідно до обмежень енергоспоживання та необхідності забезпечення надійного зв’язку в умовах обмеженої інфраструктури.

Окрім технічних обмежень, до вимог, що висувалися до розроблюваної системи бездротового зв'язку для надзвичайних ситуацій, було додано ще одну важливу умову: уся інфраструктура має бути повністю доступною, власною та керованою безпосередньо оператором системи. Такий підхід продиктований тим, що залежність від інфраструктури, яка належить третім сторонам або контролюється ними, не гарантує її надійної доступності у критичних умовах або може призводити до зниження якості послуг чи їх повної недоступності.

З огляду на обмеження у доступності, можливості керування та адаптивності існуючих інфраструктурних рішень, а також зважаючи на висновки, зроблені у попередніх частинах дослідження, для побудови системи було обрано технологію радіозв'язку LoRa. Саме вона, завдяки низькому енергоспоживанню, здатності до створення приватних мереж і великому радіусу дії при мінімальній інфраструктурі, виявилася найбільш придатною для забезпечення автономної роботи у надзвичайних умовах.

Базова архітектура запропонованого рішення орієнтована на специфікації LoRaWAN. Водночас система зазнала функціонального розширення порівняно зі стандартною архітектурою: було додано механізми підтвердження доставки повідомлень (ACK-повідомлення) та можливість ретрансляції пакетів між вузлами користувачів. Таким чином, запропонована система виходить за межі класичної LoRaWAN-концепції, поєднуючи її переваги із новими можливостями, що критично важливі для забезпечення живучості та надійності мережі у випадку надзвичайних ситуацій. Загальну архітектуру запропонованого рішення буде докладніше представлено у наступному підрозділі.

3.2.2 Базова та розширена архітектура сенсорної мережі

Початкова архітектура розробленої системи базувалася на специфікаціях LoRaWAN [87], однак у процесі подальшого розвитку вона вийшла за межі класичної моделі шляхом впровадження механізмів прямої комунікації між домашніми пристроями та організації багатохопової передачі пакетів.

У попередніх розділах було розглянуто чинники та обмеження, які обумовили вибір технології LoRa та архітектури LoRaWAN як основи для створення запропонованого рішення. На цьому етапі описується загальна архітектура розробленої системи, її функціональні можливості та ключові характеристики.

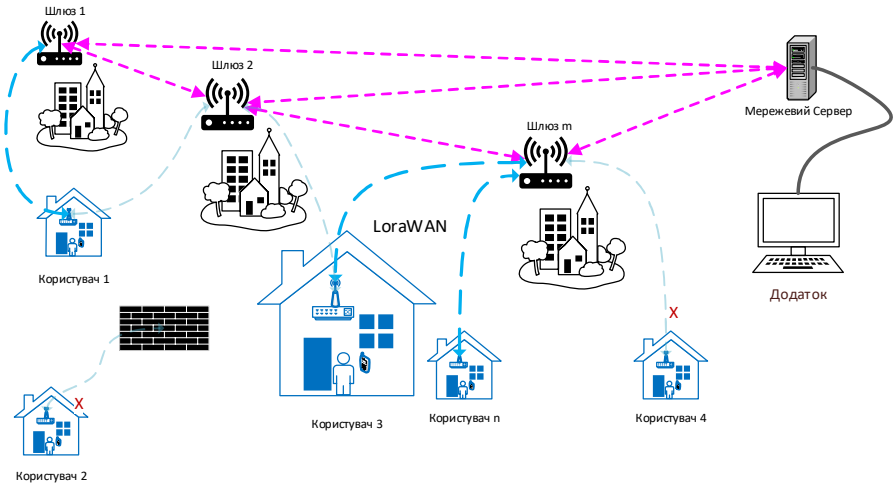

Рис. 3.3 – Базова архітектура сенсорної мережі LoRAWAN

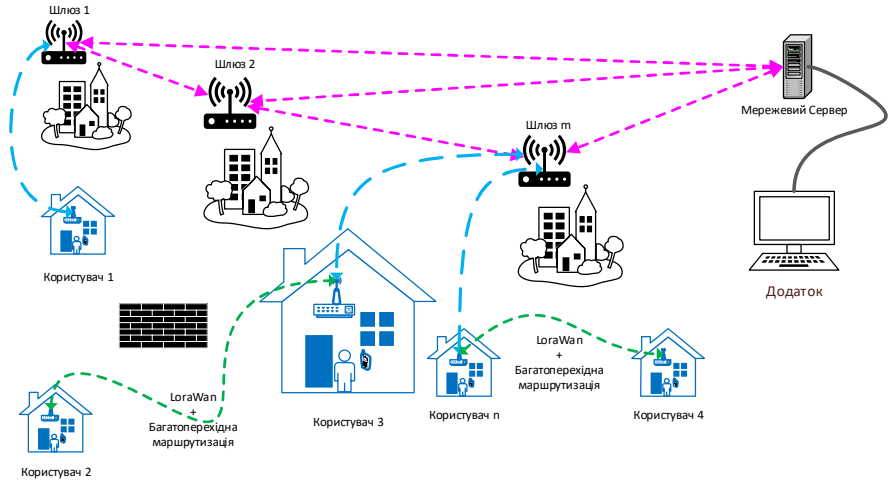

Рис. 3.4 – Розширена версія архітектури сенсорної мережі LoRAWAN

На Рис. 3.3 та Рис 3.4 подано високорівневе зображення основних компонентів системи у двох варіаціях: базовій версії, що відповідає специфікаціям LoRaWAN, та розширеній версії із підтримкою багатохопової маршрутизації та самоорганізації. Такий підхід забезпечує більшу стійкість мережі до відмов інфраструктури та розширює зону покриття без необхідності залучення додаткових ресурсів.

На Рис. 3.3 зображено декілька людей, які перебувають у приміщеннях своїх домівок, обладнаних спеціальними кінцевими вузлами системи. Ці кінцеві пристрої забезпечують можливість обміну повідомленнями між членами родини та друзями.

Щоб уникнути плутанини з іншими типами пристроїв користувачів (наприклад, смартфонами), у подальшому тексті ці кінцеві вузли умовно називатимуться "домашні пристрої". Їх передбачається встановлювати як у житлових приміщеннях, так і на робочих місцях з метою забезпечення функціональності прийому та передачі повідомлень у надзвичайних ситуаціях. Домашні пристрої працюють відповідно до класу A специфікації архітектури LoRaWAN, що передбачає енергоефективний режим роботи з асинхронною передачею даних та обмеженими часовими вікнами для прийому.

Шлюзи, зображені у середній та верхній частинах Рис. 3.3 виконують роль проміжних вузлів, що ретранслюють повідомлення від домашніх пристроїв до мережевого сервера. Завдяки особливостям роботи мережі, передача даних від одного вузла може бути прийнята кількома шлюзами одночасно, що формує топологію типу "зірка-зірка", згідно зі специфікацією архітектури LoRaWAN.

У типовій реалізації шлюзи часто використовують інтернет-з'єднання для передачі пакетів між кінцевими пристроями та мережевим сервером, зокрема через стільникові мережі 3G або 4G. Однак у запропонованій системі, враховуючи очікувану недоступність стільникового зв'язку у надзвичайних ситуаціях, шлюзи об'єднані між собою за допомогою бездротової сітчастої мережі на основі стандарту IEEE 802.11. Це дозволяє забезпечити безперервний

обмін даними між шлюзами та мережею навіть за умов повного відключення інтернету.

Варто зазначити, що бездротові mesh-мережі, які відповідають вимогам даної системи щодо топології, зони покриття та пропускної здатності, є технологічно зрілими рішеннями та вже впроваджені на практиці [88]. Оскільки ця частина системи не входить до базової специфікації LoRaWAN, її детальний аналіз у даному дослідженні не проводиться. Для спрощення проєктування припускається, що шлюзи мають стабільне та пряме підключення до мережевого сервера.

Крім того, інфраструктура шлюзів та бездротових маршрутизаторів живиться від джерел резервного електроживлення - акумуляторних батарей або джерел безперебійного живлення (UPS), що дозволяє забезпечити їхню працездатність у перші години після виникнення надзвичайної ситуації навіть за умови масштабного знеструмлення.

Мережевий сервер, зображений у верхньому правому куті Рис. 3.3, приймає усі повідомлення від кінцевих вузлів, які були успішно демодульовані шлюзами, та обробляє їх. Зокрема, одним з етапів обробки є усунення дублікатів повідомлень, що можуть виникати через прийом одного пакета кількома шлюзами одночасно.

У типовій реалізації LoRaWAN мережевий сервер зазвичай розміщується у хмарних обчислювальних середовищах. Проте у запропонованій системі, виходячи з вимог автономності в умовах надзвичайної ситуації, сервер працює локально - без потреби у зовнішньому Інтернет-з'єднанні. Такий підхід забезпечує вищу стійкість системи до зовнішніх збоїв і підвищує її надійність.

На мережевому сервері також розгортається прикладне програмне забезпечення, яке виконує обробку отриманих повідомлень від кінцевих пристроїв. Його функціонал включає аналіз даних, прийняття рішень та ініціювання відповідних дій, таких як активація тривожних сигналів або надсилання зворотних повідомлень. Зібрана та оброблена інформація надається

органам управління надзвичайними ситуаціями та групам швидкого реагування у вигляді наочних інструментів підтримки прийняття рішень - таких як інтерактивні діаграми або теплові карти.

Таким чином, мережевий сервер виступає критично важливою ланкою в інфраструктурі, забезпечуючи централізовану координацію та ефективне управління ресурсами під час надзвичайної ситуації.

У базовій версії системи, яку було запропоновано та змодельовано, передача даних здійснюється виключно у висхідному напрямку - від користувацьких вузлів до центрального прикладного сервера. Однак архітектура LoRaWAN передбачає також можливість передачі даних у низхідному напрямку, тобто від прикладного сервера до кінцевих пристроїв, що відкриває перспективу для реалізації повноцінної двосторонньої взаємодії.

У межах цього дослідження запропоновано використати зазначену можливість для забезпечення механізму зворотного зв'язку із кінцевими користувачами. Зокрема, пропонується інформувати користувачів про статус доставки їхніх повідомлень - наприклад, чи було отримано їхнє повідомлення центральним застосунком. Такий підхід сприятиме підвищенню довіри користувачів до системи, забезпеченню їх обізнаності про стан комунікацій.

Пересилання мережевих пакетів між кінцевими пристроями сенсорної мережі

Архітектура LoRaWAN передбачає використання топології типу "зірка - зірка", у якій не реалізовано можливість прямої комунікації між окремими вузлами мережі. Це створює низку обмежень у проєктуванні систем, зокрема необхідність проходження всіх повідомлень від кінцевих користувацьких пристроїв до мережевого сервера виключно через шлюзи, навіть незважаючи на те, що фізичний рівень LoRa-радіозв’язку технічно дозволяє здійснювати прямі передавання між пристроями.

Такий підхід є виправданим для застосувань, у яких пристрої працюють автономно від батарей і більшу частину часу перебувають у режимі енергоощадження. Вони активуються лише періодично - наприклад, для зняття показників із сенсора, надсилання зібраних даних та подальшого повернення в режим сну. Однак у контексті надзвичайних ситуацій, де елементи інфраструктури можуть виходити з ладу без попередження, така архітектурна модель виявляється недостатньо надійною.

У подібних умовах доцільним є використання механізмів прямої взаємодії між пристроями, що дозволяє забезпечити певний ступінь відмовостійкості системи. Зокрема, кінцеві пристрої, які залишаються в зоні дії мережі, можуть виконувати функції ретрансляторів для повідомлень від сусідніх пристроїв, які перебувають поза зоною покриття шлюзів, але все ще мають потребу у передаванні інформації до мережевого сервера. Такий механізм дозволяє частково компенсувати втрату інфраструктурної доступності й забезпечити безперервність інформаційного обміну в критичних умовах.

Таким чином, запропонована система розширює базові можливості типової інфраструктури IoT, яка використовує однорангову модель зв’язку типу «вузол-шлюз», за рахунок введення механізму ретрансляції повідомлень між кінцевими пристроями. Йдеться про те, що у визначених обставинах кінцеві пристрої, розміщені в домогосподарствах, можуть передавати повідомлення, отримані від інших вузлів, які самостійно не мають доступу до шлюзів або мережевого сервера.

На Рис 3.4 два приклади реалізації такої можливості. У першому випадку пристрій користувача, що перебуває поза зоною досяжності будь-якого шлюзу, має змогу передавати повідомлення завдяки тому, що сусідній пристрій (розташований у межах досяжності шлюзу) приймає ці повідомлення і ретранслює їх до серверної частини системи. У другому випадку пристрій, який перебуває на межі зони покриття шлюзу і ризикує втратити зв’язок через нестабільні умови радіосигналу, також отримує вигоду від багаторівневої

маршрутизації: повідомлення передається через інший, більш стабільно підключений вузол.

Для забезпечення функціонування цієї логіки передбачається, що у разі надзвичайної ситуації пристрої переходять з енергоощадного режиму сну до активного режиму, що дозволяє не лише передавати власні повідомлення, а й виконувати роль проміжного вузла ретрансляції. Такий підхід дозволяє суттєво підвищити стійкість системи до втрати окремих елементів інфраструктури та підтримувати безперервність комунікацій навіть у складних умовах.

Користувацькі термінали для для взаємодії з сенсорною мережею

У межах запропонованої системної архітектури передбачається, що громадяни матимуть у розпорядженні компактні користувацькі пристрої, встановлені в їхніх помешканнях або на робочих місцях. Ці пристрої слугуватимуть засобом зв’язку в умовах надзвичайної ситуації, коли звичні телекомунікаційні канали - мобільні мережі, фіксований інтернет тощо, можуть бути недоступними. Для того, щоб пристрої успішно інтегрувалися у запропоновану комунікаційну систему, вони повинні відповідати ряду функціональних та технічних вимог:

1. Бути оснащеними радіомодулем для передавання та приймання пакетів у частотному діапазоні, що використовується IoT-технологіями (зокрема, LoRa);

2. Містити бездротові інтерфейси ближнього радіозв’язку, такі як Wi-Fi або Bluetooth, для локальної взаємодії з іншими пристроями або з особистим пристроєм користувача;

3. Мати вбудований дисплей (LCD, OLED або e-ink) для виведення службової та інформаційної індикації;

4. Забезпечувати фізичний інтерфейс для взаємодії з користувачем, наприклад, за допомогою кнопок або сенсорних елементів;

5. Характеризуватися низьким енергоспоживанням, що дозволяє продовжити автономну роботу в умовах відсутності енергопостачання;

6. Мати компактні габаритні розміри, що полегшує їх встановлення у побутових умовах;

7. Підтримувати живлення через стандартні порти micro-USB або USB-C у штатному режимі;

8. Мати можливість автономного живлення від батарей або вбудованих акумуляторів у разі зникнення електропостачання.

Рис. 3.5 – Плата розробника з вбудованим ESP32

Рис. 3.6 – Прототип користувацького пристрою з сонячним фотоелементом

Користувацькі пристрої побудовані на базі енергоефективного системного модуля ESP32 від компанії, який має інтегровану підтримку Wi-Fi. До нього підключено LoRa-трансивер, що забезпечує можливість довготривалого бездротового зв’язку на великій відстані. На Рис. 3.5 представлено тестову плату

розробника з дисплеєм, під яким припаяний LoRa-модуль. Рис. 3.6 - прототип користувацького пристрою, змонтований у 3D-друкованому корпусі.

3.2.2.1 Взаємодія користувача з сенсорною мережею

Взаємодія кінцевих користувачів із системою здійснюється через спеціальні пристрої, розміщені в оселях громадян, як показано на рисунку 4.5.

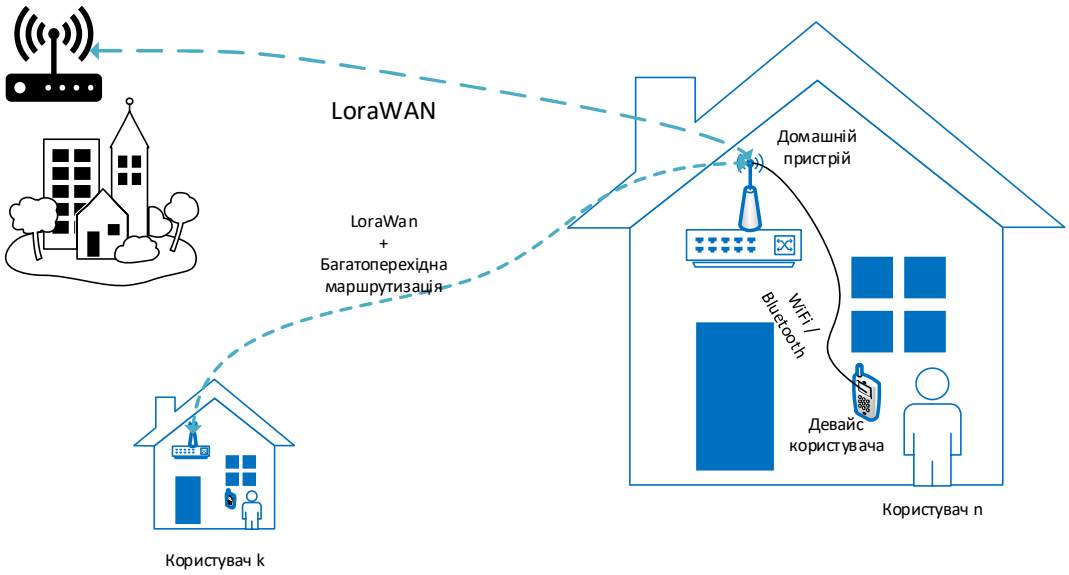

Рис. 3.7 – Схема взаємодії користувача з сенсорною мережею

Користувачі можуть передавати інформацію за допомогою фізичних кнопок пристрою або через програму, встановлену на персональному пристрої (наприклад, смартфоні, планшеті чи ноутбуці). Такі домашні пристрої базуються на енергоефективних вбудованих модулях, реалізованих на основі мікросхем типу SoC (System-on-Chip), що забезпечують підтримку радіозв’язку Wi-Fi або Bluetooth, а також оснащені LoRa-трансивером.

З одного боку, короткодіапазонні радіоінтерфейси (Wi-Fi або Bluetooth) використовуються для локальної взаємодії з пристроєм користувача, зокрема для налаштування чи оновлення параметрів. З іншого боку, радіомодуль LoRa виконує функцію каналу дальнього радіозв’язку, за допомогою якого

користувачі передають свій статус безпеки до центрального сервера. Через ту ж саму інфраструктуру сервер надсилає повідомлення до відповідного адресата - іншого домашнього пристрою або підключених до нього персональних пристроїв.

Оскільки усі повідомлення на сервері є зашифрованими та містять інформацію про географічне розташування їх джерела, виникає можливість обробки таких даних алгоритмічними засобами з метою швидкої агрегації інформації. Це дозволяє формувати надійну оперативну картину ситуації для підтримки процесів планування, моніторингу та ухвалення рішень органами державного управління або службами екстреного реагування.

Формат взаємодії користувача з системою через домашній пристрій суттєво відрізняється до початку надзвичайної ситуації та після її настання. У наступному розділі розглянуто ці два сценарії більш докладно.

Домашній пристрій системи призначений для забезпечення користувачів можливістю надсилати та отримувати короткі текстові повідомлення, обрані зі списку заздалегідь визначених варіантів (наприклад: «Усі в безпеці», «Потрібна медична допомога»). Крім того, передбачено функціонал створення персоналізованих повідомлень відповідно до конкретних потреб користувача (наприклад: «Немає інформації про родину Петренків»).

Для локальної взаємодії пристрій обладнаний модулем короткодіапазонного радіозв’язку, що функціонує як звичайна точка доступу Wi-Fi, до якої можуть підключатися користувачі. Після підключення відкривається вебінтерфейс, розміщений на самому пристрої, який дозволяє обрати необхідне повідомлення або створити нове. Альтернативно, цей процес конфігурації може здійснюватися через мобільний додаток, який використовує з’єднання Bluetooth для комунікації з пристроєм. На рисунку 3.7 представлено макет інтерфейсу користувача для налаштування повідомлень на екрані смартфона.

Рис. 3.7 – Макет вебінтерфейсу редагування та налаштування повідомлень до настання надзвичайної ситуації

Рис. 3.8 – Макет вебінтерфейсу де надається вибір повідомлення для надсилання після виникнення надзвичайної ситуаці

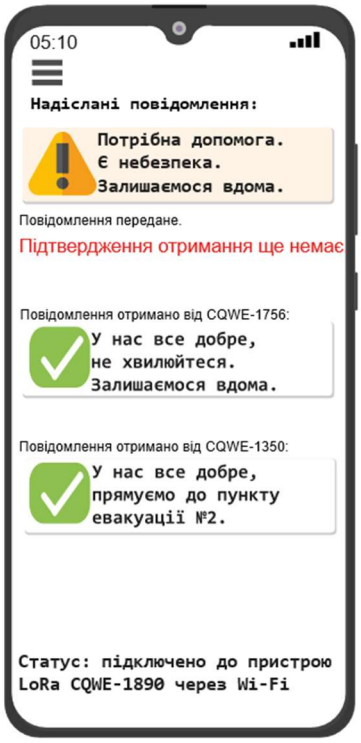

Рис. 3.9 – Макет вебінтерфейсу де наявне відображення неприйнятого вихідного повідомлення та отриманих текстів у післяаварійний період.

У разі виникнення надзвичайної ситуації користувачі можуть взаємодіяти з власними домашніми пристроями безпосередньо. Це забезпечує простий інтерфейс для надсилання та отримання коротких повідомлень. За допомогою кнопок та вбудованого РК-дисплея користувач має змогу обрати повідомлення (як зі списку попередньо визначених, так і створених самостійно) та ознайомитися з вхідними повідомленнями. Такий спосіб є найшвидшим для комунікації за допомогою пристрою, хоча за зручністю він може поступатися спеціалізованому мобільному застосунку. Водночас у разі ймовірного знеструмлення домашній пристрій, що живиться від батарейок, залишається готовим до використання.

Крім того, користувачі можуть здійснювати взаємодію з пристроєм за допомогою звичних особистих пристроїв (наприклад, смартфонів або ноутбуків), під’єднуючись до нього через Wi-Fi або Bluetooth. Прикладом такого підключення є інтерфейс мобільного застосунку - вебсторінки, яка дозволяє

сформувати та передати повідомлення, а також переглянути статус переданих та отриманих повідомлень (див. Рис. 3.8 та Рис. 3.9).

3.3 Моделювання роботи сенсорної мережі в реальних умовах

З метою аналізу поведінки системи зв'язку на базі LoRa в умовах, наближених до реальних, було змодельовано репрезентативну частину міста Ірпінь – середнього за розміром населеного пункту Київської області з населенням близько 65 000 осіб. За даними останнього перепису та відкритих статистичних джерел, для моделювання було обрано житлову частину центрального району міста. Загальна чисельність населення в межах цієї ділянки становить приблизно 27 486 осіб, які проживають у близько 7328 домогосподарствах, розміщених на площі орієнтовно 5,1 км².

Втім, враховуючи нерівномірну щільність забудови, основна частина населення сконцентрована в межах компактнішої ділянки розміром приблизно 3,45 км², тоді як інші частини включають зелені зони, сквери та території з низькою щільністю забудови. Для уточнення меж були проаналізовані житлові квартали згідно з офіційним кадастром та генеральним планом міста.

З метою спрощення розрахункової моделі, вибрана ділянка була апроксимована прямокутником розміром 1,4 км × 2,6 км, а кількість домогосподарств була заокруглена до 7500. Таке узагальнення дозволило зберегти похибку просторової щільності на рівні менш ніж 2 %, що є прийнятним у межах початкового моделювання (див. табл 0.0). При цьому було прийнято кілька базових припущень: домогосподарства рівномірно розподілені по всій території, а рельєф місцевості вважається плоским без значних перепадів висот.

Таблиця 3.1 – Відхилення між реальними даними ро населення та спрощеною моделлю

Параметр:	Реальні дані	Модель	Відхилення
Кількість населення	27486	28000	1,83 %
Кількість домогосподарств	7328	7500	2,29 %
Заселена площа (км²)	3,45	3,5	1,42 %
Щільність домогосподарств (на км²)	2 124	2 143	0,88 %

З метою забезпечення достовірності симуляційного експерименту була виконана оцінка відповідності вхідних параметрів моделі реальним демографічним і географічним характеристикам. Таблиця 3.1 демонструє, що відхилення між реальними статистичними даними та значеннями, прийнятими для моделювання, не перевищує 2,3 % для жодного з параметрів. Це свідчить про прийнятну точність спрощеної моделі, що дозволяє вважати її достатньо репрезентативною для цілей подальшого аналізу сценаріїв у межах дослідження

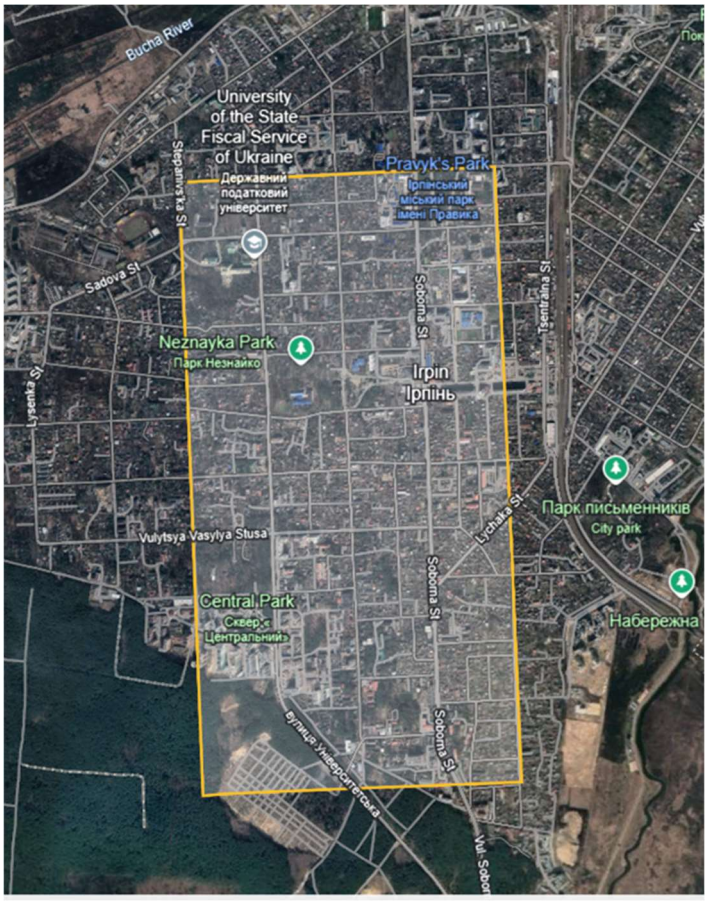

Рис 3.10 – Супутниковий знімок Ірпеня з накладеними географічними межами дослідження

На відповідному зображенні (рис. 3.10) представлено супутниковий знімок центральної частини Ірпеня з накладенням меж моделювання.

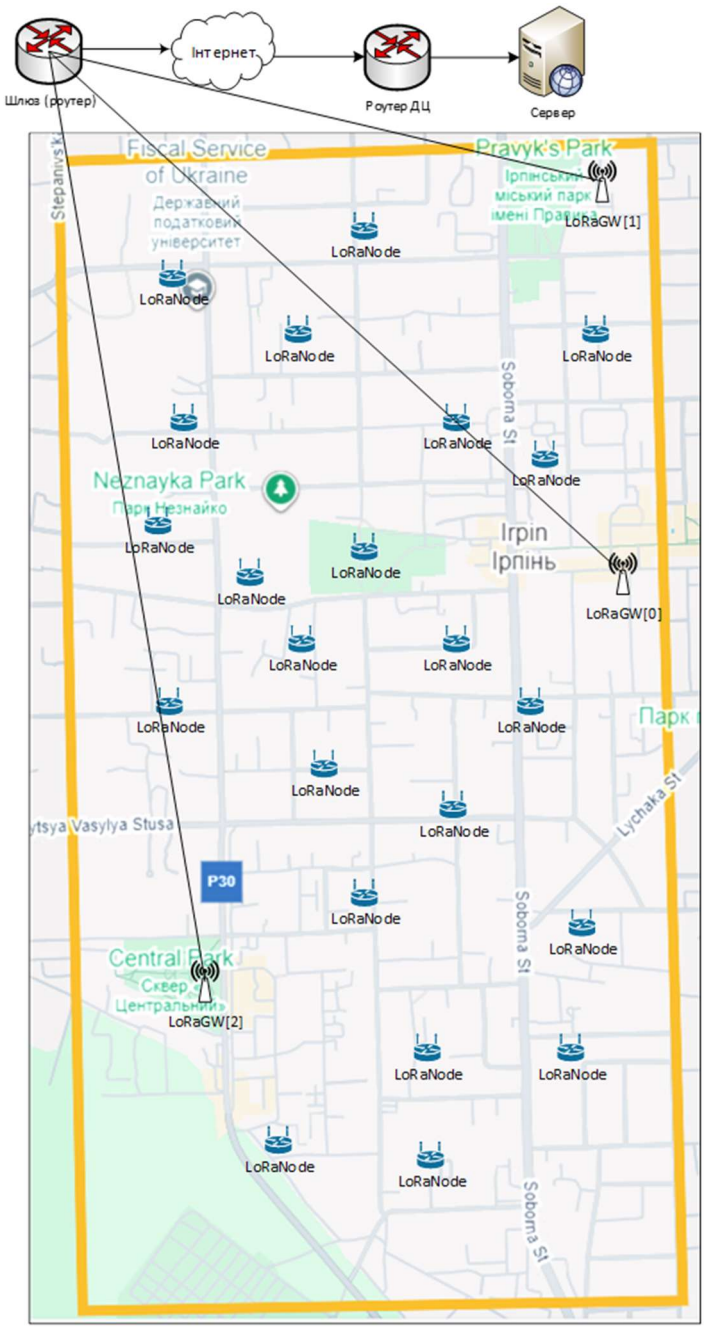

Рис 3.11 – Архітектура мережі LoRaWAN, змодельована у програмному середовищі

Рис 3.11 демонструє архітектуру мережі LoRaWAN, змодельовану у програмному середовищі з урахуванням розміщення вузлів, шлюзів і маршрутизаторів у межах цієї зони.

Варто зазначити, що в умовах реального розгортання системи доцільно застосовувати точніші геопросторові дані: цифрові моделі рельєфу, картографію щільності забудови та параметри ослаблення радіосигналу при проходженні через будівельні конструкції, зокрема зовнішні стіни багатоповерхових будинків.

3.3.1 Визначення основних параметрів роботи мережі

З огляду на поставлену мету - оцінити продуктивність системи в умовах масової взаємодії користувачів після виникнення надзвичайної ситуації, експерименти, наведені в цьому дослідженні, зосереджені саме на аналізі цієї фази. Інші аспекти, зокрема ініціалізація шлюзів або вузлів користувачів, не розглядаються докладно.

Симуляційні випробування розпочинаються з короткого етапу підготовки, під час якого всі пристрої (зокрема вузли користувачів, шлюзи та мережевий сервер) виконують відповідні процедури ініціалізації. Після цього настає період бездіяльності, коли жодні пакети не передаються через радіоканал. Цей етап відповідає стандартному режиму роботи системи до настання надзвичайної ситуації. Така процедура є спільною для всіх симуляцій, описаних у межах цього дослідження.

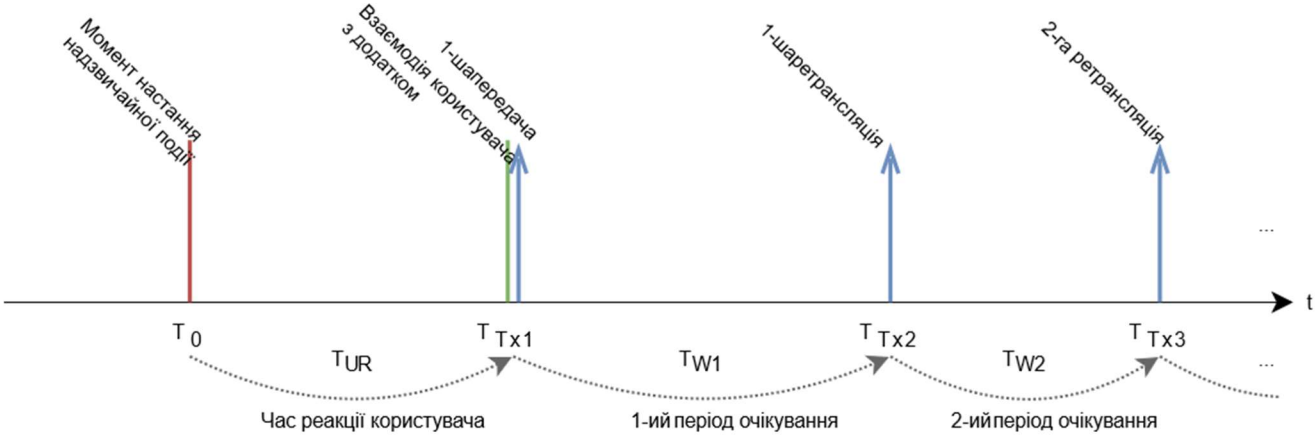

Рис 3.12 – Часовий графік активності користувацьких вузлів після настання надзвичайної ситуації

На Рис 3.12 представлено послідовність подій і дій, що відбуваються на одному з користувацьких вузлів у симульованій мережі. Вважається, що на момент часу $T_0 = 3600\,c.$ секунд настає надзвичайна ситуація, після чого завершуються період попередньої бездіяльності. З цього моменту користувачі починають взаємодіяти зі своїми пристроями. Час реакції користувача позначено як T_{UR} і моделюється як неперервна рівномірна випадкова величина в діапазоні від 0 до 120 секунд. Взаємодія користувача з пристроєм одразу ініціює передачу першого пакета, яка відбувається у момент часу $t = T_{Tx1} = T_0 + T_{UR}$

Після першої передачі користувацький вузол очікує випадковий проміжок часу перед виконанням наступної передачі (або повторної передачі), яка відбувається у момент часу $t = T_{Tx2} = T_0 + T_{UR} + T_{W1}$. Далі, після ще одного випадкового інтервалу очікування, відбувається третя передача пакета в момент часу $t = T_{Tx3} = T_0 + T_{UR} + T_{W2}$, потім - четверта передача і так далі. Часові інтервали між передачами T_{W1}.та T_{W2} моделюються як неперервні рівномірні випадкові величини в межах від 0 до 300 секунд.

З огляду на те, що система призначена для підтримки швидкого реагування аварійних служб у перші хвилини після надзвичайної ситуації, усі симуляції обмежуються періодом в одну годину після моменту події, незалежно від того, чи залишилися ще не надіслані пакети. Враховуючи, що деякі параметри моделювання залежать від випадкових величин (наприклад, розташування шлюзів на карті), існує ймовірність нерівномірного розподілу компонентів на досліджуваній території. Для усунення цього ефекту результати кожного експерименту усереднювались на основі 10 повторних запусків з різними значеннями ініціалізації генератора випадкових чисел

Для оцінки ефективності запропонованої системи в умовах реалістичного сценарію необхідно визначити низку параметрів, обумовлених її проєктною специфікацією. Ці параметри вимагають попередньої параметризації, а також ухвалення низки технічних рішень. Таблиця 3.2 узагальнює ключові значення та конфігурації, що формують базовий сценарій для моделювання.

Таблиця 3.2 – Загальні розміри та параметри, застосовані у моделюванні

Параметр:	**Значення:**
Кількість домашніх пристроїв	7500
Кількість шлюзів	75
Потужність передавання (домашні пристрої)	рівномірно(10...22) дБм, з кроком 1 дБм
Потужність передавання (шлюзи)	14 дБм
Розмір корисного навантаження (домашні пристрої)	12 байт
Розмір корисного навантаження (шлюзи)	7 байт
Фактор розширення (SF)	рівномірно(SF7...SF12)
Смуга пропускання	125 кГц
Коефіцієнт кодування (CR)	4/8
Повідомлень на один пристрій	1
Пакетів на один пристрій	3 (1 оригінальний + 2 повторних)
Інтервал між пакетами	рівномірно(0...300) с

Передусім, кількість користувацьких вузлів у системі становить 7500 одиниць. Це значення відповідає реальній щільності населення на розглянутій території. Потужність передавача для кінцевих пристроїв варіюється в межах від 10 до 22 дБм з кроком 1 дБм. Значення обираються випадковим чином за рівномірним законом розподілу. Такий підхід моделює реальні умови розміщення пристроїв, які можуть суттєво відрізнятись, зокрема через товщину та матеріал стін, висоту розташування пристроїв, внутрішнє планування будівель тощо.

