

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

Навчально-науковий інститут телекомунікаційних систем

Кафедра електронних комунікацій та інтернету речей

«На правах рукопису»

УДК 621.391

До захисту допущено:

ВО завідувача кафедри

_____Анатолій МАКАРЕНКО

«__» _____ 20__ р.

Магістерська дисертація

на здобуття ступеня магістра

**за освітньо-професійною програмою «Системи електронних
комунікацій та Інтернету речей»**

зі спеціальності 172 «Електронні комунікації та радіотехніка»

на тему: «Дослідження радіотехнологій мереж Інтернету речей»

Виконав:

студент II курсу, групи ЦС-41мп

Кузьмінський Артем Ростиславович

Науковий керівник:

Доцент кафедри ЕКІР ІТС,

Носков В'ячеслав Іванович

Рецензент:

Незалежний експерт з телекомунікацій, кандидат
технічних наук,

Вахрушев Володимир Платонович

Засвідчую, що у цій
магістерській дисертації немає
запозичень з праць інших авторів
без відповідних посилань.

Студент _____

Київ – 2025 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей

Рівень вищої освіти – другий (магістерський)

Спеціальність – 172 «Електронні комунікації та радіотехніка»

Освітньо-професійна програма «Системи електронних комунікацій та Інтернету речей»

ЗАТВЕРДЖУЮ

ВО завідувача кафедри

_____Анатолій МАКАРЕНКО

«___» _____ 2025 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Кузьмінському Артему Ростиславовичу

1. Тема роботи «Дослідження радіотехнологій мереж Інтернету речей», науковий керівник дисертації Носков В'ячеслав Іванович, доцент, затверджені наказом по університету від 3 листопада 2025 р. № 4772-с.
2. Термін подання студентом роботи 18 грудня 2025 р.
3. Об'єкт досліджень: мережа Інтернету речей
4. Вихідні дані до роботи: сучасні наукові публікації, стандарти та технічні характеристики бездротових радіотехнологій IoT (LoRa/LoRaWAN, ZigBee, Z-Wave, NB-IoT, LTE-M, Wi-Fi HaLow, 5G тощо), а також інструменти програмного моделювання (NS-3, OMNeT++). Структурований план порядку розробки матеріалів магістерської дисертації.

5. Перелік завдань, які потрібно розробити:

- Провести аналіз сучасного стану розвитку мереж Інтернету речей, визначити основні сфери застосування та проблеми впровадження.
- Виконати порівняльний огляд технічних характеристик ключових радіотехнологій IoT, визначити їх переваги та недоліки.
- Обрати критерії для оцінки ефективності радіотехнологій (діапазон дії, пропускна здатність, затримка, енергоефективність, вартість тощо).
- Провести порівняльний огляд симуляторів NS-3 та OMNeT++, оцінити їхні можливості, обмеження та застосовність для досліджуваних сценаріїв.
- Сформулювати задачу моделювання обраних технологій у середовищі NS-3 та/або OMNeT++, сформулювати сценарії дослідження та налаштування параметрів мережі.
- Розробити алгоритм проведення експерименту та аналізу результатів.
- Надати практичні рекомендації щодо вибору та застосування радіотехнологій для різних типів IoT-додатків (розумні міста, промисловість, агротехніка, медицина тощо).

6. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо), презентація обсягом 11 слайдів: 1) Тема та мета магістерської дисертації; 2) Архітектура Інтернету речей; 3) Основні сфери застосування IoT; 4) Класифікація та порівняння радіотехнологій в рамках IoT; 5) Критерії ефективності та порівняння симуляторів; 6) Методика моделювання в NS-3; 7) Методика моделювання в OMNeT++; 8) Методологія та алгоритм проведення експерименту; 9) Практичні рекомендації. Матриця вибору; 10) Практичні кейси використання IoT; 11) Висновки по роботі.

7. Орієнтовний перелік публікацій:

- Носков , В. І. ., & Кузьмінський, А. Р. . (2025). ПОРІВНЯЛЬНИЙ

АНАЛІЗ РАДІОТЕХНОЛОГІЙ МЕРЕЖ ІОТ . Збірник матеріалів Міжнародної науково-технічної конференції «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ», 85–87. вилучено із <https://conferenc-journal.its.kpi.ua/article/view/330926>

- Кузьмінський, А. Р., Носков, В. І., & Бондарчук, А. П. (2025). Гібридний підхід поєднання NB-IoT з LoRa. Телекомунікаційні та інформаційні технології, (2 (87)), 134–148. <https://doi.org/10.31673/2412-4338.2025.029573>

8. Дата видачі завдання: 04.03.2025 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Концепція Інтернету речей	10.03.2025	
2	Радіотехнології Інтернету речей	10.05.2025	
3	Визначення критеріїв порівняння та огляд інструментів моделювання	15.06.2025	
4	Методика дослідження радіотехнологій Інтернету речей на основі моделювання	30.10.2025	
5	Рекомендації щодо застосування радіотехнологій IoT	25.11.2025	
6	Вступ, Висновки	05.12.2025	
7	Чистовий варіант магістерської роботи, плакати	12.12.2025	

Студент

Артем КУЗЬМІНСЬКИЙ

Науковий керівник

В'ячеслав НОСКОВ

РЕФЕРАТ

Магістерська дисертація складається з 112 сторінок, 37 рисунків, 5 таблиць. Було використано 61 джерело.

Мета роботи: визначення критеріїв оцінювання та дослідження радіотехнологій Інтернету речей, розробка методики дослідження радіотехнологій за допомогою симуляторів, а також формування практичних рекомендацій, що стосуються вибору оптимальних технологій для різних сфер застосування IoT.

Актуальність теми: стрімкий розвиток мереж Інтернету речей вимагає ефективних та енергоощадних засобів бездротового зв'язку, здатних забезпечити надійну передачу даних між великою кількістю пристроїв. Різноманітність радіотехнологій, що пропонують різні діапазони частот, особливо якщо розглядати сучасні реалії з великим впливом РЕБ, швидкість передачі, рівень енергоспоживання та вартість, зумовлює необхідність їх глибокого аналізу. Результати дослідження є важливими для вибору оптимальних рішень у таких сферах, як розумні міста, промисловий IoT, сільське господарство, охорона здоров'я та транспорт.

Задачі роботи:

- Провести аналіз сучасного стану розвитку мереж Інтернету речей та визначити ключові сфери їх застосування.
- Виконати порівняльний огляд технічних характеристик радіотехнологій LoRa/LoRaWAN, ZigBee, Z-Wave, NB-IoT, LTE-M, Wi-Fi HaLow, 5G та інших.
- Визначити критерії оцінки ефективності радіотехнологій (діапазон дії, швидкість передачі, енергоспоживання, стійкість до перешкод, вартість).
- Сформулювати задачу моделювання обраних технологій, виконати аналіз симуляторів, сформулювати сценарії дослідження та налаштування параметрів мережі.

- Розробити алгоритм проведення експерименту та аналізу результатів.
- Надати рекомендації з вибору радіотехнологій для різних типів IoT-додатків.

Об'єкт дослідження: Мережа Інтернету речей.

Предмет дослідження: радіотехнології, що використовуються для побудови мереж Інтернету речей.

Ключові слова: Інтернет речей, IoT, LoRa, ZigBee, NB-IoT, LTE-M, Wi-Fi HaLow, 5G, радіотехнологія, NS-3, бездротовий зв'язок, моделювання.

ABSTRACT

Objective: The objective of this thesis is to identify evaluation criteria and investigate radio technologies used in the Internet of Things (IoT), as well as to develop practical recommendations for selecting optimal wireless solutions for various IoT application domains.

Relevance of the Topic: The rapid growth of IoT systems requires wireless communication technologies that are energy-efficient, scalable, and capable of ensuring reliable data transmission for large numbers of devices. The diversity of available radio technologies with different frequency bands, transmission rates, energy consumption levels, and cost necessitates a comprehensive comparative analysis, especially considering modern challenges such as increased radio-electronic interference. The results of this study are important for selecting optimal solutions in smart cities, industrial IoT, agriculture, healthcare, and transportation.

Tasks:

- To analyze the current state of IoT networks and identify key application domains.
- To perform a comparative review of the technical characteristics of LoRa/LoRaWAN, ZigBee, Z-Wave, NB-IoT, LTE-M, Wi-Fi HaLow, 5G, and other technologies.
- To define evaluation criteria for radio technologies (coverage range, data rate, energy consumption, interference resistance, cost).
- To formulate a simulation problem in NS-3 or OMNeT++, including the development of research scenarios and network parameter configurations.
- To compare the performance of selected technologies under different traffic loads and propose recommendations for practical deployment.
- To provide guidelines for choosing radio technologies for different types of IoT applications.

Keywords: Internet of Things, LoRa, ZigBee, NB-IoT, LTE-M, Wi-Fi HaLow, 5G, radio technology, NS-3, wireless communication, simulation.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ	10
ВСТУП	12
1 КОНЦЕПЦІЯ ІНТЕРНЕТУ РЕЧЕЙ.....	14
1.1 Архітектура та загальна характеристика Інтернету речей.....	14
1.2 Основні сфери застосування IoT	21
1.3 Проблеми та виклики розвитку Інтернету речей	27
1.4 Висновки до розділу 1	34
2 РАДІОТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ.....	35
2.1 Огляд, технічні характеристики, переваги та недоліки радіотехнологій в мережах IoT	35
2.2 Результати досліджень радіотехнологій IoT в наукових роботах	52
2.3 Висновки до розділу 2.....	56
3 МЕТОДИКА ДОСЛІДЖЕННЯ РАДІОТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ МОДЕЛЮВАННЯ	58
3.1 Ключові критерії порівняння радіотехнологій.....	58
3.2 Огляд інструментів моделювання	61
3.3 Популярні засоби моделювання мереж NS-3 та OMNeT++ та їх порівняння.....	64
3.4 Методологія постановки задачі моделювання мереж IoT	71
3.5 Опис архітектури моделі в середовищі моделювання.....	74
3.5.1 Архітектура моделі в середовищі NS-3	74
3.5.2 Архітектура моделі в середовищі OMNeT++	77
3.6 Алгоритм проведення експерименту та аналізу результатів	80
3.7 Висновки до розділу 3.....	82

4 РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ РАДІОТЕХНОЛОГІЙ ІОТ..	84
4.1 Критерії вибору технології для певної сфери застосування.....	84
4.2 Практичні приклади використання кожної технології в IoT	89
4.3 Вибір оптимальних технологій для різних типів IoT-додатків	99
4.4 Висновки до розділу 4.....	101
ВИСНОВКИ.....	103
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	105

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

6LoWPAN – IPv6 over Low-Power Wireless Personal Area Networks (IPv6 поверх малопотужних бездротових персональних мереж)

API – Application Programming Interface (Інтерфейс прикладного програмування)

AR – Augmented Reality (Доповнена реальність)

BLE – Bluetooth Low Energy (Bluetooth з низьким енергоспоживанням)

CAPEX – Capital Expenditure (Капітальні витрати)

CRN – Cognitive Radio Networks (Когнітивні радіомережі)

eMBB – Enhanced Mobile Broadband (Розширений мобільний широкосмуговий доступ)

eNodeB – Evolved Node B (Базова станція в мережах LTE)

GUI – Graphical User Interface (Графічний інтерфейс користувача)

IEEE – Institute of Electrical and Electronics Engineers (Інститут інженерів з електротехніки та електроніки)

IIoT – Industrial Internet of Things (Промисловий Інтернет речей)

LoRa – Long Range (Технологія модуляції великого радіусу дії)

LoRaWAN – Long Range Wide Area Network (Мережевий протокол для LoRa)

LPWAN – Low-Power Wide-Area Network (Енергоефективна мережа далекого радіусу дії)

LTE – Long-Term Evolution

LTE-M – Long-Term Evolution for Machines (LTE для машин/пристроїв)

OSI – Open Systems Interconnection (абстрактна мережева модель для комунікацій і розроблення мережевих протоколів)

NOMA – Non-Orthogonal Multiple Access (Метод неортогонального множинного доступу в системах стільникового зв'язку 5-го покоління)

MAC – Media Access Control (Управління доступом до середовища)

mMTC – Massive Machine-Type Communications (Масові міжмашинні комунікації)

M2M – Machine-to-Machine (Міжмашинна взаємодія)

NB-IoT – Narrowband Internet of Things (Вузькосмуговий Інтернет речей)

NED – Network Description (Мова опису мережі в OMNeT++)

NGN – Next Generation Networks (Мережі наступного покоління)

OPEX – Operating Expense (Операційні витрати)

PDR – Packet Delivery Ratio (Коефіцієнт доставки пакетів)

QoS – Quality of Service (Якість обслуговування)

RFID – Radio Frequency Identification (Радіочастотна ідентифікація)

RedCap – Reduced Capability (5G зі зниженою функціональністю)

RESP – Responsiveness (Швидкість реагування)

Rx – Receive / Reception (Приймання, приймальний канал)

SDN – Software-Defined Networking (Програмно-конфігуровані мережі)

TCP/IP – Transmission Control Protocol/Internet Protocol (Набір протоколів, який є основою передачі даних в інтернеті)

Tx – Transmit / Transmission (Передавання, передавальний канал)

UE – User Equipment (Обладнання користувача, наприклад телефон)

URLLC – Ultra-Reliable Low-Latency Communications (Наднадійний зв'язок з низькою затримкою)

WPAN – Wireless Personal Area Network (Бездротова персональна мережа)

WSN – Wireless Sensor Networks (Бездротові сенсорні мережі)

АСКТП – Автоматизована система керування технологічним процесом

НКЕК – Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій

ВСТУП

Ми живемо в час, де інформаційні технології стрімко розвиваються, створюючи передумови для появи нових концепцій та рішень, що змінюють усі сфери життєдіяльності людини. Однією з ключових технологічних парадигм сьогодення є Інтернет речей або ж IoT, так як він забезпечує взаємодію між фізичними та цифровим світами. Він перетворює звичні пристрої на елементи єдиної мережі, здатної до автоматичного обміну даними, аналізу та прийняття рішень без прямого втручання людини. Завдяки цьому концепція Інтернету речей знаходить дедалі ширше застосування у великій кількості сфер, від розумних міст, промисловості, енергетики та медицини до, транспорту, чи, наприклад, військового застосування.

Ефективність IoT-мереж значною мірою визначається вибором радіотехнологій для бездротової передачі даних між пристроями. Різні технології відрізняються дальністю дії, швидкістю обміну інформацією, енергоспоживанням, стійкістю до перешкод і вартістю обладнання. У сучасних мережах використовуються як малопотужні технології ближнього радіусу дії (Bluetooth, ZigBee, Z-Wave), так і рішення широкого покриття (LoRa/LoRaWAN, NB-IoT, LTE-M, 5G). Кожна з них має специфічні переваги й обмеження, що необхідно враховувати при проектуванні мереж для конкретних завдань та сценаріїв використання.

Дослідження різноманітних радіотехнологій дозволяє оцінити їхню придатність для побудови ефективних IoT-мереж, передбачити можливі проблеми та визначити оптимальні стратегії їх впровадження. Використання методів моделювання та порівняльного аналізу може сприяти оцінці продуктивності технологій у різних умовах, зокрема при високій щільності пристроїв або за наявності зовнішніх завад, таких як системи РЕБ, що набули широкого застосування на всій території України після початку повномасштабної війни. Такий підхід дає змогу розробникам і дослідникам обирати найбільш доцільні технології відповідно до конкретних сценаріїв

використання та специфіки умов, у яких функціонуватиме мережа.

В основі Інтернету речей лежить ідея зв'язку між різноманітними пристроями, обладнаними датчиками та здатними до обміну даними через мережу. Така мережа пристроїв створює неймовірний потенціал для впровадження новітніх технологій та різноманітних інноваційних рішень.

Актуальність цього дослідження зумовлена необхідністю обґрунтованого вибору радіотехнологій для побудови надійних, масштабованих мереж Інтернету речей. Сучасні IoT-мережі характеризуються високою щільністю підключених пристроїв та різноманітністю сценаріїв використання, що створює додаткові вимоги до стійкості зв'язку, якості передачі даних і оптимізації енергоспоживання.

Отже, метою цієї магістерської роботи є проведення розгляду та аналізу радіотехнологій, що знаходять своє застосування у мережах IoT, з метою визначення їх технічних характеристик, переваг і обмежень. Дослідження включає порівняння технологій ближнього та широкого радіусу дії, розгляд методів моделювання IoT-мереж у спеціалізованому середовищі, яке дозволяє оцінити продуктивність, затримки, коефіцієнт доставки пакетів та інші критично важливі параметри. Отримані результати можуть дати змогу сформулювати обґрунтовані рекомендації щодо оптимального вибору радіотехнологій для конкретних ситуацій побудови надійних IoT-мереж.

1 КОНЦЕПЦІЯ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Архітектура та загальна характеристика Інтернету речей

Сучасний Інтернет зазнав фундаментальної трансформації: від апаратно орієнтованого середовища, що базувалося на комп'ютерах, оптоволоконних лініях та Ethernet-кабелях, до середовища, орієнтованого на сервіси та ринки, де взаємодія відбувається через інтегровані програмні платформи. Інтернет речей (IoT) уявляє собою концепцію світу, де мільярди об'єктів із вбудованими інтелектуальними системами, засобами комунікації, датчиками та виконавчими механізмами підключені до мереж на основі протоколу IP, що дозволяє цим об'єктам обмінюватися даними, аналізувати їх і виконувати певні дії без прямого втручання людини [1].

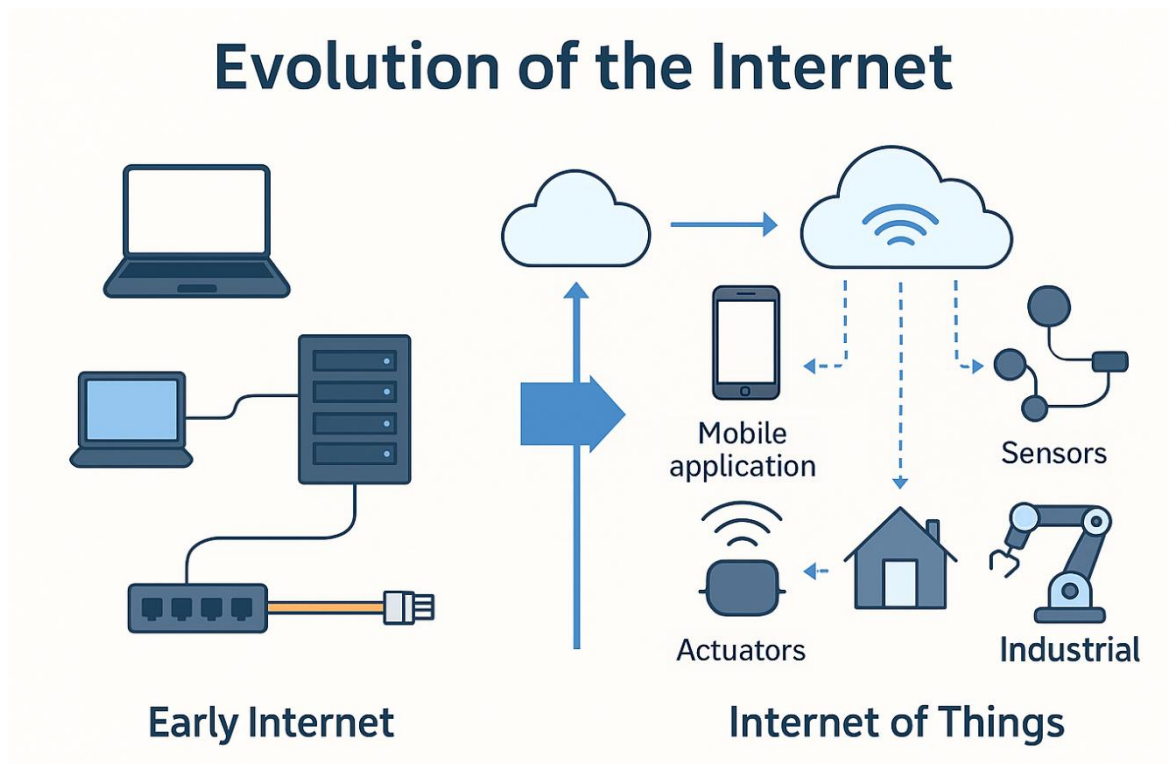


Рисунок 1.1 – Еволюція Інтернету

Розумні об'єкти, або просто «речі», є основними елементами IoT: це предмети повсякденного життя, доповнені мікроконтролерами, радіопередавачами, датчиками, виконавчими механізмами та стеками протоколів, придатними для зв'язку в обмежених середовищах, де цільове

обладнання має обмежені ресурси [1]. Завдяки цьому вони здатні збирати дані з навколишнього середовища, обробляти їх і взаємодіяти з фізичним світом, забезпечуючи функціонування розумних систем.

Оскільки IoT є складною системою, яка складається з великої кількості взаємопов'язаних елементів, для її ефективного функціонування необхідна чітко структурована архітектура. Архітектура IoT визначає принципи взаємодії між різними рівнями та елементами системи – від сенсорних та виконавчих пристроїв до мережевих компонентів і прикладних сервісів. Вона слугує основою для забезпечення надійності, масштабованості та енергоефективності IoT-мереж, дозволяючи координувати обмін даними, управління ресурсами та обробку інформації у реальному часі.

Станом на сьогодні не існує загальноприйнятих стандартів або технологій, що домінують серед платформ і пристроїв Інтернету речей. Різні рішення базуються на власних підходах, спираючись на різноманітні стандарти та технології. У результаті, впровадження IoT-систем часто вимагає від користувачів вивчення, налаштування та інтеграції різних архітектур, що ускладнює процес і подовжує його тривалість. Щоб подолати ці виклики, організації, які займаються розробкою стандартів у сфері інформаційно-комунікаційних технологій, докладають зусиль для створення технічних специфікацій, призначених для систем Інтернету речей. Серед найбільш відомих – архітектурна основа від IEEE, рекомендації ITU-T, а також стандарти, запропоновані ініціативою oneM2M. У промисловому секторі, в рамках промислового Інтернету речей (IIoT), особливо важливими є стандарт Open Platform Communications Unified Architecture (OPC UA) та специфікації, розроблені консорціумом Industry IoT [2].

Архітектура Інтернету речей може варіюватися залежно від конкретної реалізації. Водночас вона має спільні риси з традиційними системами автоматизованого керування технологічними процесами (АСКТП). Крім того, IoT можна розглядати як складову мереж наступного покоління, оскільки його архітектурна модель багато в чому нагадує структуру NGN. Як

уже зазначалося, існує далеко не один варіант архітектури IoT: вона може складатися з різної кількості рівнів – від базових трирівневих (пристрої – шлюз – додатки) до більш розгорнутих багаторівневих моделей із проміжними прошарками збору, обробки та аналітики даних. Збільшення кількості рівнів архітектури дозволяє підвищити гнучкість та масштабованість системи, забезпечити більш ефективну обробку даних на проміжних етапах, а також підсилює безпеку та надійність обміну інформацією.