Передані повідомлення в межах системи мають невеликий обсяг навантаження що складає приблизно від 12 до 20 байт. Такий розмір обрано як компроміс між мінімально можливою довжиною кодування заздалегідь визначених повідомлень (які можуть бути представлені одним байтом) та короткими інформативними текстовими повідомленнями, що вміщуються у кілька байтів.

Фактор розширення LoRa SF який використовується кінцевими вузлами, варіюється від SF7 до SF12 і призначається випадковим чином за рівномірним законом розподілу. Такий підхід дозволяє розмістити велику кількість пристроїв

у групах, що не зазнають взаємних колізій під час передачі, навіть без знання про можливі інтерференції між ними. Подібний розподіл використовує властивість ортогональності сигналів, що передаються з різними значеннями SF (як було описано в розділі 1.1.1), що дає змогу забезпечити одночасну передачу повідомлень без взаємних завад.

Такий спосіб призначення SF не вимагає попередніх знань про конкретні умови розгортання мережі чи навколишнє середовище. Водночас, у більш контрольованому сценарії можна було б реалізувати ефективнішу стратегію розподілу значень SF, наприклад, до початку надзвичайної ситуації (тобто до моменту T_0, як зазначено на Рис 3.12), шляхом періодичної передачі службових повідомлень між вузлами та центральним застосунком.

Окрім цього, для зменшення часу перебування в ефірі, параметри LoRa були налаштовані таким чином: ширина смуги пропускання - 125 кГц, коефіцієнт корекції помилок (FEC) - 4/5.

Щодо кількості шлюзів, у дослідженні розглядаються два варіанти: 75 та 10 одиниць. У рамках запропонованого сценарію враховано, що унаслідок одночасної реакції великої кількості користувачів - надсилання повідомлень упродовж короткого проміжку часу - може виникнути перевантаження мережі. Одним зі способів зменшення цього ефекту є розгортання інфраструктури з більш високою щільністю шлюзів порівняно зі стандартними конфігураціями LoRaWAN, де передбачено рівномірніший розподіл трафіку у часі, а один шлюз може забезпечити покриття для понад 10 000 пристроїв [89].

З огляду на це, базовим варіантом для моделювання обрано розгортання 75 шлюзів, що відповідає співвідношенню 100:1 між кількістю кінцевих пристроїв і кількістю шлюзів. Проте, як зазначалося, у разі виникнення надзвичайної ситуації, такої як військові дії або руйнування інфраструктури, лише частина встановлених шлюзів може залишитися в експлуатації. Тому додатково розглядається знижена конфігурація, за якої функціонують лише 10 шлюзів. Такий підхід дає змогу здійснити порівняння між сценаріями з високою та

низькою щільністю мережевої інфраструктури, щоб краще оцінити вплив параметрів мережі на загальну продуктивність системи в різних умовах.

У підсумку, було встановлено значення 3 як типову кількість пакетів, які надсилає кожен користувацький вузол (тобто одне основне повідомлення та два повторних передавання). Згідно зі схемою на Рис 3.12, це означає, що жодна додаткова передача пакету не відбувається до моменту T_{Tx3}. Це значення кількості передач на один вузол є умовно обраним, однак воно також визначає граничний інтервал між взаємодією користувача та завершенням передачі повідомлень - орієнтовно 10 хвилин, що є обґрунтованим часом реагування в умовах надзвичайної ситуації.

Слід зауважити, що симуляційні дослідження, представлені у наступному підрозділі 3.4, містять додатковий аналіз впливу кількості повторних передавань на загальну продуктивність системи. Зазначені налаштування та тимчасові параметри є спільними для всіх експериментів, описаних у розділі 3.4, за винятком випадків, коли прямо вказано про зміну конфігурації (наприклад, за варіації кількості домашніх пристроїв, кількості шлюзів тощо).

3.3.2 Використання програмного фреймворку OMNet++ для моделювання роботи сенсорної мережі

Для аналізу можливостей запропонованої системи було використано симуляційне середовище OMNeT++ [90] - розширювану, модульну та компонентно-орієнтовану бібліотеку на мові C++ разом із відповідним фреймворком. У поєднанні з FLoRa [91], спеціалізованим фреймворком для наскрізного моделювання мереж LoRa, ця платформа забезпечує можливість проведення повномасштабних симуляцій. OMNeT++ є одним із найпоширеніших засобів дискретно-подійного моделювання, що активно використовується у наукових дослідженнях. У свою чергу, FLoRa реалізує повну архітектуру

LoRaWAN [92], а також містить достовірну модель фізичного рівня LoRa, яка базується на результатах попередніх експериментальних досліджень [93].

На Рис 3.11 наведено знімок графічного інтерфейсу симуляційної програми: користувацькі пристрої рівномірно розміщені по території міста, шлюзи розташовані між ними, а мережевий сервер та відповідні модулі маршрутизації розміщено за межами зони дослідження.

Однак для моделювання архітектури розширеної системи (зокрема, з урахуванням функціональності переспрямування пакетів між кінцевими пристроями) були внесені суттєві модифікації в структуру фреймворку FLoRa.

Внесені зміни здебільшого стосуються модуля LoRaNode, який відповідає за моделювання роботи домашніх пристроїв у мережі. Цей модуль містить два вкладені підмодулі: LoRaNodeApp, що керує прикладним рівнем, та LoRaNic, який реалізує функціональність мережевого інтерфейсу для протоколу LoRa.

Підмодуль LoRaNodeApp реалізує логіку переспрямування пакетів між пристроями та дозволяє застосовувати різні алгоритми та стратегії пересилання. Серед них - як найпростіші, наприклад, черга FIFO, так і складніші, контекстно-залежні підходи, що враховують параметри навколишнього середовища, зокрема отримання підтверджень ACK, якість прийому сигналу або часову актуальність повідомлень.

Другий підмодуль, LoRaNic, також є складовим модулем і забезпечує реалізацію функцій рівня MAC (LoRaMAC) та фізичного рівня (LoRaRadio) для пристроїв, що використовують технологію LoRa. На рисунках 3.13-3.15 представлено ієрархію вкладених модулів, як її відображає графічний інтерфейс середовища моделювання OMNeT++.

Домашні пристрої змодельовані в OMNeT++ за допомогою складеного модуля LoRaNode з фреймворку FLoRa (Рис 3.13), який включає кілька вкладених модулів, що відповідають за прикладний та мережевий рівні (Рис 3.14 та Рис 3.15).

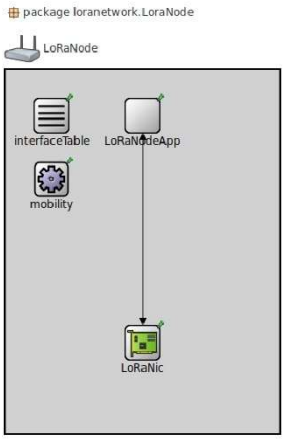

Рис 3.13 – Модуль LoRaNode, який відповідає домашньому пристрою, включає модуль застосунку (LoRaNodeApp) та мережевий модуль (LoRaNic).

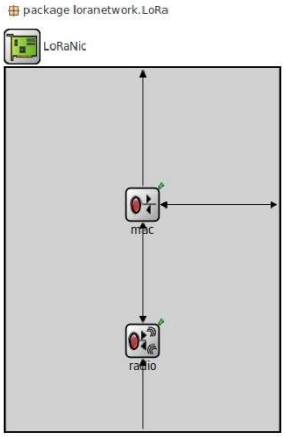

Рис. 3.14 – Модуль LoRaNic, який забезпечує можливості підключення до мережі LoRa, містить MAC-модуль (LoRaMAC) та радіомодуль (LoRaRadio).

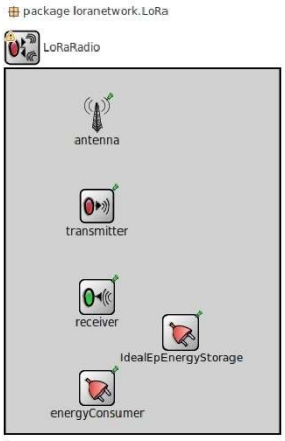

Рис. 3.15 – Модуль LoRaRadio, який реалізує фізичний рівень мережі, містить фізичні компоненти, необхідні для забезпечення зв’язку за технологією LoRa.

У подібний спосіб, модулі шлюзів LoRaWAN, що надаються у складі симуляційного середовища FLoRa, мають вкладену структуру, аналогічну до тієї, яка використовується для кінцевих пристроїв. Така архітектура враховує розширені апаратні можливості шлюзів LoRa, зокрема щодо одночасної демодуляції сигналів з кількох джерел та підтримки більш широких можливостей мережевого з'єднання.

Крім того, модуль NetworkServerApp, який моделює роботу центрального прикладного сервера мережі, також реалізований як складовий модуль і має вкладену структуру, подібну до структури попередніх компонентів. У рамках цього дослідження даний модуль було модифіковано для підтримки обробки пакетів, що були переспрямовані кінцевими пристроями. Це дозволяє коректно ідентифікувати та обробляти дублікатні повідомлення, а також реалізувати функцію відправлення відповідних повідомлень у зворотному напрямку.

3.4 Оцінювання впливу змін параметрів роботи для базової та удосконаленої сенсорної мережі

У цьому підрозділі представлено та проаналізовано результати комп'ютерного моделювання системи, реалізованої на основі модифікованої архітектури LoRa, що розглядається у межах даного дослідження. Симуляції виконувалися із застосуванням середовища OMNeT++, із використанням різних конфігурацій системи. На першому етапі було змодельовано базову архітектуру, що відповідає специфікації LoRaWAN та передбачає лише однонаправлену передачу пакетів від кінцевих пристроїв (домашніх вузлів) безпосередньо до шлюзів, без механізмів підтвердження доставки або ретрансляції.

Подальший аналіз мав на меті оцінити здатність базової архітектури протистояти викликам критичного сценарію - зокрема, надзвичайної ситуації, що призводить до масового одночасного трафіку з боку тисяч користувачів у короткий проміжок часу. У наступних симуляціях було досліджено ефективність

удосконаленої версії системи, яка, на відміну від базової, підтримує двосторонній зв’язок із підтвердженням доставки, а також реалізує механізм пересилання пакетів між домашніми пристроями. Такі модифікації суттєво підвищують надійність обміну повідомленнями між користувачами у випадку відмови інфраструктурних компонентів.

Останній етап дослідження було присвячено аналізу чутливості системи до змін ключових параметрів, які було визначено у підрозділі 3.3.1. Зокрема, розглянуто вплив таких факторів, як кількість шлюзів, параметри радіопередачі, рівень повторних передач та інші аспекти, що визначають загальну здатність системи підтримувати обмін даними в умовах критичних навантажень.

3.4.1 Дослідження роботи базової сенсорної мережі

Результати та аналітичні висновки, представлені у цьому підрозділі, слугують наближеним оцінюванням спроможності базової архітектури системи забезпечити ефективний обмін повідомленнями у критичних умовах, що виникають внаслідок надзвичайної ситуації. Зокрема, досліджено масштабованість системи, що передбачає аналіз її функціонування при різній кількості кінцевих пристроїв (домашніх вузлів), а також вплив часткових відмов інфраструктури шлюзів на загальну доступність зв’язку для користувачів.

Окрему увагу приділено впливу фактору розширення спектру SF - одного з ключових параметрів радіопередачі в LoRa - на продуктивність системи. Це дозволяє надалі провести обґрунтоване порівняння базової архітектури з модифікованим варіантом системи, що передбачає механізми підвищення надійності, зокрема підтримку ретрансляції пакетів та підтвердження доставки повідомлень.

Масштабованість сенсорної мережі

Щільність кінцевих пристроїв є ключовим чинником, що визначає масштабованість запропонованої комунікаційної архітектури, у той час, як другорядний, але також вагомий вплив справляє щільність розміщення шлюзів. У сукупності ці параметри формують критичні обмеження, притаманні архітектурі LoRaWAN, насамперед у контексті перевантаження мережі. Згідно з моделлю середовища, викладеною у підрозділі 3.3 на прикладі району міста Ірпінь, щільність кінцевих пристроїв у конфігурації «один пристрій на домогосподарство» становить приблизно 7500 вузлів або близько 2124 вузлів/км².

Однак варто зазначити, що аналогічні сценарії в інших регіонах можуть характеризуватися суттєво вищою або нижчою густотою населення, що прямо впливатиме на результати функціонування системи. У зв’язку з цим, у даному підрозділі здійснюється моделювання масштабованості системи шляхом варіювання кількості кінцевих пристроїв, при незмінних інших параметрах (географічні розміри, кількість шлюзів, параметри модуляції LoRa тощо). Такий підхід дозволяє виявити граничні межі працездатності архітектури та обґрунтувати доцільність майбутнього застосування алгоритмічних і технічних засобів оптимізації, спрямованих на підвищення ефективності системи в умовах зростаючого навантаження.

Рис. 3.16 та Рис. 3.17 демонструють здатність користувацьких пристроїв успішно передавати щонайменше один, два або три LoRa-пакети до прикладного рівня системи, що є важливим критерієм оцінки ефективності зв’язку в умовах надзвичайної ситуації. На графіках зображується відсоток користувацьких вузлів, які успішно передали ≥1, ≥2 або 3 LoRa-пакети до центрального застосунку, залежно від кількості користувацьких вузлів у системі (в межах від 100 до 18 000). Важливо зазначити що на графіках вісь x позначається як квадрат 1 і відповідає значенням: $1E2 = 1 \times 10^2$, $1E3 = 1 \times 10^3$, $1E4 = 1 \times 10^4$

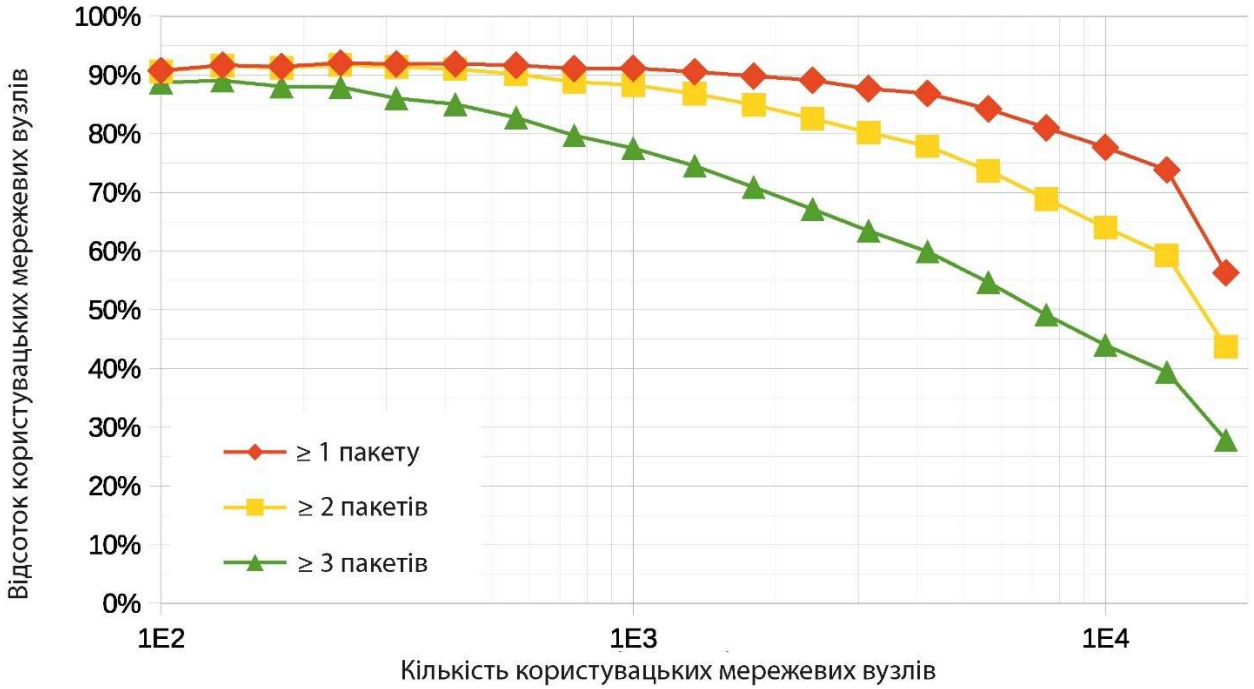

Рис 3.16 – Відсоток користувацьких вузлів, які успішно передали ≥1, ≥2 або 3 LoRa-пакети до центрального застосунку у повноцінному режимі зі 75 шлюзами

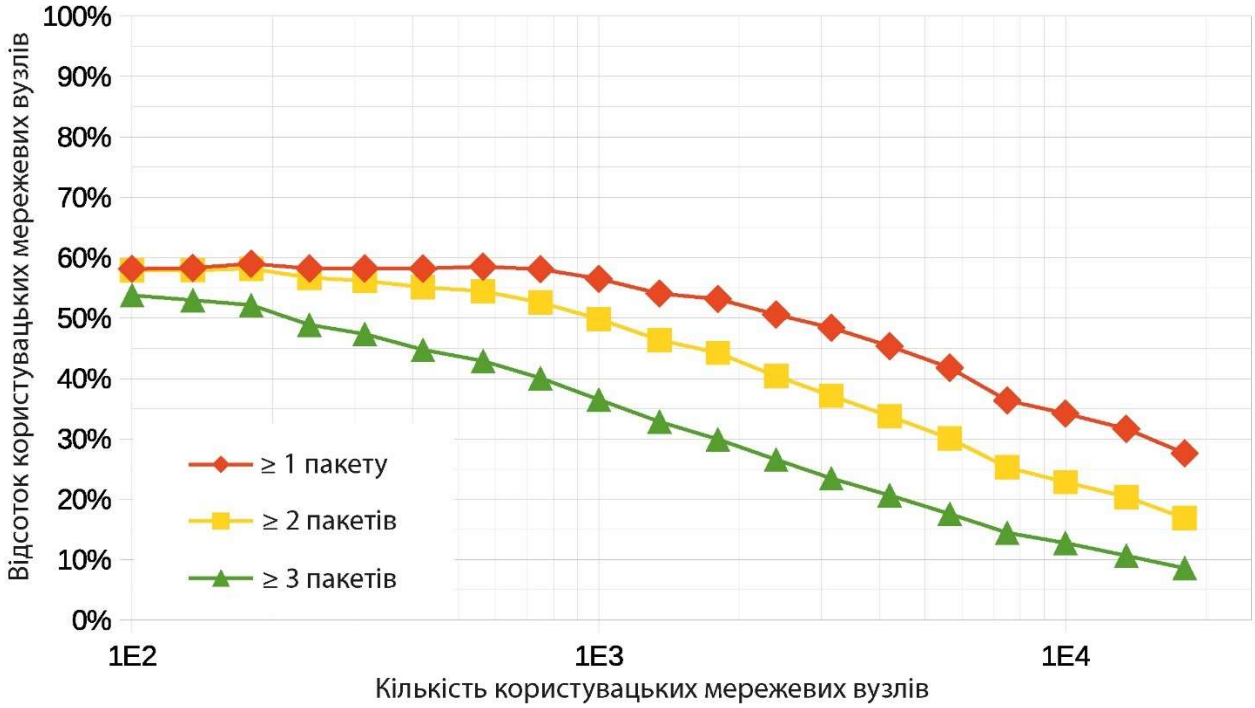

Рис 3.17 – Відсоток користувацьких вузлів, які успішно передали ≥1, ≥2 або 3 LoRa-пакети до центрального застосунку у аварійному режимі зі 10 функціонуючими шлюзами

У першому випадку (Рис 3.16) розглядається сценарій з високою щільністю шлюзів, тобто повністю функціональною інфраструктурою з 75 шлюзами, що забезпечують передачу даних від кінцевих пристроїв. За цих умов система демонструє високі показники надійності: майже всі пристрої можуть успішно передати хоча б один пакет, а значна частина - усі три заплановані пакети, що свідчить про високий рівень пропускної здатності та низький рівень колізій у мережі

У другому випадку (Рис 3.17) проаналізовано зменшену інфраструктуру зв'язку, де внаслідок надзвичайної ситуації в експлуатації залишаються лише 10 шлюзів, що імітує пошкодження мережі. За таких умов відсоток пристроїв, здатних здійснити хоча б одну успішну передачу, суттєво знижується, що підкреслює чутливість системи до втрати вузлів інфраструктури та обмежену масштабованість при низькій надлишковості мережевих ресурсів.

Помаранчева лінія на Рис 3.16 ілюструє відсоток користувацьких вузлів, які успішно передали щонайменше один пакет. У діапазоні від 100 до 1000 вузлів цей показник залишається практично незмінним на рівні 90 %, що свідчить про високу надійність передачі даних при помірному навантаженні. Проте зі збільшенням кількості вузлів вище кількох тисяч спостерігається поступове зниження успішності, яке різко погіршується після межі ≈10 000 пристроїв. Це пов'язано з різким зростанням ймовірності колізій, що унеможливлює ефективну багаторазову передачу повідомлень.

Жовта та зелена лінії відповідають частці вузлів, які змогли передати щонайменше два або три пакети відповідно. Ці лінії демонструють подібну динаміку, проте із більш вираженим спадом. Вочевидь, зростання навантаження на мережу критично впливає на повторні передачі, що особливо важливо для систем зв'язку в надзвичайних ситуаціях, де надійність доставлення кількох повідомлень від кожного пристрою є бажаною.

У випадку низької щільності шлюзів (Рис 3.17), графік демонструє аналогічні тренди, але з суттєво гіршими показниками. Навіть за невеликої

кількості вузлів, відсоток успішних передач помітно нижчий, а максимальний показник досягає лише ≈ 60 %. Це наочно демонструє, що зменшення кількості шлюзів у разі відмов або пошкодження значною мірою погіршує можливість абонентів зв’язатися з центральною системою.

Важливою особливістю обох графіків на Рис 3.16 та Рис 3.17 є спостереження, що хоча деякі вузли взагалі не можуть встановити зв’язок із центральним застосунком, інші - здатні здійснити передачу двічі або навіть тричі. Це свідчить про нерівномірний розподіл можливостей доступу до мережі серед кінцевих пристроїв, що є серйозною проблемою з точки зору ефективного використання мережевих ресурсів.

Зокрема, вузли, яким вдалося передати повідомлення, можуть продовжувати здійснювати повторні передачі вже успішно доставленої інформації, що призводить до зайвого використання радіоефірного часу. Це своєю чергою створює перешкоди для вузлів, які ще не змогли надіслати свої повідомлення, зменшуючи ймовірність їх успішної передачі через колізії або перевантаження шлюзів.

Одним із можливих підходів до розв'язання цієї проблеми є запровадження механізму підтвердження доставки повідомлення у вигляді відповідного зворотного пакета підтвердження ACK, який надсилається центральним застосунком у відповідь на успішну передачу даних. Отримання такого підтвердження дає змогу вузлу припинити подальші ретрансляції, тим самим зменшуючи навантаження на мережу та покращуючи її пропускну здатність.

У наступному розділі 4.3.2 така концепція ACK повідомлень буде детально розглядатися як частина двосторонньої комунікації, що є технічно реалізованою у межах специфікацій LoRaWAN. Автори аналізують ефективність запровадження ACK-повідомлень та вивчають компроміси, пов’язані з їх використанням - зокрема, затримки, збільшення кількості переданих пакетів і енергоспоживання.

Отже, масштабованість системи залежить не лише від кількості кінцевих пристроїв і шлюзів (тобто їхньої щільності на км²), а й від швидкості, з якою ці пристрої здійснюють передачу повідомлень. У ситуаціях, подібних до змодельованого сценарію надзвичайної ситуації, коли велика кількість вузлів одночасно намагається передати дані в обмежений проміжок часу, пропускна здатність технології радіозв'язку LoRa може виявитися недостатньою для забезпечення стійкої та масштабованої роботи мережі. Це особливо актуально для середовищ з високою щільністю розміщення пристроїв, де ризик перевантаження мережі суттєво зростає. Таким чином, ефективність системи суттєво обумовлена не лише технічними характеристиками радіотехнології, але й параметрами її впровадження та сценаріями її використання.

Вплив щільності шлюзів та відмов інфраструктури на ефективність роботи сенсорної мережі

У межах архітектури LoRaWAN передача даних від домашніх пристроїв до прикладного рівня на мережевому сервері здійснюється через один або кілька доступних шлюзів. Тому кількість шлюзів, які охоплюють певну територію, прямо впливає на ймовірність успішного прийому пакетів. Інтуїтивно зрозуміло, що підвищення щільності розміщення шлюзів має позитивно впливати на загальний показник успішної доставки пакетів PDR, адже це збільшує шанси, що хоча б один зі шлюзів отримає сигнал із достатнім співвідношенням сигнал/шум SNR для його коректної демодуляції та подальшої ретрансляції. Інакше кажучи, у мережі стає більше "вух", здатних "почути" трансляцію повідомлень.

Проте розгортання шлюзової інфраструктури зазвичай пов'язане зі значними витратами, тож їх кількість повинна бути обґрунтована й оптимально спланована. Це створює важливу дилему: з одного боку, якщо задано певний цільовий рівень продуктивності (наприклад, 50 %, 95 % або 99 % успішних доставок), слід встановлювати лише ту кількість шлюзів, яка здатна забезпечити

цей рівень. З іншого боку, в умовах надзвичайної ситуації, що розглядається в межах цього дослідження, не можна гарантувати безперебійне функціонування всієї інфраструктури - тому слід очікувати певного зниження якості обслуговування.

З огляду на це, у даному розділі було змінено вихідний (базовий) сценарій: для моделювання використовувалися варіанти системи з різною кількістю шлюзів - від надмірної кількості (1000 одиниць) до крайньо обмеженого випадку (всього один шлюз). Метою такого аналізу є виявлення зв’язку між щільністю розгортання шлюзів і показниками ефективності системи, а також оцінка доцільності вибору 75 шлюзів як базового варіанту і визначення, наскільки критичним буде зниження їх кількості у разі деградації інфраструктури.

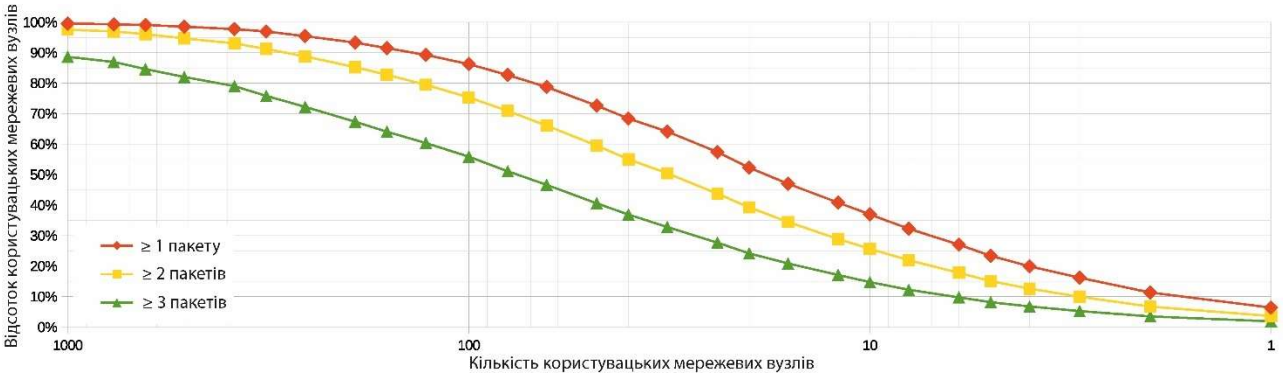

Рис 3.18 – Відсоток користувацьких вузлів, які успішно передали ≥1, ≥2 або 3 LoRa-пакети до центрального застосунку, залежно від кількості доступних у системі шлюзів (у діапазоні від 1000 до 1).

На Рис 3.18 показано, який відсоток із 7500 користувацьких пристроїв здатен успішно передати дані до центрального прикладного сервера, а також скільки разів ці передачі можуть відбутися (не менше одного, двох або трьох повідомлень), залежно від кількості розгорнутих шлюзів, що приймають LoRa-пакети. Звернімо увагу, що вісь X на графіку має логарифмічну шкалу, що дозволяє наочно відобразити динаміку при великих розбіжностях у чисельності шлюзів.

Згідно з отриманими результатами, які підтверджують висновки з підрозділу 3.4.1.1, чим більше шлюзів розгорнуто, тим вищий відсоток користувачів зможе успішно передати свої повідомлення. Особливо різкий приріст ефективності спостерігається при малій кількості шлюзів: навіть незначне збільшення їх числа істотно впливає на ймовірність успішної доставки пакетів. Це добре видно у правій частині графіка.

Натомість у центральній частині графіка, де кількість шлюзів уже наближається до оптимального значення, подальше нарощування їх кількості забезпечує лише незначне покращення показника успішної передачі. Таким чином, спостерігається ефект спадної віддачі: що більше шлюзів уже розгорнуто, то менший виграш у продуктивності забезпечує кожен додатковий вузол. Це свідчить про необхідність ретельного планування інфраструктури з урахуванням доцільності витрат та очікуваного рівня надійності.

Хоча результати, подані на Рис 3.18, демонструють, що збільшення кількості шлюзів підвищує ймовірність успішної доставки повідомлень до прикладного сервера, така стратегія має суттєві обмеження. По-перше, у міру зростання кількості шлюзів (сотні або навіть тисяча), приріст показників успішності стає мінімальним. Наприклад, використання приблизно 100 шлюзів забезпечує успішну передачу повідомлень від 86 % користувачів, а збільшення цієї кількості до 300 дозволяє досягти лише ≈ 96 % покриття. Це свідчить про зменшення ефективності кожного додаткового шлюзу після досягнення певного рівня насиченості мережі.

По-друге, економічна доцільність такої масштабної інфраструктури викликає сумніви. Один шлюз у середньому у 20 разів дорожчий за кінцевий пристрій користувача, а його розгортання вимагає значно більше часу, технічних ресурсів та подальших витрат на обслуговування та енергозабезпечення. Враховуючи ці фактори, надмірне збільшення кількості шлюзів не є оптимальним шляхом покращення продуктивності системи. Замість цього

доцільним є пошук балансованого рішення між щільністю інфраструктури та її вартісною ефективністю.

Визначити оптимальну кількість шлюзів складно, оскільки на це впливають як технічні аспекти, так і економічні обмеження. Проте для ухвалення рішень можна застосувати певні статистичні підходи. Наприклад, у базовому сценарії, який передбачає розгортання 75 шлюзів, приблизно 80 % користувацьких пристроїв мають змогу хоча б один раз надіслати повідомлення до прикладного сервера. Цей показник, з одного боку, може бути достатнім для формування загального уявлення про ситуацію у зоні надзвичайної події й орієнтаційної оцінки рівня ураження територій. З іншого боку, це означає, що значна частина користувачів залишиться поза межами системи, особливо якщо деякі шлюзи вийдуть з ладу.

Крім того, зважаючи на те, що після надзвичайної події (наприклад, через руйнування будівель) певна частина інфраструктури може стати недоступною, доцільним є розгляд сценаріїв із надмірним резервуванням. Такий підхід як цілеспрямоване перевищення мінімально необхідної кількості шлюзів може виступати як стратегія зменшення ризику втрати зв'язку у критичних зонах та забезпечення більшої стійкості системи до непередбачуваних відмов.

Вплив на роботу мережі від використання різних факторів розширення спектру SF

Фактор розширення спектра SF є ключовим параметром у технології LoRa, оскільки саме він визначає щільність спектра модуляції з розширенням частот CSS. У спрощеному вигляді SF контролює баланс між дальністю зв’язку, швидкістю передачі даних і енергоспоживанням.

Вищі значення SF (наприклад, SF11 або SF12) забезпечують кращу чутливість прийому та більший радіус дії, що дозволяє передавати дані на більші відстані. Однак це досягається ціною зниження швидкості передачі та

збільшення енергоспоживання, а також збільшення часу перебування сигналу в ефірі. Натомість нижчі значення SF (наприклад, SF7 або SF8) забезпечують менший час в ефірі, вищу пропускну здатність і нижче енергоспоживання, але мають менший радіус дії через знижену стійкість до шуму (тобто потребу в більшому SNR).

У попередніх сценаріях конфігурація пристроїв передбачала випадкове використання значень SF від 7 до 12, з рівномірним розподілом імовірностей. Такий підхід дозволяє ефективно використовувати ортогональність сигналів із різними SF - передавання від кількох вузлів із різними SF можуть співіснувати одночасно без взаємних перешкод, і всі сигнали можуть бути успішно демодульовані одним шлюзом.

Однак вибір SF впливає не лише на окремий пристрій, а й на ефективність усієї системи. Наприклад, вузол із високим SF може охопити більшу зону покриття, підвищуючи ймовірність успішної доставки своїх пакетів. Водночас збільшений час передачі в ефірі підвищує ризик колізій, особливо якщо інші вузли використовують той самий SF. Отже, хоча вибір SF може бути вигідним з погляду індивідуального пристрою, це може негативно позначитися на глобальній продуктивності системи, особливо за високої щільності вузлів.

У цьому експерименті було змінено значення SF, які використовують користувацькі вузли для передавання даних до шлюзів. Метою було визначити, яке саме значення SF є найпридатнішим для заданої системної конфігурації - як для випадку з високою щільністю шлюзів, так і з низькою.

Спочатку систему було змодельовано таким чином, щоб усі вузли використовували однакове значення SF - від SF7 до SF12. Далі було визначено усі можливі комбінації SF - наприклад, діапазони SF7-SF12, SF7-SF11, SF7-SF10 тощо. Для кожної комбінації здійснювалась симуляція, у якій вузли випадковим чином обирали SF зі вказаного діапазону, причому всі значення мали однакову ймовірність вибору.

Такий підхід дозволяє оцінити, наскільки ефективно працює система при різних стратегічних налаштуваннях SF, і зрозуміти, чи певні значення або комбінації SF призводять до підвищення пропускної здатності або зменшення колізій, зокрема, в умовах масової взаємодії користувачів після надзвичайної ситуації. Це дослідження також має практичну цінність при проєктуванні конфігурацій IoT-мереж у сценаріях з обмеженим числом шлюзів або великим навантаженням.

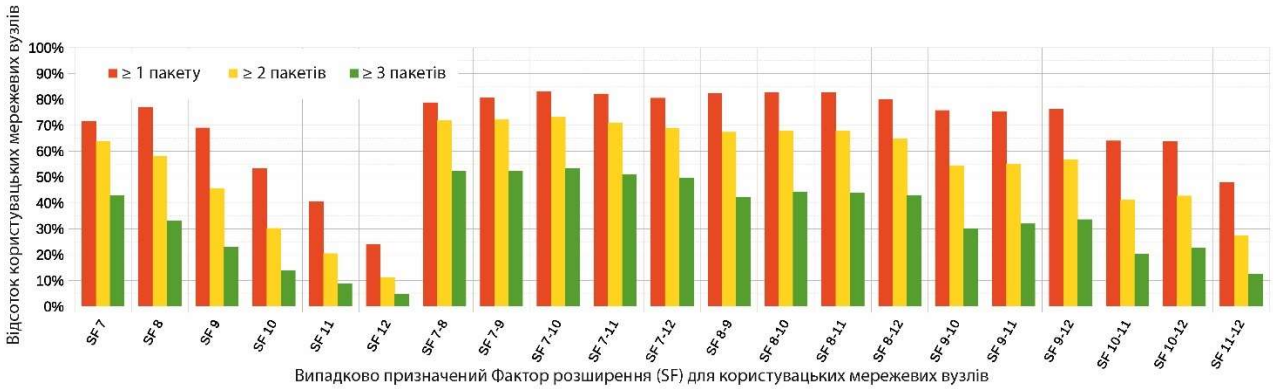

Рис 3.19 – Відсоток користувацьких вузлів, які успішно передали ≥1, ≥2 або 3 LoRa-пакети до центрального застосунку, залежно від значень SF, випадково призначених вузлам за рівномірним розподілом у повноцінному режимі зі 75 шлюзами

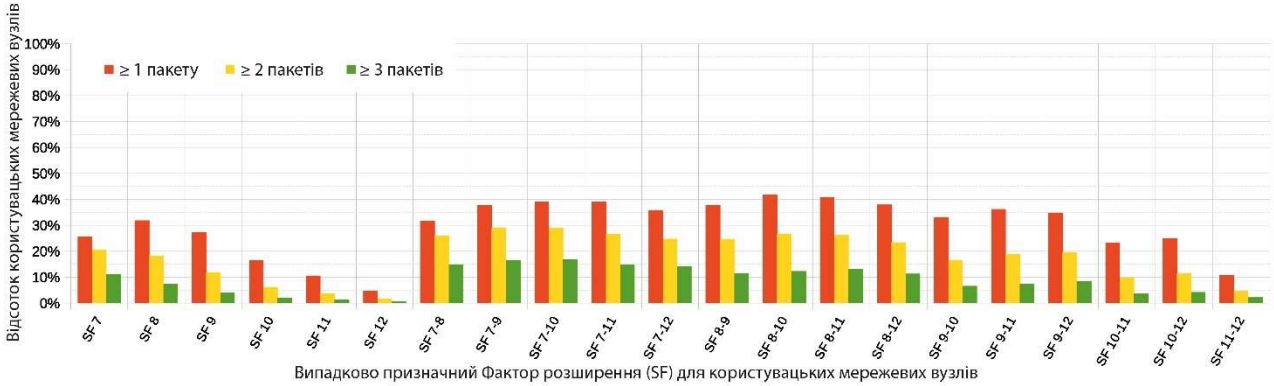

Рис 3.20 – Відсоток користувацьких вузлів, які успішно передали ≥1, ≥2 або 3 LoRa-пакети до центрального застосунку, залежно від значень SF, випадково призначених вузлам за рівномірним розподілом у аварійному режимі зі 10 функціонуючими шлюзами

На рисунку 3.19 та рисунку 3.20 наведено відсоток користувацьких вузлів, які змогли успішно передати повідомлення до прикладного рівня щонайменше один, два або три рази для всіх можливих комбінацій факторів розширення (SF). Рис 3.19 демонструє результати для сценарію з високою щільністю шлюзів, у свою чергу Рис 3.20 зображає результати для низької щільності шлюзів.