Рисунок 1.2 – Еталонна, спрощена архітектура Інтернету речей [5]

Еталонна архітектура Інтернету речей, зображена вище, отримана в результаті порівняння кількох платформ Інтернету речей, включаючи як платформи з відкритим кодом, так і власницькі. Еталонну архітектуру, запропоновану в [5] і відтворену на рисунку 1.2, можна розширити, враховуючи моделі, визначені в стандарті IEEE для архітектурної основи для Інтернету речей [6] і в Рекомендації ITU-T Y.2060 [7]. Таким чином ми

можемо визначити більш повну еталонну архітектуру, яка здатна добре абстрагувати архітектуру більшості найсучасніших платформ IoT [2].

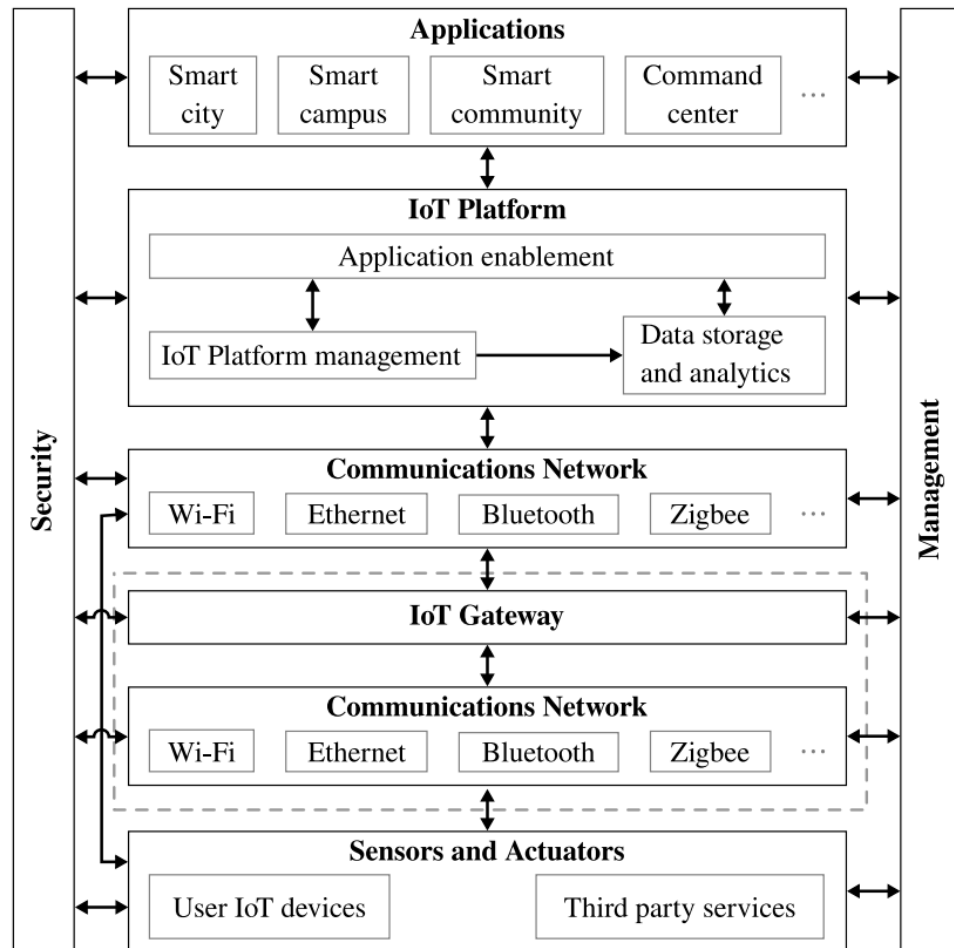


Рисунок 1.3 – Семирівнева архітектура Інтернету речей [2]

Дана архітектура включає сім основних компонентів (як от варіант архітектури від Європейського інтеграційного проекту «IoT-A, Internet of Things – Architecture»): датчики й актуатори (виконавчі пристрої), IoT-платформу, комунікаційну мережу, IoT шлюз, прикладні програми, систему керування та засоби забезпечення безпеки.

При порівнянні моделі передачі даних у традиційному Інтернеті та в архітектурі IoT-A помітна низка відмінностей. У IoT-A виокремлюють два ключові поняття, а саме: мережа з обмеженнями та мережа без обмежень [4].

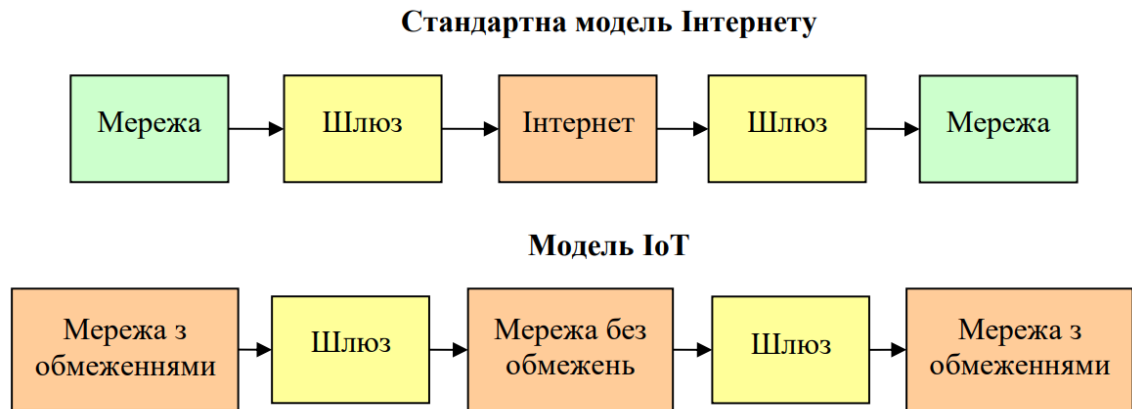


Рисунок 1.4 – Порівняння моделей передачі даних в Інтернеті і в IoT [4]

Перша характеризується низькою пропускнуою здатністю (менше 1 Мбіт/с, як у стандарті IEEE 802.15.4) та значними затримками. Друга, навпаки, забезпечує високі швидкості передачі (десятки Мбіт/с і більше) та за своїми властивостями наближена до сучасного Інтернету.

Але все ж повернемося до варіанту архітектури зображеної на рисунку 1.3 Почнемо розгляд з найнижчого, першого рівня архітектури IoT [2]:

Датчики і виконавчі пристрої (актуатори)

Датчики – це пристрої, які здійснюють вимірювання фізичних характеристик навколишнього середовища (наприклад, температури або вологості) або параметрів інших систем (наприклад, електричного струму). Актуатори, в свою чергу, виконують дії за запитами з IoT, наприклад, включають чи вимикають певні пристрої.

Сенсори й актуатори можуть суттєво відрізнятися за типами вимірюваних параметрів, способами комунікації та взаємодії з користувачем, а в окремих випадках бути ще й «розумними», тобто здатними до попередньої обробки даних. В архітектурі IoT зазвичай розрізняють користувацькі IoT-пристрої (наприклад, датчики температури, які встановлюються безпосередньо користувачем) та сторонні сервіси (що надають дані через REST API, зокрема метеорологічні служби).

Мережа комунікацій

Забезпечує обмін даними між сенсорами, актуаторами, IoT-

платформами та шлюзами. Вона реалізує фізичний, каналний і мережевий рівні відповідно до моделі OSI. На мережевому рівні застосовуються такі протоколи:

- *IPv4* – 32-бітні адреси, через що може бути дефіцит унікальних адрес.
- *IPv6* – 128-бітні адреси, практично необмежений адресний простір.
- *6LoWPAN* – адаптаційний протокол, для використання *IPv6*.

На фізичному та каналному рівнях найчастіше використовуються бездротові технології, які відрізняються за радіусом дії, швидкістю передачі даних та топологією мережі, про які ми будемо говорити у наступному пункті.

Шлюз IoT

Виконує роль проміжного рівня між IoT-пристроями та IoT-платформою. Оскільки різні пристрої можуть використовувати різні мережі зв'язку, протоколи та формати даних, шлюз забезпечує їхню уніфікацію. Він надає єдине середовище обміну даними з платформою, перетворюючи протоколи та формати у сумісні. У практичних умовах зазвичай використовується кілька шлюзів, кожен обслуговує свою групу IoT-пристроїв.

Платформа IoT

Це центральний вузол IoT-системи, що забезпечує контроль та моніторинг підключених датчиків і виконавчих пристроїв за допомогою застосунків. Вона складається з трьох основних блоків:

- *Управління платформою IoT*: включає створення та конфігурацію користувацьких акаунтів із відповідними правами доступу, інтеграцію та керування пристроями (як сенсорами, так і актуаторами), а також контроль роботи платформи – перевірку стану системи, журналів подій, резервне копіювання, оновлення програмного забезпечення тощо.
- *Зберігання та аналітика даних*: забезпечує прийом, обробку та тимчасове зберігання даних від сенсорів, а також їхній аналіз.

- *Забезпечення застосунків:* надає інструменти для розробки та розгортання додатків у межах IoT-системи. Це можуть бути API, інтеграції зі сторонніми сервісами тощо.

Додатки

Додаток – це програмний компонент, який виконує певне завдання, пов’язане з обробкою даних, отриманих від сенсорів, та/або керуванням актуаторами. Прикладами додатків можуть бути графічний інтерфейс (GUI), що відображає дані із сенсора у часовій динаміці або кнопка, яка дозволяє користувачу вмикати або вимикати певний пристрій та ін.

Одним із найбільш типових та простих додатків, які легко реалізуються більшістю IoT-платформ, є так звані правила. Це завдання (наприклад, керування актуатором, виконання певної операції, надсилання попередження користувачу тощо), що можуть активуватися подіями.

Безпека

Блок безпеки забезпечує конфіденційність, цілісність та доступність даних у IoT-системі. Його функції включають автентифікацію користувачів, захист приватності, контроль доступу, моніторинг та аудит подій безпеки, а також керування ключами та сертифікатами.

Управління

Блок управління відповідає за координацію роботи IoT-системи, взаємодіючи з усіма компонентами. Він включає управління відмовами, моніторинг продуктивності системи, керування мережею, а також віддалену конфігурацію та оновлення пристроїв.

Отож, з огляду на багаторівневу структуру Інтернету речей та різноманітність його компонентів, стає зрозуміло, що ефективність системи значною мірою залежить від конкретного сценарію використання. Кожна сфера застосування – від розумних міст до промислових підприємств, медичних закладів чи агротехнічних систем – накладає власні вимоги на функціональні можливості, продуктивність та безпеку IoT-мереж. Тому подальший аналіз доцільно зосередити на розгляді основних напрямів

використання IoT, що дозволяє оцінити вплив технологічних рішень на реальні застосування та підкреслити практичну цінність цих систем.

1.2 Основні сфери застосування IoT

Без сумніву, ми можемо сказати, що розвиток Інтернету речей сьогодні виходить далеко за межі теоретичних моделей і технічних рішень, перетворюючись на практичний інструмент для модернізації різних сфер життя та діяльності людини. Завдяки здатності поєднувати фізичні об'єкти з цифровими сервісами IoT забезпечує новий рівень автоматизації, моніторингу й управління. У різних сферах діяльності IoT проявляє себе по-різному, демонструючи власний потенціал у підвищенні ефективності, безпеки та якості життя. Його використання дозволяє створювати нові моделі взаємодії між людьми, технікою та інформаційними системами, забезпечуючи безперервний обмін даними та можливість прийняття рішень у реальному часі.

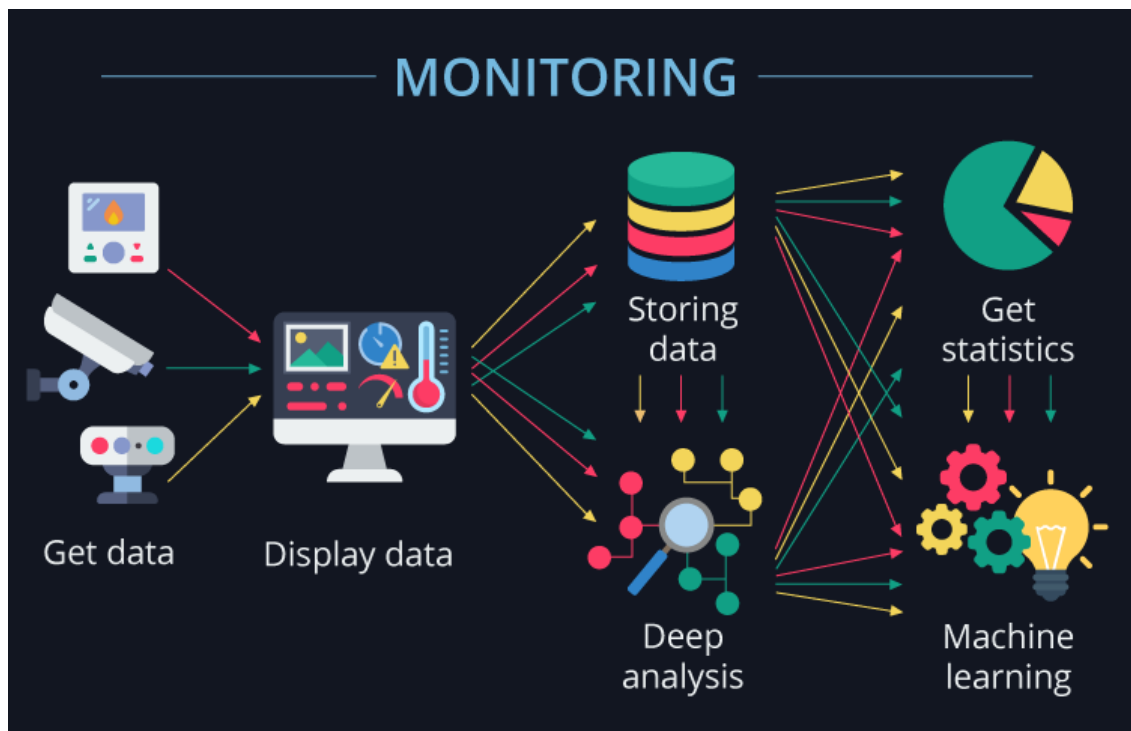


Рисунок 1.5 – Рішення Інтернету речей для моніторингу [13]

Один з прикладів застосування IoT – це, звичайно ж, моніторинг, який, в свою чергу, є корисним в будь-якій сфері застосування. У довгостроковій перспективі результати моніторингу можна збирати та застосовувати для отримання поглиблених знань. Накопичені дані датчиків допомагають отримувати детальну та змістовну статистику, оцінювати продуктивність обладнання з різних точок зору, виявляти нові закономірності та тенденції тощо. Моніторинг є важливою допомогою в проактивному обслуговуванні, оскільки користувачі IoT-систем отримують можливість виявити проблеми до того, як буде завдано шкоди, та вжити необхідних заходів [9, 13].

Підключені пристрої створюють цілісну картину стану навколишнього середовища, здоров'я пацієнтів, роботи обладнання чи інфраструктури, а також допомагають контролювати побутові об'єкти – від транспорту до «розумних» будинків. Система IoT не обмежується лише передаванням і відображенням даних сенсорів: вона здатна аналізувати отримані показники, виявляти аномалії, прогнозувати відмови та визначати першопричини несправностей. Таким чином, порівняння поточних даних із допустимими значеннями, збереженими в хмарі, дозволяє системі для моніторингу, наприклад, залізничного транспорту, визначити, що певний компонент перебуває на межі виходу з ладу [13].

Використання систем Інтернету речей відкриває низку переваг, серед яких ключовою є можливість постійного вимірювання та контролю процесів у фізичному середовищі. Відомий управлінський принцип «те, що можна виміряти – можна покращити» особливо актуальний у цьому контексті. Завдяки сенсорам і засобам моніторингу IoT забезпечує безперервний збір даних про стан об'єктів та явищ, що створює основу для прийняття рішень і підвищення ефективності керованих процесів [10].

Практичні сфери застосування IoT умовно поділяють на два великі сегменти – бізнесовий і споживчий. Уже сьогодні споживачам добре знайомі «розумні» пристрої, такі як носимі сенсори для контролю здоров'я та

фізичної активності, системи «розумного дому», камери відеоспостереження чи автомобілі з елементами автопілоту. Водночас найбільший економічний ефект на початковому етапі очікується саме у бізнес-середовищі. IoT здатний радикально вплинути на ефективність підприємств, забезпечуючи прогнозне обслуговування обладнання, оптимізацію використання активів та зростання продуктивності [9, 10].

Аналітики виділяють кілька ключових сфер, де вплив IoT може бути найбільш відчутним: виробництво, міська інфраструктура, охорона здоров'я, роздрібна торгівля, транспорт, та інші. Цей поділ є умовним, однак він дозволяє виокремити основні напрями, у яких реалізується найбільший потенціал Інтернету речей.

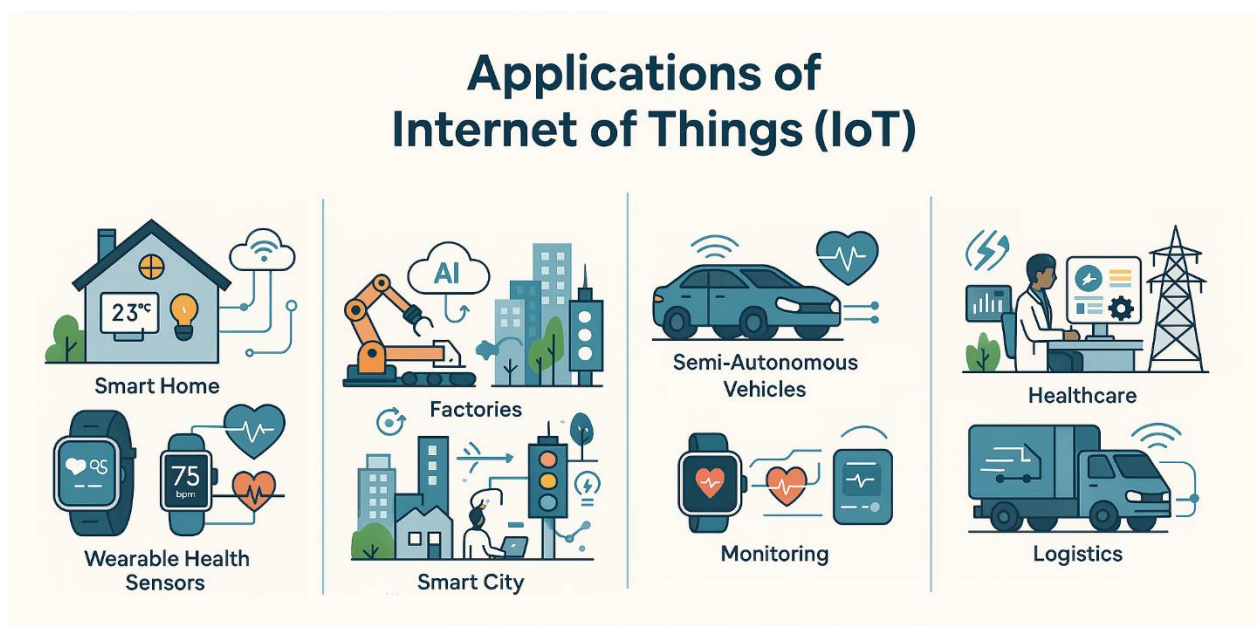


Рисунок 1.6 – Основні сфери застосування технологій Інтернету речей

Виробниче середовище є одним із провідних напрямів застосування IoT завдяки можливості цифровізації та кількісної оцінки результатів роботи. У таких системах зазвичай вже застосовуються автоматизація й системи керування, проте інтеграція IoT дозволяє значно підвищити ключові показники ефективності та обґрунтувати інвестиції. Тисячі датчиків, що працюють у локальних контурах управління окремими машинами чи

виробничими лініями, можуть бути об'єднані в єдину систему збору та аналізу даних. Це забезпечує комплексне бачення процесів і відкриває можливості для глобальної оптимізації. Серед основних переваг застосування IoT у виробництві варто відзначити виявлення аномалій, запобіжне технічне обслуговування та прогнозування відмов обладнання на основі кореляцій даних сенсорів.

Міста можуть отримати вигоду від використання Інтернету речей для покращення своєї роботи та послуг у різних сферах, таких як транспорт і паркування, вуличне освітлення, споживання енергії та ін. Стратегічна мета полягає у створенні комплексного підходу, що забезпечує цілісне бачення міських процесів і узгоджені дії між різними системами. Для цього необхідно автоматизувати окремі підсистеми та забезпечити їхню взаємодію через обмін зібраними даними.

Додатки для здоров'я та фізичної активності у поєднанні з носимими пристроями забезпечують постійний моніторинг активностей користувача та життєво важливих показників. Концепція «quantified self» [10] забезпечує детальні та безперервні дані, що відкриває нові можливості для індивідуалізації медичної практики на основі точних даних замість усереднених показників.

У *автомобільній сфері* найбільш помітним застосуванням IoT є самокеровані та автономні транспортні засоби. Вони спираються на комплексне сенсорне спостереження за оточенням і алгоритми штучного інтелекту для автономної навігації. Через вимоги до швидкодії та безпеки частина обробки даних відбувається безпосередньо в автомобілі, тоді як інформація про ситуації та їх результати надсилається в хмару для вдосконалення алгоритмів і картографії. Дані, зібрані з підключених автомобілів, також використовуються для аналізу типових сценаріїв використання, характеристик батарей, частоти несправностей та інших показників, що допомагає удосконалювати продукцію та створювати додаткові сервіси, наприклад оренду автомобілів чи каршерінг без участі

водія. Розробляються також мережі «автомобіль–автомобіль» для підвищення безпеки та ефективності, що попереджають про небезпечні умови на дорозі. У логістиці та транспортуванні IoT використовується для відстеження вантажів, а в промисловості та сільському господарстві – для моніторингу обладнання, ґрунту, посівів і тварин у віддалених або важкодоступних районах.

Енергетичні компанії можуть отримати вигоду від IoT через «розумні» мережі та лічильники, що дозволяють контролювати споживання та навантаження. Це дає змогу постійно вимірювати навантаження та відповідно регулювати виробництво. Такий адаптивний підхід допомагає ефективно балансувати попит і пропозицію, оскільки зберігання енергії поки що є економічно неефективним.

Смартземлеробство використовує IoT для підвищення ефективності та передбачуваності сільськогосподарського виробництва. Датчики та гаджети дозволяють моніторити кліматичні умови, стан ґрунту, вологість, освітлення та інші параметри для оптимального вирощування культур. Використання агродронів і автономних роботів дозволяє збирати дані, проводити обстеження полів, боротися зі шкідниками та автоматизувати рутинні процеси, такі як посів чи оранка. Системи «від початку до кінця» інтегрують різні датчики та аналітику для оптимізації виробництва, управління ресурсами та логістики, забезпечуючи більш сталий і високопродуктивний аграрний бізнес [14].



Рисунок 1.7 – Приклади використання IoT в аграрній сфері [14, 15]

У домашніх системах IoT здебільшого застосовується для автоматизації побутових процесів та підвищення комфорту користувачів через контроль безпеки, освітлення, температури та роботу «розумних» пристроїв. Голосові помічники, що підключені до Інтернету, можуть виступати як пункт управління іншими домашніми пристроями.

Отож, як можна побачити, IoT без сумніву знаходить широке застосування у багатьох сферах – від розумних міст і транспорту до медицини та сільського господарства. Проте, як і будь-яка технологія, він має свої обмеження та проблеми, що потребують особливої уваги. Серед них, звичайно ж, ключовими є забезпечення безпеки даних, ефективне управління великою кількістю пристроїв, енергоефективність та масштабованість систем. Успішне подолання цих викликів є ключовим для повноцінного впровадження IoT і максимізації його потенціалу. Тому в наступному розділі ми зосередимося саме на основних проблемах та викликах розвитку Інтернету речей.

1.3 Проблеми та виклики розвитку Інтернету речей

Розвиток Інтернету речей відкриває величезні можливості для підвищення ефективності, автоматизації та персоналізації у різних галузях. Проте інтенсивне використання IoT супроводжується рядом складнощів, які можуть обмежити його потенціал і стати перешкодою для повсюдного впровадження. Ключові виклики пов'язані з безпекою даних, масштабованістю систем, управлінням великою кількістю пристроїв та енергоефективністю.

Поширення IoT змінило спосіб взаємодії людей зі світом та передовими технологіями. Від найменшого смарт-годинника до появи автономних транспортних засобів, від розумних будинків до розвитку розумних міст, IoT відіграє певну роль у розвитку технологій та цивілізації людського суспільства. Технологія IoT має значний економічний та екологічний вплив, так як підключені пристрої передбачають велике споживання енергії та управління даними, що в свою чергу створює питання безпеки за захисту [16].

На рисунку 1.8 показано мережу спільного цитування наукових публікацій та їх взаємозв'язки за період 2019–2024 років. Як видно, теми Інтернету речей, кібербезпеки та енергоефективності тісно переплетені. Через тісний зв'язок між публікаціями та велику кількість цитувань можна зробити висновок, що питання, пов'язані насамперед із забезпеченням безпеки та енергоефективності IoT, залишаються надзвичайно актуальними і потребують особливої уваги у подальшому розвитку технології.

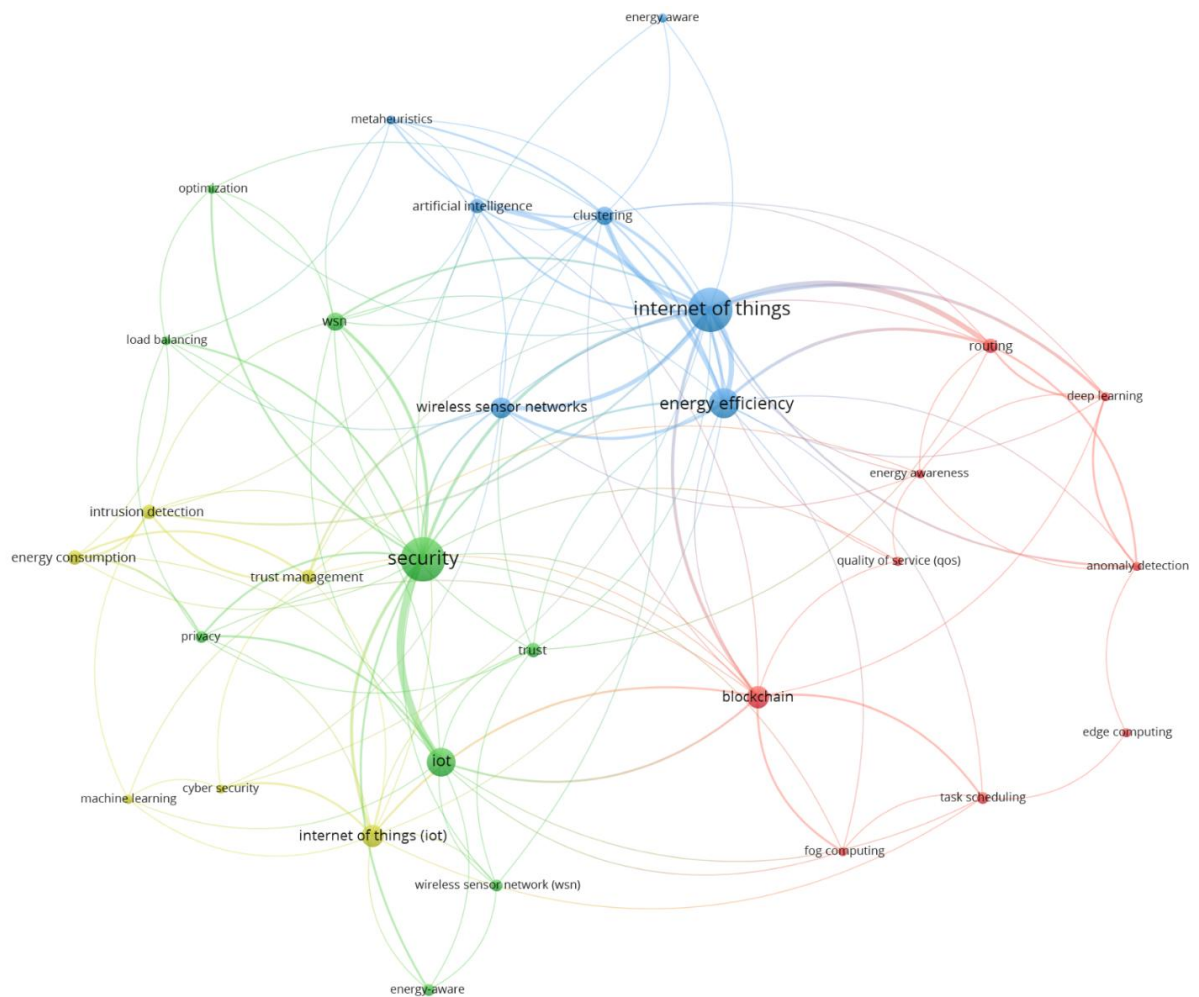


Рисунок 1.8 – Візуалізація цитування публікацій з «IoT», «енергетики» та «безпеки» [16]

Концепція Інтернету речей (IoT) швидко розвивалася протягом останнього десятиліття, і очікується, що кількість підключених пристроїв перевищить 30 мільярдів до кінця 2025 року. Поява Масового Інтернету речей (MIoT) стосується підмножини систем IoT, що характеризуються величезною кількістю, що характеризуються величезною кількістю пристроїв, що генерують великі обсяги даних і потребують високомасштабованої інфраструктури. Величезні масштаби MIoT створюють значні проблеми, які можна розподілити на чотири критичні області [17]:

- *Масштабованість мережі*, де багато пристроїв повинні взаємодіяти без перевантаження мережевої інфраструктури.
- *Керування даними*, де величезні обсяги даних повинні оброблятися,

зберігатися та аналізуватися в режимі реального часу.

- *Енергоефективність*, де пристрої, особливо ті, що знаходяться у віддалених або важкодоступних місцях, повинні працювати з обмеженими енергоресурсами.
- *Безпека та конфіденційність*, де забезпечення цілісності та безпеки величезних розподілених мереж стає дедалі складнішим зі зростанням кількості пристроїв.

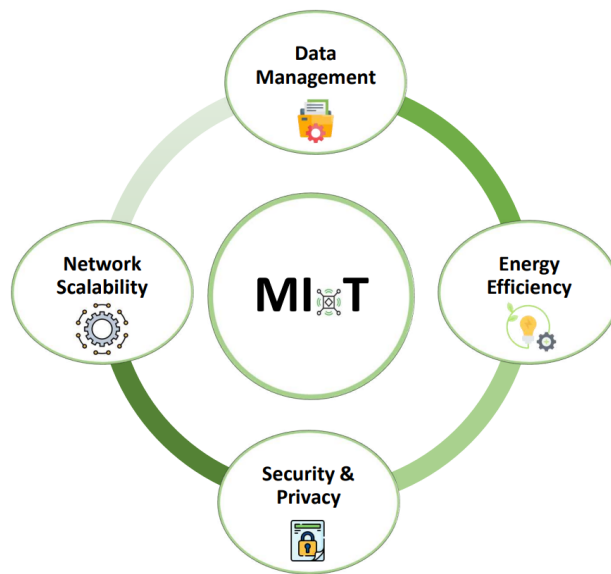


Рисунок 1.9 – Основні виклики МІоТ

Однією з ключових проблем Масового Інтернету речей (МІоТ) є масштабованість, оскільки стрімке зростання кількості пристроїв створює значні навантаження на мережеву інфраструктуру. У надщільних середовищах, де працюють IoT-системи, складно одночасно забезпечити високу продуктивність, низьку затримку, ефективний розподіл ресурсів та надійність зв'язку.

Основні труднощі масштабування мереж IoT включають [17]:

- *Щільність пристроїв і перевантаження мережі*. Велика кількість підключень призводить до втрат пакетів, зростання затримки та QoS.
- *Вимоги до затримки*. Для застосувань у реальному часі (автономний

транспорт, промислова автоматизація) критично важлива мінімальна затримка. Це потребує оптимізованих протоколів маршрутизації та використання обчислень на периферії (edge computing).

- *Розподіл ресурсів.* Зі зростанням кількості пристроїв ускладнюється управління смугою пропускання, енергоспоживанням та обчислювальними потужностями. Перспективними є підходи з використанням ШІ для динамічного управління ресурсами.
- *Управління завадами.* У надщільних мережах виникають проблеми накладання сигналів, що знижує якість зв'язку. Вирішенням є адаптивне керування потужністю та завадостійкі протоколи.
- *Протокольна сумісність.* Традиційні протоколи не були розраховані на мільярди пристроїв. Тому необхідні нові або адаптовані рішення, здатні мінімізувати навантаження на мережу та енергоспоживання.

Сучасні рішення для подолання викликів масштабованості в IoT мережах ґрунтуються на кількох ключових технологіях. Одним із найперспективніших напрямів є когнітивні радіомережі (CRN), які забезпечують динамічний доступ до спектра. Завдяки цьому IoT-пристрої можуть використовувати вільні частотні діапазони у певний момент часу, що суттєво знижує перевантаження мереж із великою кількістю пристроїв.

Іншим рішенням є використання міліметрових хвиль (mmWave), які відкривають доступ до широких смуг частот і забезпечують високі швидкості передавання даних. Це дає змогу підтримувати велику кількість одночасних з'єднань, особливо в міських умовах.

Також значного поширення набувають програмно-визначені мережі (SDN), які відокремлюють площину керування від площини передавання даних. Це дає змогу централізовано управляти ресурсами та гнучко адаптувати мережу до змінних умов трафіку й щільності пристроїв.

Зрештою, архітектури обчислень на межі (Edge) та у тумані (Fog) дозволяють переміщати обробку даних ближче до пристроїв IoT. Це сприяє зменшенню затримок і навантаження на основну мережу, а також забезпечує

обробку даних в реальному часі.

У системах МІоТ ключовим викликом є управління даними, оскільки мільярди пристроїв генерують величезні обсяги інформації. Основні труднощі пов'язані з п'ятьма аспектами: обсяг, різноманітність, швидкість, безпека та енергоефективність. Дані у смарт-містах можуть досягати терабайтів на добу, що перевантажує централізовані хмарні центри обробки. Крім того, ІоТ-пристрої продукують різні типи даних – від структурованих сенсорних показників до відео та логів, що ускладнює їх інтеграцію в єдину систему. Не менш важливим є фактор швидкості: медичні чи транспортні додатки потребують обробки даних у реальному часі, чого не можуть забезпечити традиційні пакетні системи. Додатково значно зростає поверхня атак, що підвищує ризики втрати цілісності та конфіденційності інформації. Нарешті, через обмежені ресурси ІоТ-пристроїв виникає потреба в енергоощадному управлінні даними [17].

Сучасні рішення для подолання цих викликів передбачають кілька підходів. Edge та Fog обчислення, про які вже згадувалося вище, знову стануть у нагоді, так як дозволять виконувати попередню обробку даних ближче до джерела, що знижує затримку й навантаження на хмарні системи. Перспективною є технологія навчання, яка дозволяє тренувати алгоритми ШІ локально, передаючи лише оновлені параметри моделей, а не «сирі» дані, що підвищує приватність і ефективність. Нарешті, платформи потокової обробки (Apache Kafka, Spark Streaming) забезпечують роботу з високошвидкісними потоками даних у реальному часі, що особливо важливо для медицини, смарт-міст та промислової автоматизації.

Енергоефективність є критичним аспектом МІоТ, оскільки вона безпосередньо впливає на довговічність, надійність та масштабованість розгортання ІоТ. Велика кількість малопотужних пристроїв, що працюють у мережах МІоТ, вимагає розробки енергоефективних протоколів зв'язку, методів обробки даних та рішень для управління ресурсами.

Основні труднощі забезпечення енергоефективності в ІоТ зумовлені

обмеженим ресурсом акумуляторів, заміна яких часто є технічно складною або економічно недоцільною, а також високими енерговитратами на передачу й обробку масивних обсягів даних. Ситуацію ускладнюють перевантаження мережі та інтерференція сигналів у щільних середовищах, що призводить до повторних передач і додаткового виснаження батарей, вимагаючи нових підходів для забезпечення довгострокової стійкості систем у контексті розгортання 5G та 6G [17].

Сучасні рішення для підвищення енергоефективності в МІoT зосереджені на зниженні споживання енергії при збереженні продуктивності. Перспективним напрямом є використання технологій збору енергії з навколишнього середовища (сонячна, вітрова, радіочастотна), що дозволяє зменшити залежність від батарей. Широкого поширення набули LPWAN-технології (LoRaWAN, Sigfox, NB-IoT), які забезпечують енергоефективний зв'язок на великі відстані. Нарешті, у сучасних дослідженнях активно застосовується машинне навчання, яке прогнозує споживання енергії та в режимі реального часу оптимізує розподіл ресурсів у динамічних IoT-середовищах.

Швидке масштабування мереж IoT та їх неоднорідність створюють *серйозні виклики у сфері кібербезпеки*, зокрема проблему надійної автентифікації мільярдів пристроїв, які через обмежені обчислювальні ресурси не здатні підтримувати складні криптографічні алгоритми. Критичними завданнями залишаються забезпечення цілісності та конфіденційності чутливих даних, захист приватності користувачів від витоків, а також реалізація безпечних механізмів оновлення програмного забезпечення для усунення вразливостей. Ситуацію додатково ускладнює необхідність масштабування рішень безпеки без втрати продуктивності мережі та високий ризик фізичного втручання у роботу пристроїв, що часто розміщуються у неконтрольованих зонах.

Одним із перспективних напрямів є розробка легких криптографічних алгоритмів, які враховують обмеженість ресурсів IoT-пристроїв. Вони

забезпечують достатній рівень безпеки при мінімальних витратах обчислювальної потужності та енергії. В свою чергу, блокчейн-технології застосовуються для створення децентралізованих і захищених реєстрів, які дозволяють реалізувати автентифікацію пристроїв, контроль цілісності даних та безпечні транзакції без потреби в центральному довірчому вузлі. Це робить МІoT-мережі більш стійкими до атак. Важливу роль відіграють системи виявлення вторгнень на основі ШІ.

Таблиця 1.1 – Короткий підсумок проблем ІoT та можливих рішень

Критична область	Найважливіші проблеми	Короткі рішення / підходи
Масштабованість мережі	1. Щільність пристроїв → мережеві затори. 2. Жорсткі вимоги до затримки у реальному часі. 3. Протокольні й архітектурні обмеження (legacy).	• LPWAN / CRN / mmWave для розвантаження та додаткових ресурсів. • Edge/Fog і оптимізовані маршрути для зниження затримок. • SDN + AI-кероване управління ресурсами; адаптовані легкі протоколи.
Керування даними	1. Величезний обсяг даних (storage / bandwidth). 2. Необхідність обробки в реальному часі (velocity). 3. Гетерогенність форматів (variety).	• Edge/Fog для попередньої обробки й зменшення трафіку. • Поточкові платформи (Kafka, стрімінг) для real-time обробки. • Агрегація/стиснення даних; гібридне зберігання (edge + cloud).
Енергоефективність	1. Обмежені батареї та важкодоступність заміни живлення. 2. Енерговитрати на передачу великих обсягів даних. 3. Збільшене споживання через перешкоди/повторні передачі.	• LPWAN та енергооптимізовані протоколи. • Energy harvesting (сонце, RF) та енергоменеджмент. • Edge-обробка і агрегація для мінімізації передавання; energy-aware маршрутизація.
Безпека та конфіденційність	1. Масштабна автентифікація/авторизація пристроїв. 2. Захист цілісності й конфіденційності чутливих даних. 3. Безпечні OTA-оновлення та фізичний захист пристроїв.	• Легкі криптопротоколи + апаратні корені довіри (secure elements). • Шифрування на кінцях, захищені канали, та механізми аудиту (blockchain – там, де потрібно). • Безпечні та підписані OTA-механізми; IDS на основі ШІ для виявлення аномалій.

1.4 Висновки до розділу 1

У першому розділі дипломної роботи було розглянуто концепцію Інтернету речей як ключової складової сучасних інформаційно-комунікаційних технологій. Увагу було приділено архітектурі IoT та її основним рівням – від датчиків та виконавчих пристроїв, до IoT платформ та рівня додатків, на якому відбувається безпосереднє відображення даних із сенсорів. Це дозволило визначити системність підходу до побудови IoT-рішень та їхню здатність інтегруватися з різними технологіями.

Було детально розглянуто основні області застосування IoT, серед яких розумні міста, промисловість, транспорт, медицина, агротехніка та інші. В кожній із цих сфер Інтернет речей відкриває нові можливості для підвищення ефективності, оптимізації процесів, покращення якості послуг і прийняття рішень на основі даних.

Водночас окреслено ключові виклики, що стоять перед розвитком IoT, а саме проблеми безпеки, масштабованості, керування даними та енергоефективності. Їхнє вирішення є критично важливим для успішного функціонування масових IoT-систем та забезпечення їхньої надійності й довгострокової стійкості.

Узагальнюючи, можна сказати, що розділ надав цілісне уявлення про концепцію Інтернету речей, його архітектурні особливості, прикладні можливості та основні проблеми розвитку. Це створює основу для подальшого дослідження технологічних аспектів IoT і пошуку шляхів підвищення ефективності його впровадження.

2 РАДІОТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Огляд, технічні характеристики, переваги та недоліки радіотехнологій в мережах IoT

Радіотехнології можна назвати фундаментальною основою функціонування Інтернету речей. Вони забезпечують бездротову передачу даних між пристроями, сенсорами та мережевими вузлами, що є невід’ємною складовою IoT мереж. Вибір технології зв’язку визначає енергоспоживання, дальність дії, пропускну здатність і загальну ефективність IoT-систем. Оскільки сфери застосування IoT різноманітні – від побутових пристроїв до промислових систем і розумних міст, – існує широкий спектр радіорішень, кожне з яких має власні технічні особливості, переваги та обмеження. Деякі з цих технологій спрямовані на передачу великих обсягів даних з високою швидкістю, інші - на низькошвидкісну передачу невеликих обсягів даних, забезпечуючи при цьому ефективне використання електроенергії [18].

У світі Інтернету Речей спосіб передачі та отримання інформації є ключовим аспектом для забезпечення функціональності різноманітних пристроїв та датчиків, підключених до мережі. У контексті інтернет екосистеми речей, зв’язок з датчиками та виконавчими пристроями може відбуватися як через, наприклад, мідні дроти, так і через бездротові персональні мережі [18]. Останні, в свою чергу, мають найбільше розповсюдження, та велике значення.

Як показано на рисунку 2.1, кожна радіотехнологія має власний компроміс між дальністю дії та швидкістю передачі даних. Наприклад, технології короткого радіусу дії, такі як Bluetooth або ZigBee (IEEE 802.15.4), забезпечують низьку швидкість передавання даних, проте відзначаються низьким енергоспоживанням і простотою інтеграції у побутові пристрої. Натомість стільникові технології (2G–5G) та NB-IoT охоплюють значно більші відстані, забезпечуючи при цьому середню або високу швидкість передавання інформації. Особливе місце займають рішення класу LPWA

(Low Power Wide Area), наприклад та ж LoRa, що дозволяє передавати невеликі обсяги даних на великі відстані з мінімальним енергоспоживанням. Саме це робить їх ідеальними для розподілених сенсорних мереж і “розумних міст”.

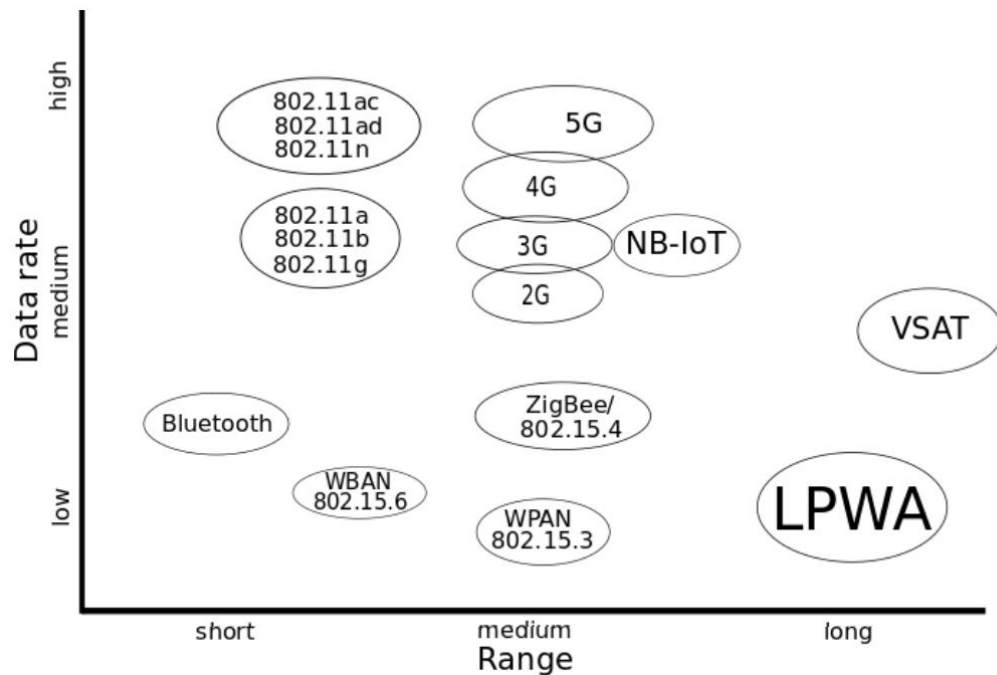


Рисунок 2.1 – Дальність дії та швидкість передачі деяких бездротових технологій [19]

В свою чергу, на рисунку 2.2 показано порівняння технологій за критеріями енергоефективності та вартості підключення. З нього видно, що LPWA-технології (зокрема LoRa, Sigfox та ін.) забезпечують найкраще співвідношення між тривалістю роботи пристроїв від батареї та низькою вартістю терміналів. У той час як супутникові та стільникові рішення мають значно вищі витрати, вони забезпечують глобальне покриття та високу надійність зв'язку. Таким чином, вибір радіотехнології в IoT визначається балансом між енергоспоживанням, вартістю, дальністю дії та вимогами до швидкості передавання даних.