Аналіз результатів показує, що вибір менших значень SF (зокрема SF7 до SF9) - які забезпечують меншу дальність, але і коротший час перебування пакета в ефірі, дає суттєво кращі результати порівняно з більшими SF (наприклад, SF11 або SF12).

Це пов’язано з кількома факторами:

1. Менший SF дозволяє швидше передавати дані, зменшуючи загальне навантаження в ефірі;

2. Коротший час передавання зменшує ймовірність колізій, що є критично важливим у сценаріях масової взаємодії користувачів;

3. Незважаючи на меншу дальність, висока щільність шлюзів компенсує цю втрату, забезпечуючи стабільний прийом повідомлень навіть при низькому SF.

Натомість використання великих SF значно збільшує час передачі, що веде до вищої ймовірності колізій, особливо при великій кількості активних вузлів. Це знижує ефективність передачі навіть попри те, що великі SF забезпечують кращу чутливість прийому.

Рис 4.19 та Рис 4.20 також ілюструє вплив паралельного використання різних факторів розширення SF на ефективність мережі. Загалом комбінації з двох або більше SF демонструють кращі результати, ніж використання одного SF. Наприклад, сумісне використання SF7 і SF8 є ефективнішим, ніж застосування будь-якого з них окремо.

Найширша комбінація (від SF7 до SF12), яка, як зазначено в розділі 3.3.1, використовувалась у базовій конфігурації, не забезпечує найвищих показників

ефективності. Це вказує, що включення високих SF (наприклад, SF11, SF12) негативно впливає на продуктивність.

Причини цього криються в особливостях модуляції:

1. Збільшення значення SF подвоює час перебування пакета в ефірі, що збільшує ймовірність колізій;

2. Коли всі SF обираються з однаковою ймовірністю (рівномірний розподіл), вузли з більшими SF мають суттєво гірші умови передачі, що знижує загальний відсоток успішних доставок.

Водночас, виключення високих SF (наприклад, 11–12) з комбінації, або використання зміщеного розподілу на користь менших SF, суттєво покращує пропускну здатність системи та зменшує затримки.

Для покращення продуктивності системи доцільно не тільки дозволити одночасне використання кількох SF, але й ретельно налаштувати їх розподіл, з урахуванням співвідношення «час в ефірі - рівень колізій», щоб зменшити перевантаження каналу та підвищити надійність передачі.

3.4.2 Дослідження роботи удосконаленої сенсорної мережі з використанням механізму ACK

У системі зв’язку, описаній у попередніх розділах, існує принципове обмеження - односпрямований потік даних. Інформація передається винятково від користувацьких вузлів до центрального застосунку, що, безумовно, дозволяє екстреним службам отримувати важливі відомості для координації дій. Проте відсутність зворотного зв’язку для користувачів обмежує можливість інтерактивної взаємодії з системою та знижує її ефективність у кризових умовах.

Впровадження відповідей у вигляді пакетів-підтверджень (ACK) від серверної частини до домашніх пристроїв дозволяє вирішити кілька важливих задач:

1. Зменшення кількості непотрібних повторних передач, адже користувач отримує підтвердження про успішне доставлення повідомлення;

2. Підвищення довіри та залученості користувачів, оскільки система надає їм зворотну інформацію;

3. Можливість використовувати ACK-пакети для передачі повідомлень від інших користувачів (наприклад, від друзів чи родини), завдяки чому формується двостороння взаємодія навіть у складних умовах обмеженого зв’язку.

Таким чином, підтримка двостороннього обміну дозволяє не лише знизити навантаження на мережу, а й розширити функціональні можливості системи у напрямі парадигми "Інтернету людей" (IoP), у якій громадяни відіграють активну роль не лише як споживачі, але і як постачальники інформації. Це має критичне значення в умовах надзвичайних ситуацій, де своєчасність і взаємодія є запорукою ефективної допомоги та зниження людських втрат.

Підтвердження у зворотному напрямку (низхідні ACK-пакети) вже передбачені архітектурою LoRaWAN, хоча вони рідко застосовуються в батарейних пристроях через необхідність економії енергії. Незважаючи на це, їх реалізація є відносно простою й може істотно зменшити загальну кількість переданих пакетів у мережі. Це, у свою чергу, знижує ймовірність колізій під час передачі та підвищує ймовірність успішної доставки повідомлень більшою кількістю користувацьких вузлів.

Однак, перед впровадженням такого механізму необхідно врахувати два ключові аспекти:

1. ACK-пакети також займають радіоканал, конкуруючи з повідомленнями у висхідному напрямку, і таким чином можуть знижувати ефективність передавання від вузлів до шлюзів.

2. Прийом ACK-пакетів не гарантується - вони також піддаються впливу колізій та перешкод у радіоефірі, що може унеможливити належне спрацьовування зворотного механізму.

Для того, щоб оцінити вплив ACK-повідомлень на продуктивність системи, було реалізовано простий механізм підтвердження, і проведено порівняльний аналіз трьох сценаріїв:

1. Без використання ACK-пакетів (базовий варіант);

2. З надсиланням ACK-повідомлень, але без реакції з боку користувацьких вузлів (тобто вони все одно продовжують передавати повідомлення незалежно від підтвердження);

3. З ACK-пакетами та зупинкою ретрансляцій після отримання підтвердження.

Цей аналіз дозволяє визначити не лише технічну доцільність впровадження ACK-механізму, але й баланс між покращенням продуктивності та додатковим навантаженням на радіоканал, що є особливо важливим в умовах надзвичайної ситуації.

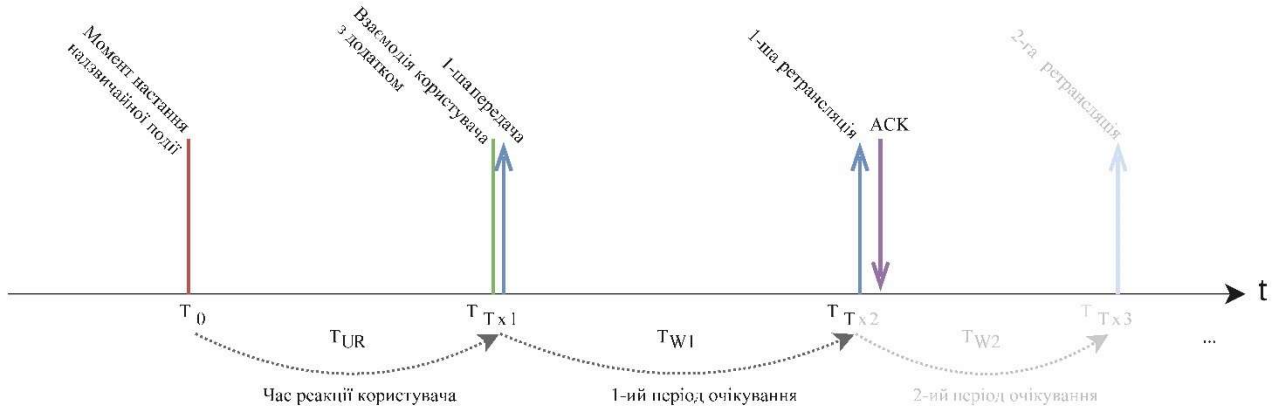

Рис 3.21 – Часовий графік активності користувацьких вузлів після настання надзвичайної ситуації, включаючи пакети підтвердження ACK

На Рис 3.21 зображено графік подій та дій, які відбуваються на одному з користувацьких вузлів після активації механізму зворотного підтвердження (ACK). У порівнянні з базовим сценарієм (див. Рис 3.12), тепер на вузол може надійти низхідний ACK-пакет від центрального застосунку. Залежно від конфігурації, вузол після отримання такого підтвердження припиняє подальші

ретрансляції, що дозволяє зекономити ефірний час і забезпечити більшу пропускну здатність мережі для інших учасників.

У проведених симуляціях ACK-пакети мають той самий обсяг (12 байт), що й пакети, передані у висхідному напрямку з домашніх пристроїв. Такий підхід дозволяє імітувати можливість включення в ACK не лише підтвердження, а й корисного вмісту, наприклад, повідомлень від інших користувачів. Це відкриває шлях до реалізації двосторонньої комунікації між цивільними, і таким чином наближує систему до парадигми Інтернету людей IoP, де користувачі не лише джерела даних, але й активні учасники інформаційного обміну.

Серед різноманітних експериментів, проведених у межах базового сценарію, описаного в попередньому розділі, у цьому підрозділі було вирішено зосередитися на впливі використання ACK-повідомлень при різних значеннях коефіцієнта розширення спектра SF.

Цей фокус дослідження обрано з огляду на критичну роль, яку SF відіграє у продуктивності LoRa-комунікацій. Порівнюючи результати із та без використання ACK-повідомлень для різних значень SF (від SF7 до SF12), необхідно з’ясувати:

1. Чи покращується загальний рівень успішної доставки повідомлень завдяки зворотному підтвердженню?

2. Наскільки зменшується кількість непотрібних ретрансляцій, які перевантажують ефір?

3. Чи існує оптимальне значення SF, при якому ACK-повідомлення приносять найбільшу користь, не створюючи додаткових колізій або перевантаження каналу?

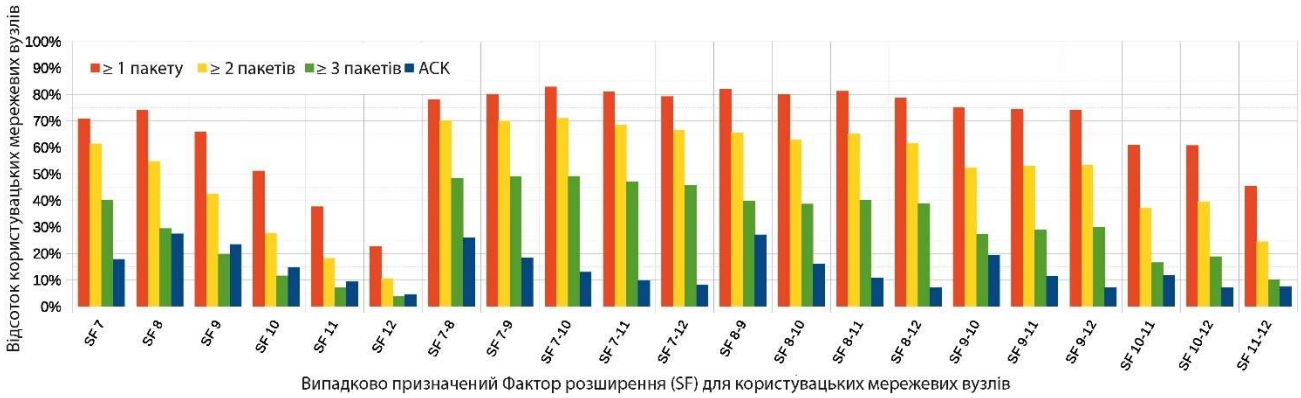

Рис. 3.22 – Відсоток користувацьких вузлів, які успішно передали ≥1, ≥2 або 3 пакети до центрального застосунку та отримали від нього підтвердження (ACK), залежно від значень SF випадково призначених за рівномірним розподілом, у сценарії повноцінного режиму зі 75 шлюзами

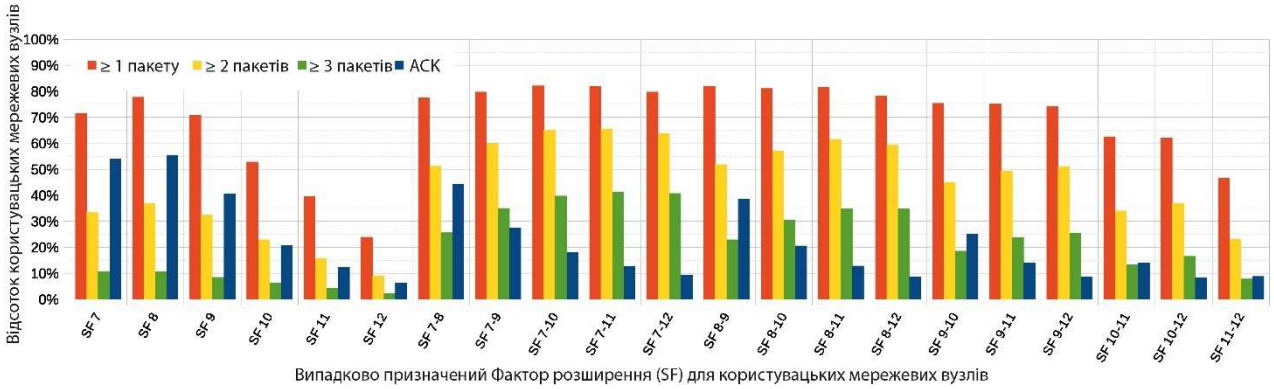

Рис. 3.23 – Відсоток користувацьких вузлів, які успішно передали ≥1, ≥2 або 3 пакети до центрального застосунку та отримали від нього підтвердження (ACK), залежно від значень SF випадково призначених за рівномірним розподілом, у аварійному режимі зі 10 функціонуючими шлюзами.

На Рис. 3.22 та Рис. 3.23 представлено результати симуляцій, що демонструють вплив використання підтверджень доставки (ACK) на продуктивність системи передачі повідомлень у надзвичайних ситуаціях. Графік на Рис. 3.22 ілюструє сценарій, у якому ACK дозволені, однак пристрої продовжують повторно передавати повідомлення незалежно від отримання підтвердження. У такому випадку спостерігається незначне зниження продуктивності (на ≈3 %) порівняно з базовим варіантом без ACK через

додаткове навантаження в ефірі. Проте така схема вперше дозволяє реалізувати механізм зворотного зв’язку - деякі вузли отримують підтвердження про успішну доставку, що є важливим для користувачів у критичних умовах. У свою чергу, графік Рис. 3.23 демонструє ситуацію, коли вузли припиняють повторні передачі після отримання ACK. У цьому випадку не лише зростає загальна кількість успішних передач хоча б одного повідомлення, але й суттєво зменшується кількість надлишкових передач, що дозволяє звільнити ефірний простір і збільшити відсоток отриманих ACK. Це особливо важливо з огляду на обмежену пропускну здатність LoRa у сценаріях з масовим одночасним трафіком. Таким чином, запровадження ACK з механізмом припинення ретрансляцій дозволяє оптимізувати використання радіоканалу, знизити колізії та забезпечити очікуваний користувачами зворотний зв’язок. Додатково встановлено, що використання менших коефіцієнтів розширення спектра (SF7-SF9) забезпечує кращу ефективність як для передачі повідомлень, так і для прийому ACK, завдяки меншому часу перебування в ефірі. В цілому, результати свідчать, що застосування двосторонньої комунікації зі зворотним зв’язком не лише покращує технічні характеристики системи, а й сприяє підвищенню довіри користувачів та відповідає концепції "Інтернету людей", у якій громадяни виступають як активні учасники обміну інформацією в надзвичайних умовах.

Пересилання мережевих пакетів між вузлами користувачів

Аналіз, проведений у підрозділі 3.4.1, засвідчив, що за умов моделювання розглянутого сценарію базова архітектура LoRaWAN не здатна забезпечити надійний канал зв’язку для всіх користувачів. Особливо це стосується ситуацій, коли частина інфраструктури стає недоступною внаслідок надзвичайної ситуації, що призводить до втрати можливості доступу до системи значною частиною вузлів. Утім, впровадження підтверджень доставки (ACK-повідомлень) і реалізація двосторонньої комунікації (як було розглянуто в підрозділі 3.4.1.2)

дозволяє не лише забезпечити користувачів зворотним зв’язком, але й виступає в ролі механізму управління перевантаженням мережі. Окрім цього, поява зворотного каналу відкриває перспективу для побудови більш складних архітектур системи, що відповідають вимогам до сучасних рішень в умовах надзвичайних ситуацій та сприяють підвищенню її стійкості і функціональності.

Спираючись на результати попередніх експериментів, у цьому підрозділі до функціональних можливостей користувацьких вузлів додається здатність ретранслювати пакети інших вузлів у напрямку до шлюзів. Основною метою такого вдосконалення є підвищення відсотка користувачів, що успішно передають свої повідомлення до центрального застосунку. Відтепер кожен користувацький вузол під час періодів очікування перед черговими передаваннями (T_{W1}, T_{W2} тощо, як описано в підрозділі 4.5.1 і проілюстровано на Рис. 3.12), переходить у режим прослуховування і зберігає у буфер отримані пакети від сусідніх вузлів. Надалі, під час власної передачі, частина цих збережених повідомлень також передається. Такий підхід дозволяє вузлам, які перебувають на периферії системи або взагалі поза зоною дії шлюзів, отримати додаткову можливість доставити свої дані до центрального застосунку. Це особливо актуально за наявності механізмів контролю перевантажень, таких як використання ACK-повідомлень, розглянутих у попередньому підрозділі. Варто підкреслити, що запропоноване розширення виходить за межі стандартної архітектури LoRaWAN, яка за своєю природою не підтримує безпосередню взаємодію між вузлами, хоча апаратні можливості LoRa-радіо це дозволяють.

Для оцінки впливу механізму ретрансляції повідомлень інших вузлів на загальну ефективність системи було проведено моделювання базового сценарію із додаванням 7500 користувацьких вузлів, здатних до ретрансляції, при двох варіантах щільності розміщення шлюзів - високій (75 одиниць) та низькій (10 одиниць). У всіх варіантах було активовано надсилання підтверджень (ACK-пакетів) від центрального застосунку до домашніх пристроїв. Кожен користувацький вузол спочатку надсилає свої повідомлення (до трьох разів),

допоки не буде отримано підтвердження. У цей період вузли також зберігають у буфер усі повідомлення, отримані від сусідніх пристроїв, за умови, що приймання можливе згідно з фізичними властивостями технології LoRa (достатній рівень сигналу, відсутність колізій тощо). Тільки після завершення власної передачі або отримання ACK-повідомлення вузол починає ретранслювати частину збережених повідомлень інших пристроїв.

Для кількісної оцінки ефективності такої стратегії було виконано серію симуляцій, у межах яких вузлам дозволялося ретранслювати від 0 (для контрольного порівняння) до 10 пакетів. Вибір повідомлень з буфера здійснювався випадковим чином, без урахування додаткових параметрів, таких як час прибуття, адреса джерела або якість прийому. Такий підхід дозволяє ізольовано дослідити вплив лише самої кількості ретрансляцій на продуктивність системи, уникаючи складності, пов'язаної з реалізацією просунутих алгоритмів прийняття рішень на вузлах.

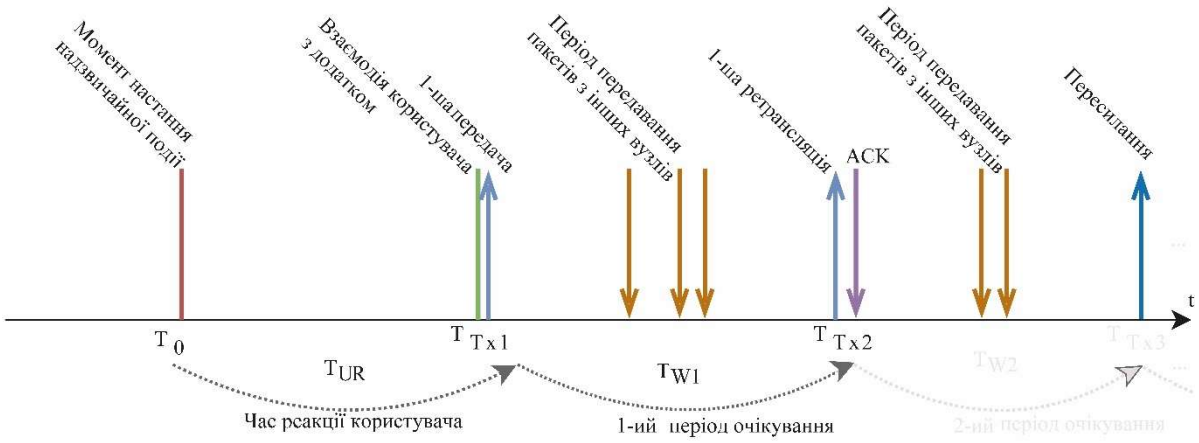

Рис. 3.24 – Часовий графік активності користувацького вузла після надзвичайної ситуації, включаючи ACK-повідомлення у низхідному напрямку та пересилання пакетів.

На Рис. 3.24 представлено розклад подій та дій, що виконуються на одному з користувацьких вузлів у контексті розширеного сценарію з можливістю ретрансляції та використанням ACK-повідомлень. Порівняно з базовою моделлю

(див. Рис. 3.12), тепер у системі реалізовано зворотний зв’язок: у разі успішного отримання низхідного ACK повідомлення від центрального застосунку, вузол припиняє подальші повторні передачі свого повідомлення. Це дозволяє значно скоротити час ефірної активності вузла, зменшуючи ймовірність колізій і вивільняючи ресурси ефіру для інших вузлів мережі. Таким чином, додавання підтверджень (ACK) не лише покращує взаємодію з кінцевим користувачем, а й сприяє підвищенню загальної ефективності комунікацій у системі.

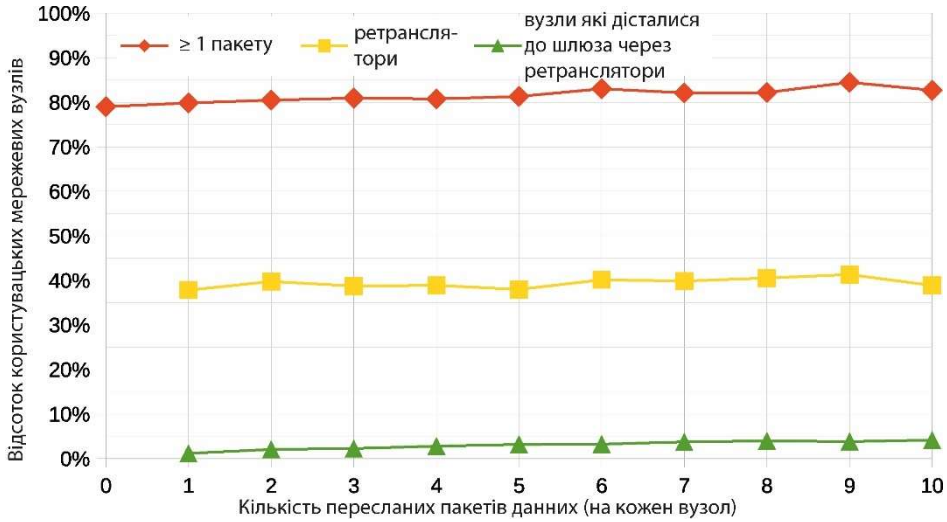

Рис 3.25 – Відсоток користувацьких вузлів, які успішно передали ≥1 пакет до центрального застосунку у повноцінному режимі зі 75 шлюзами

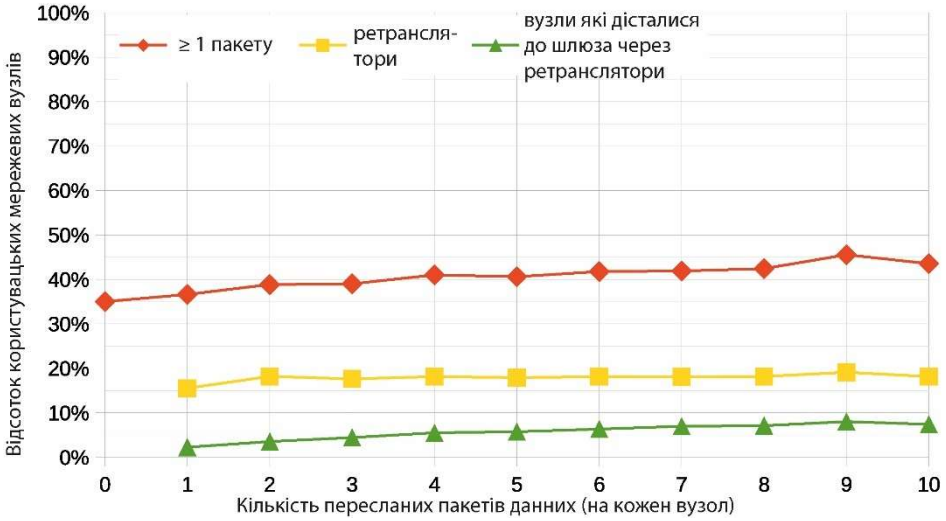

Рис 3.26 – Відсоток користувацьких вузлів, які успішно передали ≥1 пакет до центрального застосунку у обмеженому режимі з 10 шлюзами

На Рис 3.25 та Рис 3.26 помаранчевим позначено відсоток користувацьких вузлів, які успішно передали ≥1 пакет до центрального застосунку, жовтим позначено відсоток вузлів що працюють як ретранслятори повідомлень інших вузлів, зеленим позначено відсоток вузлів які досягають центрального застосунку лише через ретрансляцію.

Представлені графіки демонструють, що така функціональність має позитивний ефект на загальну продуктивність системи: кількість пристроїв, які успішно передають повідомлення до центрального додатка, зростає у порівнянні зі сценарієм без ретрансляції. Наприклад, на графіку (Рис 3.25), що відповідає конфігурації з високою щільністю шлюзів, відсоток успішно переданих повідомлень зріс з 79 % до 84,5 %. У випадку з низькою щільністю шлюзів (Рис 3.26) цей показник збільшився з 35 % до 45,5 %.

Крім того, графіки свідчать про поступове зростання частки вузлів, які змогли встановити зв’язок із центральним додатком виключно завдяки ретрансляції - тобто за участі сусідніх пристроїв. Без механізму ретрансляції ці вузли були б повністю ізольованими від системи, тому запропонований підхід істотно підвищує стійкість мережі.

Разом з тим, існує недолік: ретрансльовані повідомлення потрапляють до системи з певною затримкою, оскільки передаються після основної сесії передачі повідомлень. Відповідно, інформація, яка міститься в таких пакетах, досягає центрального додатка із запізненням.

3.4.2.1 Чутливість мережі до зміни параметрів роботи

У процесі моделювання та визначення базової архітектури системи було встановлено низку ключових параметрів проєктування, зокрема таких, як розмір корисного навантаження пакетів або інтервал між повторними передаваннями. Обрані значення є обґрунтованими для умов розглянутого сценарію (наприклад, розмір корисного навантаження не може дорівнювати нулю чи перевищувати

максимальний розмір пакета, допустимий у мережі (MTU), а час між повторними передаваннями має забезпечувати баланс між швидкістю реагування та уникненням перевантаження мережі).

Водночас не виключено використання альтернативних конфігурацій. З огляду на це, у цьому підрозділі виконується аналіз чутливості архітектури системи до зміни зазначених параметрів. Мета полягає в тому, щоб глибше зрозуміти, яким чином варіація цих налаштувань впливає на ефективність функціонування системи та її здатність забезпечувати користувачів можливістю комунікації для отримання відомостей про безпеку членів родини та близьких у ситуаціях надзвичайного характеру.

Вплив збільшення кількості дозволених повторних пересилань пакетів

Як було докладно описано в підрозділі 3.3, після взаємодії користувача з пристроєм, вузол-користувач виконує три передавання повідомлення. Перше передавання відбувається одразу після взаємодії, а два наступні - після випадкових інтервалів очікування (T_{W1}.та T_{W2}, як зображено на Рис. 3.12). Повторні передавання позитивно впливають на загальну ефективність системи, оскільки збільшують імовірність успішної доставки повідомлень до центрального застосунку. Водночас, вони супроводжуються низкою витрат, зокрема: збільшенням часу перебування сигналу в ефірі, навантаженням на мережу, зростанням ризику колізій та перешкод, а також підвищеним споживанням енергії (останній аспект у цій роботі не розглядається).

Відсутність зворотного каналу у вигляді повідомлень-підтверджень (ACK) зі сторони застосунку значно спрощує архітектуру системи, однак позбавляє вузли-користувачі змоги з’ясувати, чи потребуються подальші повторні передавання. З метою дослідження впливу кількості повторних передавань на ефективність роботи системи, у цьому експерименті було змінено параметр

кількості таких передавань для всіх вузлів. Зокрема, було змодельовано ситуації, у яких кожен вузол надсилає від 1 до 20 повідомлень (тобто з 0 до 19 повторних передавань). Аналіз виконано щодо ключової метрики - частки унікальних вузлів, які успішно доставили принаймні одне повідомлення до центрального застосунку.

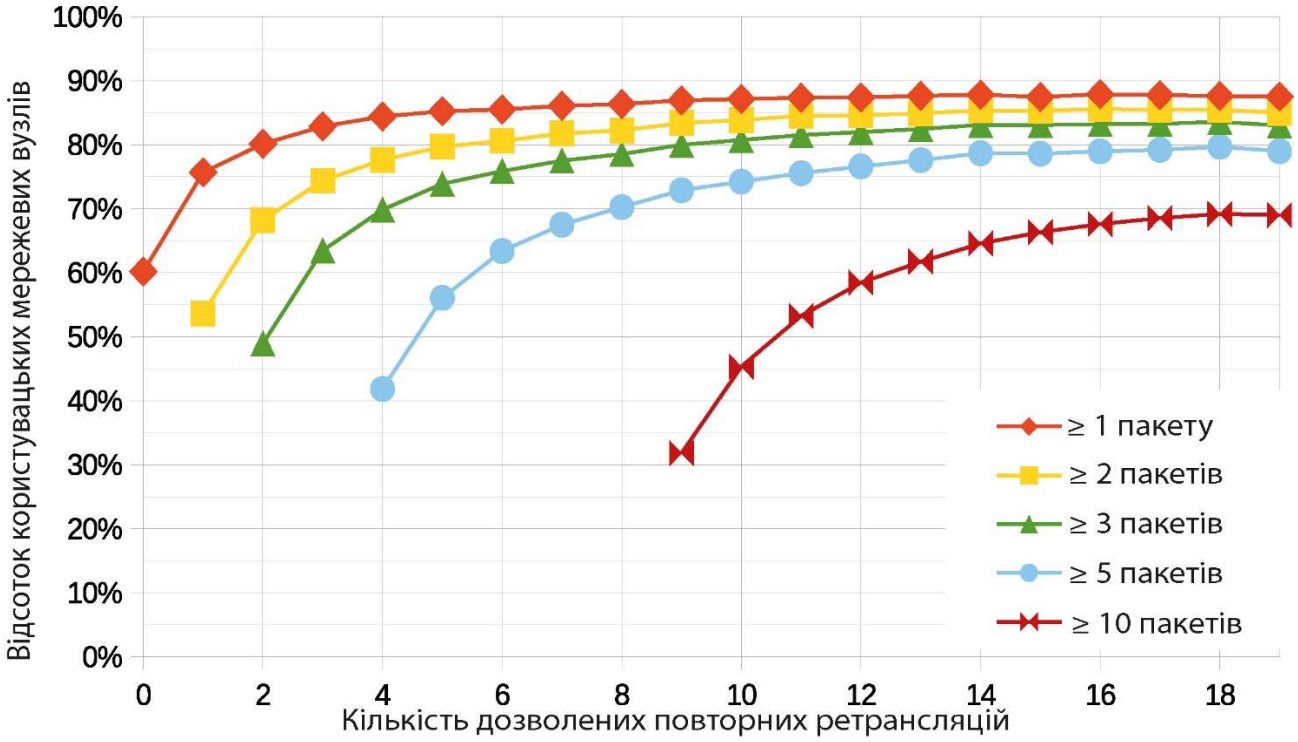

Рис. 3.27 – Відсоток користувацьких вузлів, які успішно передали ≥1, ≥2, ≥3, ≥5 або ≥10 LoRa-пакетів до центрального застосунку, залежно від кількості дозволених ретрансляцій на вузол, для нормального сценарію роботи з 75 шлюзами

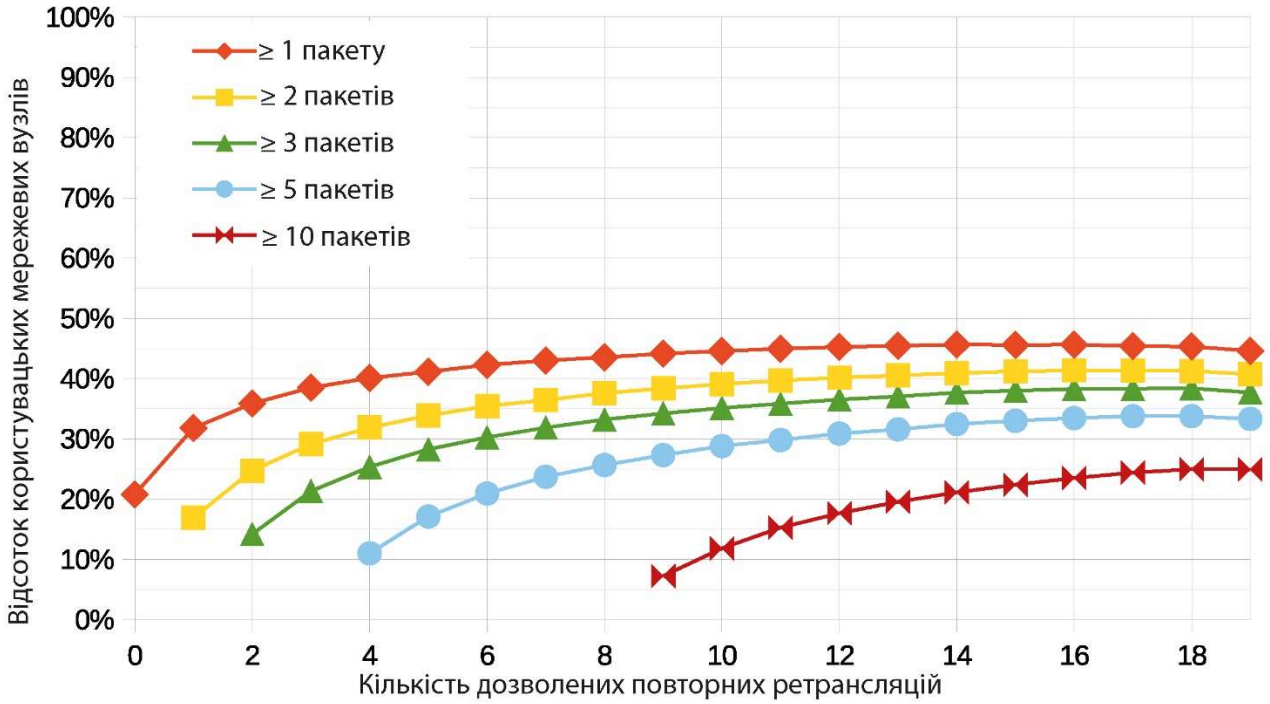

Рис. 3.28 – Відсоток користувацьких вузлів, які успішно передали ≥1, ≥2, ≥3, ≥5 або ≥10 LoRa-пакетів до центрального застосунку, залежно від кількості дозволених ретрансляцій на вузол, для аварійного сценарію з 10 шлюзами.