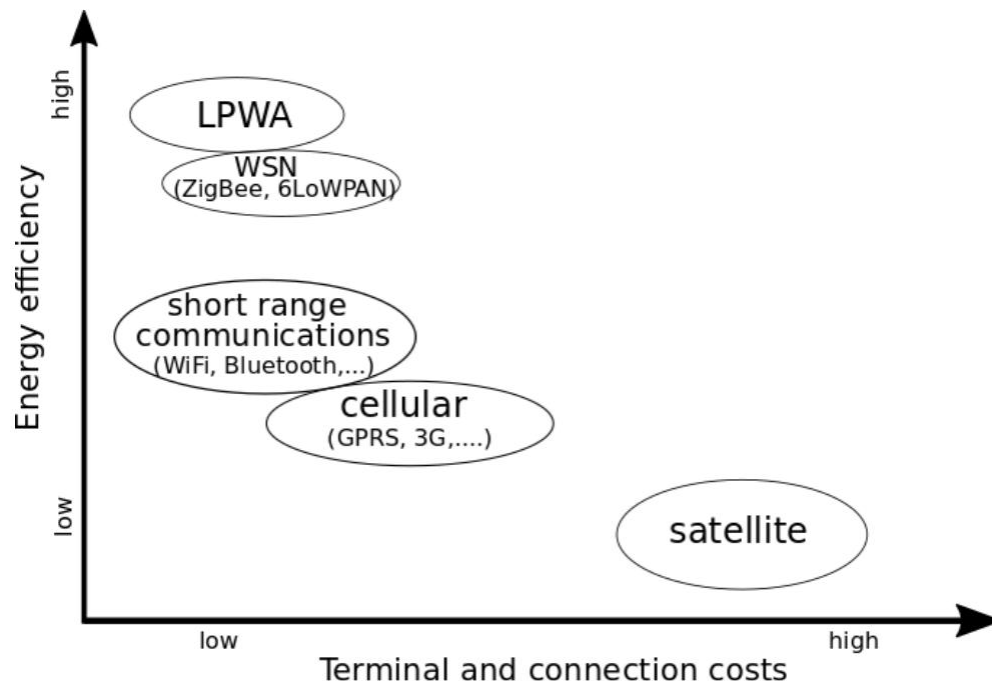


Рисунок 2.2 – Енергоефективність та вартість терміналів і підключення бездротових технологій [19]

- Bluetooth та Bluetooth Low Energy (BLE)

Bluetooth – це технологія короткодіапазонного бездротового зв’язку, розроблена організацією Bluetooth Special Interest Group (SIG) і стандартизована як IEEE 802.15.1. SIG керує специфікаціями та впроваджує нові функції до існуючого стандарту. Bluetooth працює в неліцензованому діапазоні 2,4 ГГц (ISM band), використовуючи технологію частотного перестрибування (FHSS – Frequency Hopping Spread Spectrum), яка поділяє діапазон на 79 каналів по 1 МГц. Це дозволяє зменшити перешкоди та забезпечує надійність з’єднання навіть у насиченому радіочастотному середовищі [21].

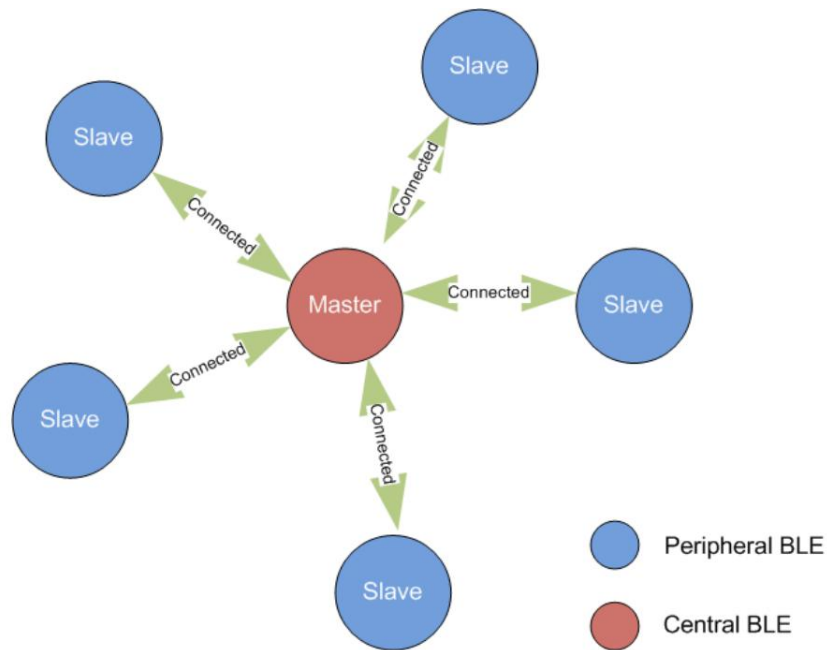


Рисунок 2.3 – Зіркова топологія мережі з пристроями BLE [22]

Типова топологія мережі Bluetooth або ж BLE – зірка, де центральний пристрій (master) координує роботу підлеглих (slave) вузлів, як показано на рисунку 2.3. Обмін даними відбувається за принципом тимчасового поділу дуплексу (TDD), який виділяє часові слоти для кожного пристрою.

Таблиця 2.1 – Порівняння різних класів пристроїв Bluetooth [20]

Клас	Максимальна потужність передачі	Радіус дії	Bluetooth Low Energy	Класичний Bluetooth
Клас 1	100 мВт (+20 дБм)	До 100 м (328 футів)	Поширений у промисловому застосуванні, підтримує зв'язок на великі відстані з низьким енергоспоживанням.	Поширений у промисловому застосуванні, забезпечує надійне з'єднання на великі відстані.
Клас 1.5 ¹	10 мВт (+10 дБм)	До 30 м (98 футів)	Найпоширеніший у побутовій електроніці, використовується в смартфонах, носимих пристроях та периферійних пристроях.	Розумні замки, фітнес-трекери та бездротові аудіопристрої.

Продовження таблиці 2.1

Клас 2	2,5 мВт (+4 дБм)	До 10 м (33 фути)	Найпоширеніший у побутовій електроніці, використовується в смартфонах, носимих пристроях та периферійних пристроях.	Поширений у побутовій електроніці, використовується для гарнітур, клавіатур та мишей.
Клас 3	1 мВт (0 дБм)	До 1 м (3 фути)	Менш поширений, використовується в нішевих застосуваннях, що вимагають зв'язку на коротких відстанях.	Менш поширений, використовується в застосуваннях з мінімальними вимогами до дальності.
Клас 4 ²	0,5 мВт (-3 дБм)	До 0,5 м (1,5 фута)	Рідкісний, гіпотетичний клас для застосування з наднизькою потужністю та дуже короткою дальністю дії.	Рідкісний, нечасто використовуваний або стандартизований.

¹ Клас 1.5 обговорюється рідше, ніж інші класи, але він існує у специфікаціях Bluetooth. Він пропонує хороший компроміс для пристроїв, яким потрібен більший радіус дії, ніж Класу 2, але не потрібна повна потужність Класу 1.

² Клас 4 не є стандартною класифікацією у специфікації Bluetooth, але включено сюди для теоретичної повноти у сценаріях з наднизьким енергоспоживанням.

Bluetooth має кілька класів потужності, що визначають дальність зв'язку – від кількох метрів до понад 100 метрів, більш детальноше можемо побачити це у таблиці 2.1. Із моменту створення технологія пройшла значний розвиток – від Bluetooth 1.0 до Bluetooth 5.0, кожна версія якого покращувала швидкість передачі, стабільність та енергоефективність.

Bluetooth Low Energy (BLE) – це енергоефективна версія стандарту Bluetooth, представлена починаючи з Bluetooth 4.0 і вдосконалена в Bluetooth 5.0. BLE спеціально розроблена для пристроїв Інтернету речей (IoT), де критичними є низьке енергоспоживання, компактність та довговічність роботи від батареї. Пристрої BLE споживають у кілька разів менше енергії, ніж класичні Bluetooth-рішення, і здатні працювати довгий час на одній малій батарейці типу “таблетка”. Завдяки цьому BLE широко використовується у

портативних сенсорах, фітнес-трекерах, розумних годинниках, системах моніторингу здоров'я тощо [3, 21].

- ZigBee та Z-Wave

Технологія ZigBee була розроблена у 2001 році, а пізніше вдосконалена специфікацією ZigBee PRO у 2007 році, яка є повністю зворотно сумісною та містить поліпшення, зокрема покращену безпеку [22, 23]. ZigBee побудована на стандарті IEEE 802.15.4, який визначає фізичний (PHY) та канальний (MAC) рівні, тоді як мережевий рівень забезпечує маршрутизацію, розподіл адрес та керування бездротовою мережею.

ZigBee підтримує три типи топологій – зіркову, деревоподібну та комірчасту (mesh), що дозволяє з'єднати до 65000 вузлів. Така масштабованість робить технологію зручною для масових IoT-впроваджень, наприклад у “розумних містах” або промислових системах. У комірчастій топології роль маршрутизаторів виконують спеціальні вузли, що розширюють зону покриття мережі.

Для енергозбереження ZigBee дозволяє налаштовувати періоди сну вузлів, що суттєво збільшує час автономної роботи. Пристрої ZigBee поділяються на повнофункціональні (FFD) – можуть бути координатором, маршрутизатором чи звичайним пристроєм, та спрощені (RFD) – лише кінцеві вузли з мінімальним споживанням енергії.

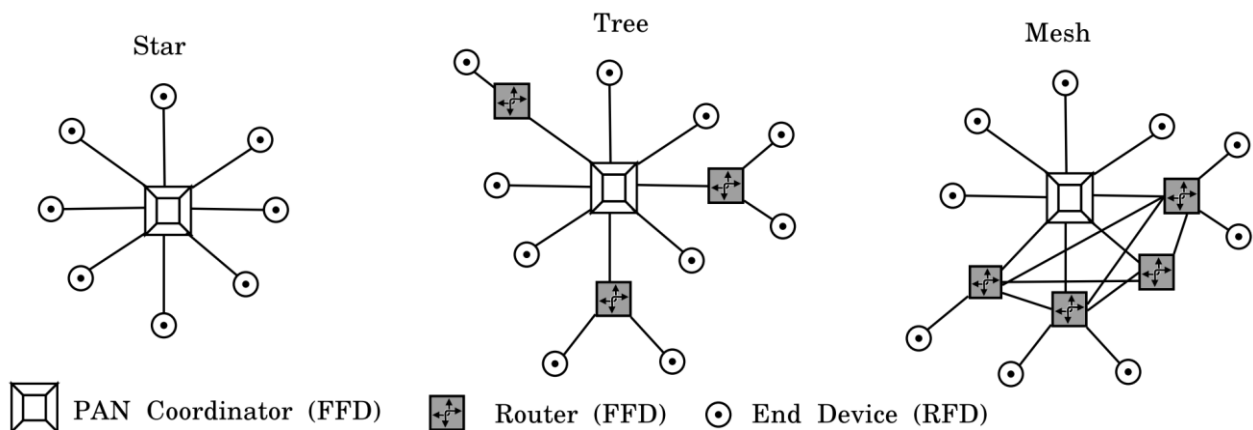


Рисунок 2.4 – Основні топології IoT [21]

До прикладів реалізацій належать ZigBee LightLink (використовується у системах розумного освітлення, як Philips Hue) або ж ZigBee Green Power, що дозволяє працювати пристроям без батарей, використовуючи енергію з навколишнього середовища [23] та інші. Таким чином, ZigBee є енергоефективною, масштабованою та безпечною технологією, оптимальною для мереж сенсорів, систем розумного дому, автоматизації будівель та моніторингу навколишнього середовища.

В свою чергу технологія Z-Wave була розроблена компанією ZenSys Corp. у 2001 році для домашньої автоматизації і базується на стандарті ITU-T G.9959. Вона використовує комірчасту, mesh топологію (приклад на рисунку 2.4), у якій кількість пристроїв обмежена 232 вузлами, а обмін даними здійснюється через сусідні вузли, що підвищує надійність та стабільність зв'язку.

Z-Wave працює в діапазонах 868,42 МГц (Європа) та 908,42 МГц (США), використовуючи вузькосмутову модуляцію з частотним зсувом (FSK). На фізичному, каналному, мережевому та транспортному рівнях Z-Wave застосовує механізм CSMA/CA для уникнення колізій. Більшість пристроїв у мережі перебувають у сплячому режимі, активуючись лише при необхідності, що суттєво знижує енергоспоживання.

Новіша версія протоколу – Z-Wave Plus (2013 р.) – забезпечує покращене енергоспоживання, розширену дальність дії та підвищену безпеку. Управління стандартом здійснює Z-Wave Alliance, до складу якої входить понад 600 компаній, серед яких, наприклад, Siemens та Huawei. Отже, Z-Wave, як і ZigBee, є стабільною, надійною та малопотужною технологією, орієнтованою на системи розумного дому, де важливими є невелика затримка, сумісність між пристроями та довговічність батарей [23]

▪ LoRa та LoRaWAN

LoRa (Long Range) – це бездротова технологія фізичного рівня, розроблена для передавання даних на великі відстані з низьким енергоспоживанням. Вона використовує модуляцію з розширенням спектра

на основі розкиду частоти (Chirp Spread Spectrum, CSS), що забезпечує високу чутливість приймача та стійкість до завад.

LoRa працює у неліцензованих діапазонах частот ISM, що робить її доступною для широкого використання в мережах Інтернету речей. Технологія дозволяє забезпечити передачу даних на відстань до 15 км у сільській місцевості та до 2–5 км у міських умовах, залежно від навколишнього середовища та параметрів передавача. Швидкість передачі даних змінюється від 0,3 до 50 кбіт/с, що є цілком достатнім для сенсорних IoT-додатків, які передають невеликі обсяги даних.

Для управління мережевою інфраструктурою поверх LoRa використовується протокол LoRaWAN (LoRa Wide Area Network) – це протокол канального та мережевого рівнів, який визначає правила обміну даними між пристроями та шлюзами. Мережа LoRaWAN має зіркоподібну архітектуру, у якій кінцеві пристрої (end devices) передають дані до шлюзів (gateways), що далі надсилають їх до мережевого сервера. Сервер виконує маршрутизацію, керування безпекою та розподілом ресурсів [3, 24].

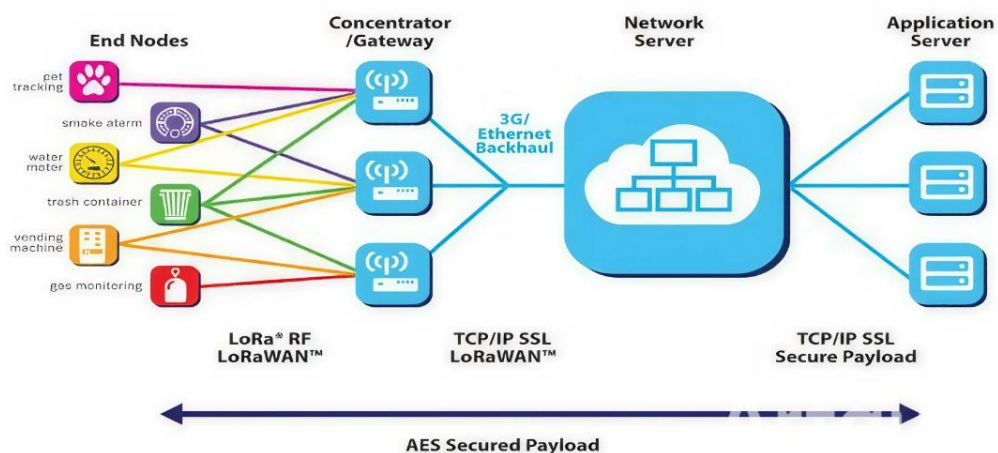


Рисунок 2.5 – Архітектура мережі LoRaWAN [3]

Залежно від режиму роботи, LoRaWAN-пристрої поділяються на три класи [3]:

- Клас А – мінімальне енергоспоживання; передача ініціюється пристроєм, а прийом відбувається у короткі часові вікна після передачі.
- Клас В – додаткові синхронізовані вікна прийому, що дозволяє серверу ініціювати обмін.
- Клас С – приймач постійно відкритий, що забезпечує мінімальну затримку, але збільшує споживання енергії.

Архітектура LoRaWAN включає чотири основні компоненти:

- Кінцеві вузли (End Nodes) – пристрої з сенсорами або виконавчими елементами, які періодично передають дані. Вони живляться від батарей і більшу частину часу перебувають у “сплячому” режимі для економії енергії.
- Шлюзи (Gateways/Concentrators) – приймають сигнали від вузлів по радіоканалу і передають їх у транзитну мережу (Ethernet, Wi-Fi або стільниковий зв’язок).
- Мережевий сервер (Network Server) – відповідає за управління мережею, контролює доступ, усуває дублювання пакетів, здійснює перевірку безпеки та коригує швидкість і потужність передавання даних.
- Сервер додатків (Application Server) – відповідає за обробку, зберігання та візуалізацію отриманих даних.

Основними перевагами LoRaWAN є низьке енергоспоживання, великий радіус дії, висока пропускна здатність мережі та здатність підтримувати велику кількість пристроїв. Завдяки цим характеристикам LoRaWAN широко застосовується у розумних містах, системах моніторингу довкілля, розумному сільському господарстві та енергетичних мережах.

▪ NB-IoT та LTE-M

Технології NB-IoT (Narrowband Internet of Things) та LTE-M (Long-Term Evolution for Machines) є двома основними стандартами класу LPWAN, розробленими консорціумом 3GPP у рамках Release 13 для обслуговування масового міжмашинного зв'язку (mMTC). На відміну від ZigBee чи Z-Wave,

вони функціонують у ліцензованому стільниковому спектрі (4G LTE з перспективою інтеграції у 5G), що забезпечує високу надійність, безпеку операторського класу та глобальне покриття завдяки використанню існуючої інфраструктури мобільних операторів.

Технологія NB-IoT була створена з акцентом на максимальне енергозбереження, високу щільність підключень та глибоке проникнення сигналу. Вона використовує дуже вузьку смугу частот – 180 кГц, що еквівалентно одному ресурсному блоку (PRB) в мережі LTE. Це дозволяє сигналу ефективно проникати крізь товсті стіни, підвальні приміщення та підземні комунікації, де звичайний мобільний зв'язок недоступний. NB-IoT підтримує виключно зіркоподібну топологію (рисунок 2.3, 2.4), де кінцеві пристрої напряму з'єднуються з базовою станцією, що спрощує архітектуру мережі.

Для досягнення надзвичайно низького енергоспоживання NB-IoT використовує механізми глибокого сну, такі як PSM (Power Saving Mode) та eDRX (extended Discontinuous Reception). Через свою архітектуру, низьку швидкість передачі даних (до 250 кбіт/с) та досить високу затримку, технологія не підтримує «хендовер» (тобто перемикання між базовими станціями), тому вона оптимальна для статичних пристроїв. До прикладів застосування належать розумні лічильники (води, газу, електроенергії), датчики заповненості сміттєвих баків, системи моніторингу парковок та аграрні сенсори для вимірювання вологості ґрунту.

У свою чергу, технологія LTE-M (також відома як LTE Cat-M1) була розроблена як більш збалансоване рішення, що пропонує компроміс між енергоефективністю, швидкістю передачі даних та мобільністю. Вона використовує ширшу смугу частот – 1.4 МГц, що дозволяє досягати вищих швидкостей (до 1 Мбіт/с) та значно меншої затримки (10-15 мс) порівняно з NB-IoT [25, 26].

	LTE-M	NB-IoT
Building penetration	●●●●○	●●●●●
Battery life	●●●●○	●●●●●
Data rate	●●○○○	●○○○○
Latency	●●●●●	●○○○○
Handover	●●●●●	●○○○○
mobile applications	●●●●●	●●●○○
stationary applications	●●●●○	●●●●●
Application examples		

Рисунок 2.6 – Переваги та недоліки обох стільникових стандартів [25]

Ключовою перевагою LTE-M є повна підтримка мобільності завдяки механізму хендовера, отож LTE-M пропонує кращі умови для мобільних пристроїв, так як дозволяє пристроям безперервно передавати дані під час руху, тоді як NB-IoT краще підходить для стаціонарних застосувань [25]. Технологія також підтримує передачу голосу через VoLTE (Voice over LTE), що розширює спектр її застосувань. Хоча енергоспоживання LTE-M дещо вище, ніж у NB-IoT, воно залишається на хорошому рівні.

Впровадження технологій мобільного Інтернету речей в Україні активно розвивається, зокрема завдяки зусиллям провідних мобільних операторів. Станом на 2024-2025 роки, основний фокус зосереджений на розгортанні мереж NB-IoT, тоді як LTE-M все ще перебуває більше на етапі тестування.

Оператор Київстар можна назвати флагманом у цій сфері. Оператор розгорнув національну мережу NB-IoT, яка покриває більшість великих міст та ключові регіони країни. Компанія активно просуває цю технологію для бізнес-клієнтів.

Інші великі оператори, як-от Vodafone Ukraine та lifecell, також розвивають свої IoT-платформи та проводять тестування технологій NB-IoT та LTE-M. Вони пропонують бізнес-клієнтам IoT-рішення, які часто базуються на традиційних мобільних мережах (2G/4G), але з поступовим переходом до спеціалізованих стандартів LPWAN.

Загалом можна сказати, що, перш за все, NB-IoT уже посів свою нішу в розвитку мереж Інтернету речей в Україні та продовжує активно використовуватися, особливо в таких галузях, як енергетика, комунальне господарство, агросектор тощо. Завдяки поєднанню низького енергоспоживання, великої зони покриття та можливості інтеграції в існуючу інфраструктуру операторів мобільного зв'язку, NB-IoT став одним із ключових напрямів розвитку технологій LPWAN.

▪ 5G та його можливості для IoT

Технологія 5G є не просто еволюційним кроком після 4G, а революційною парадигмою, розробленою для підтримки широкого спектра нових застосунків, де Інтернет речей відіграє одну з центральних ролей. На відміну від попередніх поколінь, які були орієнтовані переважно на мобільний інтернет для людей, архітектура 5G з самого початку створювалася для задоволення трьох кардинально різних, але взаємодоповнюючих сценаріїв використання, що є фундаментальними для IoT.

Ці три ключові напрями, визначені Міжнародним союзом електрозв'язку (ITU), формують так званий "трикутник 5G" [27, 28]:

- eMBB (Enhanced Mobile Broadband) – розширений мобільний широкопasmовий доступ.

- URLLC (Ultra-Reliable Low-Latency Communications) – наднадійний зв'язок з низькою затримкою.
- mMTC (Massive Machine-Type Communications) – масові міжмашинні комунікації.

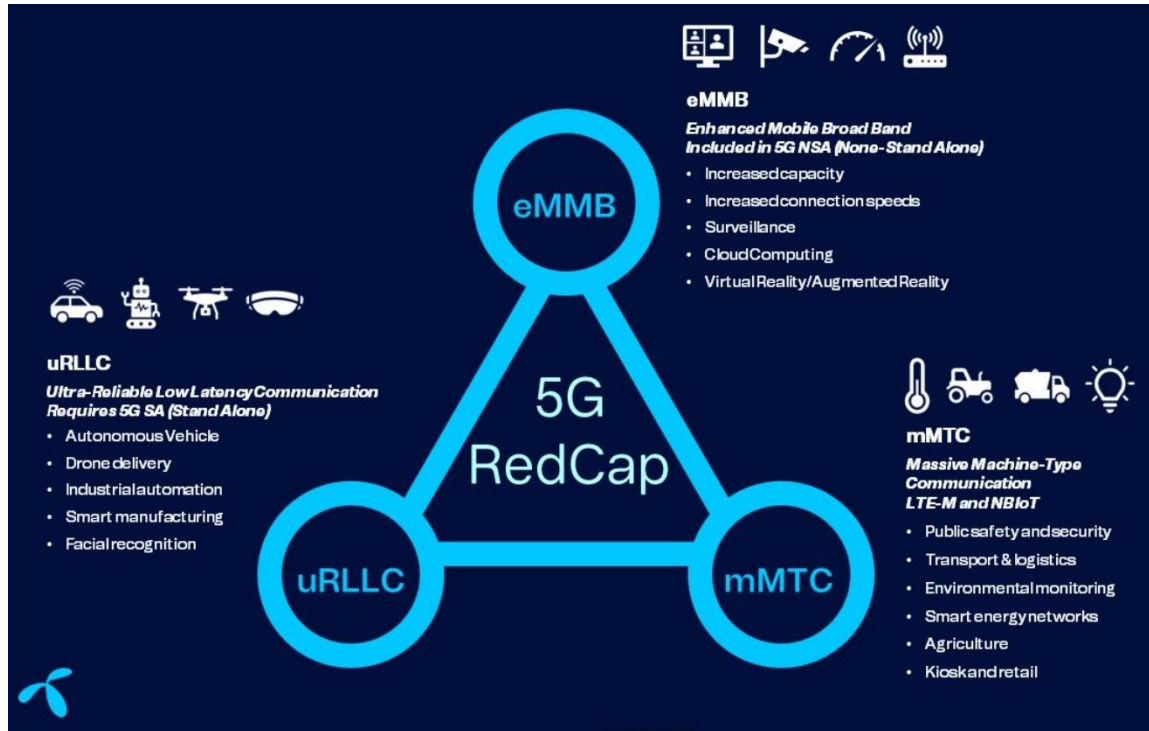


Рисунок 2.7 – Ключові напрями використання технології 5G

eMBB (Розширений мобільний широкосмуговий доступ) забезпечує надвисокі швидкості передачі даних (понад 10 Гбіт/с) та велику ємність мережі. Для IoT це відкриває можливості, що вимагають обробки величезних обсягів інформації. Наприклад, у системах "розумного міста" це дозволяє передавати відео з тисяч камер спостереження у високій роздільній здатності (4K/8K) для аналітики в реальному часі. В промисловості eMBB є основою для застосунків доповненої реальності (AR), де інженер, одягнувши AR-окуляри, може отримувати інструкції та 3D-схеми, накладені на реальне обладнання, що значно прискорює ремонтні роботи.

URLLC (Наднадійний зв'язок з низькою затримкою) є однією з головних інновацій 5G. Цей режим гарантує передачу даних із затримкою,

близькою до 1 мілісекунди, та надійністю понад 99,999%. Такі характеристики є критично важливими для систем, де будь-яке зволікання може мати катастрофічні наслідки. До прикладів належать автономний транспорт, де автомобілі обмінюються даними для уникнення зіткнень (V2V), промислова автоматизація для керування роботами на виробництві з високою точністю, віддалена хірургія (телемедицина) та керування розумними електромережами (Smart Grid).

mMTC (Масові міжмашинні комунікації) є прямим розвитком існуючих LPWAN-технологій, таких як NB-IoT та LTE-M, які будуть повністю інтегровані в екосистему 5G. Цей напрям дозволяє підключати величезну кількість пристроїв на обмеженій території – до 1 мільйона на квадратний кілометр. Ці пристрої, як правило, є простими сенсорами, що передають невеликі обсяги даних і можуть працювати від батареї роками. mMTC є фундаментом для глобального Інтернету речей: від "розумного сільського господарства" з тисячами датчиків вологості ґрунту до "розумних будівель" та логістичних мереж, де відстежується кожен контейнер [27, 28].

Для реалізації цих можливостей 5G використовує такі ключові технології, як "мережеві зрізи" (Network Slicing), що дозволяє створювати віртуальні, ізольовані мережі з гарантованими параметрами (швидкість, затримка) для кожного типу IoT-застосунку на спільній фізичній інфраструктурі, та граничні обчислення (Edge Computing), які переносять обробку даних ближче до пристроїв, зменшуючи затримки та навантаження на мережу.

Найновішим досягненням у стільникових технологіях у сфері Інтернету речей є 5G RedCap. 5G RedCap, скорочення від 5G Reduced Capability (5G зі зниженою можливістю); також відомий як 5G NR-Light, є значним доповненням до сімейства 5G. Хоча початковий реліз 5G був спрямований на покращений мобільний широкосмуговий доступ (eMBB), наднадійний зв'язок з низькою затримкою (uRLLC) та масовий машинний зв'язок (mMTC),

виникла потреба в рішенні, яке могло б охопити додатки, що знаходяться між цими крайнощами.

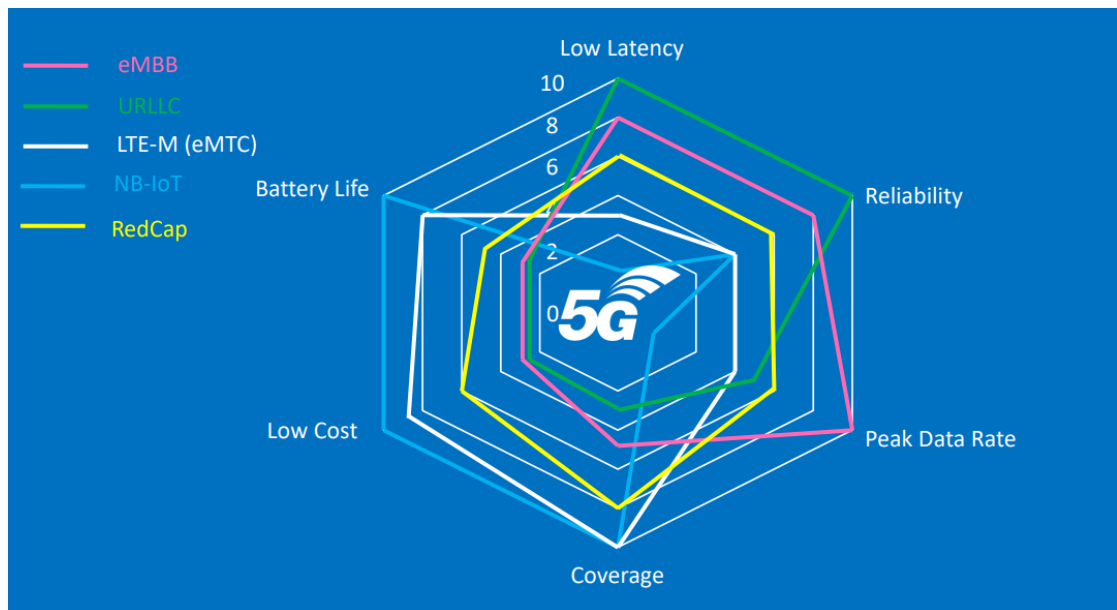


Рисунок 2.8 – Діаграма порівняння можливостей технологій сімейства 5G [29]

5G RedCap пропонує кілька переваг для IoT-застосунків, зокрема:

Вища пікова швидкість передачі даних: 5G RedCap може підтримувати пікові швидкості передачі даних, набагато вищі, ніж LTE Cat-1. Це означає, що 5G RedCap може підтримувати програми, які потребують більшої пропускної здатності даних, такі як відеоспостереження або моніторинг інтелектуальних мереж.

Менша затримка: 5G RedCap пропонує затримку, порівнянну з існуючими технологіями 4G LTE, яка значно нижча, ніж затримка в більшості технологій LPWA, таких як NB-IoT. Це означає, що 5G RedCap може підтримувати програми, що потребують передачі даних майже в режимі реального часу, такі як промислова автоматизація та програми інтелектуальних мереж.

Покращене енергоспоживання: 5G RedCap може допомогти підвищити енергоефективність пристроїв Інтернету речей, що може подовжити термін служби цих пристроїв від батареї. Це важливо для

застосувань, які використовують пристрої з живленням від батареї, такі як носимі пристрої або датчики [28].

Розвиток 5G в Україні також є стратегічним пріоритетом, хоча повномасштабне впровадження внесло суттєві корективи у початкові плани. Незважаючи на складні умови, і регулятор (НКРЕ), і провідні мобільні оператори, такі як Київстар, Vodafone та lifecell, підтверджують наміри щодо запуску мережі. Відповідно до заяв офіційних осіб та представників компаній, на кінець 2025 – початок 2026 року планується старт пілотних проектів та тестових запусків 5G у великих містах, а зараз оператори проводять масові апгрейди обладнання для підготовки до процесу впровадження 5G. Цей процес розглядається не лише як технологічне оновлення, але і як важливий елемент повоєнної відбудови та цифрової трансформації економіки країни.

Впровадження 5G матиме довгостроковий та потужний вплив на розвиток Інтернету речей в Україні. Якщо початкові етапи розгортання будуть, імовірно, сфокусовані на наданні послуг eMBB для споживачів, то справжня революція для IoT відбудеться з повноцінним запуском режимів URLLC та mMTC. Це створить технологічні передумови для модернізації ключових галузей української економіки

Таким чином, 5G виступає не просто як технологія зв'язку, а як гнучка та потужна платформа, що здатна задовольнити будь-які вимоги сучасного та майбутнього Інтернету речей.

▪ Wi-Fi та Wi-Fi HaLow для IoT

Wi-Fi є однією з найпоширеніших бездротових технологій, яка завдяки своїй присутності у кожному домі та офісі через що і стала стандартом де-факто для багатьох IoT-пристроїв. Базуючись на сімействі стандартів IEEE 802.11 (a/b/g/n/ac/ax), традиційний Wi-Fi працює переважно в діапазонах 2.4 ГГц та 5 ГГц. Його ключовою перевагою є висока пропускна здатність, що дозволяє передавати великі обсяги даних, як-от відеопотоки, та легкість інтеграції завдяки використанню існуючої мережевої інфраструктури.

Для Інтернету речей традиційний Wi-Fi є ідеальним рішенням для пристроїв, що потребують високої швидкості та мають постійне джерело живлення. До таких належать камери відеоспостереження, розумні колонки, телевізори та інша побутова техніка. Проте, для масового IoT, особливо для автономних сенсорів, класичний Wi-Fi має суттєві недоліки:

- Високе енергоспоживання: Wi-Fi-модулі швидко виснажують заряд батарей, що робить їх непрактичними для пристроїв, які мають працювати роками без обслуговування.
- Обмежений радіус дії: Сигнал у діапазонах 2.4/5 ГГц погано проникає крізь перешкоди і зазвичай покриває лише кілька десятків метрів, чого недостатньо для великих об'єктів.
- Перевантаженість мережі: Велика кількість IoT-пристроїв, підключених до одного роутера, може створювати перешкоди та знижувати стабільність мережі, особливо в зашумленому діапазоні 2.4 ГГц.

Для адаптації до нових викликів стандарт Wi-Fi отримав декілька важливих доповнень. Наприклад, поправка IEEE 802.11s розширила його можливості для роботи у складних мережах, таких як комірчаста (mesh) та бездротові ad-hoc мережі, що підвищує гнучкість розгортання [21].

Спеціалізованою відповіддю на потреби IoT та бездротових сенсорних мереж (WSN) став стандарт Wi-Fi HaLow, ратифікований як IEEE 802.11ah. Він був розроблений для усунення головних недоліків традиційного Wi-Fi. Ключова інновація Wi-Fi HaLow полягає у використанні діапазону частот 900 МГц. Це забезпечує дві фундаментальні переваги:

- Збільшений радіус дії: Завдяки змінам на фізичному рівні (PHY), дальність зв'язку зростає до 1 кілометра.
- Краща проникність сигналу крізь стіни та інші фізичні перешкоди.

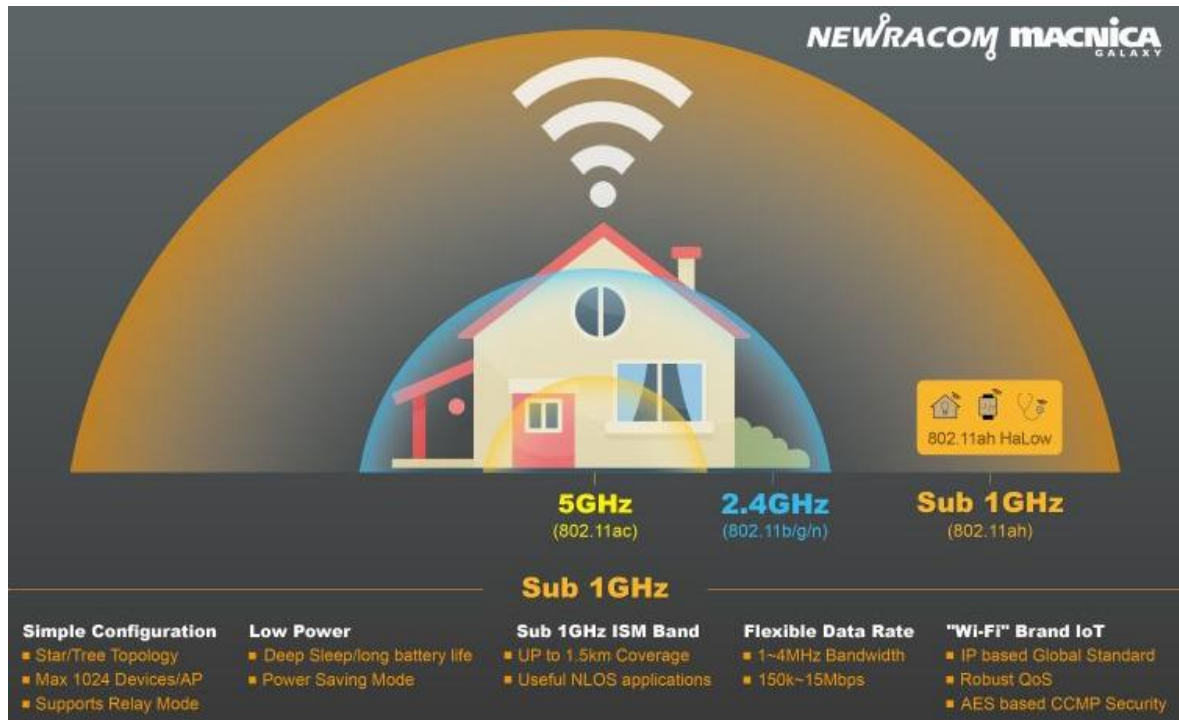


Рисунок 2.9 – Візуальне порівняння Wi-Fi 2.4/5 МГц з Wi-Fi HaLow

Wi-Fi HaLow досягає нижчого енергоспоживання, зберігаючи при цьому перевагу у більшому радіусі дії. Це стало можливим завдяки вдосконаленим механізмам сну на MAC-рівні та енергоефективним приймачам на фізичному рівні. Хоч пропускна здатність HaLow і нижча, ніж у класичного Wi-Fi, вона все одно перевищує можливості інших LPWAN-технологій.

Таким чином, Wi-Fi HaLow поєднує переваги екосистеми Wi-Fi (стандартизація, IP-протоколи, висока безпека WPA3) з характеристиками LPWAN (низьке енергоспоживання, великий радіус дії). Це робить його оптимальним для таких сфер, як промисловий IoT (IIoT) або, наприклад, автоматизація будівель, розумне сільське господарство.

1.2 Результати досліджень радіотехнологій IoT в наукових роботах

У наукових публікаціях представлено різноманітні дослідження, що аналізують ефективність, обмеження та застосування радіотехнологій у

контексті Інтернету Речей. Ці дослідження охоплюють різні види технологій, від глобальних мереж з низьким енергоспоживанням (LPWAN) до локальних персональних мереж, а також новітні підходи до управління ресурсами, забезпечення безпеки та підвищення масштабованості. Аналіз цих робіт дозволяє скласти комплексну картину поточного стану галузі та її майбутніх напрямків розвитку.

Наприклад, у роботі [31] автори розглядають еволюцію від міжмашинної взаємодії (M2M) до повноцінного IoT, де акцент зміщується з апаратного забезпечення на програмне та хмарні платформи. У статті пропонується п'ятирівнева архітектура IoT (об'єкти, мережа, управління сервісами, додатки, бізнес), що дозволяє структурувати складну екосистему. Автори підкреслюють, що для успішної роботи IoT необхідний комплексний підхід, що включає сенсори, мережі та комунікаційні технології, такі як RFID, Wi-Fi, Bluetooth та стільникові мережі.

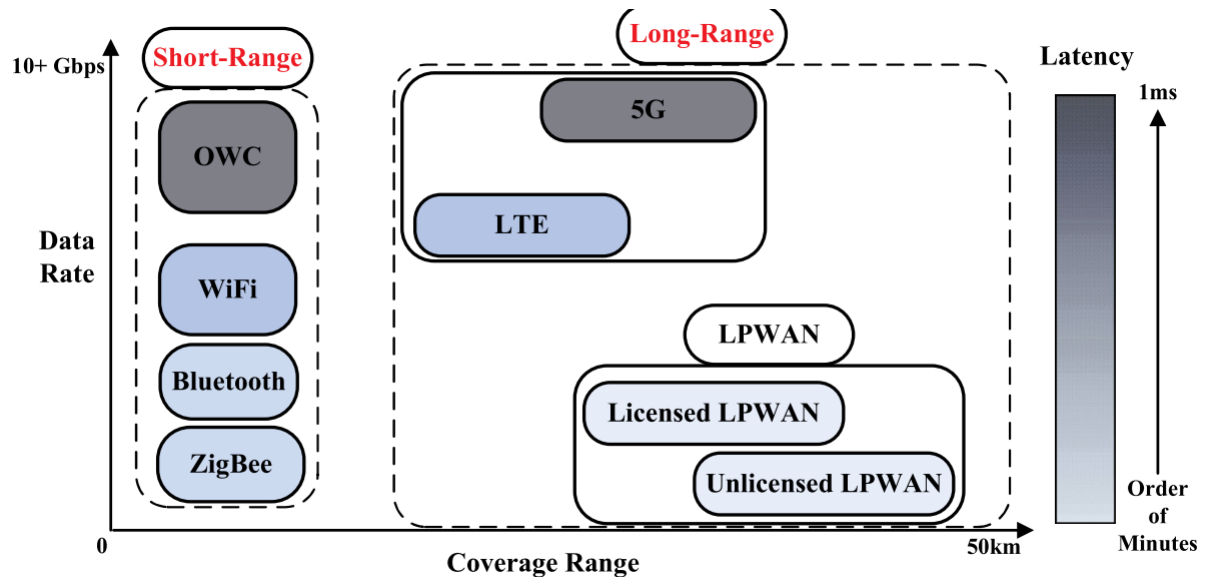


Рисунок 2.10 – Ілюстрація особливостей технологій підключення IoT з точки зору швидкості передачі даних, покриття та затримки.

В іншій статті [32], класифікуються існуючі бездротові технології за радіусом дії та вказуються на ключові технічні проблеми, що

перешкоджають масовому підключенню пристроїв. Автори зазначають, що з прогнозованим зростанням кількості пристроїв до сотень мільярдів, існуючі технології стикаються з фундаментальними обмеженнями, і пропонують розглядати нові підходи, такі як стискаюче зчитування (compressive sensing) та неортогональний множинний доступ (NOMA - технологія доступу до радіоресурсів у бездротових мережах, яка дозволяє декільком користувачам одночасно використовувати ті самі ресурси (частоту, час або код), але з різними рівнями потужності) для майбутніх стандартів.

В свою чергу, автори статті [33] зосереджуються на критично важливому моменті – а саме, аспекті безпеки. Вони систематизують відомі вразливості відповідно до стеку TCP/IP, щоб надати як новачкам, так і експертам чітке уявлення про поточний стан безпеки IoT. Дослідження підкреслює, що швидке та широке впровадження IoT створює значні проблеми безпеки, особливо для протоколів з обмеженими ресурсами. Інші дослідження підтверджують, що гетерогенність пристроїв, обмежені обчислювальні ресурси та складність систем з багатьма зацікавленими сторонами вимагають нових, цілісних підходів до безпеки [34]. Наприклад, у роботі, присвяченій безпеці в медичному IoT, наголошується на необхідності створення захищеної комунікаційної інфраструктури через неструктурований формат обміну даними між носимими пристроями, що робить їх вразливими до загроз.