На Рис. 3.27 та Рис. 3.28 зображено залежність частки вузлів-користувачів, які змогли успішно передати не менше ніж 1, 2, 3, 5 або 10 повідомлень у напрямку до центрального застосунку, від кількості дозволених повторних передавань для кожного вузла. Отримані результати однозначно демонструють: чим більше дозволених повторних передавань, тим більша частка вузлів досягає центрального застосунку з хоча б одним повідомленням. Проте зростання цієї метрики має асимптотичний характер і не досягає ідеального значення у 100 %. Подібна насичувальна поведінка спостерігається як для сценарію з високою щільністю шлюзів (Рис. 3.27), так і для сценарію з низькою щільністю (Рис. 3.28), де кількість активних шлюзів становить відповідно 75 і 10 одиниць.

Це свідчить про те, що із збільшенням кількості передавань проблема нерівномірного доступу до каналу залишається: частина вузлів майже завжди досягає мети, передаючи всі повідомлення, тоді як інші - не можуть цього зробити, незалежно від кількості спроб. Так само як і у базовому сценарії, це

означає нераціональне використання часу перебування в ефірі та пропускної здатності мережі. Отже, просте збільшення кількості повторних передавань не вирішує проблему збалансованого доступу до ресурсу.

Система, запропонована в дослідженні, має на меті забезпечити механізм зв'язку для населення у перший критичний період після надзвичайної ситуації, зокрема протягом першої години після події. Отже, безконтрольне багаторазове повторення передавання повідомлень вузлами-користувачами не лише призводить до нераціонального використання радіоефіру, пропускної здатності мережі та енергоресурсів, а й зумовлює надмірне зростання затримок у доставці повідомлень. Враховуючи, що інтервали між передаваннями визначаються як рівномірно розподілена випадкова величина в межах від 0 до 300 секунд, можна оцінити, що за період у 3600 секунд (тобто одна година) можливо не більше ніж 12 передавань: $\frac{3600\text{с.}}{\max[0,300]c.} = 12$. Таким чином, якщо дозволити понад 12 повторних передавань, існує ймовірність, що симуляція завершиться до того, як деякі вузли встигнуть передати усі свої повідомлення.

Цей ефект добре простежується на Рис. 3.27, де видно тенденцію до легкого зниження частки успішних передавань. Для візуалізації цієї особливості на діаграмах застосовано червонуватий фон, що сигналізує про потенційні втрати ефективності системи за умов надмірної кількості передавань

Вплив часу очікування між повторними передачами пакетів

Як зазначено в розділі 4.1, після взаємодії користувача домашній пристрій надсилає повідомлення до трьох разів. Перше передавання ініціюється одразу після взаємодії користувача з пристроєм, тоді як два наступні повторні передавання (ретрансляції) здійснюються з певною затримкою - після інтервалів очікування T_{W1}.та T_{W2}, як зображено на Рис. 3.12.

Інтервал очікування між передаваннями пакетів створює компроміс між швидкістю реагування системи (тобто частотою надсилання повідомлень вузлами) та надійністю передавання (тобто ймовірністю виникнення колізій у радіоканалі). У певних ситуаціях може бути пріоритетним отримання швидких, хоча й менш точних даних - з метою якнайшвидшої побудови первинного плану реагування на наслідки надзвичайної ситуації. Натомість в інших випадках доцільніше надати перевагу більш надійній передачі, яка забезпечує повільніший, але стабільний і достовірний канал зв'язку для кінцевих користувачів.

Система має на меті забезпечити можливість обміну повідомленнями між населенням у перші години після надзвичайної ситуації, зокрема протягом першої години після її виникнення. Тому дозволяти кінцевим вузлам передавати повідомлення необмежену кількість разів є недоцільним: це призводить до зайвого використання ефірного часу, перевантаження мережі та надмірного споживання енергії. Крім того, з часом значна частина повідомлень почне надходити із суттєвою затримкою щодо моменту виникнення події.

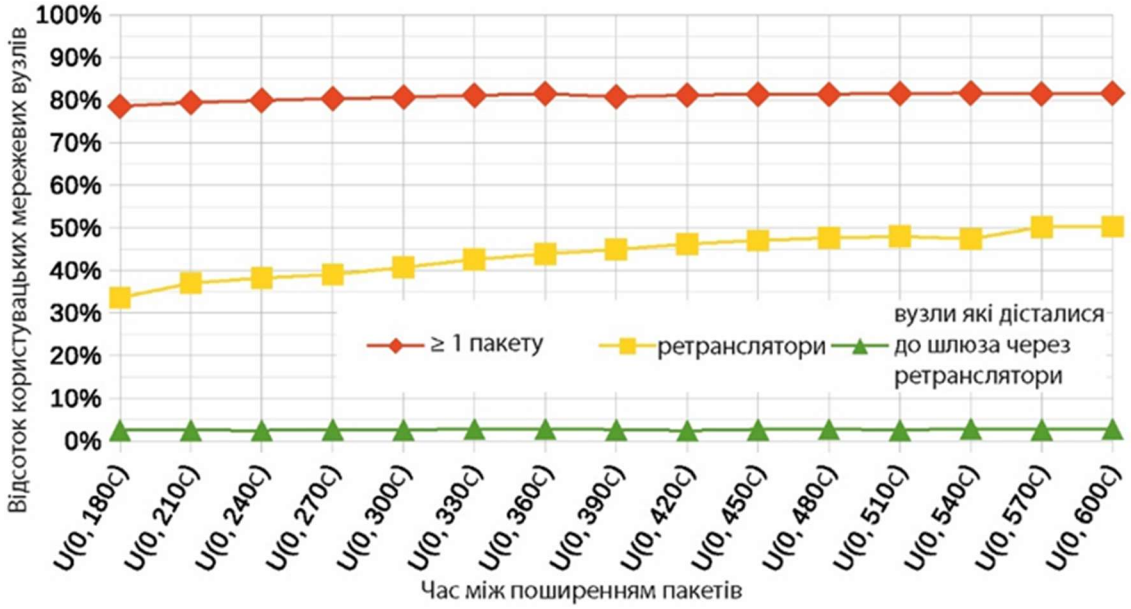

Рис. 3.29 – Відсоток користувацьких домашніх пристроїв, які успішно передали ≥1 пакет до центрального застосунку залежно від часу очікування між предачами з високою щільністю шлюзів у 75 шт.

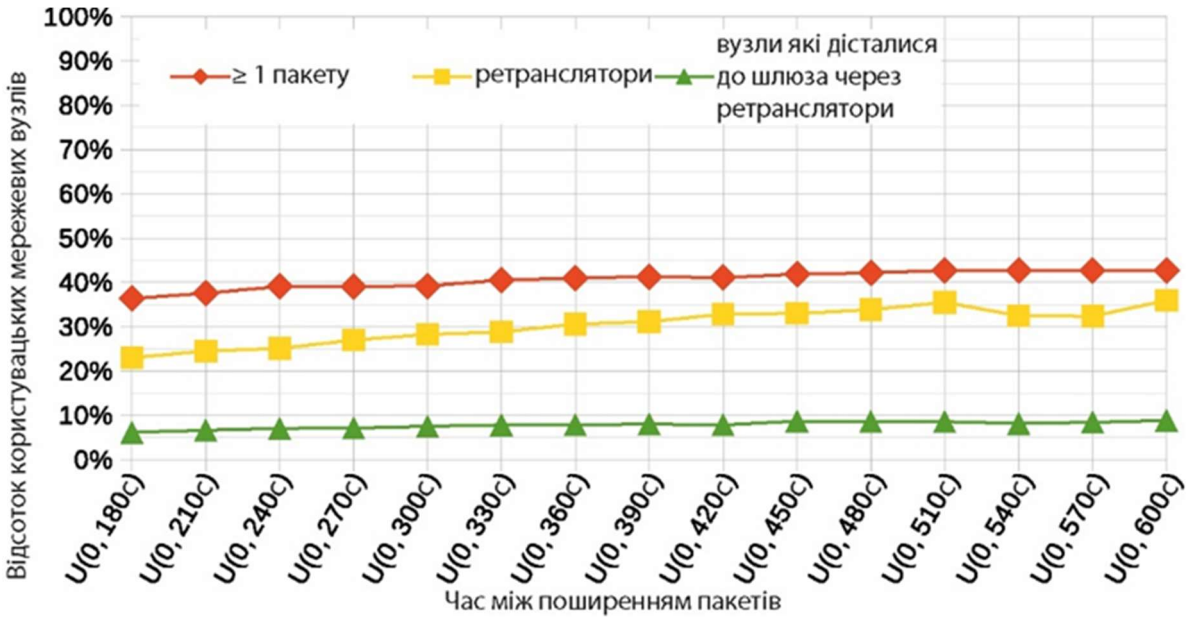

Рис. 3.30 – Відсоток користувацьких домашніх пристроїв, які успішно передали ≥1 пакет до центрального застосунку залежно від часу очікування між предачами з низькою щільністю шлюзів у 10 шт.

На Рис 3.29 та Рис 3.30 помаранчевим позначено відсоток користувацьких вузлів, які успішно передали ≥1 пакет до центрального застосунку, жовтим позначено відсоток вузлів що працюють як ретранслятори повідомлень інших вузлів, зеленим позначено відсоток вузлів які досягають центрального застосунку лише через ретрансляцію.

У моделюванні зображеного на Рис 3.29 та Рис 3.30 використано рівномірно розподілену випадкову змінну для затримки між передаваннями в межах від 0 до 300 секунд. За умови загальної тривалості симуляції 3600 секунд, це означає, що за весь час вузол теоретично може встигнути здійснити не більше 12 передавань (3600 / 300 = 12). Отже, якщо дозволити більше ніж 12 повторних передавань, деякі вузли можуть не встигнути надіслати всі свої пакети до завершення симуляції. Це спостерігається на Рис. 3.30, де показано тенденцію до зниження рівня успішності передачі повідомлень.

Вплив розміру корисного навантаження в мережевому пакеті

Під час визначення параметрів системи, було встановлено фіксований розмір корисного навантаження у 12 байт. Це значення використовувалося у всіх попередніх симуляціях і становить компроміс між мінімалістичними попередньо заданими повідомленнями (які можна закодувати одним байтом) та короткими текстовими повідомленнями, які займають кілька байтів. Окрім фактичних даних, що передаються користувачами, пакети містять також службову інформацію, зокрема заголовки канального рівня (MAC), біти кодування LoRa та інші поля, які залишаються незмінними незалежно від дій користувача. У подальших симуляціях було проведено аналіз впливу зміни розміру корисного навантаження на здатність домашніх пристроїв успішно передавати пакети.

Такий аналіз є важливим, оскільки здатність системи ефективно передавати повідомлення довільного вмісту та розміру є критичною умовою для забезпечення інформаційних потреб користувачів у межах парадигми «Інтернету людей» IoP в умовах надзвичайної ситуації. З цією метою архітектуру LoRaMoto було протестовано з різними розмірами корисного навантаження, щоб оцінити вплив цього параметра на ефективність роботи системи.

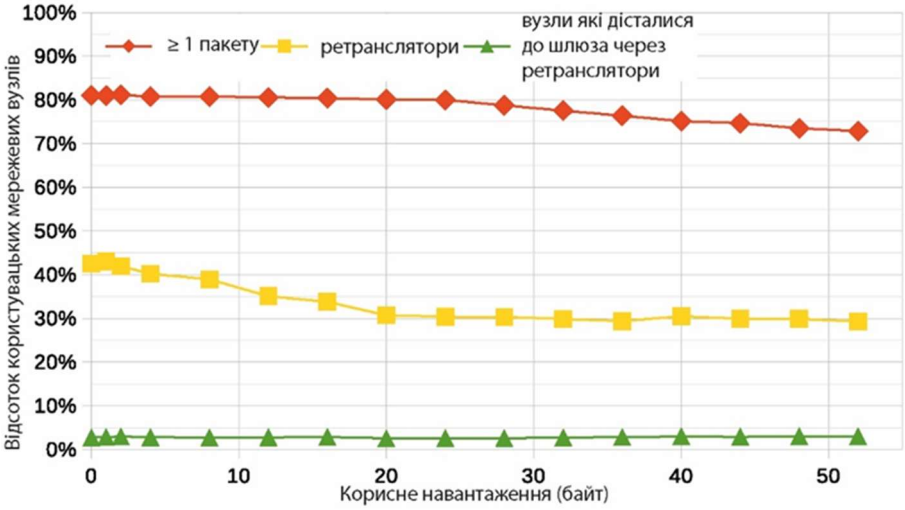

Рис. 3.31 – Відсоток користувацьких домашніх пристроїв, які успішно передали ≥1 пакеу до центрального застосунку залежно від розміру корисного навантаження, у режимі роботи з 75 шлюзами.

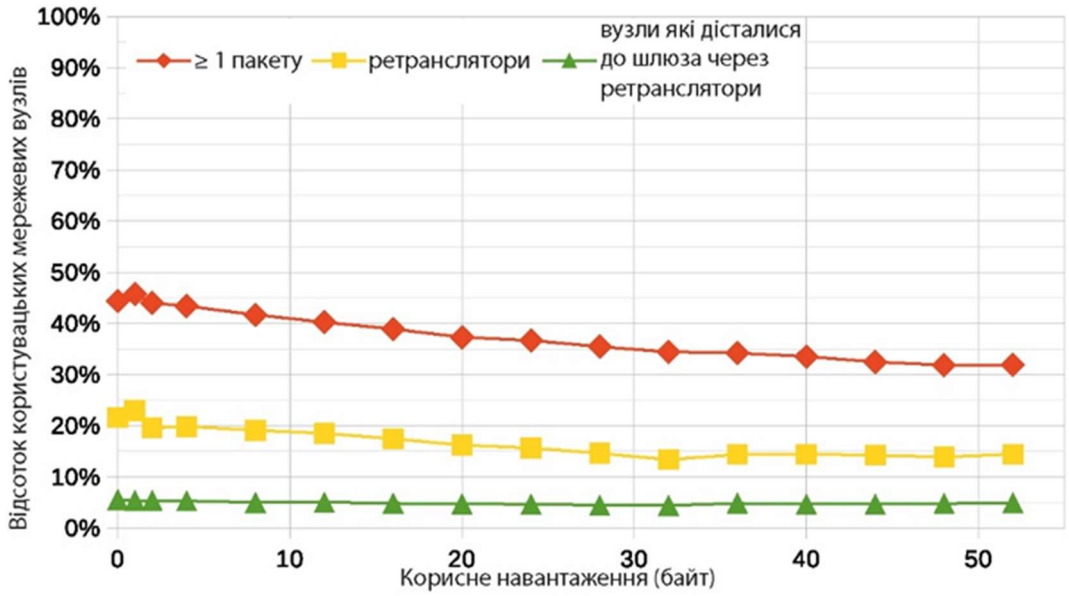

Рис. 3.32 – Відсоток користувацьких домашніх пристроїв, які успішно передали ≥1 пакеу до центрального застосунку залежно від розміру корисного навантаження, у аварійному режимі роботи з 10 шлюзами.

На Рис. 3.31 та Рис. 3.32 показано відсоток домашніх пристроїв, які можуть успішно зв’язатися із застосунком, залежно від розміру корисного навантаження повідомлення: від 0 байт (тобто порожнє повідомлення, що містить лише заголовки та інші службові поля) до 51 байта (максимальний розмір навантаження, який підтримується всіма значеннями SF).

Графіки демонструють, що при високій щільності шлюзів розмір повідомлення має незначний вплив на частку пристроїв, які можуть встановити зв’язок із центральним застосунком (різниця між крайніми значеннями складає приблизно 5 %). Натомість у сценаріях з низькою щільністю шлюзів вплив розміру повідомлення є набагато суттєвішим: при вже низькому загальному рівні зв’язку, різниця між мінімальним і максимальним навантаженням призводить до погіршення продуктивності приблизно на 15 %.

Таким чином, прийом і пересилання пакетів домашніми пристроями від сусідніх вузлів значно більш чутливі до розміру повідомлення у випадках, коли кількість активних шлюзів є обмеженою. Окрім цього, навіть за незмінної

кількості шлюзів, зі збільшенням розміру повідомлень зменшується ймовірність того, що домашні пристрої братимуть участь у пересиланні пакетів у системі.

Цей ефект слід враховувати користувачам системи під час створення власних повідомлень: довші повідомлення можуть спричинити затримки в комунікації порівняно з коротшими.

Висновки до розділу 3

У третьому розділі дисертаційної роботи було проведено симуляційне моделювання роботи сенсорної мережі з використанням розробленого методу прийняття рішень щодо вибору її конфігурації. Досліджено вплив ключових параметрів мережі: кількості шлюзів, масштабів мережі, способів маршрутизації та використання підтверджень доставки (ACK) – на показники продуктивності мережі в умовах обмеженого радіопокриття та високого навантаження.

Проаналізовано типові сценарії, що моделюють роботу мережі в середовищі з обмеженим доступом до інфраструктури а також ефективність різних стратегій покращення доступності мережі.

Проведено порівняльний аналіз конфігурацій базової сенсорної мережі та модифікованих варіантів, що включають багаторазові ретрансляції, механізм підтверджень доставки ACK та функціонал пересилання пакетів між кінцевими вузлами. Розглянуто вплив масштабування на показники успішності доставки пакетів даних та охоплення мережі.

Визначено що традиційна архітектура демонструє суттєві обмеження при великій кількості вузлів, тоді як включення функцій повторної передачі й пересилання дозволяє зменшити втрати пакетів і покращити стійкість мережі без збільшення кількості шлюзів.

Комплексне врахування спектральних параметрів сигналу дозволяє підвищити відсоток успішно переданих повідомлень у сенсорній мережі за рахунок використання службових повідомлень що підтверджують отримання

пакету даних, ефект від використання повідомлень що підтверджують отримання пакету даних особливо помітний у режимі роботи мережі з недостатньою кількістю шлюзів де відсоток успішно переданих повідомлень збільшується в середньому на 40%.

Удосконалено метод взаємодії вузлів сенсорної мережі, який за рахунок використання розробленої моделі мультипротокольної сенсорної мережі оскільки успішність передачі пакетів у сенсорній мережі істотно залежить від кількості шлюзів задіяних у топології.

Отримані результати підтверджують ефективність розробленого методу та демонструють здатність адаптуватис конфігурацію мережі до змін середовища.

4 РОЗРОБКА ПРОТОКОЛУ САМООРГАНІЗАЦІЇ З МНОЖИННИМ ВИКОРИСТАННЯМ ФАКТОРУ РОЗШИРЕННЯ МОДУЛЯЦІЇ

Використання автономної технології LoRa для побудови сенсорних мереж, незалежно від архітектури LoRaWAN, розглядалося різними дослідниками. У більшості випадків такі дослідження зосереджуються на вивченні окремих аспектів продуктивності або на вирішенні конкретної задачі нприклад пов’язаної з розгортанням систем у складних умовах експлуатації. Лише незначна частина робіт підходить до теми дослідження з широкої та узагальнюючої перспективи.

У цьому розділі розроблено, проаналізовано та обговорено мінімалістичний протокол маршрутизації на основі векторної відстані для самоорганізованих сеносорних мереж побудованих на базі технології LoRa. Запропонований протокол має просту архітектуру, що дозволяє його реалізацію на мікроконтролерах з обмеженими обчислювальними ресурсами. При цьому він враховує особливості радіотехнології LoRa для обчислення оптимальних маршрутів між парами вузлів. Основну увагу приділено фактору розширення модуляції SF, який визначає компроміс між дальністю передавання сигналу та швидкістю обміну даними. Застосування різних значень SF генерує квазіортогональні сигнали що за певних умов дозволяє здійснювати одночасні передавання на одній частоті без взаємних завад. Крім того, в роботі було використано функцію CAD яку підтримують сучасні LoRa-чипи, для виявлення активності в ефірі та автоматичного налаштування приймача на відповідний SF вхідного пакета.

У роботі також запропоновано нову метрику - час в ефірі (ToA), яка враховує можливість сенсорної мережі LoRa здійснювати одночасні передавання на одній частоті без взаємних завад. Ця метрика визначає найоптимальніший маршрут між двома вузлами, базуючись на сумарному часі передавання даних (тобто загальному часу перебування в ефірі) вздовж усього шляху. Для оцінки ефективності запропонованого протоколу самоорганізації, а

також для порівняння ToA з іншими популярними метриками, було використано програмний фреймворк FLoRa у поєднанні з симулятором OMNeT++ .

Експерименти проводилися в конфігураціях мереж, що включали до 64 вузлів. У межах моделювання проаналізовано основні показники продуктивності, зокрема коефіцієнт доставки пакетів PDR, пропускну здатність, затримку, тощо. Результати дозволили порівняти запропоновану метрику з іншими відомими стратегіями маршрутизації.

4.1 Попередні дослідження автоматичного визначення та застосування множинного фактору розширення модуляції

Як зазначено в розділі 1.2.2, LoRa-радіочипи поділяються на дві основні категорії: одноканальні трансивери для кінцевих вузлів та багатоканальні цифрові чипи базового рівня, призначені для шлюзів LoRaWAN. Пристрої першої категорії розраховані на роботу в напівдуплексному режимі, використовуючи лише один канал і один фактор розширення SF одночасно. В контексті архітектури LoRaWAN такі вузли зазвичай періодично здійснюють передавання в висхідному напрямку, а приймання низхідних повідомлень відбувається значно рідше і згідно з попередньо визначеною схемою частот і факторів розширення SF. Натомість LoRa-чипи для шлюзів, які належать до другої категорії, мають значно більші можливості обробки сигналів DSP, що дозволяє їм паралельно демодулювати кілька вхідних передач на різних частотах та з різними значеннями SF. За потреби вони також здатні здійснювати одночасні передавання у зворотному напрямку.

Якщо залишити осторонь архітектуру LoRaWAN то декілька кінцевих вузлів, оснащених одноканальними LoRa-трансіверами, можуть обмінюватися даними безпосередньо між собою. Для реалізації такої взаємодії всі вузли мають бути налаштовані з однаковими радіопараметрами: частотою, шириною смуги, коефіцієнтом корекції помилок CR та фактором розширення модуляції SF.

У контексті сенсорної мережі вузли зазвичай розміщуються на різних відстанях один від одного та в різних умовах навколишнього середовища. Це означає, що кожен потенційний зв'язок між парою вузлів має власні фізичні характеристики. Для LoRa мережі може означати що для кожного індивідуального каналу зв'язку потрібне різне мінімальне значення SF. Оскільки LoRa-пристрої здатні працювати лише з одним SF одночасно, для забезпечення взаємодії між усіма вузлами в одній мережі необхідно застосовувати єдине значення SF. Таке спільне мінімальне значення як правило є більшим за найменше потрібне для окремих зв'язків, що змушує систему використовувати повільніший режим передачі даних, ніж це було б можливо при індивідуальній оптимізації.

LoRa-радіочипи підтримують спеціальний режим роботи CAD, який дозволяє виявляти початок передавання в ефірі з мінімальним енергоспоживанням. Принцип його дії полягає у короткочасному ввімкненні приймача для швидкого сканування радіоканалу, після чого пристрій переходить у сплячий режим і порівнює прийнятий сигнал із зразком преамбули пакета. Увесь процес відбувається надзвичайно швидко і є значно енергоефективнішим ніж постійна спроба приймання пакета. Цей механізм може бути ефективно використаний у мережах з кінцевими вузлами оснащеними одноканальними LoRa-трансіверами: цей мехвнізм дозволяє їм автоматично виявляти, налаштовуватись і успішно приймати пакети з будь-яким фактором розширення SF, за умови попередньо налаштованої частоти.

Для цього на кінцевому вузлі реалізується алгоритм, який постійно ініціює перевірку ефіру на наявність вхідних передач. Якщо сигнал виявлено, розпочинається спроба прийому з використанням найшвидшого доступного SF. У разі невдачі, пристрій послідовно переходить до прийому з вищими значеннями SF. Такий підхід дозволяє вузлам у мережі динамічно змінювати SF залежно від параметрів вхідного пакета, замість використання фіксованого значення. У результаті канали зв'язку між окремими парами вузлів можуть

функціонувати на індивідуально оптимальному рівні SF, не обмежуючись вимогами інших з’єднань у мережі. Однак, для забезпечення надійної роботи такого механізму, довжина преамбули має бути збільшена приблизно до 12 символів на відміну від стандартного значення у 8 символів прийнятого в специфікації LoRaWAN.

Стратегію використання множинних значень SF що ґрунтується на можливостях CAD-режиму в LoRa яку вперше реалізував Мартен Вестенберг. У своєму проекті Мартен Вестенберг використовує звичайну вбудовану плату з підтримкою LoRa на базі мікроконтролерів ESP8266 або ESP32 яку було перетворено на шлюз LoRaWAN . Згодом Яап Браам портував цей код на мову Lua, що дозволило запускати його у середовищі NodeMCU, яке часто використовується на пристроях із ESP8266 .

У подальших роботах, зокрема згаданих у розділі 3.2, Конг Тан Дуонг та Мен Кюн Кім запропонували власну схему ASFS, що дозволяє підвищити пропускну здатність шляхом підтримки мульти-SF у конфігурації з одноканальними LoRa-модулями. У їхній реалізації приймач тричі перевіряє преамбулу в порядку зростання значень SF починаючи з SF7. Якщо преамбула виявляється тричі поспіль на певному SF, приймач вважає його потенційно коректним і здійснює спробу приймання пакета. Автори стверджують, що їхній ітеративний підхід дозволяє повністю уникнути помилкового вибору SF (тобто зменшити частку хибних визначень до 0 %). Але залишається незрозумілим, чи йдеться про 100 % коректно оброблених вхідних пакетів, чи про 100 % правильно демодульованих переданих повідомлень. На жаль, вихідний код цієї реалізації публічно не доступний, що ускладнює її відтворення в подальших дослідженнях.

4.1.1 Розробка та впровадження механізму визначення множинного фактору розширення модуляції

Спираючись на концепцію описаних вище підходів заснованих на виявленні передач із використанням множинних SF, було розроблено та експериментально перевірено власну реалізацію концептуального прототипу, з метою оцінки можливості застосування цієї стратегії на апаратному рівні для побудови сенсорних

мереж. Для цього було використано кілька вбудованих пристроїв моделей TTGO та T-BEAM від виробника LILYGO. Програмування плат здійснювалося в середовищі Arduino IDE, а взаємодія з одноканальними LoRa-трансіверами типу SX1276 реалізовувалась за допомогою бібліотеки RadioLib [94].

Підхід до реалізації механізму виявлення передач у LoRa з підтримкою множинних SF базується на ітераційному процесі, який постійно сканує радіоканал з використанням усіх доступних значень SF.

Не знайомий з результатами дослідження Конг Тан Дуонга та Мен Кюн Кіма на момент реалізації мною не було застосовано послідовне сканування кожного фактору розширення SF у прямому порядку (тобто SF7 → SF8 → SF9 → ... → SF12 → SF7 ...).

Натомість було обрано альтернативну стратегію з пріоритетним скануванням: значення SFn перевіряється вдвічі частіше за $SFn + 1$ (наприклад, SF7 сканується вдвічі частіше ніж SF8, SF8 сканується вдвічі частіше за SF9 і так далі). Така схема дозволяє надавати перевагу швидшим параметрам модуляції, зберігаючи при цьому здатність до прийому пакетів з більшими SF. Нижче наведено алгоритм, який ілюструє основну логіку реалізованої стратегії сканування SF.

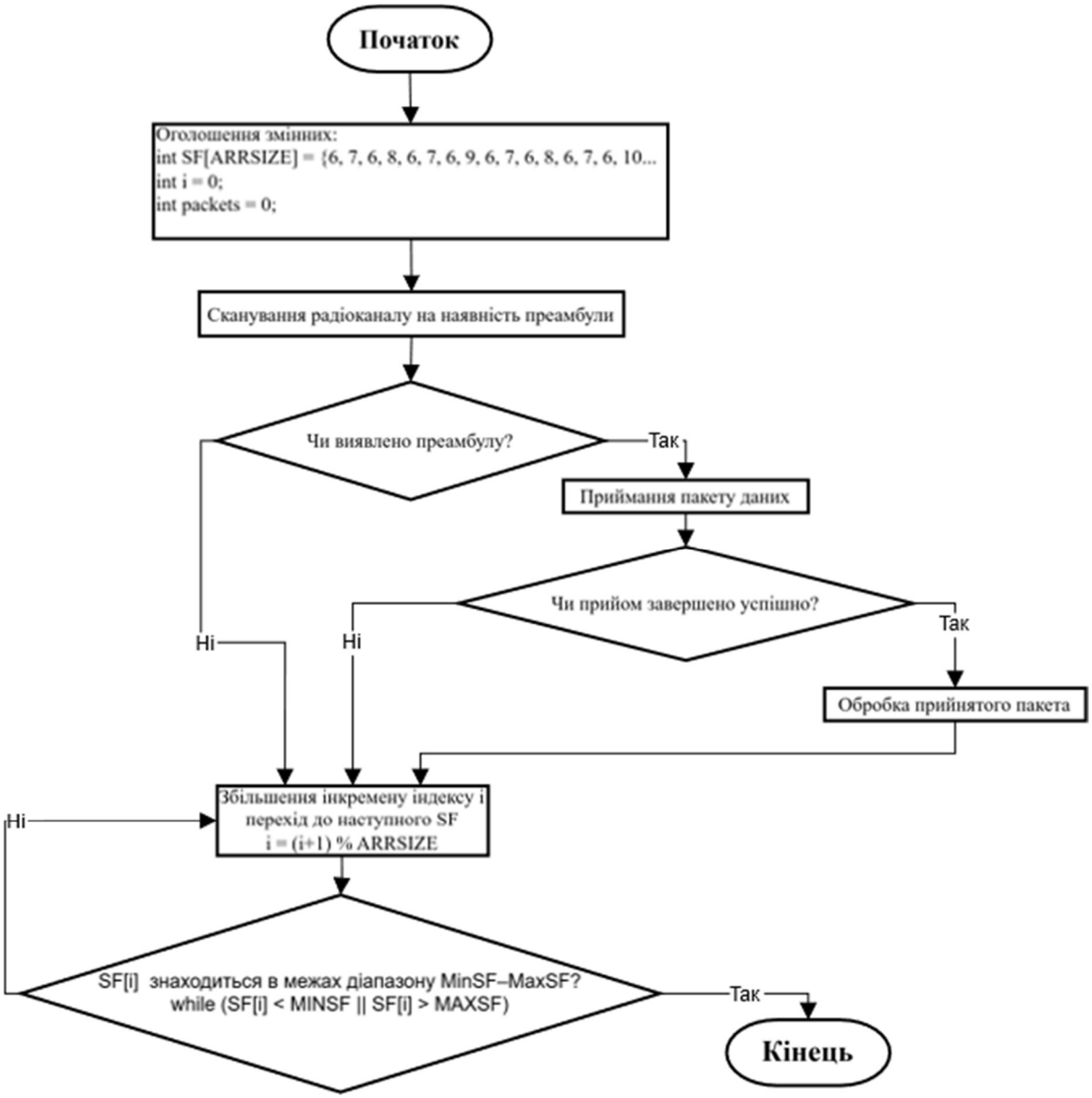

Рис. 4.1 – Процес вдвічі більшого циклічного сканування менших за значенням факторів розширення SF

У запропонованому на Рис. 4.1 алгоритмі програмного забезпечення реалізовано алгоритм циклічного сканування радіоефіру з використанням різних значень фактора розширення SF для технології LoRa. На початковому етапі формується масив, елементами якого є попередньо визначені значення SF. Далі, у рамках основного циклу, для кожної ітерації алгоритм встановлює поточний SF із масиву та виконує налаштування відповідного параметра радіомодуля. Після цього здійснюється сканування радіоканалу з метою виявлення преамбули, яка

свідчить про наявність активності у мережі LoRa з даним параметром SF. У разі детектування преамбули система ініціює процедуру приймання пакета даних; якщо приймання здійснено успішно (відсутні помилки передачі), отриманий пакет передається до функції обробки, яка здійснює його подальший аналіз.

Після завершення спроби прийому відбувається автоматичний перехід до наступного елемента масиву SF. При цьому здійснюється перевірка, чи входить нове значення SF у допустимий діапазон, визначений параметрами MIN SF та MAX SF. Якщо поточне значення виходить за межі вказаного діапазону, здійснюється ітераційний пошук наступного припустимого SF. Таким чином, алгоритм забезпечує циклічне сканування всіх можливих конфігурацій SF, які відповідають визначеним обмеженням, з метою своєчасного виявлення та приймання повідомлень, що надходять від різних пристроїв у мережі.

Загалом, описаний підхід дозволяє підвищити ефективність моніторингу радіоефіру та оптимізувати процес приймання повідомлень у гетерогенних IoT-середовищах, де різні вузли мережі можуть працювати із застосуванням різних параметрів SF. Така методика є доцільною для сценаріїв, що потребують гнучкого та динамічного налаштування параметрів прийому для забезпечення сумісності із широким спектром IoT-пристроїв.

4.1.2 Оцінювання ефективності методу автоматичного визначення множинного фактору модуляції

Реалізований алгоритм виявлення передач із використанням множинних значень SF було протестовано із залученням кількох пристроїв TTGO LoRa32 та T-Beam. У рамках експерименту один із пристроїв виконував роль передавача, що надсилав пакети з використанням різних SF, тоді як решта пристроїв функціонували як приймачі налаштовані з різними конфігураціями параметрів прийому.

Оцінювання працездатності алгоритму здійснювалося шляхом передавання пакетів із використанням різних значень фактору розширення SF з боку передавача (не менше 100 пакетів для кожного SF), із паралельною фіксацією статистики прийому на інших пристроях. У ході експерименту тестувалися різні комбінації SF як для передавача, так і для приймачів (наприклад передавання з SF7 та SF8 або прийом у діапазоні SF6–SF9). У результаті було виявлено, що коли як передавач, так і приймачі були налаштовані на однаковий діапазон із трьох послідовних SF (наприклад, SF7, SF8 та SF9), до 99,2 % пакетів успішно приймалися.

Водночас якщо приймачі прослуховували ті SF які не використовувалися передавачем, показник прийому знижувався приблизно на 5 %. Цей фактор є критично важливим для проектування реальних сенсорних LoRa мереж, оскільки налаштування вузлів на моніторинг "неактивних" SF може призводити до зменшення ефективності обміну даними та втрати пакетів. Дослідження також показало, що розширення діапазону до чотирьох послідовних SF (наприклад, SF6–SF9) призводить до незначного погіршення результату до рівня 96,7 % успішного прийому. Підсумкові результати експериментів з різними конфігураціями передавачів і приймачів наведено в таблицях 4.1, 4.2 та 4.3.

Таблиця 4.1 – Результати прийому пакетів у режимі мульти-SF: передавач передає на SF7 та SF8, а приймачі прослуховують у різних діапазонах факторів розширення SF.

Tx	Rx 1	Rx 2	Rx 3	Rx 4	Rx 5	Rx 6
SF7, 8	SF7, 8	SF7, 8	SF7, 8	SF6, 7, 8	SF7, 8, 9	SF6, 7, 8, 9
870 пакетів	99,1%	98,7%	99,5%	94,6%	94,7%	92,7%

Таблиця 4.2 – Результати прийому пакетів у режимі мульти-SF: передавач передає на SF7, SF8, SF9, а приймачі прослуховують у різних діапазонах факторів розширення SF.

Tx	Rx 1	Rx 2	Rx 3	Rx 4	Rx 5	Rx 6
SF7, 8, 9	SF7, 8, 9	SF7, 8, 9	SF7, 8, 9	SF7, 8, 9	SF7, 8, 9, 10	SF 7, 8, 9, 10
1997 пак.	98,7%	99,2%	98,9%	93,8%	94,3%	89,7%

Таблиця 4.3 – Результати прийому пакетів у режимі мульти-SF: передавач передає на SF7, SF8, SF9, SF10, а приймачі прослуховують у різних діапазонах факторів розширення SF

Tx	Rx 1	Rx 2	Rx 3	Rx 4	Rx 5
SF7, 8, 9, 10	SF7, 8, 9, 10	SF7, 8, 9, 10	SF7, 8, 9, 10	SF7, 8, 9, 10	SF7, 8, 9, 10
2524 пак.	94,0%	96,9%	96,6%	95,1%	90,7%

Отримані результати виявилися дуже подібними до тих, що були опубліковані Кімом та співавторами, навіть попри відмінності у реалізованих стратегіях з виявлення передач із множинними SF. Потенційним напрямом удосконалення запропонованого підходу може бути запровадження декількох послідовних перевірок преамбули перед спробою прийому пакету – аналогічно до реалізацій, наведених у літературі [95]. Обидві незалежні ініціативи, попри різницю в деталях, підтверджують можливість ефективного використання множинних значень SF на пристроях з одноканальними LoRa-трансіверами. Це відкриває перспективу для побудови сеносрних мереж у яких кожне з'єднання між парою вузлів може динамічно використовувати найшвидше можливе значення SF, незалежно від параметрів інших з'єднань у мережі.