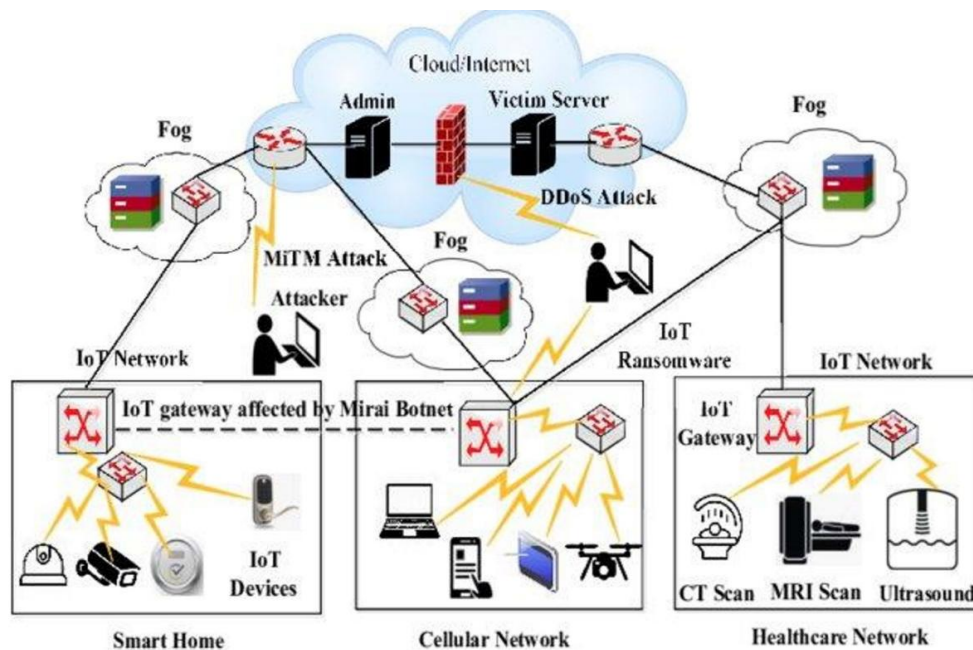


Рисунок 2.11 – Сценарії атак на мережі Інтернету речей у різних сферах застосування [34]

Значна частина наукових робіт присвячена порівняльному аналізу провідних технологій глобальних мереж з низьким енергоспоживанням (LPWAN). У дослідженні [35] автори на основі практичних вимірювань роблять висновок, що NB-IoT, хоч і є дорожчим та менш енергоефективним, забезпечує вищу надійність та пропускну здатність (до 264 біт/с при затримці 837 мс) завдяки роботі в ліцензованому спектрі. LoRaWAN, навпаки, є більш енергоефективним (споживання енергії на передачу 44-байтного повідомлення було на 1.7 мА*г меншим, ніж у NB-IoT) і дешевшим у розгортанні. Схожі висновки роблять і автори інших статей, зазначаючи, що LoRaWAN має переваги у тривалості роботи батареї, ємності мережі та вартості, тоді як NB-IoT виграє у якості обслуговування (QoS), затримці, надійності та дальності дії. У більш широкому порівнянні, що включає також Sigfox, підтверджується, що NB-IoT демонструє найкращу масштабованість, а Sigfox та LoRaWAN випереджають його за ємністю мережі, автономністю пристроїв та вартістю.

У сегменті персональних та локальних мереж домінують BLE та

Zigbee. Оглядова стаття [36] аналізує еволюцію BLE, відзначаючи її ключову роль як енергоефективного стандарту для носимих пристроїв та розумного дому. Однак автори виділяють і серйозні виклики: проблеми з керуванням живленням, інтерференція в завантаженому діапазоні 2.4 ГГц, обмежена масштабованість та значні вразливості безпеки. Технологія Zigbee, що базується на стандарті IEEE 802.15.4, досліджується в контексті її надійності та продуктивності в mesh-мережах. Робота [37] порівнює продуктивність Zigbee, Thread та Bluetooth Mesh і показує, що при збільшенні розміру мережі та обсягу даних Zigbee та Thread демонструють значно менші затримки, ніж Bluetooth Mesh, що робить їх кращим вибором для чутливих до затримок додатків у великих мережах.

Таким чином, аналіз наукових робіт показує, що вибір радіотехнології для Інтернету речей не зводиться до пошуку одного «універсального» стандарту. Важливо знаходити баланс між різними характеристиками: надійністю та швидкістю передачі даних, енергоефективністю, вартістю та можливістю масштабування мережі. Дослідження також виділяють два ключові виклики для всієї галузі: забезпечення безпеки в мережах з різнорідними пристроями, що мають обмежені ресурси, і розробку нових методів доступу до мережі, здатних підтримувати мільярди підключень. Це означає, що розвиток радіотехнологій для IoT буде спрямований не лише на покращення окремих стандартів, а й на створення інтегрованих, безпечних та масштабованих комунікаційних систем.

1.3 Висновки до розділу 2

У другому розділі дипломної роботи було детально розглянуто радіотехнології, що забезпечують функціонування Інтернету речей, їхні технічні характеристики, переваги та обмеження. Було охарактеризовано широкий спектр бездротових рішень – від локальних технологій короткого радіусу дії, таких як Bluetooth, BLE, ZigBee та Z-Wave, до глобальних

LPWAN-рішень (LoRa, NB-IoT, LTE-M) та сучасних стільникових стандартів 5G і 5G RedCap. Для кожної технології було визначено ключові параметри: дальність дії, швидкість передачі даних, енергоефективність, масштабованість і вартість реалізації, а також наведено приклади сфер застосування – від розумного дому та промислових систем до “розумних міст” і агротехнічних рішень.

В ході дослідження було виявлено, що вибір оптимальної технології є компромісом між низкою ключових параметрів, таких як дальність дії, пропускна здатність, енергоефективність, вартість розгортання та надійність. Детально проаналізовано переваги та недоліки кожного стандарту: від гнучкості та низької вартості рішень у неліцензованому спектрі (LoRaWAN, Zigbee) до високої надійності та якості обслуговування у ліцензованих стільникових мережах (NB-IoT, LTE-M, 5G).

На основі аналізу сучасних наукових робіт було виділено два основні виклики для всієї галузі. Перший – це забезпечення комплексної безпеки в умовах гетерогенності та обмежених ресурсів кінцевих пристроїв. Другий – проблема масштабованості та ефективного управління мільярдами з'єднань, що вимагає розробки нових методів доступу до мережі.

Узагальнюючи, можемо сказати, що другий розділ надав комплексне уявлення про сучасний стан і перспективи розвитку радіотехнологій для Інтернету речей, продемонстрував їхні можливості й обмеження та створив основу для подальшого дослідження ефективності впровадження IoT у конкретних практичних сценаріях. Це створює теоретичну основу для обґрунтованого вибору технологій для практичної реалізації IoT-систем та формування задачі моделювання їхньої роботи, що буде розглянуто у наступних розділах.

3 МЕТОДИКА ДОСЛІДЖЕННЯ РАДІОТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ МОДЕЛЮВАННЯ

1.1 Ключові критерії порівняння радіотехнологій

Для проведення об'єктивного аналізу та постановки задачі моделювання ефективності радіотехнологій у мережах Інтернету речей необхідно визначити набір ключових критеріїв, які дозволять кількісно та якісно оцінити роботу мережі в різних сценаріях. Базуючись на аналізі проблем, проведеному в попередніх розділах, зокрема щодо масштабованості та енергоефективності, для дослідження можна виділити різні критичні параметри, наприклад, такі як: діапазон дії, швидкість передачі даних, енергоспоживання, вартість, стійкість до перешкод, масштабованість, надійність, затримка [38] тощо.

Розглянемо детальніше сутність кожного з цих критеріїв та особливості їх оцінювання в контексті імітаційного моделювання.

Надійність (Reliability) та *Коефіцієнт доставки пакетів (PDR)*. У загальному розумінні надійність визначається як ступінь свободи системи від дефектів, що призводять до збоїв. Математично надійність (R) можна виразити як величину, обернену до частоти збоїв (FVT):

$$R = 1 - FVT \quad (3.1)$$

У контексті моделювання радіоканалів "збоєм" вважається втрата пакету даних через колізії, інтерференцію або затухання сигналу. Тому як кількісний показник надійності використовується Коефіцієнт доставки пакетів (Packet Delivery Ratio - PDR). Це відношення кількості успішно отриманих пакетів на сервері до загальної кількості відправлених пакетів кінцевими вузлами. Високий рівень PDR є індикатором стабільної роботи мережі[38].

Відгук (Responsiveness) та *Затримка (Latency)*. Для систем реального часу критично важливим є параметр відгуку (Responsiveness), який визначає здатність системи вчасно реагувати на запити. Згідно з підходами до оцінки

якості IoT-систем, метрика відгуку базується на часі (t_i) між відправленням запиту та його завершенням:

$$RESP = 1 - \frac{f(t_i)}{t_{max}} \quad (3.2)$$

де t_{max} - максимально допустимий час виконання операції. RESP – скорочення від Responsiveness (Швидкість реагування). У рамках моделювання цей параметр трансформується у Затримку (Latency) - час проходження пакету від джерела до призначення. Для критичних IoT-застосунків (наприклад, управління приводами або систем безпеки) мінімізація затримки є основним критерієм якості. Значення RESP ближче до 1 означає кращу швидкість реагування системи. [38].

Масштабованість (Scalability). Масштабованість є однією з ключових проблем Масового Інтернету речей (MIoT). Згідно з дослідженнями, стрімке зростання щільності пристроїв створює значні навантаження на інфраструктуру. Критерій масштабованості може оцінюватися через здатність технології (зокрема таких як LoRaWAN чи ZigBee) підтримувати високий рівень PDR та прийнятну затримку при збільшенні кількості вузлів від десятків до сотень у межах однієї комірки.

Енергоефективність (Energy Efficiency). Враховуючи, що більшість IoT-пристроїв працюють від батарей у важкодоступних місцях, енергоефективність, про яку вже неодноразово згадувалося в попередніх розділах при огляді різних радіотехнологій, є визначальним фактором довговічності системи. Оцінка цього критерію може базуватися на розрахунках споживання енергії радіомодулем у різних станах, таких як передача (Tx), прийом (Rx) сигналу, та, наприклад, режим сну (Sleep mode).

Діапазон дії (Coverage Range). Цей критерій визначає максимальну відстань, на якій приймач здатний коректно декодувати сигнал від передавача з допустимим рівнем помилок. Для IoT-систем цей параметр є критичним, оскільки пристрої часто розміщуються у важкодоступних місцях (підвали, колодязі, залізобетонні конструкції) або на значних відстанях від

шлюзу, наприклад, у сценаріях розумного землеробства.

Швидкість передачі даних (Data Rate) та *Пропускна здатність (Throughput)*. Цей критерій визначає обсяг інформації, який може бути переданий через канал зв'язку за одиницю часу. У контексті Інтернету речей та імітаційного моделювання важливо розрізняти два аспекти цього показника:

- *Фізична швидкість (Data Rate)*: Номінальна швидкість передачі бітів у радіоканалі, яка залежить від ширини смуги пропускання та методу модуляції. Наприклад, у технології LoRaWAN швидкість є адаптивною і змінюється залежно від коефіцієнта розширення спектра: від ~ 0.3 кбіт/с (для максимальної дальності) до ~ 50 кбіт/с (для мінімальної дальності).

- *Пропускна здатність додатка (Goodput)*: Реальна швидкість передачі корисних даних (payload) без урахування службових заголовків (overhead) протоколів. Для технологій з малими пакетами даних службова інформація може займати значну частину пакету, суттєво знижуючи ефективну швидкість.

Вартість (Cost). Вартість, що і не дивно, також є одним з ключових критеріїв мереж IoT, так як саме від економічної доцільності та бюджету проекту залежить вибір конкретної технології та можливість подальшого масштабування мережі. Особливо це актуально для систем Масового IoT (MIoT), де мережа може налічувати тисячі пристроїв, і навіть незначна різниця у ціні одного радіомодуля суттєво впливає на загальний кошторис.

Вартість розглядається у двох аспектах:

- *CAPEX (Капітальні витрати)*: Витрати на закупівлю апаратного забезпечення (кінцеві вузли, базові станції або шлюзи) та первинне розгортання інфраструктури. Технології, що працюють у неліцензованому спектрі (як LoRaWAN), часто вимагають інвестицій у власні шлюзи, тоді як стільникові рішення (NB-IoT) використовують існуючі вишки операторів.

- *OPEX (Операційні витрати)*: Постійні витрати на експлуатацію системи. Сюди входять оплата послуг зв'язку (для ліцензованих спектрів),

витрати на технічне обслуговування, оновлення ПЗ та, що критично важливо, витрати на заміну елементів живлення. Саме тому висока енергоефективність технології прямо корелює зі зниженням операційної вартості системи в довгостроковій перспективі.

Також варто зазначити, що даний перелік критеріїв не є вичерпним, адже існують і інші параметри за якими можна проводити порівняння. Проте, наведені можна вважати основними і найбільш показовими для кількісної оцінки ефективності функціонування мережі [4, 8].

1.2 Огляд інструментів моделювання

Розробка та розгортання мереж Інтернету речей, особливо в масштабах «розумного міста» або промислових об'єктів, пов'язані зі значними капітальними витратами та технічними ризиками. Проведення натурних експериментів із сотнями або тисячами фізичних пристроїв часто є неможливим через високу вартість обладнання, складність організації тестування та неможливість відтворення ідентичних умов для повторних експериментів. У таких умовах комп'ютерне імітаційне моделювання стає ключовим етапом проектування, дозволяючи оцінити ефективність протоколів та архітектурних рішень ще до етапу фізичної реалізації.



Рисунок 3.1 Перелік деяких прикладів симуляторів для IoT [43]

Сучасний ринок програмного забезпечення пропонує широкий спектр інструментів для моделювання телекомунікаційних мереж [39]. Як зазначається в оглядових роботах, існуючі інструменти можна класифікувати за декількома категоріями:

1) Дискретно-подієві симулятори (Discrete Event Simulators). Це найпоширеніший клас інструментів для дослідження мережевих протоколів. Принцип їх роботи полягає у хронологічній обробці черги подій (наприклад, «пакет згенеровано», «пакет отримано», «таймер закінчився»). Вони забезпечують високу точність моделювання часових параметрів і дозволяють досліджувати складні мережеві топології.

Приклади: NS-3, OMNeT++, OPNET (Riverbed Modeler), NetSim.

Особливості: Ці інструменти характеризуються високою гнучкістю, наявністю деталізованих моделей фізичного та канального рівнів, а також можливістю масштабування експериментів до тисяч вузлів. Дослідники підкреслюють, що для задач оцінки продуктивності протоколів у

гетерогенних мережах (наприклад, LTE у поєднанні з LPWAN) найбільш ефективними є саме симулятори, оскільки вони дозволяють абстрагуватися від апаратних особливостей вузлів і зосередитися на мережевій взаємодії [40, 41].

2) Емулятори (Emulators). На відміну від симуляторів, які використовують абстрактні моделі, емулятори дозволяють запускати реальний бінарний код прошивки на віртуальному обладнанні. Це забезпечує максимальну наближеність до реальності, але вимагає значних обчислювальних ресурсів.

Приклади: Cooja (для ОС Contiki), Mininet-IoT.

Особливості: Емулятори ідеально підходять для налагодження вбудованого програмного забезпечення мікроконтролерів. Однак, як вказується у дослідженні, вони менш придатні для оцінки продуктивності масових мереж (Massive IoT) через обмеження ресурсів хост-машини, що ускладнює моделювання сотень вузлів у реальному часі.

3) Середовища математичного моделювання. Використовуються для аналітичних розрахунків та моделювання фізичних процесів поширення сигналів на високому рівні абстракції.

Приклади: MATLAB / Simulink.

Особливості: Забезпечують потужний математичний апарат для обробки сигналів (PHY layer) та аналітики даних, але мають обмежені можливості для моделювання повноцінної мережевої взаємодії та протоколів вищих рівнів у великих, динамічних мережах.

При виборі інструменту для дослідження радіотехнологій IoT важливими є наявність відкритих бібліотек для специфічних стандартів, активна підтримка спільноти та можливість гнучкого налаштування параметрів фізичного середовища. З огляду на це, а також враховуючи необхідність дослідження масштабованості мережі, для подальшого детального аналізу в рамках даної роботи буде доцільно зосередитись на двох з найбільш популярних симуляторах з відкритим кодом – NS-3 та

OMNeT++.

1.3 Популярні засоби моделювання мереж NS-3 та OMNeT++ та їх порівняння

Серед широкого спектра програмних засобів, розглянутих у попередньому підрозділі, особливе місце в наукових дослідженнях та інженерній практиці займають дискретно-подієві симулятори з відкритим вихідним кодом. Найбільш популярними, зручними та функціональними представниками цього класу є NS-3 (Network Simulator 3) та OMNeT++. Обидва інструменти мають багаторічну історію розвитку, активну спільноту розробників та велику базу верифікованих моделей, що робить їх дуже зручним інструментом для моделювання мереж IoT. Однак, попри спільну мету, вони суттєво відрізняються за архітектурою, підходами до проектування сценаріїв та можливостями візуалізації. Для обґрунтованого вибору інструменту в рамках даної роботи необхідно детально проаналізувати особливості кожного з них.

Network Simulator 3 (NS-3) – це дискретно-подієвий мережевий симулятор з відкритим вихідним кодом, орієнтований насамперед на використання в наукових дослідженнях та освітніх цілях. Програмне забезпечення характеризує поведінку комп'ютерної мережі, дозволяючи користувачеві моделювати топологію системи, визначати вузли (хаби) та з'єднання між ними, а також забезпечує візуалізацію потоку пакетів [40, 41].

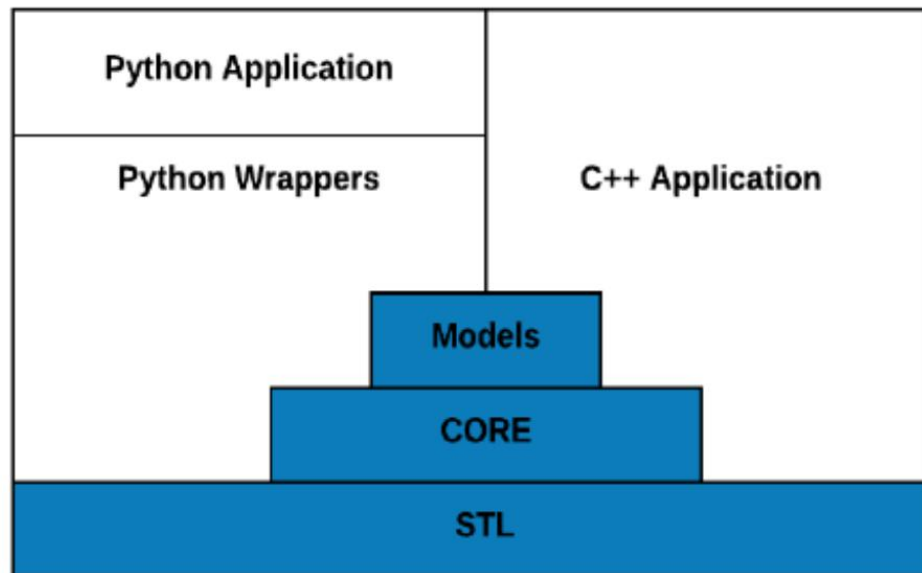


Рисунок 3.2 – Архітектура NS-3 [40]

Ядро NS-3 написане на мові C++, що забезпечує високу продуктивність та ефективне управління пам'яттю. Для написання сценаріїв моделювання передбачено опціональний API на мові Python. Серед ключових технічних характеристик варто виділити:

- Підтримка операційних систем: Windows (XP, Vista, 7, 10), FreeBSD, Linux/GNU та Mac OS X.
- Мінімальні системні вимоги: 5 ГБ дискового простору та 256 МБ оперативної пам'яті.
- Реалістичність: Сутності протоколів спроектовані так, щоб бути максимально наближеними до реальних комп'ютерних систем. Це спрощує інтеграцію відкритого мережевого програмного забезпечення та зменшує потребу в переробці моделей для симуляції.
- Підтримка віртуалізації: Використання легковагових віртуальних машин.

Архітектура трасування: NS-3 має вбудовану структуру для збору статистики та трасування, що дозволяє налаштовувати вихідні дані без необхідності перезбирати ядро симуляції. NS-3 розроблений як заміна популярного попередника NS-2, проте він не є просто його оновленою

версією і не має зворотної сумісності. Базова ідея NS-3 походить від кількох різних симуляторів, включаючи NS-2, YANS та GTNetS. Проєкт підтримується спільнотою (NS-3 Consortium) та розповсюджується під вільною ліцензією GNU GPLv2 [41]. Добре можна побачити можливості NS-3 якщо порівняти його можливості з попередньою версією NS-2 (табл. 3.1).

Таблиця 3.1 – Моделі та можливості проєкту NS-3 у порівнянні з NS-2 [41]

Рівень (Layer)	Існуючі можливості ядра NS-2	Плановані доповнення / Реалізація в NS-3
Прикладний рівень (Application Layer)	Ping, vat, telnet, FTP, multicast FTP, HTTP, імовірнісні та керовані трасами (trace-driven) генератори трафіку, веб-кеш.	API, подібний до сокетів (Sockets-like API), пірингові мережі (P2P, наприклад BitTorrent).
Транспортний рівень (Transport Layer)	TCP (багато варіантів), UDP, SCTP, XCP, TFRC, RAP, RTP. Multicast: PGM, SRM, RLM, PLM.	Емуляція стека TCP (Linux, BSD), DCCP, додаткові високошвидкісні варіанти TCP.
Мережевий рівень (Network Layer)	Unicast: IP, Mobile IP, загальні дистанційно-векторні алгоритми та алгоритми стану каналу, IPinIP, маршрутизація від джерела (source routing), Nixvector. Multicast: SRM, загальні централізовані. MANET: AODV, DSR, DSDV, TORA, IMEP.	Повна підтримка IPv4, повна підтримка IPv6, NAT, підтримка маршрутизації ORP/Click. Протоколи маршрутизації: BGP, OSPF, RIP, IS-IS, PIM-SM, IGMP/MLD.
Канальний рівень (Link Layer)	Черги (Queueing): Diffserv, DropTail, RED, RIO, WFQ SRR, Semantic Packet Queue, REM, Priority, VQ. Протоколи: ARP, HDLC, GAF, супутниковий Aloha.	Нова модель 802.11, варіанти 802.11 (mesh, QoS), 802.16 (WiMax), TDMA, CDMA, GPRS.
Фізичний рівень (Physical Layer)	Двосторонній канал (Two Way), затінення (Shadowing), всеспрямовані антени (Omni Antennas), енергетична модель, супутниковий ретранслятор.	Фізичні рівні стандартів IEEE 802, канали із завмираннями Релея (Rayleigh) та Райса (Rician), GSM.