Крім того, застосування стратегії multi-SF дає попередню відповідь на запитання щодо того, яким чином специфічні особливості технології LoRa можуть бути використані для побудови плоских, децентралізованих mesh-мереж.

4.2 Векторний протокол для самоорганізації в сенсорних мережах

Для розгортання та оцінювання саморганізованих LoRa мереж було розроблено та реалізовано проактивний гібридний протокол маршрутизації на рівнях L2/L3 дистанційно-векторного класу, який враховує специфічні особливості радіотехнології LoRa. Основним принципом проєктування була мінімізація обчислювальної складності протоколу, щоб забезпечити його працездатність на пристроях із обмеженими ресурсами, зокрема на мікроконтролерах з інтегрованим LoRa-модулем.

Крім того, протокол здатен ефективно використовувати особливості множинних факторів розширення SF, зокрема їх різний радіус дії та квазіортогональність дозволяє здійснювати одночасні передавання між різними парами вузлів. Для досягнення цієї мети також запропонувно нову метрику маршрутизації – ToA з підтримкою мульти-SF, яка враховує загальний час перебування пакета в ефірі ToA вздовж усього маршруту до місця призначення.

Застосування цієї метрики дозволяє мінімізувати час передавання пакета та покращити ключові показники ефективності мережі за певних умов її функціонування.

Основні характеристики розробленого протоколу включають:

1. Відстань-вектор – найкращі маршрути до будь-якого пункту призначення обчислюються у розподілений спосіб на всіх вузлах мережі, базуючись на інформації, отриманій від сусідніх вузлів;

2. Проактивність – вузли мережі періодично розсилають інформацію про доступні маршрути незалежно від наявності трафіку користувацьких даних. Це дозволяє підтримувати актуальність маршрутів та забезпечити їхню готовність до використання у будь-який момент;

3. Гібридна модель рівнів OSI (канальний + мережевий) – об’єднання двох рівнів у спрощену архітектуру мінімізує складність реалізації та знижує вимоги до обчислювальних ресурсів пристроїв на базі LoRa;

4. Урахування коефіцієнту активності – для мереж, що працюють у неліцензованих ISM-діапазонах, обмеження часу в радіоефірі у вигляді коефіцієнту активності є обов’язковими до дотримання та ці обмеження інтегруються у метрику маршруту під час її обчислення;

5. Легкість, гнучкість і конфігурованість – численні параметри протоколу, включно з метриками пакетів, можуть бути налаштовані для адаптації до конкретного сценарію використання;

6. Паралельні передачі інформація на різних SF – завдяки властивості квазіортогональності SF у LoRa можлива побудова кількох «віртуальних» мереж, що накладаються одна на одну в межах одного радіоканалу, забезпечуючи підвищену загальну пропускну здатність;

7. Метрика ToA (час в радіоефірі) – вартість маршруту обчислюється на основі загального часу передавання пакета між джерелом і призначенням.

4.2.1 Мережева топологія та адресація

Розроблений протокол маршрутизації для сенсорних мереж формує плоску топологію мережі без ієрархічного поділу вузлів – незалежно від їх апаратних характеристик або ролі на рівні прикладного програмного забезпечення. Для участі в мережі кожен вузол повинен запускати власний екземпляр протоколу, створювати та підтримувати локальну таблицю маршрутів, а також періодично обмінюватися маршрутною інформацією з сусідніми вузлами.

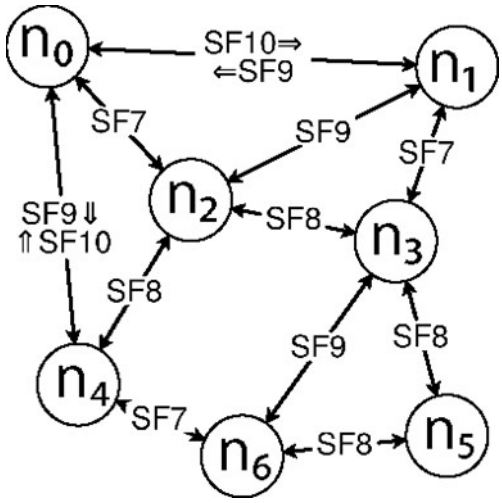

Рис 4.2 – Топологія сенсорної мережі LoRa

На рисунку 4.2 зображено топологію сеносрної LoRa мережі, що функціонує на основі розробленого протоколу маршрутизації. Передача даних між парою вузлів, які знаходяться в межах прямої досяжності, зазвичай може здійснюватися з використанням різних значень SF; на схемі вказано найшвидший (тобто найменший) SF за якого з'єднання можливе. Комунікація між віддаленими вузлами що не мають прямого зв'язку,реалізується через багатокрокову передачу пакетів з використанням маршрутів обчислених за допомогою пртоколу маршрутизації . Хоча більшість з'єднань на схемі є симетричними, деякі з них потребують різних значень SF у кожному з напрямків щоб забезпечити успішну передачу. Такі випадки можуть виникати внаслідок неоднорідних апаратних характеристик вузлів або специфіки середовища передачі як тимчасового так і постійного характеру. У результаті цього пакети, що передаються між однією і тією ж парою вузлів, можуть проходити різними маршрутами залежно від напрямку.

З метою спрощення реалізації маршрутизації та прикладних рішень було об'єднано канальний рівень (рівень 2 OSI, L2) та мережевий рівень (рівень 3 OSI, L3) в єдину логічну структуру. Такий підхід відрізняється, зокрема, від архітектури Wi-Fi 802.11+IP, де кожен рівень має власну систему адресації. Об'єднання рівнів дозволяє зменшити навантаження на мережевий трафік та

обчислювальні ресурси вузлів, хоча й може обмежувати сумісність із зовнішніми мережами. У розробленій архітектурі використовуються 2-байтні мережеві адреси в діапазоні від 0x0000 до 0xFFFF, що забезпечує до 65 536 унікальних адрес на одну мережу. Такий розмір адресного простору обрано як компромісне рішення між масштабованістю мережі, характеристиками пропускної здатності та дальністю дії LoRa, а також простотою реалізації. Водночас за потреби ця величина може бути змінена під конкретний сценарій використання.

4.2.2 Структура мережевих пакетів

Пакети даних та маршрутні пакети мають дуже схожу структуру, що схематично представлено на Рис. 4.3. Оскільки розмір пакета обмежується апаратними можливостями LoRa і не може перевищувати 256 байт, у розробленому протоколі застосовано мінімалістичний підхід до структури заголовка з метою зменшення службового навантаження. Максимальний розмір заголовка становить лише 7 байт.

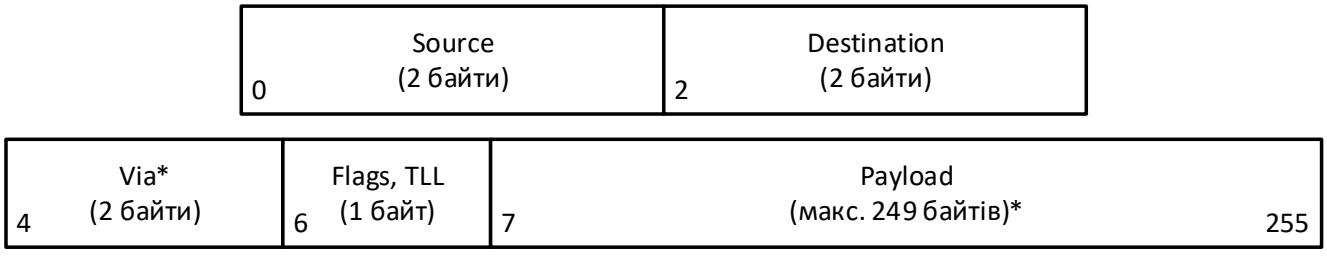

Рис. 4.3 – Структура пакету даних або пакету маршрутизації

Перші 4 байти пакета даних містять адресу вузла-джерела повідомлення та адресу кінцевого вузла-отримувача. Наступне поле Via використовується у багатоперехідних пакетах даних для позначення адреси наступного вузла на маршруті. Значення цього поля змінюється на кожному переході, коли пакет передається через проміжні вузли. На останньому кроці маршруту, або у випадку

одноперехідних пакетів, значення Via повинно збігатися зі значенням адреси кінцевого вузла-отримувача.

Байт Flags/TTL зарезервовано для позначення типу пакета якщо це потрібно прикладному рівню, а також для обліку «часу життя» пакета TTL . Це ефективно встановлює максимальну довжину маршруту на рівні 64 переходів. Останнім йде поле Payload, яке містить прикладні дані або службову інформацію протоколу маршрутизації що передається між вузлами, максимальний обсяг цього поля становить 249 байт.

Маршрутні пакети відрізняються від звичайних пакетів даних тим, що в полі Призначення замість одноадресної адреси використовується широкомовна адреса. У зв'язку з цим поле Via не потрібне і, відповідно, опускається, що дозволяє заощадити 2 байти що можуть бути додатково використані для поля Payload, розмір якого у такому випадку може сягати до 251 байта.

4.2.3 Маршрутизація

Кожен вузол у мережі запускає власний екземпляр протоколу маршрутизації, формуючи локальну таблицю маршрутів яка постійно оновлюється у процесі прийому повідомлень від сусідніх вузлів. Оскільки протокол належить до векторного, така таблиця містить перелік: усіх відомих вузлів мережі, вузла-сусіда через який можна досягти кожного з них, вартість маршруту та час дії маршруту. На основі цієї таблиці кожен вузол теоретично, здатний здійснювати комунікацію з будь-яким іншим вузлом у мережі – як безпосередньо, так і опосередковано через механізм багатоперехідної передачі . Крім того, кожен вузол виконує роль маршрутизатора для транзитного трафіку, передаючи пакети інших вузлів, що прямують через нього до місця призначення.

Окрім маршрутів до інших вузлів, кожен вузол також зберігає інформацію про маршрути що ведуть від сусідніх вузлів до нього самого. Оскільки фізичні з'єднання між сусідніми вузлами можуть бути асиметричними, протокол

маршрутизації має забезпечити зворотне інформування сусідніх вузлів про характеристики вхідних з'єднань. Це дозволяє їм коректно розраховувати маршрути у напрямку до цього вузла.

Таблиця 4.4 – Таблиця маршрутизації для вузла n0

Хост призначення	Наступний вузол (перехід)	SF	Ціна маршруту	Час до кінця існування
0x0001	0x0001	10	-	189
0x0002	0x0002	7	-	293
0x0004	0x0004	9	-	251
0x0001	0x0002	-	4	293
0x0003	0x0002	-	3	293
0x0004	0x0002	-	3	293
0x0005	0x0002	-	5	293
0x0006	0x0002	-	4	293
0x0002	0x0001	-	4	189
0x0003	0x0001	-	12	189
0x0004	0x0001	-	9	189
…	…	-	…	…
Хост призначення	Наступний вузол (перехід)	SF	Ціна маршруту	Час до кінця існування
0x0000	0x0001	9		189
0x0000	0x0002	7		293
0x0000	0x0004	10		521

У таблиці 4.4 наведено знімок стану таблиці маршрутів для вузла n0 з Рис. 4.2. У першому блоці показано три верхні записи, які відповідають прямим однохоповим маршрутам від вузла n0 до його сусідів n1, n2 та n4. Наступні записи відображають багатоперехідні маршрути до інших вузлів мережі. Це стосується як вузлів, що фізично недосяжні в межах одного переходу (наприклад, n3, n5 і n6), так і тих для яких багатоперехідний маршрут має кращу метрику ніж пряме з'єднання (зокрема, це стосується n1 і n3). Наприклад, хоча існує прямий шлях від n0 ⇒ n4, його вартість за метрикою ToA вища ніж у маршруту n0 ⇒ n2 ⇒ n4.

Другий блок записів у таблиці 4.4 містить інформацію про вхідні маршрути до вузла n0. Хоча сам вузол n0 не використовує ці дані безпосередньо для власних рішень щодо маршрутизації, він має зберігати їх та передавати своїм сусідам. Це дозволяє сусіднім вузлам дізнатися, який мінімальний SF потрібен для досягнення n0 і правильно обчислити маршрути у його напрямку.

Після успішного передавання нового маршрутного пакета, вузол-приймач обробляє його та оновлює свою локальну таблицю маршрутів відповідно до отриманої інформації. Спочатку додаються або оновлюються характеристики каналу зв’язку із сусіднім вузлом-джерелом. Далі по черзі обробляються оголошені маршрути: залежно від ситуації, вони або додаються до таблиці, або оновлюють існуючі записи, або відхиляються як нерелевантні. Схематичне представлення цього процесу наведено у вигляді схеми на рисунку 4.3.

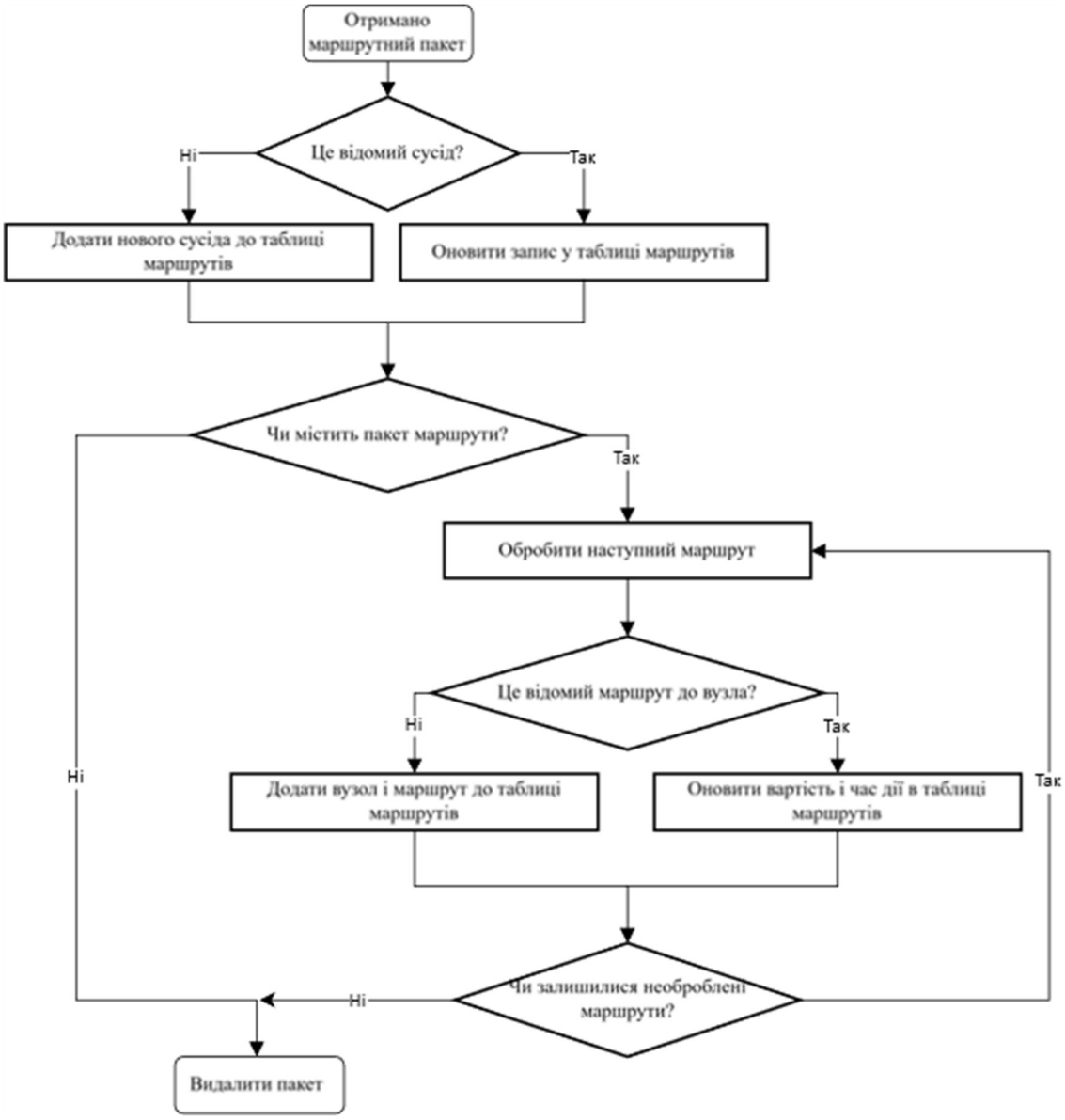

Рис 4.3 – Схема отримання нового маршрутного пакету на мережевому вузлі.

Як показано в таблиці 4.4, таблиця маршрутів може містити кілька записів, що ведуть до одного й того ж вузла, але через різні проміжні вузли. Хоча за замовчуванням протокол маршрутизації обирає маршрут із найменшою вартістю, наявність альтернативних шляхів дозволяє оперативно адаптуватися у випадку якщо основний маршрут стане недоступним або його вартість істотно зросте. Разом із тим, щоб уникнути надмірного розростання таблиці маршрутів, доцільно встановити обмеження як на загальну кількість записів так і на кількість маршрутів до одного вузла.

4.2.4 Обмін маршрутами між сусідніми мережевими вузлами

Вузли, що виконують екземпляр протоколу маршрутизації, періодично здійснюють широкомовну передачу маршрутних пакетів своїм сусідам. Таким чином вони проактивно формують топологію мережі та підтримують її актуальний стан, оновлюючи свої локальні таблиці маршрутів у міру надходження пакетів від сусідніх вузлів. Такі пакети містять у собі:

1. Інформацію про вузол-джерело (тобто його адресу);

2. 6-бітовий інкрементальний лічильник (замість TTL), який може бути використаний для оцінки втрат пакетів та колізій на каналі, що, своєю чергою, дозволяє непрямо визначити якість або завантаженість каналу зв'язку;

3. Фрагмент таблиці маршрутів вузла-джерела, тобто перелік найкращих маршрутів і їх вартостей до інших вузлів мережі.

На основі цієї інформації, а також параметрів фізичного рівня передачі LoRa (SF використаного під час передавання), вузли, які отримують широкомовний пакет оновлюють свої локальні таблиці маршрутів відповідним чином. Надалі ці вузли поширюють отримані маршрути далі до своїх сусідів коли надсилають власні широкомовні повідомлення.

Передбачається що пристрої які виконують екземпляр протоколу маршрутизації оснащені одноканальними LoRa-модулями та підтримують механізм прийому на множинних факторах розширення SF. Це дозволяє їм передавати та приймати пакети на будь-якому значенні SF у межах діапазону від SF_{min} до SF_{max}. Протокол підтримує як моно-SF метрики у яких усі вузли використовують фіксоване значення SF по всій мережі, так і мульти-SF метрики де вузли можуть динамічно змінювати SF залежно від поточного стану.

Час передачі пакету зростає вдвічі з кожним наступним SF. Тому у випадку використання мкльти-SF метрик застосовується така стратегія: широкомовні повідомлення на певному SF передаються вдвічі частіше, ніж повідомлення на SF який на одиницю вищий. Наприклад, широкомовні пакети з SF9

надсилаються вдвічі частіше, ніж пакети з SF10. Це дозволяє збалансувати вартість використання різних SF а також сприяє більш оперативному оновленню маршрутів, що базуються на швидших з’єднаннях. Передавання широкомовних пакетів на різних SF здійснюється у випадковому порядку, відповідно до ймовірнісної формули, наведеної нижче.

$$p(SF_n) = \frac{2^{SF_{max} - SF_n}}{\sum_{i=min}^{max} 2^{SF_i - SF_{min}}}$$

звідки після нормалізації

$$\sum_{i=min}^{max} p(SF_i) = 1$$

виходить:

$$p(SF_{min}) = 2^{SF_{max} - SF_{min}} \times p(SF_{max}) \quad (4.1)$$

Випадкове надсилання пакетів із використанням різних значень SF замість фіксованої послідовності також сприяє уникненню повторних колізій у випадках, коли вузли в мережі виявляються синхронізованими.

Наведений нижче на Рис 4.4 процес реалізує випадковий вибір SF у межах діапазону від SF_{min} до SF_{max}. згідно з описаною ймовірнісною моделлю:

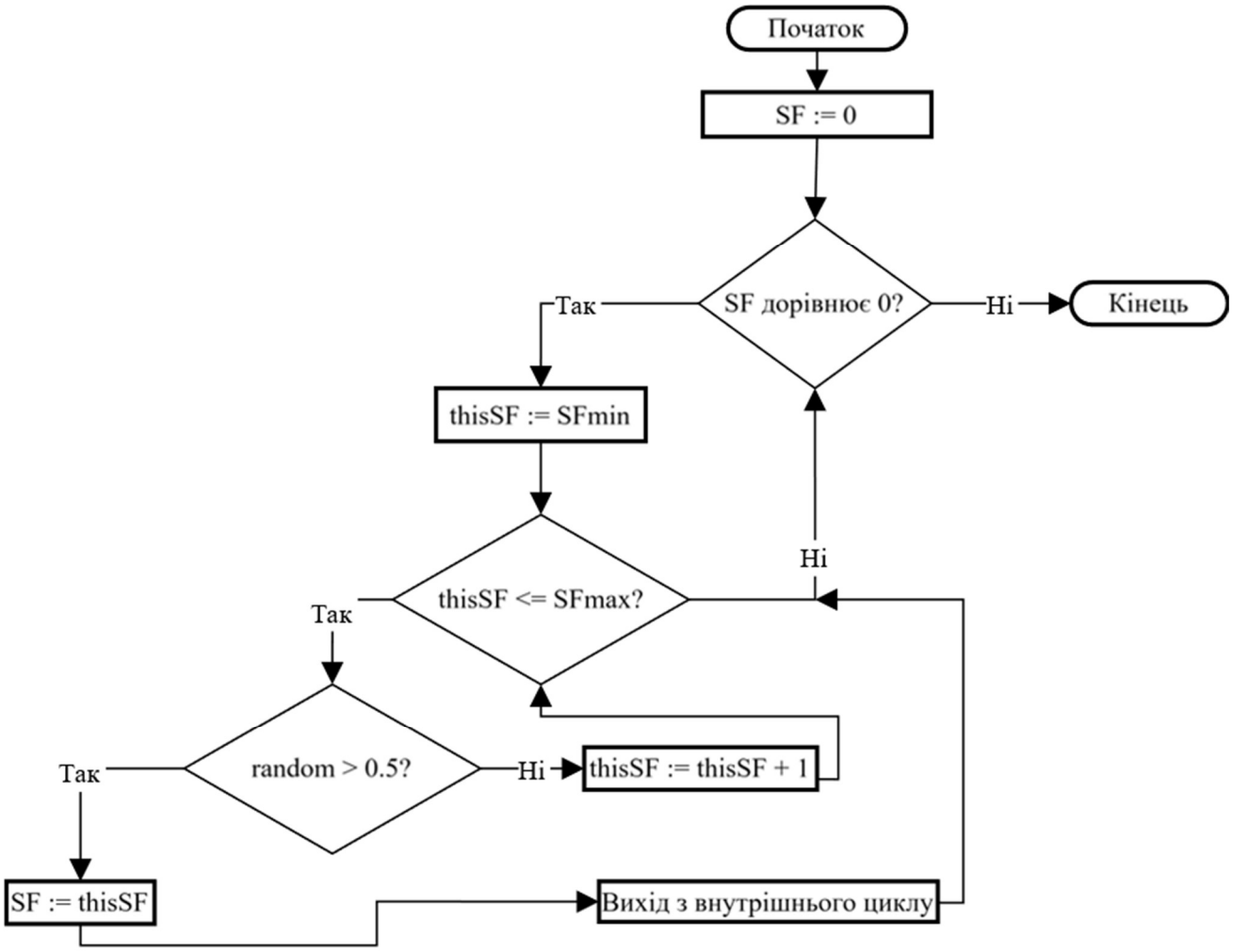

Рис. 4.4 – Випадковий вибір значення SF для широкомовної передачі маршрутного пакета

Як було зазначено в підрозділі 4.2.2, маршрутні пакети є дуже подібними до звичайних пакетів даних, за винятком того, що вони передаються лише в один хоп і використовують широкомовну адресу як адресу призначення, тому не містять поля Via. Їхнє поле Payload включає інформацію про маршрути в мережі, які оголошуються вузлом-джерелом.

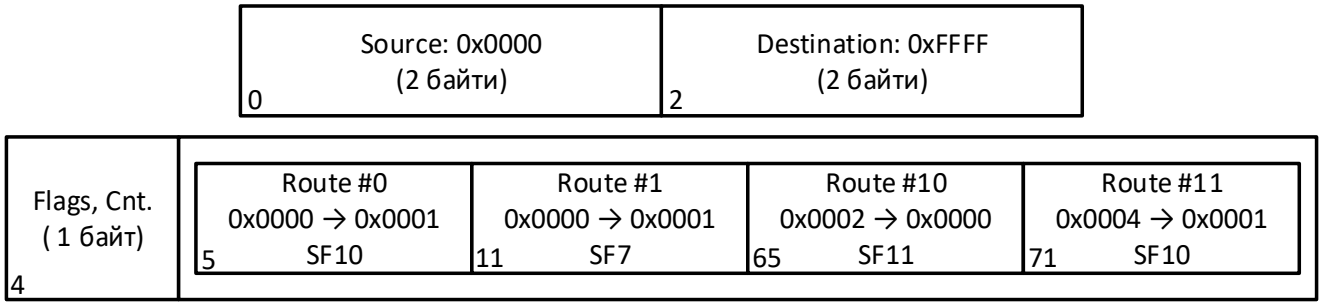

Рис 4.5 – Структура пакету маршрутизації надісланого з вузла n0

На Рис 4.5 наведено приклад маршрутного пакета (відповідного до вузла n0 з Рис. 4.2), у якому вміст Payload становлять найкращі маршрути з таблиці маршрутів, зображеної в таблиці 4.4.

У випадку коли вміст таблиці маршрутів перевищує по розміру поле Payload одного пакета, маршрути для передачі обираються випадковим чином, шляхом призначення кожному з них імовірності передачі пропорційної значенню їхньої метрики Cost. Такий підхід забезпечує частіше оновлення маршрутів до ближчих вузлів у порівнянні з далекими, підвищуючи оперативність обміну актуальною інформацією. Водночас щоб уникнути явища нестабільності, час життя маршрутів слід налаштовувати з урахуванням кількості вузлів у мережі та її топології.

Після отримання нового маршрутного пакета, вузол обробляє його та оновлює свою локальну таблицю маршрутів. Спочатку в таблицю додаються або оновлюються характеристики з’єднання із сусіднім вузлом-джерелом. Далі по черзі обробляються оголошені маршрути: кожен із них або додається до таблиці, або оновлює наявний запис.

4.2.5 Використання мережевих метрик для маршрутизації

Розроблений протокол маршрутизації може бути налаштований для використання різних стратегій маршрутизації, зокрема щодо метрики, яка застосовується для обчислення вартості можливих шляхів до вузла призначення.

Ці метрики визначають, до якого вузла слід переслати пакет для досягнення кінцевого отримувача.

Протокол підтримує кілька підходів:

1. Стратегія широкомовної маршрутизації;

2. Моно-SF метрики – зокрема поширені Лічильник переходів (HC) або Очікувана кількість передач (ETX);

3. Запропонована у роботі метрика Часу в ефірі ToA для багатофакторного середовища з множинними значеннями SF.

Найпростішим способом організації багатоперехідної передачі в межах проколу маршрутизації є стратегія широкомовного розповсюдження пакетів, яка не передбачає побудови реальних маршрутів. У такому режимі вузли зберігають у обмеженому буфері копії останніх отриманих і переданих широкомовних пакетів щоб уникнути повторного передавання одних і тих самих даних, що могло б спричинити надмірне зростання трафіку в мережі.

Більш вдосконалений варіант широкомовної стратегії, дозволяє вузлам відстежувати своїх сусідів під час передавання ними пакетів даних. У цьому випадку на останньому етапі передавання може використовуватись одноадресна передача для зменшення навантаження та підвищення ефективності доставки.

У розробленому протоколі маршрутизації реалізовано чотири метрики для сенсорних LoRa мереж, у яких усі вузли використовують єдине значення SF на рівні всієї мережі.

Першою метрикою є Лічильник переходів HC, за якої вартість маршруту визначається як кількість переходів, необхідних для досягнення пункту призначення.

Другою є метрика Очікувана кількість передач ETX, в якій вартість маршруту залежить від якості каналів зв’язку вздовж усього шляху й визначається кількістю передавань, необхідних для доставки пакета до адресата. Якість каналу між двома вузлами розраховується на основі кількості втрачених

маршрутних пакетів за певний проміжок часу: чим більше втрат, тим гірша якість з'єднання і відповідно вища його вартість.

Окрім того, доступні ще дві метрики для моно-SF конфігурацій, які розраховують вартість маршруту на основі рівня RSSI.

Перша з них оцінює вартість маршруту як суму рівнів прийому сигналу по всіх лінках маршруту:

$$\sum_{h=0}^{n} |\min (RSSI_h - 1)| \tag{4.2}$$

У такий спосіб лінки з нижчою якістю прийому сигналу матимуть вищу вартість маршруту.

Аналогічно друга метрика також використовує показник якості прийому сигналу (RSSI), але обчислює вартість маршруту як добуток значень RSSI уздовж усього шляху:

$$\prod_{h=0}^{n} |\min (RSSI_h - 1)| \tag{4.3}$$

Третьою є метрика множинного SF що є ключовим параметром технології радіозв'язку LoRa, оскільки визначає компроміс між дальністю передавання сигналу та часом, необхідним для надсилання пакета. У загальному випадку, перехід до SF на один рівень вищий (наприклад від SF7 до SF8) подвоює час передавання, або відповідне зменшення на рівень нижче знижує швидкість передавання удвічі але збільшує дальність передачі у діапазоні від ×1,25 до ×1,4 (Табл 4.5).

Пропускна здатність або час передавання також безпосередньо впливають на споживану потужність під час передавання пакета, що особливо критично для пристроїв з автономним живленням. Такий сценарій є типовим для LPWAN у сфері Інтернету речей, де радіоканал і енергетичні ресурси мають обмежений характер.

Таблиця 4.5 – Максимальна дальність передавання для різних факторів розширення SF

SF	Rx чутл.	P_{Tx}	Частота	Дист	Δ дист
7	-124 dBm	20 dBm	125 КГц	250 м.	-
8	-127 dBm	20 dBm	125 КГц	349 м.	× 1,4
9	-130 dBm	20 dBm	125 КГц	487 м.	× 1,4
10	-133 dBm	20 dBm	125 КГц	679 м.	× 1,4
11	-135 dBm	20 dBm	125 КГц	848 м.	× 1,25
12	-137 dBm	20 dBm	125 КГц	1058 м.	× 1,25

З урахуванням вищезазначених обмежень, у даному дослідженні запропоновано метрику маршрутизації Час в Ефірі (ToA), що дозволяє оцінити вартість маршруту до вузла призначення шляхом мінімізації загального часу передавання пакета «від джерела до отримувача», а також зменшення зайнятості радіоканалу.

У межах розробленого протоколу маршрутизації метрика Часу в Ефірі обчислює вартість маршруту до певного вузла з урахуванням значень SF, використаних на кожному з послідовних переходів між вузлами-передавачами. Зокрема, вартість окремого хопу $h_{l,m}$ між двома сусідніми вузлами h_l та h_m оцінюється як ступінь двійки:

$$h_{l,m} = 2^{SF_{lm} - SF_{min}} \tag{4.4}$$

де SF_{lm} – це найменше значення фактору розширення, необхідне для успішної передачі даних між вузлами h_l та h_m, а SF_{min} – мінімальне доступне в системі значення SF.

Таким чином, вартість маршруту між двома довільними вузлами h_l та h_m, які з'єднані через H проміжних вузлів, обчислюється за формулою:

$$ToA_{i,j} = \sum_{k=1}^{H} h_k = \sum_{k=1}^{H} 2^{SF_k - SF_{min}} \tag{4.5}$$

де SF_k – це значення фактору розширення, використане на кожному з H проміжних вузлів у складі маршруту. У випадку, якщо існує два або більше маршрутів із однаковим значенням метрики, надається перевага тому, у якому наступний хоп використовує менше значення SF. Якщо ж і це не дозволяє здійснити вибір (тобто маємо однакову метрику та однаковий SF на наступному кроці), вибір маршруту відбувається випадковим чином серед претендентів.

4.2.6 Механізми запобігання утворенню мережевих петель

Розроблений нами протокол маршрутизації може бути схильним до утворення маршрутних петель, зокрема у випадках, коли один із вузлів зникає з мережі, що є типовою проблемою для алгоритмів векторного класу. Для зменшення ймовірності виникнення таких ситуацій або пом’якшення їхніх наслідків, у протоколі реалізовано низку захисних механізмів:

1. Коректування відміни маршрутів – якщо прямий маршрут (тобто до сусіднього вузла в один перехід) перевищує допустимий час життя на певному вузлі, цей вузол надсилає широкомовне повідомлення про відповідний маршрут із максимально можливою вартістю. Таким чином інші вузли поступово виключають протермінований маршрут зі своїх таблиць і поширюють цю інформацію далі мережею.

Оскільки маршрутні пакети передаються без гарантії прийому, ефективність такого механізму в умовах боротьби з петлями може бути обмеженою – особливо в перевантажених мережах із високою ймовірністю колізій. Як варіант пом’якшення цієї проблеми, можна реалізувати повторне багаторазове передавання «отруєних» маршрутів перед їх остаточним видаленням на локальному вузлі

2. Утримування маршруту – коли мережевий вузол дізнається про недоступність певного маршруту (наприклад у разі відмови сусіднього вузла) він встановлює таймер. Упродовж цього періоду вузол ігнорує будь-яку вхідну

інформацію про відповідний маршрут, що дозволяє уникнути ситуації нескінченного збільшення вартості маршруту.

Однак ефективність цього механізму може бути лише частковою, оскільки її реалізація залежить від здатності вузла вчасно виявити або отримати інформацію про недоступність маршруту до початку процесу нескінченного оновлення. Крім того, така стратегія може призвести до збільшення часу збіжності мережі.

3. Максимальна вартість маршруту – усі маршрути мають обмеження за максимальною вартістю, і ті що досягають цього граничного значення, автоматично відкидаються (видалюяються). Таким чином, навіть у разі виникнення петлі з нескінченним зростанням вартості, відповідні маршрути зрештою вилучаються з таблиць.

Однак це обмеження створює компроміс між швидкістю ліквідації маршрутних петель і максимально допустимими розмірами мережі з точки зору маршрутизації (тобто максимальною кількістю рнонходів).

4. Час життя пакету (TLL) – пакети мають обмеження на максимальну кількість переходів, що становить 64. Однак це значення може бути зменшено, наприклад, до кількості відомих вузлів у мережі. Такий підхід дозволяє швидше виявляти і припиняти маршрутизування у разі потрапляння пакета в петлю, оскільки його час життя (TTL) буде вичерпано раніше.

5. Запобігання дублюванню пакетів – коли замість повноцінної маршрутизації використовується механізм flooding, кожен вузол зберігає у фіксованому буфері копії останніх пересланих ним пакетів. Якщо такий самий пакет знову надходить для пересилання, він відкидається і це дозволяє уникнути дублювання передач та утворення петель.

Цей механізм застосовується також і в режимі реальної маршрутизації, доповнюючи функцію TTL у самих пакетах. Таким чином забезпечується додатковий захист від зациклення маршрутів.

4.3 Налаштування програмного середовища для тестування протоколу самоорганізації

Для забезпечення адаптації до конкретних сценаріїв використання та умов функціонування мережі, більшість параметрів протоколу маршрутизації можуть бути налаштовані. У цьому підрозділі наведено стислий огляд найважливіших параметрів, які впливають на роботу протоколу.

Передусім, можуть бути змінені кілька аспектів, пов’язаних із технологією LoRa. Наприклад, можна налаштувати максимальне значення фактору розширення SF яке використовуватиметься у мережі, за замовчуванням це SF12 але його можна зменшити відповідно до вимог регуляторної політики у конкретному регіоні. Замість метрики ToA, встановленої за замовчуванням, можна обрати інші відомі метрики. Також можливе налаштування параметрів, пов’язаних із життєвим циклом маршрутів, зокрема часу збереження маршруту у таблиці, що дозволяє підтримувати її актуальність. Основні конфігуровані параметри наведено в таблиці 4.6.

Таблиця 4.6 – Конфігуруванні параметри в протоколі маршрутизації

Сфера:	Параметр:	Діапазон зн.:	Знач.:
LoRa	Мінімальний SF	SF7, …, SFmax	SF7
LoRa	Максимальний SF	SFmin, …, SF12	SF12
Маршрутизація	Метрика	BC, HC, ETX, RSSI, ToA	ToA
Маршрутизація	Середній інтервал широкомовної передачі маршрутів (SFmin)	0 … ∞	60 с
Маршрутизація	Час зберігання маршруту (SFmin)	0 … ∞	300 с
Маршрутизація	Макс. кількість маршрутів до одного вузла	1 … n	2
Маршрутизація	Макс. загальна кількість маршрутів	0 … 1024	1024
Маршрутизація	Пріоритет маршрутних / даних пакетів	n : 1	10 : 1
Маршрутизація	Пріоритет транзитних / локальних пакетів	n : 1	10 : 1
Регулювання	Час передачі (%)	0.1 – 100	100

Щодо передачі пакетів даних і маршрутних пакетів, передбачено можливість налаштування пріоритетів їх надсилання на рівні вузла — наприклад, у співвідношенні n : 1. Також допускається встановлення різних пріоритетів для локально згенерованих і транзитних пакетів відповідно до вимог конкретного застосування.

У цьому дослідженні використано середовище симуляції OMNeT++ розширювану, модульну, компонентну бібліотеку й фреймворк на C++, – у поєднанні з FLoRa, спеціалізованим інструментарієм для наскрізного моделювання мереж LoRa. OMNeT++ є добре відомим у науковій спільноті дискретним симулятором подій, який широко використовується в академічних дослідженнях. Разом із FLoRa він забезпечує повну реалізацію архітектури LoRaWAN та точну модель фізичного рівня LoRa-радіозв’язку, побудовану на основі експериментальних результатів попередніх досліджень.

У рамках цього проєкту було модифіковано фреймворк FLoRa шляхом вилучення специфічної функціональності LoRaWAN і додавання підтримки прямої комунікації та пересилання пакетів між кінцевими вузлами – без необхідності використання шлюзів. Це, зокрема, включає впровадження протоколу маршрутизації векторного класу з підтримкою різних методів обчислення вартості маршруту. Додатково до фреймворку було інтегровано й інші корисні можливості, зокрема механізм CAD

4.3.1 Опис тестової топології сенсорної мережі

У симуляційних експериментах використано мережу зі змінною кількістю вузлів, розташованих у двох різних топологіях: симетричній сітці розміром N × N з однаковою вертикальною та горизонтальною відстанню між вузлами що зображено на Рис. 4.6.

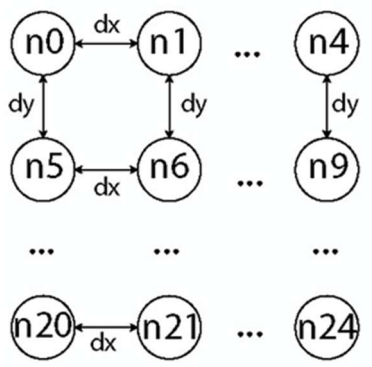

Рис. 4.6 – Симетрична сітчаста топологія з однаковою горизонтальною (dx) та вертикальною (dy) відстанню між вузлами

Та випадковій топології з вузлами, рівномірно розподіленими по обмеженій квадратній області що зображено на Рис. 4.7

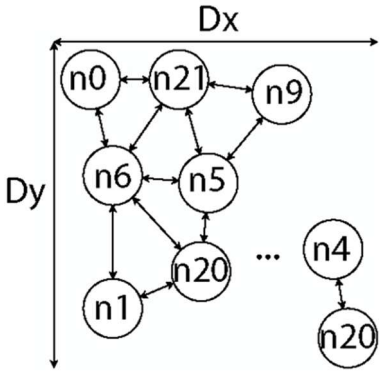

Рис. 4.7 – Випадкова топологія вузлів розподілених по області dx × dy

Кожна з двох топологій використовується для досягнення різних цілей оцінювання. Сіткова топологія з фіксованою відстанню між вузлами забезпечує регулярне та передбачуване середовище. Таким чином, після встановлення відповідного значення фактору розширення SF і потужності передавання, моно-SF маршрутизація забезпечує зв’язок або з усіма вузлами або ні з ким, продуктивність залежить виключно від властивостей обраної метрики, а не від особливостей топології мережі. Це також дозволяє перевірити, чи забезпечує певні переваги використання мульти-SF маршрутизації.

З іншого боку, випадкова топологія дозволяє оцінити, наскільки ефективно мулти-SF маршрутизація самоорганізується та адаптується до гетерогенних умов. Ця випадкова топологія дає змогу дослідити, як впливає використання різних факторів розширення SF у різних частинах мережі (тобто прагнення використовувати найшвидший можливий SF для кожного окремого з'єднання між парами вузлів) у порівнянні з використанням єдиного значення SF для всієї мережі, яке забезпечує зв'язок для всіх учасників.

Коли вузли розміщуються згідно із сітковою топологією, використовуються чотири різні відстані між ними (по вертикалі і по горизонталі): 177 м., 178 м., 247 м. та 248 м. Ці значення вибрано не довільно, а з певною метою, як показано на Рис. 4.8. Відстань 177 м дозволяє вузлам із найменшим значенням SF7 здійснювати зв'язок із сусідніми вузлами у горизонтальному, вертикальному та діагональному напрямках. Зі збільшенням відстані до 178 м діагональний зв'язок із сусідніми вузлами вже стає неможливим для SF7 – передача можлива лише по вертикалі та горизонталі. Експерименти з цими двома варіантами розміщення дозволяють оцінити вплив щільності мережі на її продуктивність. Аналогічно, зміна відстані між вузлами з 246 м до 247 м впливає на ефективність використання SF8: у першому випадку можливий діагональний зв'язок, а в другому випадку потрібен перехід на повільніший SF9.

Коли використовується випадкова топологія, вузли рівномірно розподіляються по тій самій площі, яку займає сітчаста топологія . Наприклад, у мережі з $N^2 = 36$ вузлів, для порівняння з топологією сітки, де вузли розташовані на відстані 178 м один від одного: $(5 \times 178\text{ м}) \times (5 \times 178\text{ м}) = 890\text{ м} \times 890\text{ м}$.

Це дозволяє порівняти синтетичну мережу з більш гетерогенною конфігурацією розгортання.

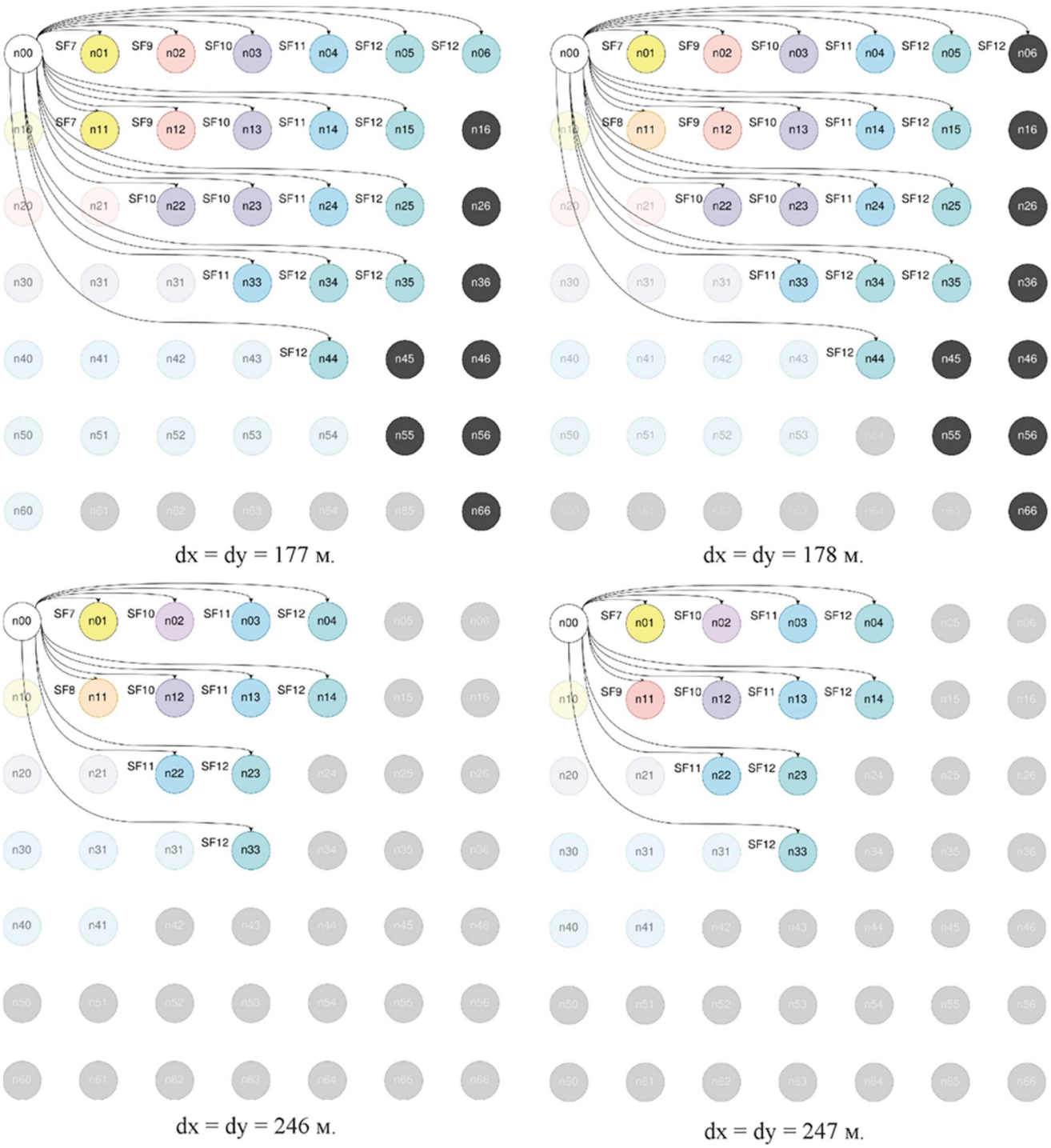

Рис. 4.8 – Мінімальні значення SF, необхідні для успішної доставки LoRa-пакета до різних вузлів від вузла n00

Зміна інтервальної відстані між вузлами з 177 м до 178 м унеможливлює діагональну передачу між суміжними вузлами при використанні SF7.

4.3.2 Характеристики мережевих вузлів та налаштування трафіку

У симуляції всі вузли налаштовані однаково, із застосуванням однакових параметрів фізичного рівня LoRa (потужність передавання, ширина смуги пропускання тощо), як зазначено в таблиці 4.7. Таким чином поведінка та продуктивність мережевих вузлів залежать виключно від положення у мережі та взаємодії з сусідніми вузлами. Більшість обраних параметрів конфігурації (SF, ширина смуги, довжина преамбули тощо) є типовими для реальних розгортань.

Відповідно до заданих параметрів у симуляторі, два вузли що використовують SF7 можуть успішно обмінюватися даними на відстані до 250 метрів. Отже, щоб досягти більш віддалених вузлів, необхідно або переходити на вищі значення SF або здійснювати пересилання пакетів через сусідні вузли, абож одночасно поєднувати обидві стратегії. Це обмеження максимальної відстані зв’язку також є підставою для вибору міжвузлових відстаней, описаних раніше в підрозділі 4.3.1.

Таблиця 4.7 – Загальні налаштування мережевих вузлів у симуляціях

Конфігурований параметр:	**Значення:**
Несуча частота	868 МГц
Ширина каналу	125 кГц
Фактор розширення спектру (SF)	7, 8, 9, 10, 11, 12
Потужність передавання	20 дБм
Коефіцієнт корекції (CR)	4/5
Довжина преамбули	16 символів

Задля повноти викладеного, у таблиці 4.6 наведено максимальні відстані передавання, яких може досягти вузол у симуляторі для всіх доступних значень SF. Ці значення залежать як від параметрів LoRa, зазначених у таблиці 4.7, так і від моделі розповсюдження радіосигналу, реалізованої в середовищі симуляції. За максимального значення 1058 м, досяжного при використанні SF12, зв’язок із віддаленими вузлами можливий лише за допомогою перехідної передачі.

Під час одного симуляційного дослвдження кожен вузол генерує загалом

$100 \times (N^2 - 1)$ унікальних пакетів даних (тобто по 100 різних пакетів для кожного з інших вузлів мережі), з фіксованим розміром 27 байт (заголовок + корисне навантаження). Передавання пакетів здійснюється поступово протягом симуляції з регулярними інтервалами: 100, 10, 1 та 0,1 секунди, що відповідає низькому, середньому, високому та граничному рівню насиченості трафіку відповідно. Пакети надсилаються у випадковому порядку, рівномірно розподіляючи навантаження між усіма вузлами мережі.

4.3.3 Порівняльний аналіз між продуктивністю реального обладнання та програмної симуляції

Було проведено простий бенчмарк, щоб перевірити, наскільки продуктивність мережі в симуляціях, реалізованих за допомогою фреймворку FLoRa, відповідає роботі реальних пристроїв. Експеримент складався з двох вузлів: один вузол безперервно передавав пакети протягом однієї години, тоді як інший здійснював їх прийом. Обмеження за часом передавання не застосовувалися тому передавач мав змогу займати ефірний час на 100 %.

Також виконано кілька симуляцій із різними розмірами навантаження для всіх значень SF від SF7 до SF12. Для кожного варіанту підраховувалася кількість отриманих пакетів, на основі чого обчислювалася фактична пропускна здатність. Паралельно проводився аналогічний експеримент на обладнанні з використанням двох пристроїв TTGO ESP32 та бібліотеки RadioLib для взаємодії з LoRa-трансівером.

У таблиці 4.7 наведено конфігурацію та налаштування вузлів, що використовувалися як у симульованому середовищі, так і в реальному експерименті. Варто зазначити, що через лабораторне розгортання реальних пристроїв на відстані лише 2 метрів один від одного, було застосовано мінімальний рівень потужності передавання, а до антени додатково під’єднано

атенюатор на 15 дБ для зменшення радіовипромінювання в навколишнє середовище.

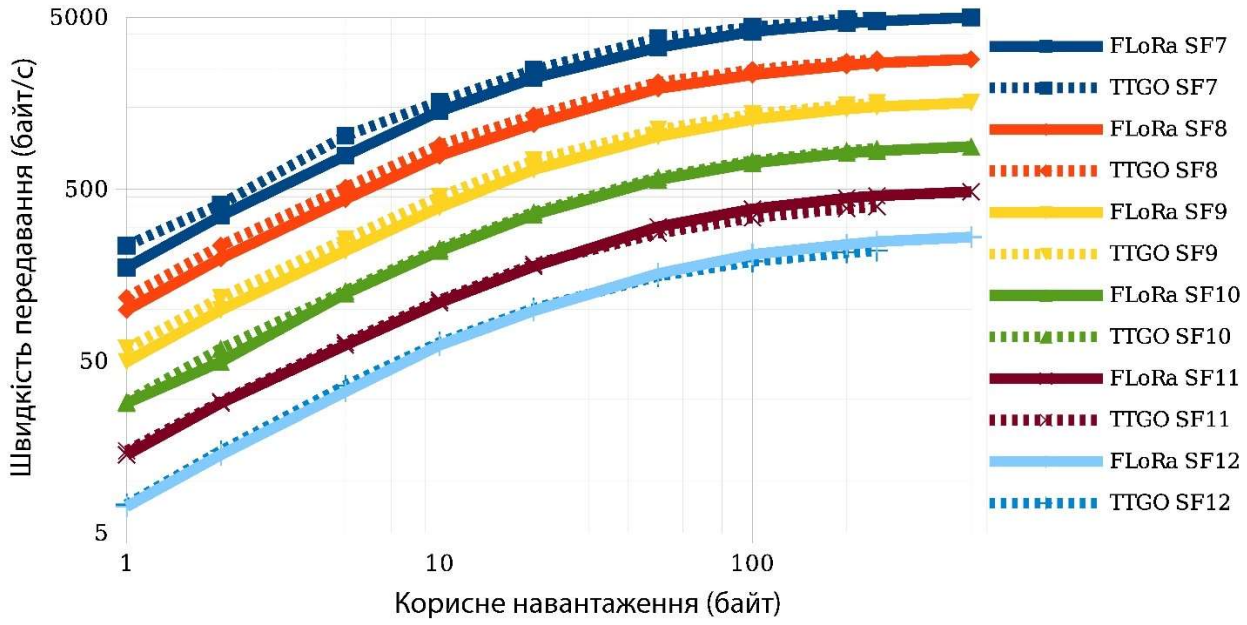

Рис 4.9 – Кореляція вимірювань отриманих з реального обладнання до даних отриманих в симуляції

На Рис 4.9 зображена максимальна односпрямована пропускна здатність за різних розмірів корисного навантаження для SF від 7 до 12. Суцільні лінії відповідають симуляціям у FLoRa, пунктирні відповідають результатам з двох пристроїв TTGO ESP32. На рисунку зображено досягнуту пропускну здатність між передавачем і приймачем як для симуляції у FLoRa, так і для фізичних пристроїв. Отримані значення варіюються від 7,4 біт/с (при мінімальному розмірі пакета 1 байт із використанням SF12) до приблизно 5 кбіт/с (при розмірі навантаження 250 байт і більше використовуючи SF7). Хоча результати симуляцій і експериментів на реальному обладнанні є загалом подібними, спостерігаються помітні відхилення.

Зокрема, при менших значеннях SF (швидших передачах) пропускна здатність на реальному обладнанні виявилася до 6 % вищою, ніж у симуляторі. Це може бути пов’язано зі способом обчислення часу передачі пакета в

програмному середовищі. Водночас продуктивність апаратних пристроїв дещо нижча при великих обсягах корисного навантаження, що ймовірно обумовлено особливостями обробки прийнятих пакетів на рівні вбудованого системного контролера (SoC).

Попри вказані відмінності, ми вважаємо, що фреймворк FLoRa є достатньо точним і забезпечує прийнятне середовище для проведення симуляційних досліджень.

4.4 Експериментальне дослідження протоколу самоорганізації

У цьому підрозділі проведено оцінювання запропонованого протоколу маршрутизації для самоорганізованих LoRa мереж. Було здійснено низку експериментів з використанням різних топологій, параметрів трафіку та конфігурацій вузлів з метою отримання детальної інформації щодо трьох ключових показників ефективності (KPI): масштабованості, пропускної здатності та затримки.

Для глибшого розуміння можливостей запропонованого протоколу експерименти виконувались із використанням різних стратегій маршрутизації та багатохопової передачі, описаних у підрозділі 5.2.5: широкомовної передачі (BC), кількості хопів (HC), очікуваної кількості передавань (ETX), рівня прийому сигналу (RSSI) та багатофакторної метрики часу в ефірі (multi-SF ToA)

4.4.1 Масштабованість сенсорної мережі за площею розгортання

Першим ключовим показником ефективності (KPI) є масштабованість, що дозволяє оцінити поведінку сенсорної мережі LoRa зі зростанням кількості вузлів. Масштабування може відбуватись двома способами: або шляхом розширення покриття (збільшення площі), або шляхом підвищення щільності вузлів при фіксованій площі.

Для дослідження поведінки розробленого протоколу маршрутизації в умовах масштабування, обумовлених особливостями радіотехнології LoRa, було проведено два набори експериментів відповідно до згаданих сценаріїв. У першому сценарії моделюється розгортання самоорганізованої сенсорної мережі зі зростанням кількості вузлів при незмінній відстані між ними що призводить до поступового збільшення охоплюваної площі. У другому досліджується поведінка мережі з фіксованою площею покриття, у межах якої поступово підвищується щільність розміщення вузлів.

З метою оцінки ефективності запропонованої мульти-SF маршрутизації на основі метрики часу в ефірі (ToA), експерименти виконувались при різних рівнях навантаження: низькому, середньому та високому. Для порівняння використовувались альтернативні стратегії маршрутизації з єдиним значенням SF : широкомовна передача (BC), кількості хопів (HC), очікуваної кількості передавань (ETX) та рівня прийому сигналу (RSSI). Мережеві розгортання моделювались із кількістю вузлів 9, 16, 25, 36, 49, 64, як у вигляді сіткової топології, так і у випадковому розподілі на еквівалентній площі. Для метрики ToA також тестувались усі можливі діапазони значень SF (SF7–8, SF7–9, SF7–10, SF7–11, SF7–12, SF8–9, SF8–10, SF8–11).

Згідно з гіпотезою, зі збільшенням кількості вузлів зростає середня відстань між довільною парою вузлів що потребує більшої кількості проміжних переходів для доставки пакетів. Це призводить до зростання кількості колізій, збільшення втрат пакетів і зниження загального PDR. Наша мета полягає у виявленні, чи дозволяє використання метрики часу в ефірі ToA у мульти-SF маршрутизації підвищити середній рівень PDR.

Спочатку моделюються розгортання мереж у регулярній сітковій топології з фіксованими горизонтальною (dx) та вертикальною (dy) відстанями між вузлами. Це означає, що зі збільшенням кількості вузлів пропорційно зростає і площа покриття. Тестуючи різні значення відстані (dx = dy), необхідно з’ясувати,

чи може протокол маршрутизації ефективно скористатися мульти-SF можливостями технології LoRa для покращення продуктивності.

Далі ті самі симуляції виконуються з єдиною відмінністю – вузли розташовуються випадковим чином у межах еквівалентної за розмірами області, що створює більш гетерогенну топологію. У таблиці 4.8 наведено використовувані варіанти топологій та їх просторові параметри.

Таблиця 4.8 – Список топологій, кількість вузлів, відстань між вузлами та загальна площа, використана в симуляції

Топологія	Кількість вузлів	Відстань між вузлами dx=dy	Площа
Сітчаста (правильної форми)	9	177 м. 178 м. 247 м. 248 м.	354 × 354 м² 356 × 356 м² 494 × 494 м² 496 × 496 м²
Випадкова	9	н/в н/в н/в н/в	354 × 354 м² 356 × 356 м² 494 × 494 м² 496 × 496 м
Сітчаста (правильної форми)	16	177 м. 178 м. 247 м. 248 м.	531 × 531 м² 534 × 534 м² 831 × 831 м² 834 × 834 м²
Випадкова	16	н/в н/в н/в н/в	531 × 531 м² 534 × 534 м² 831 × 831 м² 834 × 834 м²
…	…	…	…
Сітчаста (правильної форми)	64	177 м. 178 м. 247 м. 248 м.	1239 × 1239 м² 1246 × 1246 м² 1729 × 1729 м² 1736 × 1736 м²
Випадкова	64	н/в н/в н/в н/в	1239 × 1239 м² 1246 × 1246 м² 1729 × 1729 м² 1736 × 1736 м²

Через форму сіткової топології та крайовий ефект щільність вузлів (тобто співвідношення кількості вузлів до площі) не є сталою (Рис 4.10). Проте зі

збільшенням розміру мережі це значення асимптотично прямує до фіксованого, яке визначається виключно кількістю вузлів і відстанню між ними. Тому можна вважати що починаючи з 36 вузлів вплив крайового ефекту є незначним, тому кінцевий коефіцієнт доставки пакетів PDR визначатиметься переважно кількістю вузлів та площею покриття, а не їх щільністю.

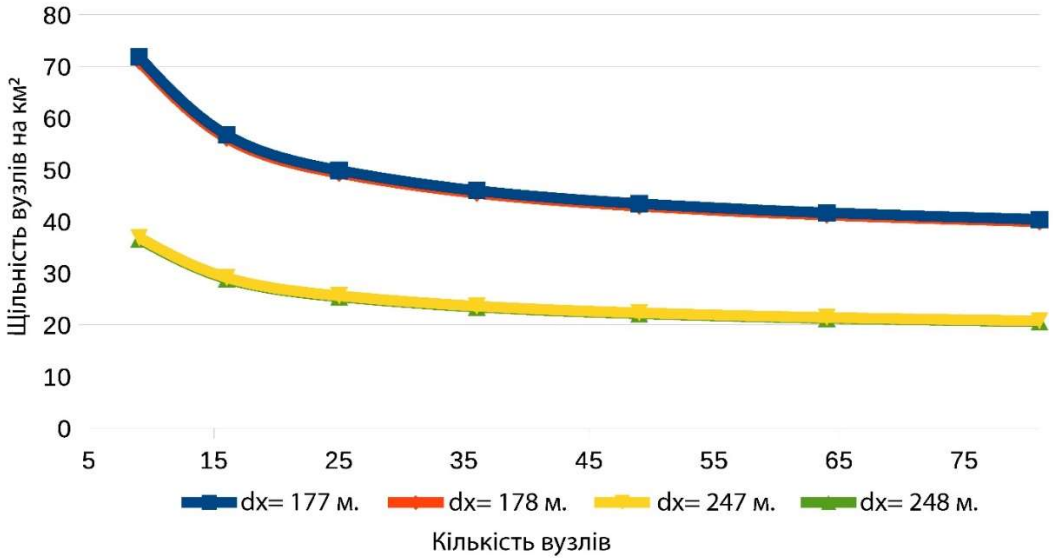

Рис. 4.10 – Щільність вузлів для різних інтервалів між вузлами

На Рис. 4.11 представлено середнє значення коефіцієнта доставки пакетів (PDR) у залежності від кількості вузлів, розгорнутих у сітковій топології, при використанні різних стратегій маршрутизації. Рис. 4.12 ілюструє ті самі експерименти для випадково розміщених вузлів на еквівалентній площі. Кожен із трьох рисунків відповідає окремому значенню відстані між вузлами.

Загальна тенденція відповідає очікуванням: PDR зменшується зі збільшенням кількості вузлів за винятком стратегій заснованих на flooding. Зокрема, у випадках низького та середнього трафіку найвищі показники PDR забезпечує стратегія передачі, що базується на широкомовній передачі (BC), з відповідно 99 % та 93 % успішно доставлених пакетів. Це пояснюється тим, що надлишковість широкомовної стратегії у поєднанні з відносною «вільністю» вузлів створює можливість дублювання пакетів, що підвищує ймовірність

успішної доставки хоча б однієї копії до адресата. Проте така надійність досягається ціною підвищеної затримки, оскільки пакети часто накопичуються в чергах на проміжних вузлах. Із підвищенням трафіку та насиченням каналів переваги BC-стратегії втрачаються вона не забезпечує значних переваг над іншими методами.

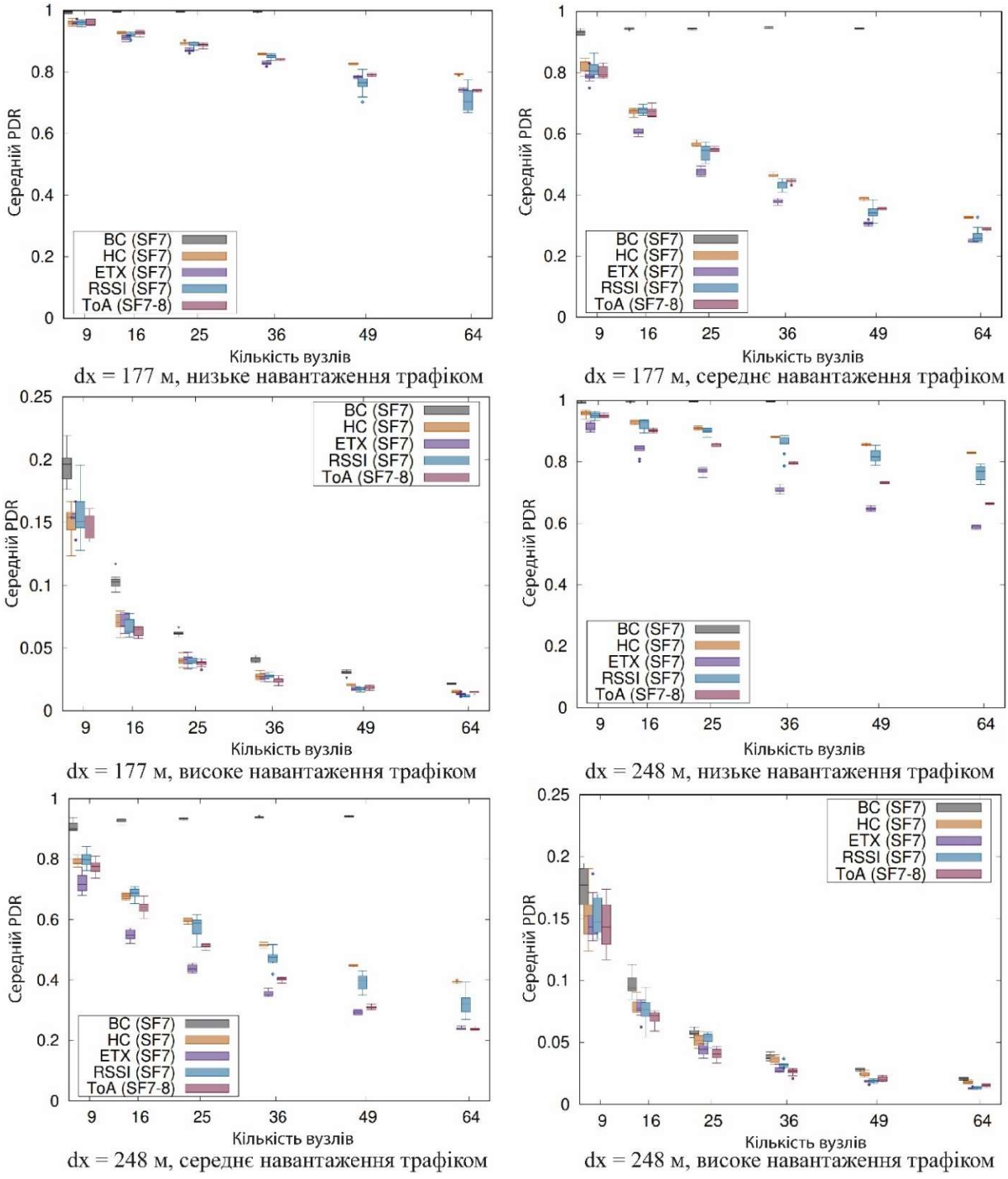

Рис. 4.11 – Середнє значення показника успішності доставки пакетів (PDR) у мережі при правильній сітчастій топологій

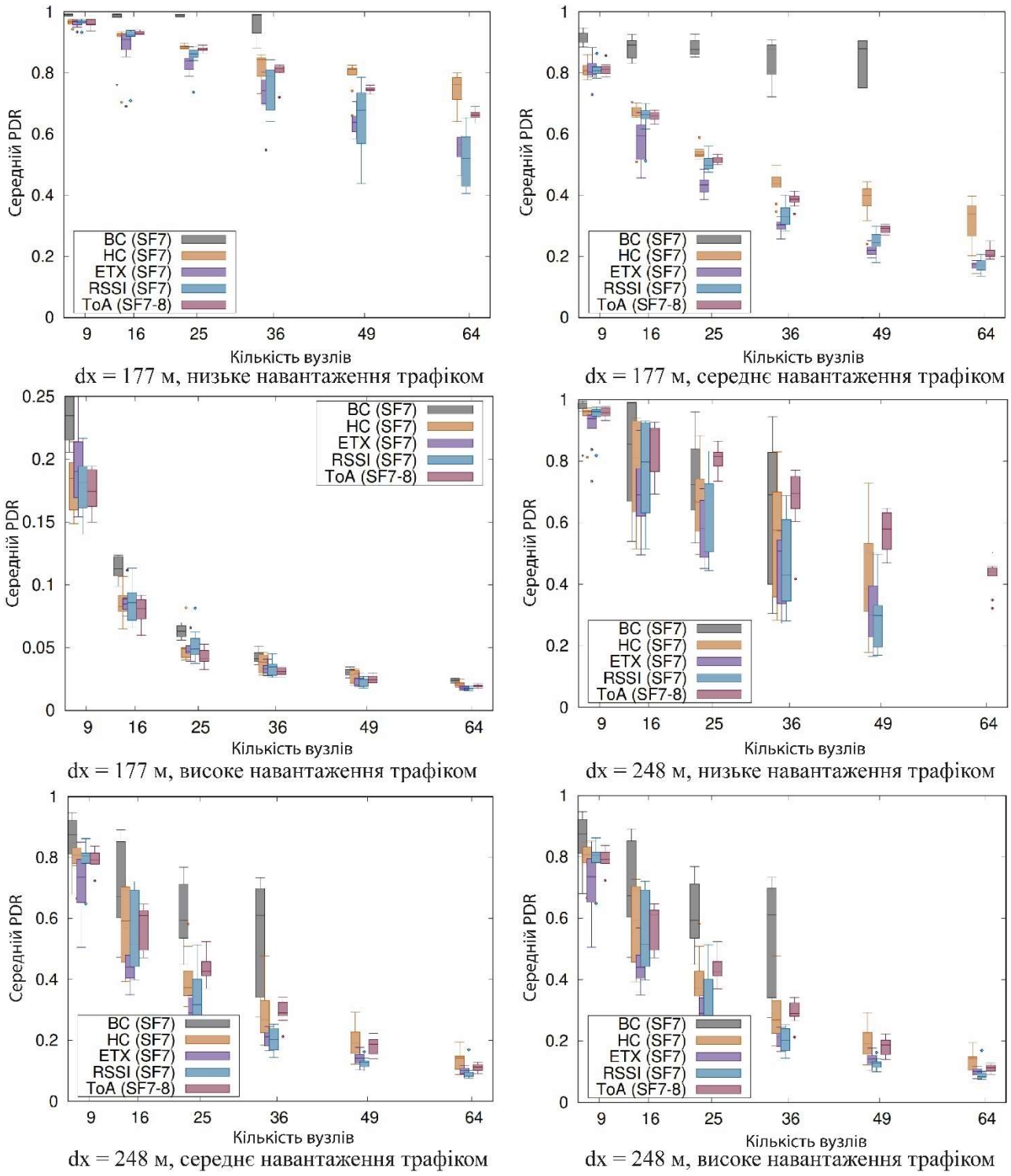

Рис. 4.12 – Середнє значення показника успішності доставки пакетів (PDR) у мережі при використані випадкової топології

Що стосується традиційних стратегій маршрутизації з фіксованим SF, найвищі показники PDR демонструє метрика HC, яка є найпростішою. Її результати майже збігаються з метрикою RSSI, яка також показує стабільну

ефективність. Метрика ETX, що враховує навантаження на мережу, демонструє гірші результати при низькому трафіку, але майже зрівнюється з HC у випадку інтенсивного навантаження.

Що ж до багатофакторної маршрутизації з використанням метрики ToA (мульти-SF), вона не демонструє суттєвих переваг щодо PDR і займає проміжну позицію між моно-SF метриками. Крім того, вона не використовує потенціал діагональних з'єднань, які можна було б задіяти за допомогою вищого SF, що дозволило б поєднувати кілька значень SF одночасно. Тому у межах сіткової топології з однаковою відстанню між усіма вузлами найбільш надійним підходом із точки зору доставки пакетів є використання простої моно-SF маршрутизації.

Симуляційні дослідження з випадковими топологіями мережі демонструють іншу картину, що добре видно на Рис. 4.12. Тут спостерігається, що метрика маршрутизації ToA із підтримкою мульти-SF забезпечує вищі показники PDR порівняно з одно-SF метриками в багатьох експериментальних сценаріях, а також характеризується стабільністю результатів (тобто меншою дисперсією) в різних симуляціях. Особливо помітне покращення у нижньому ряді рисунків з більшою площеюв 248 м. де вузли розміщені на більшій відстані один від одного.

Ці результати свідчать про те, що стратегія маршрутизації з підтримкою мульти-SF має позитивний вплив на вузли, які через своє випадкове розміщення є більш ізольованими і мають менше можливостей для зв'язку порівняно з вузлами, що перебувають у центрі мережі. Іншими словами, метрика час в ефірі ToA краще адаптується до випадкових гетерогенних топологій мережі та забезпечує збалансованішу якість обслуговування вузлів із різним ступенем центральності. Переваги цієї стратегії також простежуються за показником ефективної пропускної здатності який буде розглянуто далі в наступному підрозділі.

Таким чином, можна зробити висновок, що маршрутизаційні стратегії з підтримкою кількох значень SF, зокрема запропонована метрика ToA, можуть

мати позитивний вплив на коефіцієнт доставки пакетів (PDR) що є одним із головних показників масштабованості. Ці стратегії краще справляються з неоднорідністю каналів зв’язку, ніж інші стратегії, покращуючи загальну продуктивність мережі. Водночас, у мережах із дуже регулярною структурою, таких як сітка ці стратегії не дають переваг. Враховуючи, що в реальних розгортаннях мереж вузли зазвичай розміщуються в неоднорідних умовах та зазнають впливу різних факторів середовища (затухання, завади, кількість сусідів тощо), застосування метрики ToA у мульти-SF маршрутизації може полегшити побудову сенсорних LoRa мереж і покращити їхню ефективність.