Переваги використання NS-3 [41]:

- Модульна архітектура: Симулятор побудований як набір бібліотек, що дозволяє легко додавати нові протоколи або змінювати існуючі без необхідності переписувати ядро програми.
- Режим емуляції: Унікальна можливість взаємодіяти з реальними

мережами в реальному часі. Це дозволяє використовувати NS-3 для тестування, захоплюючи та аналізуючи пакети зі справжніх мережевих карт.

- **Висока продуктивність:** Завдяки оптимізованому управлінню пам'яттю (система агрегації) симулятор працює швидше та ефективніше, ніж попередні покоління (NS-2), уникаючи зберігання зайвих даних.
- **Реалістичність моделей:** Вузли в симуляторі спроектовані максимально подібно до реальних комп'ютерів (наявність драйверів, стеків протоколів), що забезпечує високу точність отриманих результатів.
- **Активна спільнота:** Як проект з відкритим кодом, NS-3 має велику базу розробників, якісну документацію та постійні оновлення моделей відповідно до нових стандартів.

Обмеження та недоліки NS-3:

- **Складність:** Є необхідність знання C++ та специфіки інструменту може створювати бар'єр для нових користувачів, так як будуть проблеми з налізом коду [40].
- **Обмежена підтримка Python:** Хоча API для Python існує, але все ж він є вторинним відносно C++. Це означає, що функції доступні на Python можуть бути обмеженими порівняно з C++.
- **Масштабованість:** Існують певні ліміти масштабованості при моделюванні великих мереж.

OMNeT++ (Objective Modular Network Testbed in C++) - це модульна бібліотека та фреймворк для дискретно-подієвого моделювання (discrete event simulation), написаний на C++. Інструмент доступний для громадськості з 1997 року і на сьогодні має велику базу користувачів. Він є відкритим програмним забезпеченням і розповсюджується безкоштовно для академічних та некомерційних цілей (ліцензія Academic Public License), тоді як для комерційного використання існує версія OMNEST [40, 45].

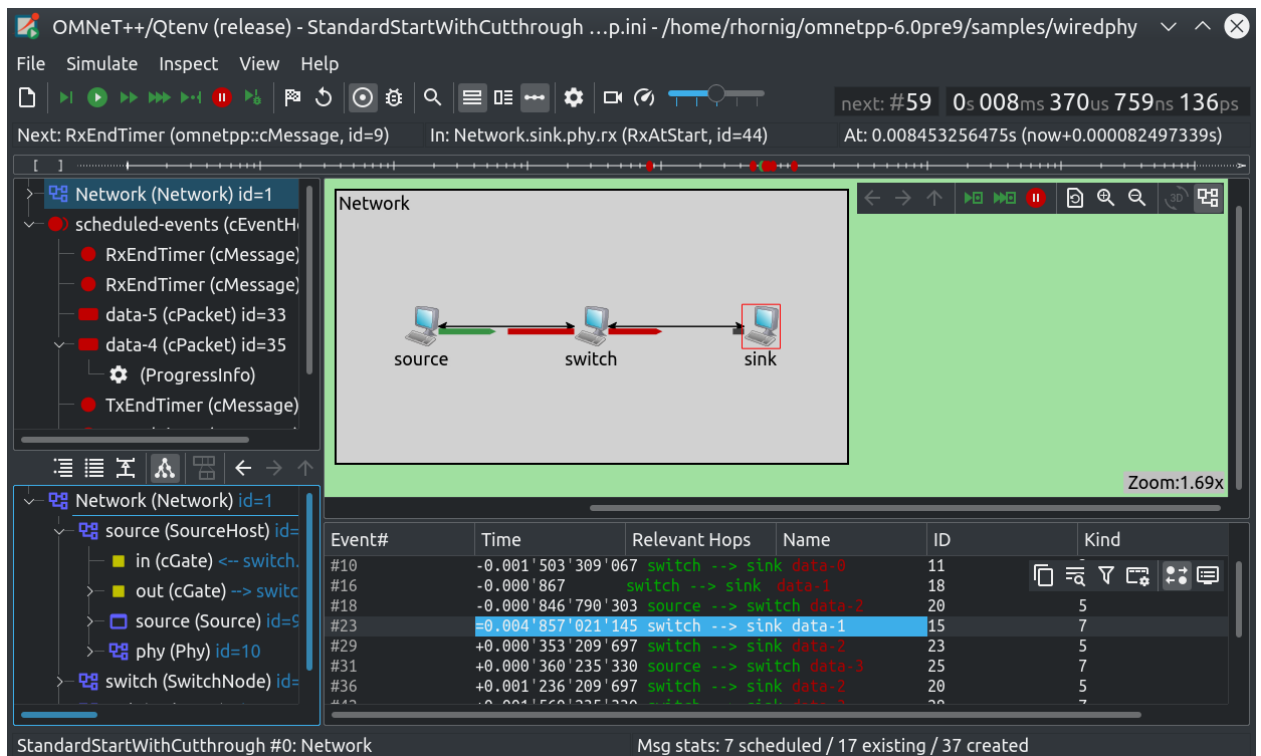


Рисунок 3.3 – Інтерфейс симулятора OMNeT++

На відміну від NS-3, OMNeT++ не є спеціалізованим симулятором лише для комп'ютерних мереж. Його архітектура є універсальною і дозволяє використовувати його для моделювання мультипроцесорних систем, розподілених апаратних комплексів, черг обслуговування та оцінки продуктивності складних програмних систем. Проте найпоширенішим сценарієм його застосування залишається саме моделювання дротових та бездротових мереж зв'язку, включаючи сенсорні мережі (WSN) та протоколи Інтернету речей.

Основою OMNeT++ є компонентно-орієнтований підхід, що забезпечує структурованість та можливість повторного використання коду. Модель складається з ієрархічно вкладених модулів:

- Прості модулі (Simple Modules): Активні компоненти, написані на C++, що реалізують логіку поведінки (обробка подій, алгоритми).
- Складні модулі (Compound Modules): Формуються шляхом об'єднання простих модулів.
- NED (Network Description): Високорівнева мова опису топології, яка

використовується для визначення структури моделі, параметрів модулів та з'єднань між ними (гейтів/портів).

Структура NED дозволяє ефективно керувати великими мережами, розділяючи визначення на окремі файли, а також динамічно змінювати топологію навіть під час виконання симуляції.

Серед технічних характеристик можна виділити [40]:

- Мова програмування: C++ (з підтримкою Java та C# в IDE).
- Підтримувані ОС: Linux (Fedora, OpenSUSE, Ubuntu, RHEL), Windows (7, 10, 11), macOS та інші UNIX-подібні системи.
- Мінімальні вимоги: 400 МБ дискового простору та 512 МБ оперативної пам'яті.
- Фреймворки: Для моделювання мереж використовуються спеціалізовані надбудови, такі як INET (основна бібліотека протоколів TCP/IP, IPv6, Ethernet), MiXiM (для бездротових мереж), Castalia (для сенсорних мереж) та Mobility Framework.

Переваги використання OMNeT++ [40, 44]:

- Потужний графічний інтерфейс (GUI): Середовище Tkenv/QtENV дозволяє візуалізувати процеси в мережі, анімувати потік даних та відстежувати зміни змінних в реальному часі, що значно полегшує демонстрацію та налаштування.
- Модульність та ієрархічність: Необмежена кількість рівнів вкладеності модулів забезпечує чіткість структури та полегшує роботу зі складними системами.
- Зручність налагодження (Debugging): Порівняно з іншими симуляторами, процес пошуку помилок та трасування (Tracing) є простішим завдяки інтегрованим інструментам Eclipse-based IDE.
- Розширюваність: Можливість легко інтегрувати власний C++ код для опису унікальної функціональності модулів.
- Універсальність: Підтримка широкого спектра протоколів (MAC, IPv6) та можливість моделювання не лише мереж, а й інших розподілених

систем.

Обмеження та недоліки OMNeT++:

- Залежність від фреймворків: "Чистий" OMNeT++ - це лише ядро симуляції. Для роботи з мережевими протоколами необхідно додатково встановлювати та вивчати зовнішні бібліотеки (наприклад, INET), кількість яких менша порівняно з базою моделей NS-3.
- Обмежена кількість протоколів "з коробки": Менший набір готових реалізацій специфічних протоколів порівняно з NS-3.
- Ліцензійні обмеження: Безкоштовна версія доступна лише для некомерційного використання.

Підсумовуючи, варто зазначити, що і OMNeT++, і NS-3 є дискретно-подієвими симуляторами, які широко використовуються для моделювання різних типів мереж, проте між ними існують фундаментальні відмінності в цільовому призначенні та гнучкості.

OMNeT++ позиціонується як симулятор загального призначення, здатний моделювати значно ширший спектр систем, ніж його конкурент. Його модульна та розширювана архітектура робить процес кастомізації та додавання нових функцій простішим, що є критичним для нестандартних досліджень. Натомість NS-3 є вузькоспеціалізованим інструментом, розробленим конкретно для IP-орієнтованих мереж. Він пропонує широкий спектр вбудованих мережеских моделей, що дозволяє швидше розпочати роботу над стандартними завданнями, однак він є менш універсальним за межами мережевої специфіки [46].

OMNeT++ часто характеризується як складніший для вивчення інструмент порівняно з NS-3, проте ця складність компенсується гнучкістю. Наприклад, хоча обидва симулятори дозволяють реалізувати методи штучного інтелекту для оптимізації мереж, OMNeT++ загалом вважається краще пристосованим для симуляцій на основі AI.

Загалом, OMNeT++ є потужнішим та гнучкішим симулятором, ніж NS-3. Однак, NS-3 простіший у вивченні та має ширший спектр вбудованих

моделей. Через це вибір симулятора залежить від конкретних цілей дослідження та типу системи, що вивчається [46].

1.4 Методологія постановки задачі моделювання мереж IoT

Ефективність та достовірність результатів імітаційного моделювання значною мірою залежать від коректності постановки задачі на початковому етапі дослідження. Упорядкування вимог до моделі дозволяє уникнути надмірної складності, яка не впливає на кінцевий результат, і, водночас, врахувати критичні фактори, що можуть визначити поведінку системи.

У контексті дослідження радіотехнологій Інтернету речей процес постановки задачі не обмежується вибором лише інструментарію, а є комплексним алгоритмом, що включає обґрунтований вибір стандартів зв'язку, детальну розробку сценаріїв розгортання мережі та визначення метрик оцінки ефективності, про які я згадував в попередніх пунктах даного розділу. Такий підхід забезпечує не лише відтворюваність експериментів, але й можливість масштабування отриманих результатів на реальні проекти впровадження IoT.

- Вибір радіотехнології для дослідження

Першим кроком у формуванні будь-якої задачі моделювання є вибір конкретної радіотехнології, яку необхідно дослідити. Наприклад, у якості демонстраційного об'єкта можна обрати NB-IoT (Narrowband IoT). Такий вибір є доцільним, оскільки NB-IoT належить до класу ліцензованих LPWAN-технологій і має низку особливостей, що впливають на побудову симуляційної моделі.

На відміну від неліцензованих рішень (наприклад, той же LoRaWAN, де головну роль відіграють колізії в спільному радіоканалі), моделювання NB-IoT вимагає врахування специфічних механізмів роботи мережі оператора. Серед них: планування радіоресурсів на базовій станції, розподіл

каналів у напрямках Uplink/Downlink, а також вплив міжкоміркової інтерференції.

Обрання саме NB-IoT дозволяє показати, як формальні характеристики стандарту - такі як гарантована якість обслуговування (QoS), висока надійність та глибоке проникнення сигналу, які відображаються у моделі та перевіряються в умовах, наближених до реальних сценаріїв мережі.

- Формування сценаріїв мережі (типи топологій, моделі трафіку).

Щоб результати моделювання були коректними та наближеними до реальних умов, експеримент потрібно будувати на основі типових сценаріїв використання, які визначає консорціум 3GPP. Тому в межах методології можна запропонувати задавати такі основні параметри сценарію:

Топологія мережі: Для NB-IoT базовою є топологія «зірка». Модель повинна включати одну або декілька базових станцій (eNodeB), до яких підключається множина користувацьких терміналів UE. Для дослідження масштабованості кількість UE має варіюватися (наприклад, від 10 до 1000 вузлів на одну соту), що дозволяє оцінити межу ємності мережі.

Модель трафіку: Оскільки NB-IoT призначений передусім для передавання телеметричних даних, використання моделей із безперервним потоком (наприклад, як для відео) є недоцільним. Оптимально застосовувати модель періодичного трафіку з малим обсягом корисних даних — приблизно 20–100 байт, що відповідає роботі розумних лічильників або сенсорів довкілля. Водночас важливо враховувати випадковість моментів передачі, щоб уникнути штучної синхронізації між вузлами та отримати більш реалістичну поведінку мережі.

Характеристики середовища передачі: Щоб правильно оцінити можливості радіоканалу, необхідно визначити модель поширення сигналу. Для міських IoT-сценаріїв доцільно використовувати моделі, які враховують затухання в умовах щільної забудови, а також додаткові втрати при проникненні сигналу всередину будівель. Це особливо важливо для NB-IoT, оскільки технологію часто застосовують у підвальних або технічних

приміщеннях (про що згадувалося в інших розділах), де якість сигналу суттєво залежить від коректного врахування цих втрат.

- Визначення метрик ефективності

Кількісна оцінка результатів моделювання повинна спиратися на систему метрик, загальні приклади яких уже були наведені у першому підрозділі цього розділу. Саме ці метрики дають змогу зіставити отримані результати з теоретичними очікуваннями та оцінити поведінку мережі за різних умов. Для демонстрації підходу в рамках методології, як приклад, можна розглянути такі показники:

- Коефіцієнт доставки пакетів (Packet Delivery Ratio - PDR): Визначається як відношення кількості пакетів, успішно прийнятих базовою станцією, до загальної кількості пакетів, згенерованих на рівні додатків сенсорів. Ця метрика є основним індикатором надійності мережі. Зниження PDR при зростанні кількості вузлів свідчить про перевантаження каналів управління або інтерференцію.
- Середня затримка (End-to-End Latency): Час, що проходить з моменту генерації пакету на сенсорі до моменту його повної обробки на стороні приймача. Для NB-IoT ця метрика включає час на встановлення RRC-з'єднання, час планування ресурсів та час безпосередньої передачі. Хоча для лічильників затримка не є критичною, її моніторинг дозволяє виявити проблеми з чергами на базовій станції.
- Енергоефективність (Energy Consumption): Розрахунок сумарної енергії, витраченої вузлом на передачу одного біта корисної інформації. У моделюванні необхідно враховувати споживання струму в різних станах радіомодуля: передача (Tx), прийом (Rx), очікування (Idle) та режим глибокого сну (PSM — Power Saving Mode). Саме коректне моделювання переходів між цими станами дозволяє підтвердити заявлений термін служби батареї, що часто з'являється в різних джерелах, а саме - 10 років.

1.5 Опис архітектури моделі в середовищі моделювання

Реалізація визначеного у попередньому підрозділі сценарію вимагає трансформації фізичних сутностей (сенсорів, шлюзів, середовища) у програмні абстракції обраного симулятора. Незалежно від інструменту, усі сучасні симулятори ґрунтуються на об'єктно-орієнтованому підході, де кожен компонент мережі, будь то сенсор, шлюз або канал передачі, подається як окремий клас чи модуль зі своїми властивостями та поведінкою. Щоб продемонструвати принципи побудови такої моделі, розглянемо архітектуру її реалізації в двох найпоширеніших інструментах моделювання мереж, про які ми говорили та розглядали: NS-3 та OMNeT++.

1.1.1 Архітектура моделі в середовищі NS-3

В NS-3 імітаційна модель будується як скрипт на мові C++, який об'єднує та налаштовує різні компоненти ядра. Для моделювання мереж NB-IoT ключовою є бібліотека `src/lte` (відома як LENA), яка містить повну реалізацію стека протоколів стільникового зв'язку, включаючи специфічні розширення для вузькосмугового інтернету речей [55].

Архітектура будь-якої симуляції в NS-3 спирається на певні фундаментальні класи та абстракції:

- *Node (Вузол)*: Базовий клас, що представляє фізичний пристрій. У сценарії NB-IoT це може бути або UE (User Equipment — кінцевий пристрій/сенсор), або eNodeB (базова станція). Вузол слугує контейнером для інших компонентів.
- *NetDevice (Мережевий пристрій)*: Програмний аналог мережевої карти та драйвера, дона "встановлюється" на Node і забезпечує його підключення до Channel. Для NB-IoT використовується специфічний клас `LteUeNetDevice` (для сенсора) та `LteEnbNetDevice` (для станції), які реалізують фізичний (PHY) та канальний (MAC) рівні.

- *Channel (Канал)*: Абстракція середовища передачі, тобто лінки які з'єднують вузли (це може бути як дротове так і бездротове з'єднання). Клас `PropagationLossModel` відповідає за розрахунок втрат сигналу. Для реалістичності часто використовують `FriisPropagationLossModel` (для відкритого простору) або `OkumuraHataPropagationLossModel` (для міської забудови).
- *Application (Додаток)*: Генератор трафіку. Для телеметрії використовується клас `UdpClient`, який надсилає пакети на сервер (`UdpServer`). Для моделювання телеметрії часто використовують `UdpEchoClient` (відправка пакетів) або `OnOffApplication` (генерація трафіку з певною періодичністю, що імітує роботу сенсорів).
- *Helpers (Помічники)*: Спеціальні класи-обгортки (наприклад, `LteHelper`, `PointToPointHelper`), які автоматизують налаштування складних параметрів стека протоколів, значно спрощуючи код моделі.

Важливою особливістю архітектури NS-3 є висока точність відповідності стандартам. Модель NB-IoT інтегрована в модуль LTE, але використовує окремі структури даних для конфігурації радіоресурсів. На рисунку 3.4 представлена структура класу `SystemInformationBlockType2` (SIB2), який відповідає за передачу параметрів доступу до мережі.

Як видно з діаграми, архітектура чітко розмежовує параметри для класичного LTE (білі блоки) та специфічні налаштування для NB-IoT (сірі блоки), такі як `NprdcchConfigCommon` (канал управління) та `NprachConfig` (канал випадкового доступу). Це підтверджує, що симулятор враховує особливості вузькосмугового доступу на рівні RRC-протоколу [58, 59].

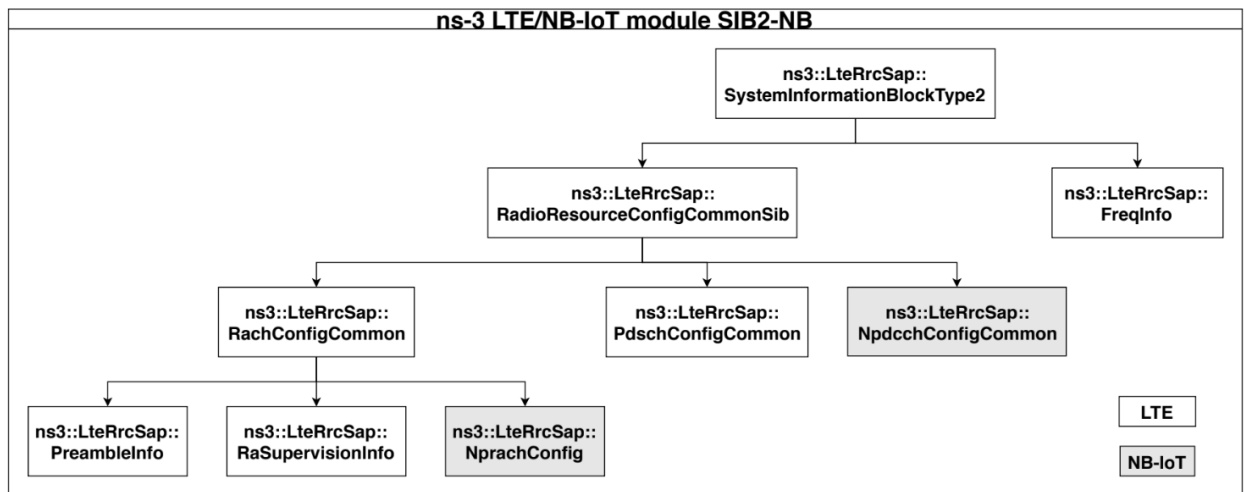


Рисунок 3.4 – Структура модуля SIB2-NB в NS-3 для конфігурації радіоресурсів [58]

Приклад програмної реалізації (C++): Для спрощення роботи зі складними класами в NS-3 використовуються так звані Helpers (Помічники), про які зазначалося вище. Нижче наведено приклад коду, що створює базову архітектуру мережі, ініціалізує стек NB-IoT та налаштовує параметри планувальника:

```

// 1. Ініціалізація помічників для LTE/NB-IoT
Ptr<LteHelper> lteHelper = CreateObject<LteHelper>();
Ptr<PointToPointHelper> epcHelper = CreateObject<PointToPointHelper>();
lteHelper->SetEpcHelper(epcHelper);

// 2. Налаштування планувальника (Scheduler) для NB-IoT
// Використовується Round Robin (RR) для розподілу ресурсів між сенсорами
lteHelper->SetSchedulerType("ns3::RrFfMacScheduler");

// 3. Створення контейнерів для вузлів: 1 БС (в нашому випадку це eNodeB)
NodeContainer enbNodes;
enbNodes.Create(1);
// Створення 10 сенсорів (UE)
NodeContainer ueNodes;
ueNodes.Create(10);

// 4. Встановлення мобільності (статичне розміщення)
MobilityHelper mobility;
mobility.SetMobilityModel("ns3::ConstantPositionMobilityModel");
mobility.Install(enbNodes); // Базова станція нерухома
mobility.Install(ueNodes);  // Сенсори нерухомі

// 5. Інсталяція стека протоколів NB-IoT на пристрої
NetDeviceContainer enbDevs = lteHelper->InstallEnbDevice(enbNodes);

// Налаштування додатків (тобто сама генерація трафіку) здійснюється
пізніше
  
```

Цей код створює мінімальну NB-IoT мережу в NS-3: одну базову станцію та 10 сенсорів, які стоять на місці та використовують Round Robin («циклічний», це алгоритм розподілу кількох завдань або навантаження в розподіленій обчислювальній системі методом перебору та упорядкування елементів за круговим циклом для доступу до радіоканалу). Він формує основу, на якій потім можна будувати трафік, моделі поширення сигналу та збір статистики. Така простенька архітектура дозволяє гнучко масштабувати мережу, змінюючи лише параметри в контейнерах `NodeContainer`, без необхідності переписування логіки взаємодії протоколів.