4.4.2 Вплив щільності розміщення вузлів на роботу сенсорної мережі

У цьому підрозділі проведено серію експериментів для аналізу масштабованості мережі за умов зростання кількості вузлів, що підвищує їхню щільність. Як основну метрику ефективності використано коефіцієнт доставки пакетів (PDR) між кінцевими вузлами усереднений для всієї мережі. Із збільшенням кількості вузлів на фіксованій площі зростає інтенсивність радіопередач, що призводить до зростання ймовірності колізій та до зниження PDR. Основна мета цього етапу дослідження це з’ясувати чи може одночасне використання кількох значень SF зменшити кількість колізій і тим самим підвищити середній PDR.

Для цього було змодельовано декілька варіантів мережевих розгортань із кількістю вузлів 9, 16, 25, 36, 49, 64 на фіксованій площі розміром 500 × 500 м². Зі збільшенням кількості вузлів при незмінній площі зростає і щільність мережі. Для оцінки ефективності запропонованого мульти-SF протоколу маршрутизації на основі метрики ToA було проведено тестування за трьома сценаріями навантаження: низьке, середнє та високе із подальшим порівнянням з іншими стратегіями: BC, HC, ETX та RSSI. Метрику ToA тестували з усіма можливими

комбінаціями SF (SF7–8, SF7–9, SF7–10, SF7–11, SF7–12, SF8–9, SF8–10, SF8–11 тощо).

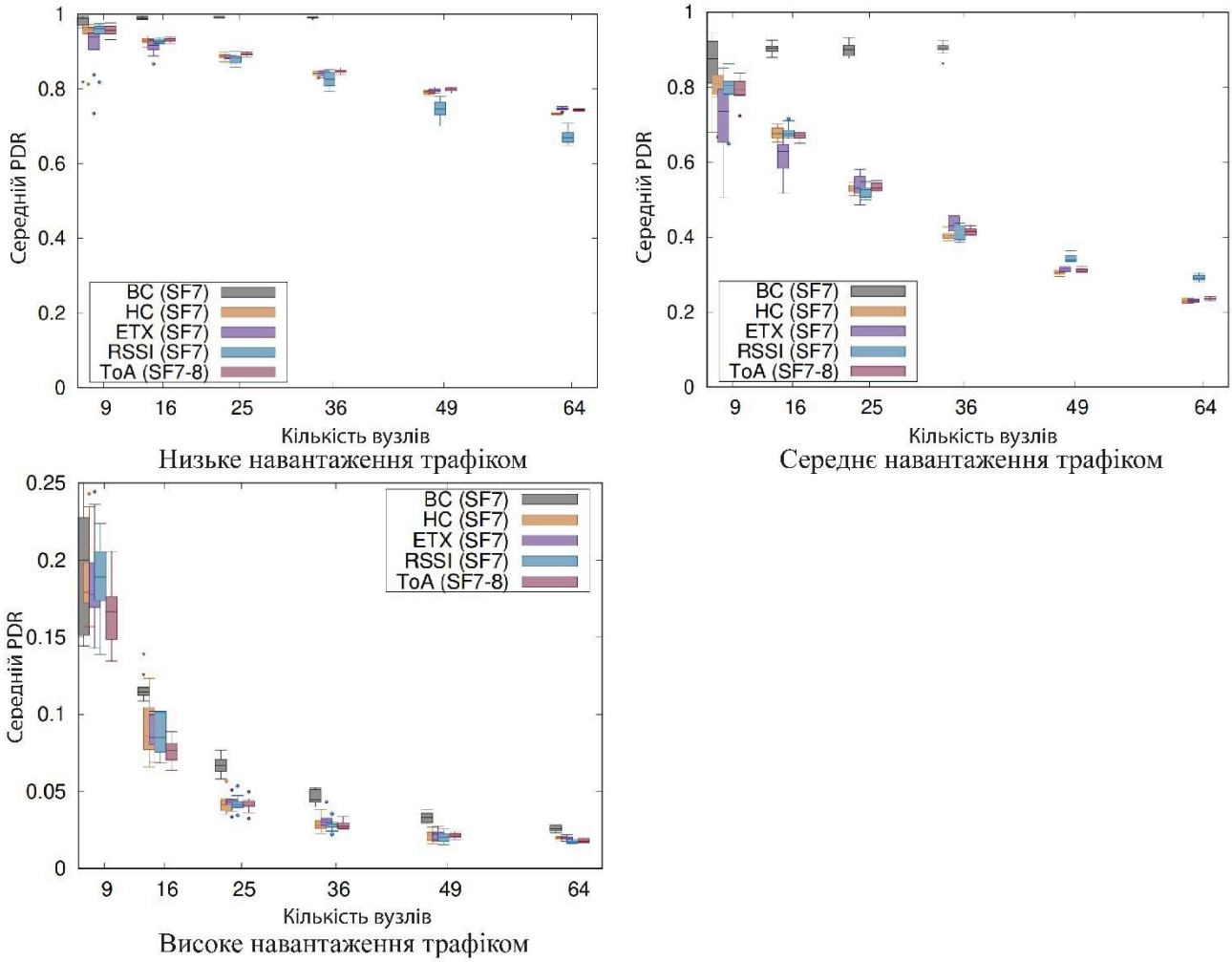

Рис. 4.13 – Середній показник успішності доставки пакетів (PDR) у мережі для вузлів у правильній сітчастій топології на фіксованій площі 500 × 500 м²

На рисунку 4.13 та рисунку 4.14 наведено середнє значення PDR залежно від кількості вузлів, за умов використання різних стратегій маршрутизації. На першому рисунку зображено результати для сітчастої топології, на другому для випадкового розміщення вузлів з рівномірним розподілом Кожен рисунок містить три підрисунки, що відповідають різним рівням трафіку: низькому, середньому та високому.

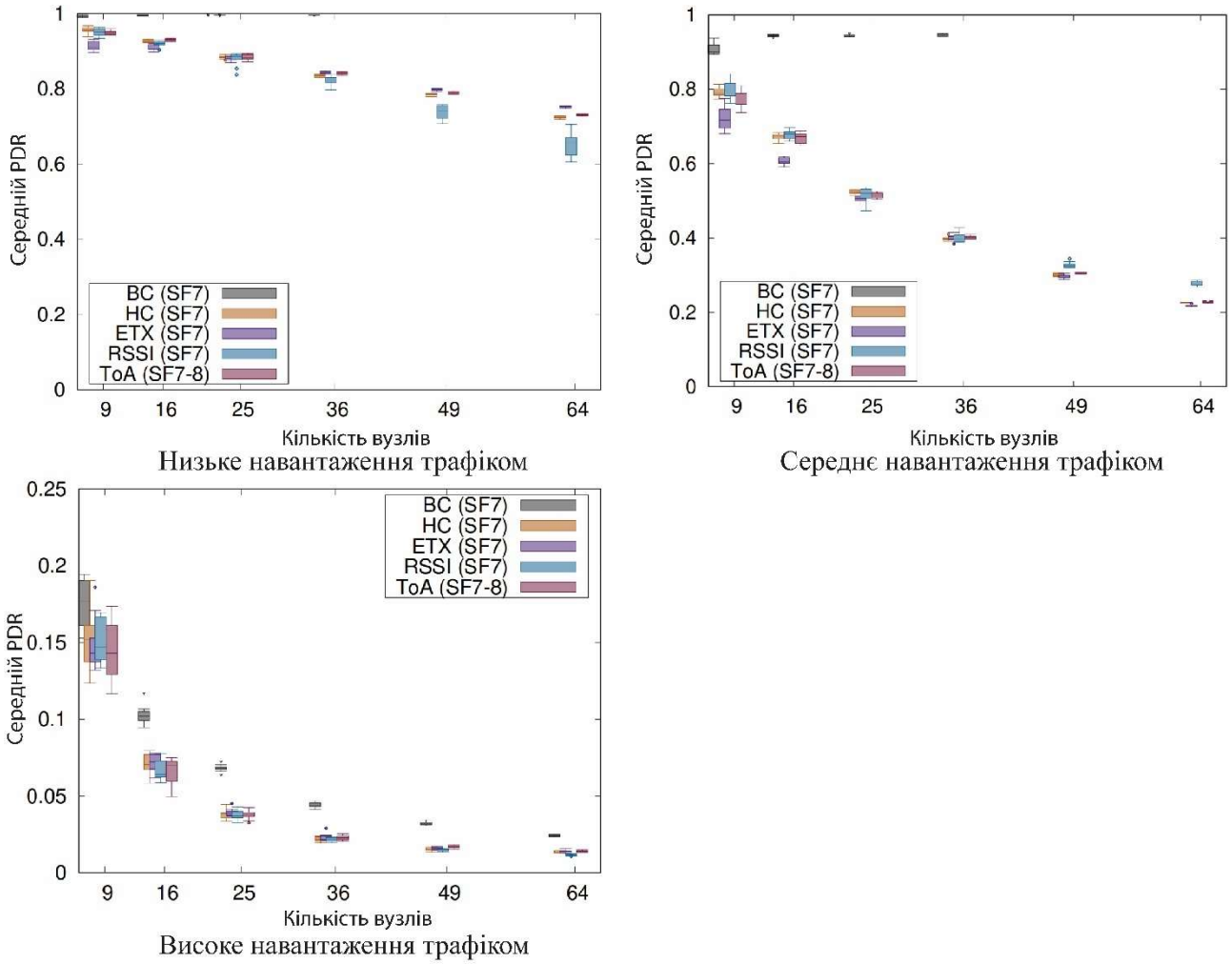

Рис. 4.14 – Середній показник успішності доставки пакетів (PDR) у мережі для вузлів у випадковій топології на фіксованій площі 500 × 500 м²

У сценаріях з низьким і середнім навантаженням стратегія BC демонструє найвищі показники PDR. Оскільки пакети передаються широкомовно і дублюються на кожному вузлі, створюючи ефект затоплення мережі, ймовірність доставки принаймні однієї копії пакета до пункту призначення є дуже високою, що компенсує потенційні колізії. Реальні стратегії маршрутизації (HC, ETX, RSSI та ToA) виявляють майже лінійну залежність між кількістю вузлів та значенням PDR. Їхні результати незначно коливаються залежно від топології та кількості вузлів, однак загальна картина залишається стабільною, що свідчить про відсутність суттєвих відмінностей між цими стратегіями в умовах помірного трафіку.

Із зростанням навантаження мережа поступово переходить у стан перевантаження, що підвищує ймовірність колізій відповідно знижує PDR. У таких умовах переваги широкомовної стратегії BC зменшуються оскільки перевантажена мережа вже не здатна ефективно ретранслювати дублікати пакетів до їх кінцевих одержувачів.

Згідно з отриманими результатами застосування мульти-SF підходу з використанням метрики ToA не забезпечує очевидної переваги над моно-SF стратегіями за показником PDR. Водночас симуляційні дослідження показують що комбінація різних SF дійсно сприяє покращенню PDR у сильно перевантажених мережах де вузли безперервно генерують трафік. У таких умовах, незалежно від топології, моно-SF маршрутизація забезпечує PDR на рівні лише ~0,001 (тобто успішно доставляється лише один пакет із тисячі) у мережі з 16 вузлами, тоді як мульти-SF стратегія на основі ToA досягає приблизно 0,01 (тобто один пакет із сотні). Отже, ефект від використання мульти-SF є помітним, хоча й недостатнім для значного покращення продуктивності в умовах регулярної та однорідної топології типу сітка.

4.4.3 Пропускна здатність сенсорної мережі

Окрім масштабованості та коефіцієнту доставки пакетів (PDR), розглянутих вище, важливим показником ефективності (KPI) для аналізу є пропускна здатність яка дозволяє оцінити який обсяг даних здатна обробляти сенсорна мережа на базі LoRa. У підрозділі 4.3.3 було проведено простий бенчмарк, що показав максимальну пропускну здатність, яку можуть забезпечити два вузли LoRa за ідеальних умов За розміру корисного навантаження, аналогічного тому, що використовується в симуляціях, досягнута пропускна здатність варіювалася від 2500 біт/с до 100 біт/с залежно від застосованого значення SF (кожне підвищення SF на один рівень зменшує швидкість приблизно вдвічі).

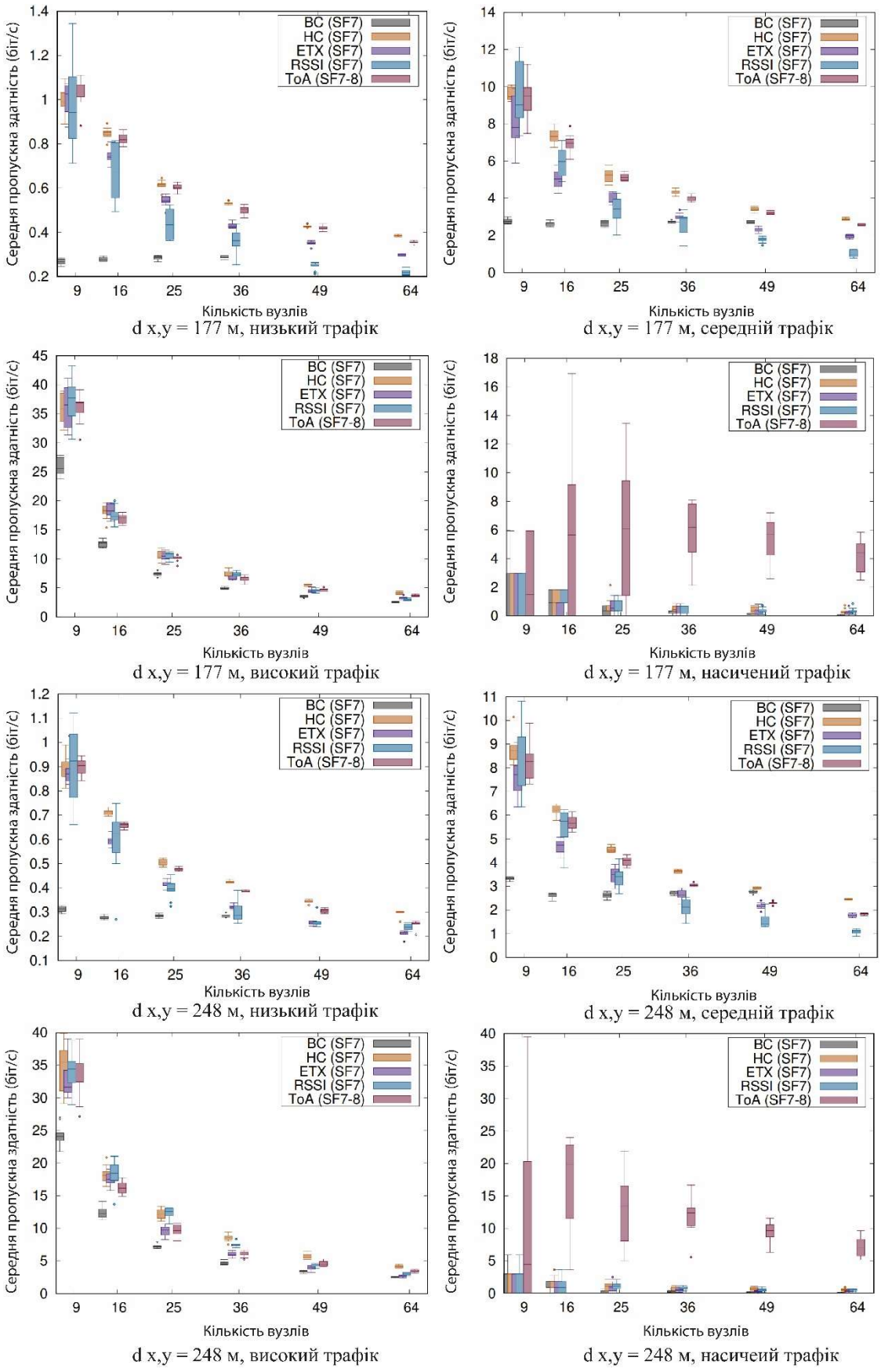

Рис 4.15 – Середня ефективна пропускна здатність мережі для різної кількості вузлів у правильній сітчастій топології

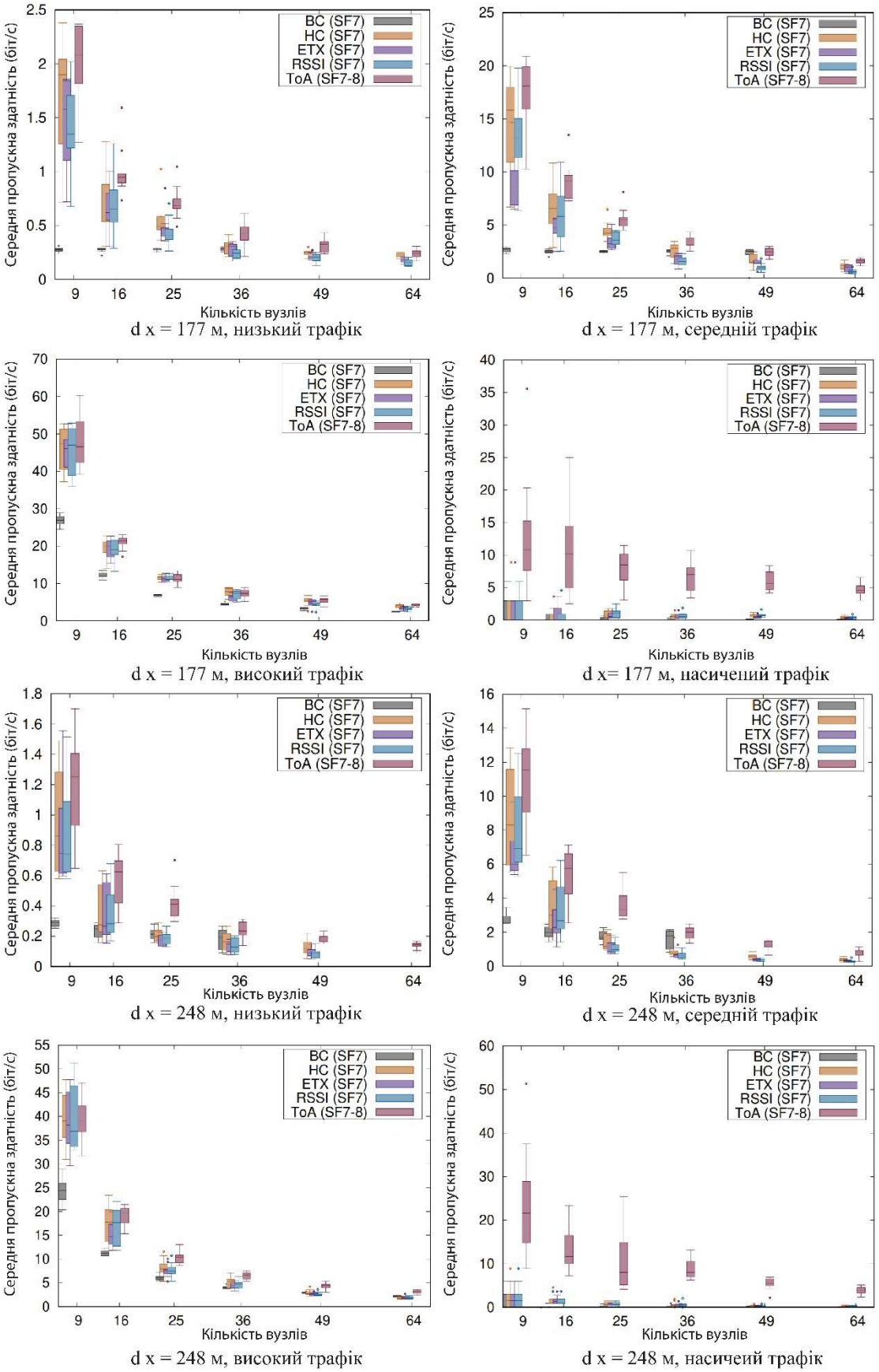

Рис 4.16 – Середня ефективна пропускна здатність мережі для різної кількості вузлів у випадковій топології

Експерименти з LoRa mesh-мережею в умовах симуляції істотно відрізняються від раніше виконаного бенчмарку. По-перше, через відсутність планувальника, який би координував передачу пакетів у мережі, неминуче виникатимуть колізії. Їхня частота залежить переважно від кількості вузлів, топології мережі та інтенсивності передавання пакетів. По-друге, частина доступного часу ефірного ресурсу буде витрачатися не на передачу корисних даних, а на широкомовну трансляцію маршрутних повідомлень. По-третє, багатоперехідна передача даних між довільними парами вузлів потребує залучення проміжних вузлів-ретрансляторів, які витрачають власний ресурс часу на передачу трафіку інших вузлів.

З огляду на ці фактори, слід очікувати, що фактичні показники пропускної здатності в умовах симуляції будуть значно нижчими, ніж ті, що були зафіксовані в умовах ідеального тестування.

На Рис 4.15 зображено середнє значення ефективної пропускної здатності досягнутої мережею яке було усереднене по всіх вузлах. Вузли були розміщені відповідно до сіткової топології з постійними горизонтальними та вертикальними відстанями 177 та 248 метрів, і дослідження проводилося за умов низького, середнього, високого та пікового (насиченого) навантаження. Кожен із чотирьох сценаріїв трафіку демонструє різну поведінку мережі, що дозволяє краще зрозуміти показник пропускної здатності в контексті сенсорних LoRa мереж.

У випадках низького та середнього навантаження як стратегії маршрутизації з одним значенням SF, так і мульти-SF підходи забезпечують подібні результати: метрики HC та ToA демонструють порівнювані значення ефективності передавання. Інші моно-SF метрики зазвичай мають дещо гірші результати. Водночас слід зауважити, що стратегії широкомовної передачі (BC) та на базі одноплатних комп’ютерів (SBC) найкращі результати за PDR, досягли цього ціною значного зниження ефективної пропускної здатності.

Із підвищенням навантаження до високого рівня метрика мульти-SF ToA забезпечує дещо кращу ефективну пропускну здатність порівняно з моно-SF метриками. Спостерігається, що ця метрика може використовувати діагональні з’єднання за рахунок переходу на вищий SF, особливо помітно це у топологіях із міжвузловими відстанями 177 та 178 м.

У сценаріях з високим трафіком, де зв’язки починають насичуватися, переваги між моно та мульти-SF підходами стають менш вираженими: деякі експерименти демонструють незначну перевагу, інші навіть погіршення. Це свідчить про те, що додаткова складність мульти-SF маршрутизації на базі ToA не завжди виправдана в умовах простої та регулярної топології.

Проте у випадку насиченого трафіку (коли всі вузли намагаються передавати пакети максимально часто) метрика мульти-SF ToA забезпечує механізм часткового розвантаження мережі. Завдяки одночасному використанню кількох SF, трафік розподіляється між накладеними шарами мережі, що частково розвантажує ефір та знижує ймовірність колізій. Таким чином, кожен вузол здатен коректно передавати хоча б кілька бітів за секунду, тоді як при використанні моно-SF метрик ефективність передавання практично дорівнює нулю.

Варто зазначити, що навіть найкращі досягнуті значення ефективністі передавання (близько 16 біт/с при SF8) є значно нижчими від ідеальних результатів, отриманих у бенчмарку в підрозділі. Але вони узгоджуються з обмеженнями самої радіотехнології та складністю досліджуваної топології і сценаріїв трафіку.

На Рис 4.16 зображено середнє значення ефективної пропускної здатності, досягнутої мережею та усередненої для всіх вузлів. Вузли розташовуються випадковим чином на площі, аналогічній до тієї, що використовувалася в попередніх експериментах. У цьому випадку метрика маршрутизації мульти-SF ToA демонструє здатність адаптуватися до гетерогенності мережі, що позитивно позначається на показниках продуктивності. У більшості проведених

експериментів найвищі значення ефективної пропускної здатності досягаються саме при використанні метрики ToA (як у режимі низького, так і середнього та високого навантаження).

Доцільно порівняти співвідношення між досягнутою ефективною пропускної здатністю та загальною пропускною здатністю, аби оцінити ефективність мережі в контексті забезпечення наскрізної передачі даних між вузлами. Наприклад, у сценарії низького навантаження для сіткової топології з 9 вузлами, розташованими на відстані 177 м, використання метрики ToA з двома SF (8 та 9) дозволяє досягти середнього пропускної здатності на рівні 1,85 біт/с, при цьому ефективна пропускна здатність становить трохи менше ніж 1,2 біт/с. За умов високого PDR (тобто за незначних втрат пакетів) це означає, що для передачі одного пакета від вузла-джерела до вузла-приймача в середньому потрібно приблизно 1,5 переходи, що відповідає масштабам даної мережі.

Варто зазначити, що це співвідношення залежить від кількості вузлів, міжвузлової відстані, навантаження та обраної стратегії маршрутизації. Значення, близьке до 1, може свідчити про використання меншої кількості переходів для передачі даних між вузлами (наприклад, завдяки використанню SF із більшим радіусом дії), тоді як вищі значення можуть вказувати на більшу кількість пересилань необхідних для доставлення одного пакета, що може бути наслідком як меншого радіусу дії SF, так і втрат пакетів.

Разом з тим рисунки які відповідають сценарію насиченого трафіку, демонструють, що вузли, які використовують мульти-SF ToA, здатні скористатися ортогональністю між різними SF, досягаючи значень ефективної пропускної здатності у межах десятків бітів за секунду.

Аналіз пропускної здатності та ефективної пропускної здатності мережі за різної кількості вузлів, топологій і рівнів навантаження засвідчив, що досягнуті вузлами швидкості передачі даних є на два-три порядки нижчими за результати, зафіксовані в умовах ідеального бенчмарку. Водночас можна зробити висновок, що одночасне використання кількох значень SF має обмежений вплив на

продуктивність у режимах низького, середнього та високого навантаження, однак відіграє критично важливу роль у сценаріях з насиченим трафіком. У таких умовах мульти-SF значно підвищує як загальну, так і ефективну пропускну здатність мережі. Це дозволяє стверджувати, що для досягнення максимальної продуктивності сенсорних LoRa мереж доцільно використовувати мульти-SF режим роботи.

4.4.4 Затримки передавання мережевих пакетів у сенсорній мережі

Останнім показником ефективності (KPI), який аналізується для запропонованого протоколу маршрутизації, є затримка пакетів. На відміну від архітектури LoRaWAN, де передавання пакетів здійснюється за принципом одного хопа і має практично незначну затримку, в контексті багатохопових mesh-мереж цей показник набуває суттєвого значення і потребує окремого розгляду.

На рисунку 4.15 показано середнє значення затримки, яку зазнають пакети під час проходження через мережу з правильною сітковою топологією та двома варіантами міжвузлової відстані (177 м. і 248 м.). У розрахунках враховуються лише ті пакети що були успішно доставлені від джерела до одержувача, пакети, які зазнали колізій і були втрачені не включено до підрахунку. Аналогічно, рисунок 4.16 демонструє результати експериментів для топологій з випадковим розміщенням вузлів на ділянці того ж самого розміру.

Результати для обох типів топологій демонструють, що метрики маршрутизації з моно-SF і з мульти-SF забезпечують подібні показники затримки, хоча в окремих випадках спостерігаються певні відмінності. Стратегії маршрутизації на основі широкомовної передачі (BC) забезпечують значно вищу затримку (до трьох порядків вище), оскільки часто призводять до перевантаження каналів зв’язку та заповнення буферів вузлів. Це свідчить про те, що вони є вкрай неефективними для багатперехіжної маршрутизації.

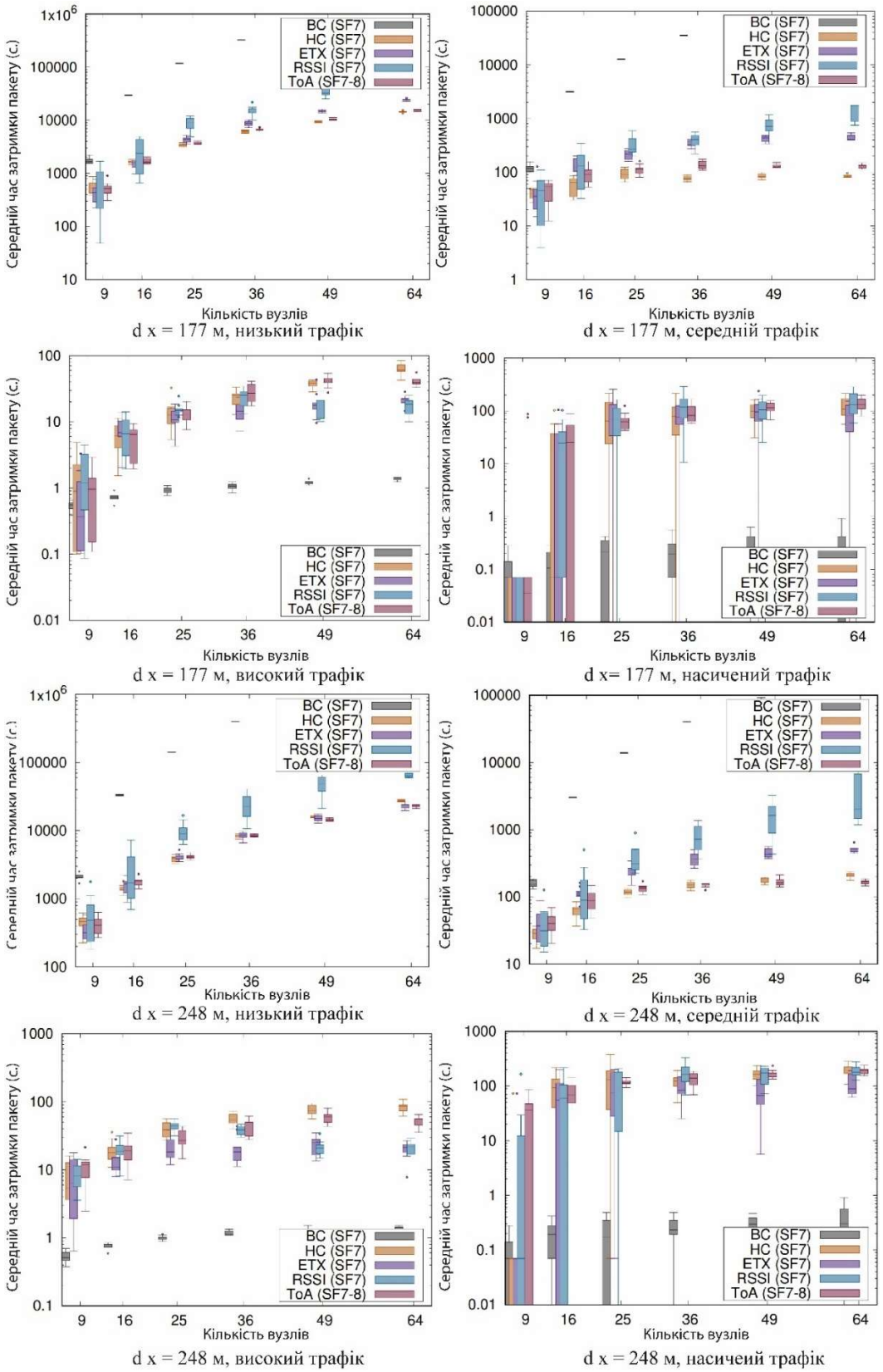

Рис. 4.15 – Середня затримка в мережі для різної кількості вузлів сітчастій топології з постійною горизонтальною та вертикальною відстанню між вузлами 177 та 248 м, із використанням різних стратегій маршрутизації.

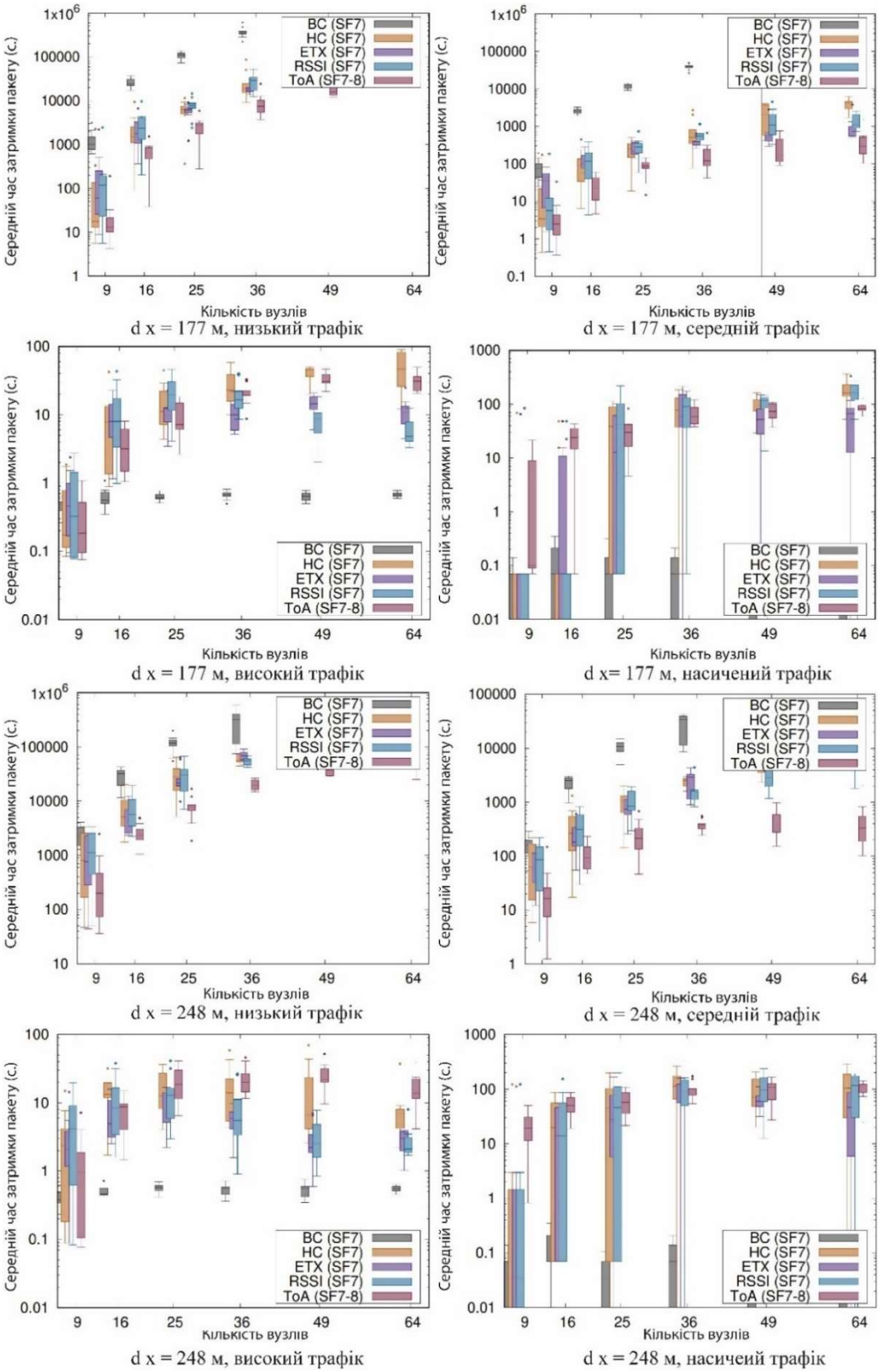

Рис. 4.16 – Середня затримка в мережі для різної кількості вузлів сітчастій топології з випадковою горизонтальною та вертикальною відстанню між вузлами 177 та 248 м, із використанням різних стратегій маршрутизації.

Метрики що базуються на моно-SF, демонструють стабільні результати, хоча окремі метрики можуть мати кращі показники в умовах різного навантаження трафіку або для різних топологій.

Використання мульти-SF підходу з метрикою ToA забезпечує найнижчі затримки у сценаріях з низьким і середнім навантаженням трафіку, особливо в умовах випадкової топології, де ця стратегія ефективно використовує різноманітність у розміщенні вузлів та характеристиках зв'язків між ними.

Слід також зазначити, що в умовах низького навантаження трафіку, коли вузли надсилають щонайбільше один пакет кожні 100 секунд, спостерігаються надзвичайно великі значення затримки в десятках тисяч секунд. Це зумовлено як кількістю переходів, необхідних для досягнення пункту призначення, так і часом очікування в буферах проміжних мережевих вузлів.

Висновки до розділу 4

У четвертому розділі дисертаційної роботи було реалізовано прототип сенсорної мережі з підтримкою багатоперехідної передачі на що дозволило здійснити перевірку ефективності запропонованого методу конфігурації мереж із застосуванням нового методу самоконфігурації. Досліджено особливості побудови самоконфігурованих мереж з гнучкою та топологією. Проаналізовано результати реальних випробувань із вимірюванням показників продуктивності у різних топологічних схемах у тому числі з використанням проміжних вузлів для ретрансляції повідомлень.

Проведено порівняльний аналіз ефективності передачі в одноперехідному та багатоперехідному режимах з урахуванням впливу перешкод, відстані між вузлами та особливостей розміщення антен.

Розглянуто вплив кількості проміжних вузлів на ймовірність доставки повідомлень і затримку поширення даних. Визначено що впровадження нового механізму маршрутизації з динамічною детекцією фактору розширення SF в

використанням метрики Час в Ефірі (ToA) суттєво підвищує надійність мережі в умовах відсутності прямої видимості з базовим шлюзом або у режимах з піковим навантаженням.

В результаті дослідження було вперше розроблено метод визначення маршруту передавання даних між вузлами сенсорної мережі, який за допомогою самоорганізації використовує подвійні фактори розширення модуляції для надання пріоритету більш швидкому передаванню даних, але одночасно перевіряє можливість передачі даних на більшу відстань.

На основі теорії зважених графів Беллмана – Форда був побудований дистанційно- векторний протокол маршрутизації, який використовує нову метрику і дозволяє визначити загальний час передавання пакету даних вздовж усього маршруту.

Під час проведення імітаційного моделювання запропонованих рішень маршрутизації було виявлено:

- Метрика «Час в ефірі» динамічно адаптується до випадкових гетерогенних топологій мережі та забезпечує достатню якість обслуговування вузлів із різним ступенем центральності (топологія з випадковим розміщенням вузлів).

- У випадку насиченого трафіку у сенсорній мережі (коли всі вузли передають пакети максимально часто) метрика «Час в ефірі» забезпечує механізм часткового розвантаження мережі. Завдяки одночасному використанню вузлами кількох факторів розширення модуляції, трафік розподіляється між накладеними шарами мережі, що частково розвантажує ефір та знижує ймовірність колізій.

- Одночасне використання декількох факторів розширення модуляції у поєднанні з новою метрикою маршрутизації забезпечує найнижчі затримки у сценаріях з низьким і середнім навантаженням трафіку, особливо в умовах випадкової топології.

ВИСНОВКИ

Дисертація присвячена дослідженню проблеми побудови, оптимізації, розгортання та тестування бездротових сенсорних мереж із застосуванням самоорганізації.

У роботі проаналізовано сучасний стан і тенденції розвитку технологій бездротових сенсорних IoT мереж з акцентом на перспективи їх використання у складних середовищах з обмеженими ресурсами. Проведено дослідження архітектур, топологій та методів конфігурації сенсорних мереж із підтримкою самоорганізації.

При проведеному аналізі виявлені недоліки існуючих рішень, а саме: обмеження щодо масштабованості, енергоефективності та здатності до самоадаптації в гетерогенних умовах експлуатації.

Основну увагу приділено моделі побудови оптимальної сенсорної мережі, застосовуючи метод багатокритеріального аналізу та теорію розподілених систем. Головними перевагами запропонованого підходу є здатність до зваженого прийняття рішень щодо конфігурації, масштабованості, енергоефективності.

У роботі представлений удосконалений метод взаємодії вузлів сенсорної мережі, який за рахунок використання розробленої моделі мультипротокольної сенсорної мережі оскільки успішність передачі пакетів у сенсорній мережі істотно залежить від кількості шлюзів задіяних у топології.

Комплексне врахування спектральних параметрів сигналу дозволяє підвищити відсоток успішно переданих повідомлень у сенсорній мережі за рахунок використання службових повідомлень що підтверджують отримання пакету даних, ефект від використання повідомлень що підтверджують отримання пакету даних особливо помітний у режимі роботи мережі з недостатньою кількістю шлюзів де відсоток успішно переданих повідомлень збільшується в середньому на 40%.

Вперше розроблено метод визначення маршруту передавання даних між вузлами сенсорної мережі, який за допомогою самоорганізації використовує подвійні фактори розширення модуляції для надання пріоритету більш швидкому передаванню даних, але одночасно перевіряє можливість передачі даних на більшу відстань.

На основі теорії зважених графів Беллмана–Форда був побудований дистанційно-векторний протокол маршрутизації, який використовує нову метрику і дозволяє визначити загальний час передавання пакету даних вздовж усього маршруту.

На основі запропонованих моделей та методів розроблено програмний комплекс, що дозволяє експериментально оцінити розроблені метод.

Результати експериментальних досліджень дозволили зробити такі висновки:

- Метрика «Час в ефірі» динамічно адаптується до випадкових гетерогенних топологій мережі та забезпечує достатню якість обслуговування вузлів із різним ступенем центральності (топологія з випадковим розміщенням вузлів).

- У випадку насиченого трафіку у сенсорній мережі (коли всі вузли передають пакети максимально часто) метрика «Час в ефірі» забезпечує механізм часткового розвантаження мережі. Завдяки одночасному використанню вузлами кількох факторів розширення модуляції, трафік розподіляється між накладеними шарами мережі, що частково розвантажує ефір та знижує ймовірність колізій.

- Одночасне використання декількох факторів розширення модуляції у поєднанні з новою метрикою маршрутизації забезпечує найнижчі затримки у сценаріях з низьким і середнім навантаженням трафіку, особливо в умовах випадкової топології.

Розроблені моделі та методи успішно впроваджено у виробничий процес ТОВ "УКР-ОН" та ТОВ "КАРНІФЕКС", та в начальний процес Державного

університету інформаційно-комунікаційних технологій що підтверджує їх практичну цінність,

Перспективними напрямками подальших досліджень є адаптація методу побудови сенсорних мереж для взаємодії з сенсорними вузлами що динамічною рухаються в мережевій топології. Також перспективним напрямком є дослідження можливості до самоорганізації використовуючи методи машинного навчання та штучного інтелекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Teel J. Comparison of Wireless Technologies: Bluetooth, WiFi, BLE, Zigbee, Z-Wave, 6LoWPAN, NFC, WiFi Direct, GSM, LTE, LoRa, NB-IoT, and LTE-M. PREDICTABLE DESIGNS. URL: https://predictabledesigns.com/wireless_ technologies_bluetooth_wifi_zigbee_gsm_lte_lora_nb-iot_lte-m/ (дата звернення: 12.05.2023).

2. Teel J. Comparison of Wireless Technologies: Bluetooth, WiFi, BLE, Zigbee, Z-Wave, 6LoWPAN, NFC, WiFi Direct, GSM, LTE, LoRa, NB-IoT, and LTE-M. PREDICTABLE DESIGNS. URL: https://predictabledesigns.com/wireless_ technologies_bluetooth_wifi_zigbee_gsm_lte_lora_nb-iot_lte-m/ (дата звернення: 12.05.2023).

3. Sigfox technical overview. Labrège : Bâtiment E-volution, 2017. 25 p. URL: https://www.ismac-nc.net/wp/wp-content/uploads/2017/08/sigfoxtechnicaloverview july2017-170802084218.pdf. (дата звернення: 12.05.2023)

4. Standardization of NB-IOT completed. 3GPP – The Mobile Broadband Standard. URL: https://www.3gpp.org/news-events/3gpp-news/nb-iot-complete (date of access: 12.05.2023).

5. A Primer on 3GPP Narrowband Internet of Things / Y. P. E. Wang та ін. IEEE Communications Magazine. 2017. Т. 55, № 3. С. 118–124. URL: https://doi.org/10 .1109/mcom.2017.1600510cm (дата звернення: 25.01.2023).

6. What is LPWAN technology - use case and applications. The IoT Academy Blogs - Best Tech & Guides. URL: https://www.theiotacademy.co/blog/lpwan-technology/ (дата звернення: 12.05.2023).

7. Evjen P. M. The Wize Protocol. https://radiocrafts.com. URL: https:// radiocrafts.com/uploads/WP016_Wize_Protocol_For_LPWAN.pdf.

8. Internet of mobile things: overview of lorawan, DASH7, and nb-iot in lpwans standards and supported mobility / W. Ayoub та ін. IEEE communications surveys &

tutorials. 2019. Т. 21, № 2. С. 1561–1581. URL: https://doi.org/10.1109/comst.2018.2877382 (дата звернення: 25.01.2023).

9. Information technology -- Radio frequency identification for item management -- Part 7: Parameters for air interface communications at 433 MHz. Official edition. International Organization for Standardization, 2014. URL: https://cdn.standards.iteh.ai/samples/57336/d6991f6287394945813d5a4416adf0dc/ISO-IEC-18000-7-2014.pdf. (дата звернення: 18.05.2023)

10. Comparative study of LPWAN technologies on unlicensed bands for M2M communication in the IoT: beyond LoRa and LoRaWAN / J. P. Queralta та ін. Procedia computer science. 2019. С. 343–350. (дата звернення: 20.05.2023)

11. Sanchez-Iborra R., Cano M.-D. State of the art in LP-WAN solutions for industrial iot services. Sensors. 2016. Т. 16, № 5. С. 708. URL: https://doi.org/10.3390/s16050708 (дата звернення: 21.05.2023).

12. Demystifying low-power wide-area communications for city IoT applications / S. Kartakis та ін. Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization, WiNTECH '16. New York, NY, USA, 2016. С. 2–8. (дата звернення: 12.06.2023)

13. Best fit cases for lpwans - white paper from ABI research. Ingenu. URL: https://www.ingenu.com/portfolio/best-fit-use-cases-for-lpwans/ (дата звернення: 12.05.2023).

14. Diachuk, O. V. (2020). Порівняльний аналіз технологій класу LPWAN. Електронна та Акустична Інженерія, 3(3), 41. https://doi.org/10.20535/2617-0965.2020.3.3.199519 (дата звернення: 12.05.2023)

15. LoRaWAN telensa LPWAN iot technology overview. URL: https://www.slideteam.net/lorawan-telensa-lpwan-iot-technology-overview-ppt-show-introduction.html (дата звернення: 04.10.2023).

16. Offering IoT solutions from physical sensors to LPWAN. RCR Wireless News. URL: https://www.rcrwireless.com/20161122/internet-of-things/qowisio-lpwan-iot-tag31-2 (дата звернення: 15.06.2023).

17. Understanding the limits of LoRaWAN / F. Adelantado та ін. IEEE communications magazine. 2017. Т. 55, № 9. С. 35–41. (дата звернення: 13.07.2023)

18. Federal Register :: Request Access. Federal Register :: Request Access. URL: https://www.ecfr.gov/current/title-47/part-15 (дата звернення: 13.07.2023)

19. LoRaWAN specification 1.1 / A.bertolaud та ін. Beaverton : LoRa Alliance, Inc., 2017. 101 с. URL: https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-1 (дата звернення: 13.07.2023).

20. Throughput, Coverage and Scalability of LoRa LPWAN for Internet of Things / Asif M. Yousuf та ін. 2018. С. 1–10. URL: https://pages.cpsc.ucalgary.ca/~mghaderi/docs/iwqos18-lora.pdf (дата звернення: 13.07.2023).

21. Cotrim J. R., Kleinschmidt J. H. LoRaWAN Mesh Networks: A Review and Classification of Multihop Communication. Sensors. 2020. Т. 20, № 15. С. 4273. URL: https://doi.org/10.3390/s20154273 (дата звернення: 13.07.2023).

22. Routing in lorawan: overview and challenges / A. Osorio та ін. IEEE communications magazine. 2020. Т. 58, № 6. С. 72–76. URL: https://doi.org/10.1109/mcom.001.2000053 (дата звернення: 13.07.2023).

23. . Chao H., Alhajyaseen W., Amini A. Improving the Energy Efficiency of Mobile Wireless Sensor Networks: A Multi-Objective Approach. 2018 IEEE 19th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM). 2018. С. 1–9. URL: https://doi.org/10.1109/WoWMoM.2018.8449743. (дата звернення: 13.07.2023)

24. Roman R., Lopez J., Mambo M. Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges. Future generation computer systems. 2018. Т. 78. С. 680–698. (дата звернення: 13.07.2023)

25. Dias J., Grilo A. LoRaWAN multi-hop uplink extension. Procedia computer science. 2018. Т. 130, № С. С. 420–430. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167739X16305635?via=ihub. (дата звернення: 13.07.2023)

26. MTI. Destination-Sequenced Distance Vector Routing (DSDV). URL: https://mti.binus.ac.id/2014/08/15/destination-sequenced-distance-vector-routing-dsdv/ (дата звернення: 03.10.2023).

27. Yang K., Ma J.-f., Miao Z.-h. Hybrid routing protocol for wireless mesh network. 2009 international conference on computational intelligence and security. Beijing, China, 2009. С. 547–551. URL: https://doi.org/10.1109/CIS.2009.48. (дата звернення: 03.10.2023).

28. Perkins C. E., Royer E. M. Ad-hoc on-demand distance vector routing. Proceedings WMCSA'99. second IEEE workshop on mobile computing systems and applications. New Orleans, LA, USA, 1999. С. 90–100. URL: https://doi.org/10.1109/MCSA.1999.749281. (дата звернення: 03.10.2023)

29. Van de Velde B. Multi-hop LoRaWAN: including a forwarding node. URL: https://texus.me/files/Paper%20Multi-hop%20LoRaWAN.pdf. . (дата звернення: 03.10.2023)

30. Synchronous lora mesh network to monitor processes in underground infrastructure / C. Ebi та ін. IEEE access. 2019. С. 1–1. URL: https://doi.org/10.1109/ACCESS.2019.2913985. . (дата звернення: 03.10.2023)

31. Enabling RPL multihop communications based on LoRa / B. Sartori та ін. 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). Rome, Italy, 2017. С. 1–8. URL: https://doi.org/10.1109/WiMOB.2017.8115756.

32. Kim S., Lee H., Jeon S. An adaptive spreading factor selection scheme for a single channel lora modem. Sensors. 2020. Т. 20, № 4. С. 1008. URL: https://doi.org/10.3390/s20041008.

33. Multi-Hop lora networks enabled by concurrent transmission / C.-H. Liao та ін. IEEE access. 2017. Т. 5. С. 21430–21446. URL: https://doi.org/10.1109/ACCESS.2017.2755858.

34. 802.15.4-2020. IEEE standard for low-rate wireless networks. На заміну 802.15.4-2015. Вид. офіц. 2020. URL: https://standards.ieee.org/ieee/802.15.4/7029/.

35. Evaluating LoRa energy efficiency for adaptive networks: from star to mesh topologies / M. N. Ochoa та ін. 2017 IEEE 13th international conference on wireless and mobile computing, networking and communications (wimob). Rome, Italy, 2017. С. 1–8. URL: https://doi.org/10.1109/WiMOB.2017.8115793. (дата звернення: 08.06.2023)

36. Abrardo A., Pozzebon A. A Multi-Hop LoRa Linear Sensor Network for the Monitoring of Underground Environments: The Case of the Medieval Aqueducts in Siena, Italy. Sensors. 2019. Т. 19, № 2. С. 402. URL: https://doi.org/10.3390/s19020402 (дата звернення: 08.06.2023).

37. Duong C., Kim M. Multi-Hop linear network based on lora. Proceedings of the conference. 2018. С. 29–33. URL: https://doi.org/10.14257/astl.2018.150.08.

38. McCauley M. RadioHead: RadioHead Packet Radio library for embedded microprocessors. AirSpayce. URL: https://www.airspayce.com/mikem/arduino/RadioHead/ (дата звернення: 08.06.2024).

39. A disaster-resilient communications network powered by the sun. disaster.radio. URL: https://disaster.radio/ (дата звернення: 08.06.2024).

40. Meshtastic. An open source, off-grid, decentralized, mesh network built to run on affordable, low-power devices. Meshtastic. URL: https://meshtastic.org/ (date of access: 08.06.2024).

41. Pymesh is the LoRa full-mesh network technology. Pymesh. URL: https://docs.pycom.io/pymesh/ (дата звернення: 08.06.2024).

42. NiceRF is a high-tech enterprise specialized in the Internet of Things industry Transceiver Module-Antenna-NiceRF. Nicerf. URL: https://www.nicerf.com/ (дата звернення: 08.06.2024).

43. Westenberg M. Single Channel LoRaWAN Gateway. GitHub. URL: https://github.com/things4u/ESP-1ch-Gateway/blob/master/README.md (дата звернення: 08.06.2024).

44. Braam J. A LoRaWan Gateway in Lua, listening to all spreading factors on one specific channel. GitHub. URL: https://github.com/JaapBraam/LoRaWanGateway (дата звернення: 08.06.2024).

45. HT-M00 Dual Channel LoRa Gateway. Heltec Automation. URL: https://heltec.org/project/ht-m00/ (дата звернення: 08.06.2024).

46. Chui M., Collins M., Patel M. The Internet of Things: Catching up to an accelerating opportunity. 2021. URL: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/iot%20value%20set%20to%20accelerate%20through%202030%20where%20and%20how%20to%20capture%20it/the-internet-of-things-catching-up-to-an-accelerating-opportunity-final.pdf. (дата звернення: 09.06.2024).

47. IoT Asset Tracking Device Evolution: Technologies and Features Driving the Next Stage of Growt. 2020. 37 c. URL: https://www.abiresearch.com/market-research/product/7778333-iot-asset-tracking-device-evolution-techno. (дата звернення: 09.06.2024).

48. Enabling Things to Talk / ред.: A. Bassi та ін. Berlin, Heidelberg : Springer Berlin Heidelberg, 2013. URL: https://doi.org/10.1007/978-3-642-40403-0 (дата звернення: 09.06.2024).

49. Rahman L. F., Ozcelebi T., Lukkien J. Understanding IoT Systems: A Life Cycle Approach. Procedia Computer Science. 2018. T. 130. C. 1057–1062. URL: https://doi.org/10.1016/j.procs.2018.04.148. (дата звернення: 09.06.2024).

50. Slama D. IgniteWorx: Design and evaluation of a system-supported methodology for IIoT project setup. 2019. URL: http://d-nb.info/1201725208/34. (дата звернення: 09.06.2024).

51. Why IoT projects fail & how to beat the odds. Software AG, 2020. 16 c. URL: https://www.idglat.com/afiliacion/whitepapers/2020-5-ar-why-iot-projects-fail-en.pdf. (дата звернення: 09.06.2024).

52. Kassab W., Darabkh K. A. A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations.

Journal of Network and Computer Applications. 2020. Т. 163. С. 102663. URL: https://doi.org/10.1016/j.jnca.2020.102663 (дата звернення: 09.06.2024).

53. Kaňuch P., Macko D., Hudec L. Survey: classification of the iot technologies for better selection to real use. 2020 43rd international conference on telecommunications and signal processing (TSP). Milan, Italy, 2020. С. 500–505. URL: https://doi.org/10.1109/TSP49548.2020.9163480. (дата звернення: 09.06.2024).

54. Coverage and Capacity Analysis of Sigfox, LoRa, GPRS, and NB-IoT / B. Vejlgaard та ін. 2017 IEEE 85th vehicular technology conference (VTC spring). Sydney, NSW, Australia, 2017. С. 1–5. URL: https://doi.org/10.1109/VTCSpring.2017.8108666. (дата звернення: 09.06.2024).

55. A Comparative Study of LoRaWAN, SigFox, and NB-IoT for Smart Water Grid / Y. Lalle та ін. 2019 Global Information Infrastructure and Networking Symposium (GIIS). Paris, France, 2019. С. 1–6. URL: https://doi.org/10.1109/GIIS48668.2019.9044961. (дата звернення: 09.06.2024).

56. NS-3. Версія 3.45. Alexandria : National Science Foundation. URL: https://www.nsnam.org/.(дата звернення: 09.06.2024).

57. Verhoeven R., Kempinski S., Meratnia N. Performance Evaluation of Wi-Fi HaLow, NB-IoT and LoRa for Smart City Applications. Proceedings of the 19th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, \& Ubiquitous Networks (PE-WASUN '22). New York, NY, USA, 2022. С. 17–24. URL: https://doi.org/10.1145/3551663.3558596. (дата звернення: 09.06.2024).

58. ADIperf: a framework for application-driven iot network performance evaluation / S. Si-Mohammed та ін. 2022 international conference on computer communications and networks (ICCCN). Honolulu, HI, USA, 2022. С. 1–8. URL: https://doi.org/10.1109/ICCCN54977.2022.9868888. (дата звернення: 09.06.2024).

59. Vannieuwenborg F., Verbrugge S., Colle D. Choosing IoT-connectivity? A guiding methodology based on functional characteristics and economic considerations. Transactions on Emerging Telecommunications Technologies. 2018. Т. 29, № 5. С.

e3308. URL: https://doi.org/10.1002/ett.3308 (дата звернення: 09.06.2024). (дата звернення: 09.06.2024).

60. FIT IoT-LAB. FIT IoT-LAB. URL: https://www.iot-lab.info/ (дата звернення: 09.06.2024).

61. SmartSantander. SmartSantander. URL: https://www.smartsantander.eu/ (дата звернення: 09.06.2024).

62. COPELABS Universidade Lusófona. COPELABS Universidade Lusófona – COPELABS Universidade Lusófona. URL: https://copelabs.ulusofona.pt/ (дата звернення: 09.06.2024).

63. EU H2020 FIESTA-IoT Project. GitHub. URL: https://github.com/fiesta-iot (дата звернення: 09.06.2024).

64. Bari F., Leung V. C. m. Automated network selection in a heterogeneous wireless network environment. IEEE network. 2007. Т. 21, № 1. С. 34–40. URL: https://doi.org/10.1109/MNET.2007.314536. (дата звернення: 09.06.2024)

65. Bari F., Leung V. Multi-Attribute network selection by iterative TOPSIS for heterogeneous wireless access. 2007 4th IEEE consumer communications and networking conference. Las Vegas, NV, USA, 2007. С. 808–812. URL: https://doi.org/10.1109/CCNC.2007.164. (дата звернення: 11.06.2024).

66. TOPSIS-based dynamic approach for mobile network interface selection / M. A. Senouci та ін. Computer networks. 2016. Т. 107. С. 304–314. URL: https://doi.org/10.1016/j.comnet.2016.04.012 (дата звернення: 11.06.2024).

67. Tzeng G.-H., Huang J.-J. Multiple attribute decision making: methods and applications. CRC Press, 2011. (дата звернення: 10.06.2024)

68. Gazis V., Alonistioti N., Merakos L. Toward a generic "always best connected" capability in integrated WLAN/UMTS cellular mobile networks (and beyond). IEEE wireless communications. 2005. Т. 12, № 3. С. 20–29. URL: https://doi.org/10.1109/MWC.2005.1452851. (дата звернення: 10.06.2024)

69. Wang L., Binet D. Best permutation: a novel network selection scheme in heterogeneous wireless networks. Proceedings of the 2009 international conference on

wireless communications and mobile computing: connecting the world wirelessly (IWCMC '09). New York, NY, USA, 2009. С. 894–899. URL: https://doi.org/10.1145/1582379.1582574. (дата звернення: 10.06.2024)

70. Hou J., O'Brien D. C. Vertical handover-decision-making algorithm using fuzzy logic for the integrated Radio-and-OW system. IEEE transactions on wireless communications. 2006. Т. 5, № 1. С. 176–185. URL: https://doi.org/10.1109/TWC.2006.1576541. (дата звернення: 11.06.2024)

71. Wenhui Zhang, "Handover decision using fuzzy MADM in heterogeneous networks," 2004 IEEE Wireless Communications and Networking Conference (IEEE Cat. No.04TH8733), Atlanta, GA, USA, 2004, pp. 653-658 Vol.2, doi: 10.1109/WCNC.2004.1311263. (дата звернення: 11.06.2024)

72. Stevens-Navarro E., Lin Y., Wong V. W. S. An mdp-based vertical handoff decision algorithm for heterogeneous wireless networks. IEEE transactions on vehicular technology. 2008. Т. 57, № 2. С. 1243–1254. URL: https://doi.org/10.1109/TVT.2007.907072. (дата звернення: 11.06.2024)

73. Markov-based vertical handoff decision algorithms in heterogeneous wireless networks / Z. Ning та ін. Computers & electrical engineering. 2014. Т. 40, № 2. С. 456–472. URL: https://doi.org/10.1016/j.compeleceng.2013.10.012 (дата звернення: 11.06.2024).

74. Cesana M., Gatti N., Malanchini I. Game theoretic analysis of wireless access network selection: models, inefficiency bounds, and algorithms. Proceedings of the 3rd international conference on performance evaluation methodologies and tools. 2008. (дата звернення: 11.06.2024)

75. AHP and game theory based approach for network selection in heterogeneous wireless networks / B. Liu та ін. 2014 IEEE 11th consumer communications and networking conference (CCNC). Las Vegas, NV, USA, 2014. С. 501–506. URL: https://doi.org/10.1109/CCNC.2014.6866617. (дата звернення: 11.06.2024)

76. Gai Y., Krishnamachari B., Jain R. Combinatorial network optimization with unknown variables: multi-armed bandits with linear rewards and individual observations. IEEE/ACM transactions on networking. 2012. Т. 20, № 5. С. 1466–1478. URL: https://doi.org/10.1109/TNET.2011.2181864. (дата звернення: 23.06.2024)

77. Henri S., Vlachou C., Thiran P. Multi-Armed bandit in action: optimizing performance in dynamic hybrid networks. IEEE/ACM transactions on networking. 2018. Т. 26, № 4. С. 1879–1892. URL: https://doi.org/10.1109/TNET.2018.2856302. (дата звернення: 23.06.2024)

78. Stoffers M., Riley G. Comparing the ns-3 propagation models. 2012 IEEE 20th international symposium on modeling, analysis and simulation of computer and telecommunication systems. Washington, DC, USA, 2012. P. 61–67. URL: https://doi.org/10.1109/MASCOTS.2012.17. (дата звернення: 23.06.2024)

79. Energy consumption analysis of LPWAN technologies and lifetime estimation for iot application / R. K. Singh та ін. Sensors. 2020. Т. 20, № 17. С. 4794. URL: https://doi.org/10.3390/s20174794 (дата звернення: 11.06.2024).

80. Miaoudakis A., Petroulakis N., Askoxylakis I. Communications in emergency and crisis situations. Advances in human factors and ergonomics. 2014. Т. 8530. С. 51–60. URL: https://doi.org/10.1007/978-3-319-07788-8_51. (дата звернення: 23.06.2024)

81. Generating crisis maps for large-scale disasters: issues and challenges / P. S. Paul та ін. Wireless public safety networks 3 / ред.: D. Câmara, N. Nikaein. 2017. С. 67–98. URL: https://doi.org/10.1016/B978-1-78548-053-9.50004-4. (дата звернення: 23.06.2024)

82. Providing real-time message delivery on opportunistic networks / R. M. Santos та ін. IEEE access. 2018. Т. 6. С. 40696–40712. URL: https://doi.org/10.1109/access.2018.2848546 (дата звернення: 25.07.2024).

83. Fischer D., Posega O., Fischbach K. Communication barriers in crisis management: a literature review. ECIS 2016 proceedings. 2016. С. 119. (дата звернення: 25.07.2024)

84. Modelling and simulation of opportunistic iot services with aggregate computing / R. Casadei та ін. Future generation computer systems. 2019. Т. 91. С. 252–262. URL: https://doi.org/10.1016/j.future.2018.09.005 (дата звернення: 25.07.2024)

85. Conti M., Passarella A., Das S. K. The Internet of People (IoP): a new wave in pervasive mobile computing. Pervasive and mobile computing. 2017. Т. 41. С. 1–27. URL: https://doi.org/10.1016/j.pmcj.2017.07.009 (дата звернення: 25.07.2024)

86. Ochoa S. F., Santos R. Human-centric wireless sensor networks to improve information availability during urban search and rescue activities. Information fusion. 2015. Т. 22. С. 71–84. URL: https://doi.org/10.1016/j.inffus.2013.05.009 (дата звернення: 25.07.2024)

87. LOCATE: A LoRa-based mobile emergency mmnagement system / L. Sciullo та ін. 2018 IEEE global communications conference (GLOBECOM). Abu Dhabi, United Arab Emirates, 2018. С. 1–7. URL: https://doi.org/10.1109/GLOCOM.2018.8647177. (дата звернення: 27.07.2024)

88. Cerdà-Alabern L., Neumann A., Escrich P. Experimental evaluation of a wireless community mesh network. Proceedings of the 16th ACM international conference on Modeling, analysis \& simulation of wireless and mobile systems (MSWiM '13). New York, NY, USA, 2013. С. 23–30. URL: https://doi.org/10.1145/2507924.2507960. (дата звернення: 27.07.2024)

89. Magrin D., Centenaro M., Vangelista L. Performance evaluation of LoRa networks in a smart city scenario. 2017 IEEE International Conference on Communications (ICC). Paris, France, 2017. С. 1–7. URL: https://doi.org/10.1109/ICC.2017.7996384. (дата звернення: 27.07.2024)

90. OMNeT++ Discrete Event Simulator. Версія 6.1.0. O. Ltd. URL: https://omnetpp.org/. (дата звернення: 29.07.2024)

91. Mariusz Slabicki, Gopika Premsankar. FLoRa - Framework for LoRa. Версія 1.1.0. 2022. URL: https://flora.aalto.fi/.

92. Slabicki M., Premsankar G., Francesco M. D. Adaptive configuration of lora networks for dense IoT deployments. 2018 IEEE/IFIP network operations and management symposium, NOMS 2018. Taipei, Taiwan, 2018. С. 1–9. URL: https://doi.org/10.1109/NOMS.2018.8406255. (дата звернення: 29.07.2024)

93. On the coverage of LPWANs: range evaluation and channel attenuation model for LoRa technology / J. Petajajarvi та ін. 2015 14th international conference on ITS telecommunications (ITST). Copenhagen, Denmark, 2015. С. 55–59. URL: https://doi.org/10.1109/ITST.2015.7377400. (дата звернення: 29.07.2024)

94. Gromes J. Universal wireless communication library for embedded devices. GitHub. URL: https://github.com/jgromes/RadioLib (дата звернення: 10.06.2024)

95. Kim S., Lee H., Jeon S. An adaptive spreading factor selection scheme for a single channel lora modem. Sensors. 2020. Т. 20, № 4. С. 1008. URL: https://doi.org/10.3390/s20041008 (дата звернення: 29.07.2024)

ДОДАТОК А

ТОВ «УКР-ОН»
м. Київ. вул. Харківське шосе, буд. 158, оф.86
ЕДРПОУ 41329131

ДОВІДКА
про впровадження результатів дисертаційної роботи
Козлова Дмитра Євгеновича

Необхідність впровадження прикладних досліджень у галузі побудови сенсорних мереж обумовлена зростаючими вимогами до їх надійності, масштабованості та енергоефективності в умовах активного розвитку технологій Інтернету речей. Зростає потреба в забезпеченні стійкості таких мереж до зовнішніх впливів та здатності адаптуватися до змін експлуатаційного середовища. Особливої актуальності це набуває при проєктуванні бездротових сенсорних мереж на основі енергоощадних технологій, зокрема LoRa, які повинні гарантувати стабільність роботи, тривалу автономність та захищене передавання даних в умовах підвищених інформаційних ризиків. Наукові результати були розроблені в рамках дисертаційного дослідження на тему «Метод побудови сенсорних мереж на базі самоорганізації». Основною метою роботи є підвищення ефективності функціонування сенсорної мережі шляхом впровадження нових методів мережевої взаємодії між вузлами.

Компанія бере на впровадження запропонований науковий **метод визначення маршруту передавання даних у сенсорній мережі**. Особливістю цього методу є **обчислення загального часу передавання повідомлення на основі векторного аналізу**, що дозволяє підвищити ефективність маршрутизації та забезпечити стабільну роботу мережі в умовах обмежених ресурсів.

Цінність даного дослідження полягає в можливості підвищення ефективності та надійності функціонування сенсорної мережі компанії за рахунок оптимізації процесу передавання даних між вузлами.

Запропоновані методи дозволяють скоротити затримки в комунікації, зменшити навантаження на мережу. У результаті впровадження компанія отримує більш стійку та адаптивну інфраструктуру сенсорної мережі, здатну забезпечувати стабільну роботу в умовах змін середовища та обмежених ресурсів.

Директор
ТОВ "УКР-ОН" _____ Гашко А.О

ДОДАТОК Б

Товариство з обмеженою відповідальністю
«КАРНІФЕКС»
Юридична адреса: Україна, 07400, м. Бровари,
вул. Москаленка Сергія, буд. 16Г, офіс 23
Код ЄДРПОУ 45370953
МФО 320984
Директор ТОВ "КАРНІФЕКС"
_____ Марков Д.В.
«2» травня 2025 р.

АКТ
про впровадження результатів дисертаційної роботи
Козлова Дмитра Євгеновича
на тему: «Метод побудови сенсорних мереж на базі самоорганізації»

Цим актом засвідчується, що результати, отримані в дисертаційному дослідженні здобувача Державного університету інформаційно-комунікаційних технологій Козлова Дмитра Євгеновича на тему «Метод побудови сенсорних мереж на базі самоорганізації», використані при реалізації проєктів розробки сенсорних IoT мереж в ТОВ "КАРНІФЕКС".

Перелік наукових результатів та їх практичне значення для впровадження в ТОВ "КАРНІФЕКС":

1. Модель сенсорної мережі, в якій за рахунок використання багатокритеріального аналізу можливо визначити оптимальну конфігурацію.

2. Метод визначення маршруту передавання даних між вузлами сенсорної мережі, в якому за рахунок обчислення загального часу передавання повідомлення використовується нова метрика маршрутизації.

Козлов Д.Є. залучався до обговорення та впровадження методу визначення маршруту передавання даних між вузлами сенсорної мережі з використанням загального часу передавання як нової метрики маршрутизації. Таким чином наукові та практичні результати дослідження можуть знайти подальше практичне застосування в процесі розробки та удосконалення сенсорних IoT мереж.

IT директор _____ «2» травня 2025 р. Іващенко Д.С.

ДОДАТОК В

ЗАТВЕРДЖУЮ
Перший проректор Державного університету інформаційно-комунікаційних технологій
Член-кореспондент НАН України, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, Заслужений діяч науки і техніки України
_____ Олександр КОРЧЕНКО
«_2_» _травня_ 2025 р.

АКТ

впровадження в освітній процес Навчально-наукового інституту Інформаційних технологій результатів дисертаційної роботи старшого викладача кафедри Інформаційних систем та технологій Державного університету інформаційно-комунікаційних технологій Козлова Дмитра Євгеновича на тему: «Метод побудови сенсорних мереж на базі самоорганізації» на здобуття наукового ступеня доктора філософії за спеціальністю 123 – Комп'ютерна інженерія.

Комісія у складі:
голова – заступник директора Навчально-наукового інституту Інформаційних технологій, Кузьміч І.Б.;
члени комісії:

1. Завідувач кафедри Комп'ютерної інженерії, кандидат технічних наук, доцент Лащевська Н.О.;
2. Завідувач кафедри Комп'ютерних наук, доктор технічних наук, професор Вишнівський В.В.;
3. Завідувач кафедри Інформаційних систем та технологій, доктор технічних наук, професор Сторчак К.П.

розглянула дисертаційну роботу Козлова Дмитра Євгеновича на тему: «Метод побудови сенсорних мереж на базі самоорганізації»
та публікації автора за матеріалами дисертаційної роботи. Результати впроваджено в освітній процес Навчально-наукового інституту Інформаційних технологій, а саме:

1. Модель мультипротокольної сенсорної мережі, яка за рахунок використання багатокритеріального аналізу та теорії розподілених систем, дозволить визначити оптимальну конфігурацію сенсорної мережі.
2. Метод визначення маршруту передавання даних між вузлами сенсорної мережі, який за рахунок удосконаленого методу взаємодії вузлів мережі та

врахування параметрів сенсорної мережі побудованої на основі теорії графів та самоорганізації дозволить підвищити середній коефіцієнт доставки повідомлень.

На основі аналізу представлених матеріалів комісія встановила, що отримані наукові результати використовуються в освітньому процесі Державного університету інформаційно-комунікаційних технологій при викладанні навчальних дисциплін: «Інформаційні мережі», «Технології Інтернету речей» спеціальності 126 «Інформаційні системи та технології».

Голова комісії:
Заступник директора
Навчально-наукового інституту
Інформаційних технологій _____ Ірина КУЗЬМІЧ

Члени комісії:
Завідувач кафедри
Комп'ютерної інженерії,
кандидат технічних наук,
доцент _____ Наталія ЛАЩЕВСЬКА

Завідувач кафедри
Комп'ютерних наук,
доктор технічних наук,
професор _____ Віктор ВИШНІВСЬКИЙ

Завідувач кафедри
Інформаційних систем та
технологій,
доктор технічних наук,
професор _____ Каміла СТОРЧАК