1.1.2 Архітектура моделі в середовищі OMNeT++

На відміну від монолітного підходу NS-3, де вся логіка часто зосереджена в одному скрипті, архітектура моделювання в OMNeT++ є навпаки модульною та ієрархічною (в NS-3 весь сценарій створюється у вигляді єдиного C++ коду, а ось в OMNeT++ мережа збирається з окремих компонентів, які можуть комбінуватися у складні структури. Така архітектура робить модель наочною і легко масштабованою). Вона базується на чіткому розділенні опису структури мережі та опису поведінки її елементів. Для моделювання IoT-систем зазвичай використовується фреймворк INET, який надає готові реалізації протоколів стека TCP/IP та моделей бездротового середовища. Для специфічних задач IoT, таких як моделювання мереж LoRaWAN, архітектура розширюється спеціалізованими модулями, наприклад, FLoRa [61], який додає підтримку модуляції LoRa на фізичному рівні.

Архітектура будь-якої моделі в OMNeT++ складається з кількох основних типів компонентів, які разом формують поведінку всієї мережі. Логіка моделювання побудована так, що кожен елемент відповідає за свою частину функціональності, а складні структури створюються шляхом їх

комбінування:

- *Простий модуль (Simple Module)*: Це, мабуть, найменший та найважливіший елемент у OMNeT++. Простий модуль можна порівняти з маленькою програмою всередині великої симуляції. У таких модулях знаходиться весь активний код, який описує поведінку мережевого об'єкта, наприклад, як він генерує пакети або реагує на події. Уся логіка зазвичай реалізована в C++, а ключовим методом є `handleMessage()`, який викликається щоразу, коли модуль отримує нову подію або повідомлення.
- *Складний модуль (Compound Module)*: Цей компонент виконує структурну функцію, слугуючи контейнером для групування інших модулів. Він не містить власного коду поведінки, а описує внутрішню архітектуру вузла (Вузол `WirelessHost` у фреймворку `INET`, який об'єднує в собі мережевий інтерфейс, модуль мобільності, стек протоколів та додатки).
- *Мережа (Network)*: Це спеціальний тип складного модуля найвищого рівня, який не має зовнішніх інтерфейсів. Саме тут визначається сценарій симуляції: задається топологія (розміщення сенсорів і шлюзів) та глобальні параметри середовища.
- *Канали та радіосередовище (Channels & Radio Medium)*: У бездротових мережах пристрої не з'єднані один з одним напряму, тому OMNeT++ використовує спеціальний глобальний модуль `RadioMedium`, який виконує роль «моделі фізичного середовища».

Структура мережі описується декларативною мовою NED (Network Description). Це дозволяє візуально конструювати мережу або описувати її параметрично. Нижче наведено загальний приклад коду NED (це не реалізація NB-IoT, так як вона буде дещо складнішою оскільки стандартний `INET` не містить моделей стільникового зв'язку по стандарту), який створює мережу з одним сервером та масштабованим масивом сенсорів:

```

import inet.node.inet.StandardHost;
import inet.node.inet.WirelessHost;
import inet.physicallayer.wireless.common.medium.RadioMedium;

network IoT_Network
{
    parameters:
        int numSensors = default(10); // Параметр кількості сенсорів
        @display("bgb=800,600");      // Розміри вікна для візуалізації

    submodules:
        // Глобальний модуль радіосередовища
        radioMedium: RadioMedium {
            parameters:
                @display("p=50,50");
        }
        // Центральний сервер (шлюз)
        server: StandardHost {
            parameters:
                @display("p=300,200;i=device/server");
        }
        // Масив бездротових сенсорів
        sensor[numSensors]: WirelessHost {
            parameters:
                @display("p=random,random;i=device/sensor");
        }
    }
}

```

У цьому прикладі модуль `radioMedium` автоматично керує зв'язком між `sensor[]` та `server` на основі їхніх координат та потужності передавачів, що значно спрощує опис складних топологій порівняно з ручним створенням каналів.

Поведінка простих модулів (наприклад, додатку сенсора) реалізується у класах C++. Ключовим методом є `handleMessage`, який обробляє всі вхідні події (наприклад, прихід пакету від мережі):

```

void SensorApp::handleMessage(cMessage *msg)
{
    if (msg->isSelfMessage()) {
        // Якщо спрацював таймер – генеруються дані телеметрії
        // (температура, вологість, стан пристрою тощо)
        sendSensorData();
        // Плануємо наступну відправку через 1 секунду (сенсор періодично
        // надсилає дані кожну секунду)
        scheduleAt(simTime() + 1.0, msg);
    }
    else {
        // Обробка вхідного пакету від мережі
        processPacket(check_and_cast<Packet *>(msg));
    }
}

```

Така простенька архітектура дозволяє легко змінювати логіку роботи пристроїв (наприклад, алгоритм енергозбереження) без зміни структури

мережі, або навпаки - масштабувати мережу до тисяч вузлів, змінивши лише один параметр у NED-файлі.

Також, як вже зазначалося вище, це лише загальний приклад, а задля специфічних задач, того ж NB-IoT, дана архітектура розширюється бібліотекою SimuLTE, де замість стандартних хостів використовуються модулі eNodeB та UE, а управління ресурсами здійснюється через глобальний модуль Binder.

1.6 Алгоритм проведення експерименту та аналізу результатів

Коректність імітаційного моделювання залежить не лише від архітектури моделі, але й від систематичності проведення експериментів. Для отримання статистично достовірних даних про роботу мережі NB-IoT (або інших обраних технологій) можна запропонувати наступний покроковий алгоритм, що охоплює етапи від налаштування параметрів до фінальної обробки даних.

Етап 1. Конфігурація параметрів фізичного (PHY) та канального (MAC) рівнів

Першим кроком є визначення вхідних параметрів симуляції, які мають відповідати специфікаціям стандарту 3GPP [32]. У середовищі моделювання (наприклад, NS-3 через `Config::SetDefault` або OMNeT++ через .ini файл) необхідно зафіксувати:

Параметри PHY: Потужність передавача (Tx Power, наприклад 23 dBm), коефіцієнт шуму приймача (Noise Figure), смугу пропускання (для NB-IoT — 180 кГц) та модель втрат сигналу (Path Loss Model).

Параметри MAC: Тип планувальника ресурсів (Round Robin або Proportional Fair), параметри таймерів для переходу в режим сну (eDRX/PSM), що є критичним для оцінки енергоефективності.

Генератори випадкових чисел (RNG): Для забезпечення статистичної

значущості результатів необхідно налаштувати «Seeds» генератора випадкових чисел. Це дозволить провести серію незалежних експериментів для одного й того ж сценарію.

Етап 2. Запуск сценарного моделювання (Scaling)

Дослідження виконується ітеративно шляхом зміни незалежної змінної — кількості вузлів у мережі. Алгоритм проведення симуляції виглядає так:

- Ініціалізація: Встановлення початкової кількості сенсорів (наприклад, $N=10$ — як вказувалося в прикладі коду в підрозділі вище).
- Виконання симуляції: запускається моделювання на визначений період часу (наприклад, 1000 секунд). Обов'язково враховується «період розігріву» (warm-up), коли початкові нестійкі процеси ще не відображають реальну поведінку мережі.
- Збільшення навантаження (інкрементація): Збільшення кількості вузлів (наприклад, +50 або $\times 2$) та повторення запуску.
- Повторення експериментів: для кожного значення навантаження симуляція виконується кілька разів (5–10), але з різними випадковими положеннями вузлів і різними seed-значеннями. Це дозволяє усереднити результат і зменшити вплив випадкових факторів.

Етап 3. Збір первинної статистики (Tracing)

Під час виконання симуляції інструмент (NS-3 або OMNeT++) генерує траси подій. Необхідно активувати збір наступних даних:

- PCAP-файли: повний дамп пакетів на рівні мережевих інтерфейсів (для аналізу в Wireshark).
- ASCII-траси: текстові логи, що фіксують події Tx (відправка), Rx (прийом) та Drop (втрата) з часовими мітками.
- Енергетичні профілі: логуювання зміни залишкового заряду батареї або часу перебування радіомодуля в активних і пасивних станах.

Етап 4. Постобробка та аналіз результатів (Parsing & Plotting)

Отримані «сирі» дані (тобто Raw Data) підлягають автоматизованій обробці (зазвичай за допомогою скриптів на Python/Pandas або MATLAB). Алгоритм аналізу включає:

- Фільтрація: відкидання службових пакетів (ARP, ICMP, RRC signaling), якщо метою є оцінка пропускнуої здатності додатків (Goodput).
- Розрахунок метрик: PDR: підрахунок унікальних пакетів, що мають пару подій «відправлено-отримано». Затримка: Обчислення різниці часу $T_{Rx} - T_{Tx}$ для кожного успішно доставленого пакету та знаходження середнього значення.
- Візуалізація: побудова графіків залежностей, де вісь X — кількість пристроїв, а вісь Y — цільова метрика (PDR, Затримка, Енергія).

В цілому можна сказати, що використання такого алгоритму забезпечує відтворюваність, об'єктивність і наукову коректність отриманих результатів, а також дозволяє проводити порівняльний аналіз різних радіотехнологій та сценаріїв їх використання.

1.7 Висновки до розділу 3

У третьому розділі магістерської дисертації було проведено комплексний аналіз методологічних критеріїв дослідження радіотехнологій Інтернету речей за допомогою засобів імітаційного моделювання. Це дозволило сформулювати алгоритм дій для оцінки ефективності мереж без необхідності розгортання дороговартісного фізичного обладнання.

В ході роботи було визначено та обґрунтовано ключові критерії порівняння технологій, серед яких пріоритетними є коефіцієнт доставки пакетів (PDR), затримка, енергоефективність та масштабованість. Саме ці метрики дозволяють об'єктивно оцінити QoS у специфічних умовах IoT.

Детальний огляд програмного забезпечення показав, що для задач дослідження радіоінтерфейсів найбільш доцільним є використання

дискретно-подієвих симуляторів. Порівняльний аналіз двох провідних інструментів - NS-3 та OMNeT++ виявив їхні архітектурні особливості, наприклад:

- NS-3 характеризується високою реалістичністю моделей (особливо для стека LTE/NB-IoT) та продуктивністю, що робить його ідеальним для перевірки мережевих протоколів.
- OMNeT++ вирізняється гнучкою модульною структурою та зручними засобами візуалізації (пристуній GUI та IDE), що спрощує проєктування нестандартних архітектур.

Важливим результатом розділу стала розробка методології постановки задачі моделювання. На прикладі технології NB-IoT було детально описано архітектуру моделі, включаючи програмну реалізацію основних компонентів (вузлів, каналів, додатків) та конфігурацію параметрів фізичного рівня згідно зі стандартами 3GPP. Запропонований покроковий алгоритм проведення експерименту, від налаштування сценарію до збору та обробки статистики, що може стати корисним для людей що захочуть спробувати провести симуляції в NS-3 та OMNet++.

Узагальнюючи, третій розділ створив необхідний інструментальний та методичний фундамент для розуміння процесів, що відбуваються в мережах IoT, що дозволяє перейти до формування практичних рекомендацій щодо вибору та застосування цих технологій у реальних проєктах.

4 РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ РАДІОТЕХНОЛОГІЙ ІОТ

1.1 Критерії вибору технології для певної сфери застосування

Ефективність, надійність та рентабельність будь-якої системи Інтернету речей безпосередньо залежать від обґрунтованого вибору певної технології для конкретної сфери. Як було показано в попередніх розділах, екосистема ІоТ характеризується надзвичайною гетерогенністю: від мініатюрних сенсорів, що передають кілька байтів інформації раз на добу, до складних роботизованих систем, які потребують керування в режимі реального часу з мінімальними затримками. Така різноманітність сценаріїв майже унеможлиблює існування єдиного «універсального» стандарту зв'язку, який би задовольняв вимоги всіх можливих застосувань.

Процес вибору радіотехнології, в цілому, можна назвати задачею оптимізації, так як інженерам доводиться шукати певні компроміси між взаємовиключними параметрами та характеристиками. Фізичні обмеження не дозволяють одночасно досягти максимальної дальності дії, високої швидкості передачі даних та мінімального енергоспоживання. Наприклад, збільшення радіусу покриття та пропускної здатності неминуче призводить до зростання енерговитрат, що, в свою чергу, є критичним для автономних пристроїв. Тому кожне технічне рішення має оцінюватися крізь призму конкретних бізнес-вимог та умов експлуатації.

Окрім суто технічних характеристик, вирішальну роль відіграють економічні та експлуатаційні фактори, такі як вартість розгортання мережі (CAPEX), операційні витрати (OPEX), масштабованість рішення та безпека передачі даних.

Щоб упорядкувати процес вибору радіотехнології, ключові критерії зручно поділити на три групи:

- вимоги до передачі даних
- умови розгортання та експлуатації
- економічні аспекти

Така класифікація дозволяє системно оцінити доступні варіанти й обрати рішення, яке найкраще відповідає потребам конкретного застосування.

Функціональні вимоги до передачі даних є одним з ключових аспектів вибору оптимальної радіотехнології для конкретного IoT-сценарію. Насамперед важливим є характер трафіку: обсяг інформації, частота її передавання та необхідна пропускна здатність каналу. Якщо система передбачає роботу з великими потоками даних, наприклад, відеоспостереженням, мультимедійними потоками або передаванням важких файлів - то використовуються лише високошвидкісні стандарти на кшталт Wi-Fi, LTE Cat-4 або 5G eMBB. Натомість більшість сенсорних IoT-пристроїв надсилають невеликі пакети телеметрії, тому застосування широкосмугових технологій для них є як технічно, так і енергетично нераціональним. У таких випадках набагато ефективнішими стають вузькосмугові рішення, наприклад NB-IoT чи LoRaWAN, що оптимізовані саме для передачі малих обсягів даних із мінімальними накладними витратами [47].

Не менш важливою є й чутливість до затримок. У критичних системах реального часу, таких як промислові роботизовані комплекси, smart-grid або керування безпілотним транспортом (особливо якщо розглядати останні події та шалений розвиток БПЛА зумовлений війною з росією) - навіть невеликі коливання затримки можуть призвести до некоректної роботи. Для таких сценаріїв необхідні технології, здатні забезпечити детерміновану наднизьку затримку на рівні одиниць мілісекунд, наприклад 5G URLLC (який в цьому році тестово почали впроваджувати деякі мобільні оператори на території України) або спеціалізовані промислові рішення Wi-Fi та Ethernet. У той же час системи екологічного моніторингу, smart metering чи розумного аграрного контролю не потребують миттєвої доставки даних: затримка у кілька секунд або навіть хвилин є цілком прийнятною. Це відкриває можливість використовувати енергоефективні технології з асинхронним

доступом та глибокими режимами сну, такі як LoRaWAN Class A, що забезпечують довготривалу автономну роботу пристроїв [24].

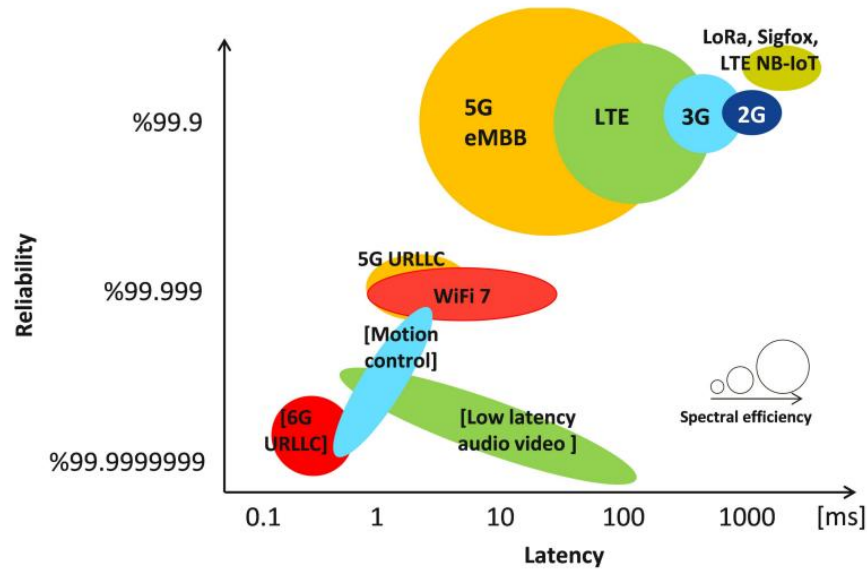


Рисунок 4.1 – Затримка та надійність різних технологій [24]

Умови розгортання та експлуатації нерідко визначають, яка саме радіотехнологія може бути використана в конкретному IoT-сценарії, адже фізичне середовище суттєво впливає на якість та стабільність зв'язку.

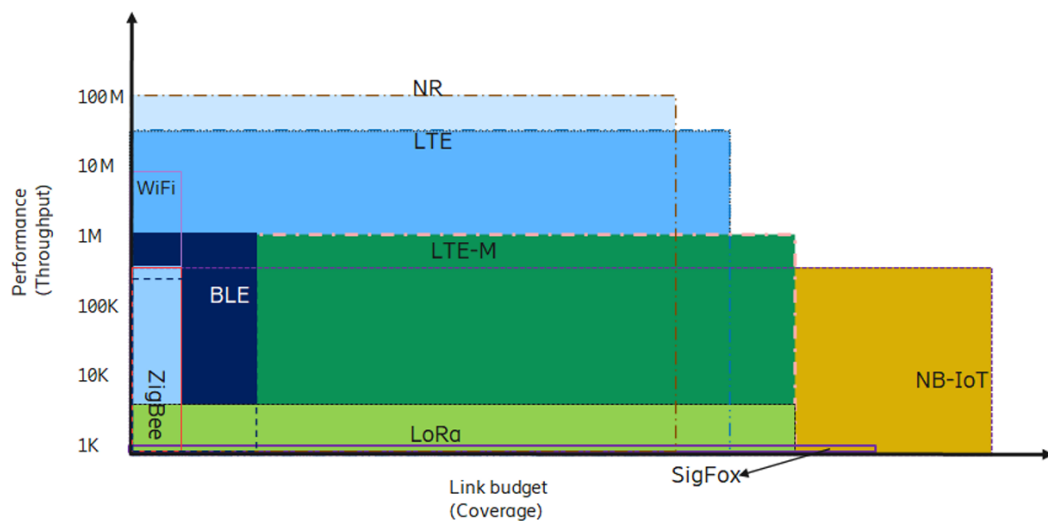


Рисунок 4.2 – Пропускна здатність та покриття різних технологій [24]

Одним з основних параметрів є радіус дії. Для компактних локальних систем, що працюють у межах однієї квартири, будинку чи офісної будівлі, цілком достатньо технологій малого радіусу — таких як ZigBee чи Wi-Fi, які добре підходять для розумного дому, автоматизації приміщень чи керування побутовими пристроями. Водночас для великомасштабних мереж, наприклад в аграрному моніторингу, логістиці або міських інфраструктурних системах, необхідні технології класу LPWAN, що забезпечують десятки кілометрів покриття при мінімальному енергоспоживанні.

Окрему роль відіграє здатність сигналу проникати крізь фізичні перешкоди. Вузли, розташовані у складних умовах — підвальних приміщеннях, колодязях, шахтах ліфтів чи за товстими бетонними стінами — потребують технологій із високим бюджетом лінії зв'язку. Саме тому стандарти, що працюють у субгігагерцовому діапазоні, такі як NB-IoT та LoRa, демонструють суттєво кращу проникність порівняно з технологіями на частотах 2.4 ГГц, які набагато сильніше згасають у складних середовищах [49].

Ще одним важливим фактором є мобільність об'єкта, який потрібно відстежувати. Якщо пристрій переміщується між різними зонами покриття, необхідна підтримка безшовного переходу між базовими станціями, тобто хендоверу. Стільникові технології на кшталт LTE-M, 5G мають цю функціональність на рівні протоколу, завдяки чому підходять для транспортних систем або носимих пристроїв (На відміну від NB-IoT, що не підтримує безперервний хендовер. Через що є певні обмеження в його використанні). Натомість деякі неліцензовані LPWAN-рішення, як-от LoRaWAN, мають обмеження щодо швидкості руху або потребують повторної реєстрації пристрою при зміні точки доступу, що звужує сферу їхнього застосування у мобільних сценаріях.

Економічні та регуляторні чинники також істотно впливають на вибір IoT-технології, оскільки саме вони визначають фінансову модель розгортання мережі та подальші експлуатаційні витрати (а замовник не

завжди хоче вкладати великі кошти). Одним із ключових питань є тип використовуваного радіоспектру. Технології, що працюють у неліцензованих діапазонах, на кшталт LoRaWAN, ZigBee чи Wi-Fi, дозволяють будувати повністю приватні мережі без необхідності сплачувати оператору за доступ до спектру або SIM-підключення. Це значно зменшує операційні витрати, але водночас покладає на власника мережі відповідальність за обслуговування інфраструктури, а також ризики, пов'язані з радіозавадами тощо. Натомість технології, що працюють у ліцензованому спектрі, такі як NB-IoT або LTE-M, забезпечують гарантовану якість обслуговування, стабільність каналу та захищеність від інтерференції [50]. Проте вони передбачають залежність від мобільного оператора та регулярні витрати на кожне підключення, що є важливим фактором при масштабуванні системи (особливо це відчутно зараз в Україні, де через постійні віялові відключення електроживлення часто може страждати мобільний зв'язок, через знеструмлення базових станцій оператора).

Окремим економічним параметром є енергоефективність, яка безпосередньо впливає на загальну вартість володіння великомасштабними IoT-розгортаннями. У мережах, де функціонують тисячі або десятки тисяч автономних датчиків, заміна батарей може стати суттєвим фінансовим тягарем, інколи навіть перевищуючи вартість самих пристроїв. Саме тому технології з оптимізованими режимами енергоспоживання, такими як PSM чи eDRX у стільникових IoT-рішеннях, або глибокий сон у LoRaWAN-вузлах, стають критичними для довготривалих проєктів. Здатність пристрою працювати 5–10 років та відкриває можливість використання IoT у важкодоступних або віддалених місцях.

Для наочності та спрощення процедури вибору, основні критерії та відповідність їм різних класів технологій зведено у таблицю 4.1.

Таблиця 4.1 – Матриця вибору радіотехнології залежно від вимог застосування

Критерій вибору	WPAN (ZigBee, BLE)	WLAN (Wi-Fi, HaLow)	LPWAN (LoRaWAN, NB-IoT)	Cellular (4G/5G)
Радіус дії	Малий (< 100 м)	Середній (< 1 км)	Дуже великий (> 10 км)	Глобальний (залежить від покриття)
Швидкість даних	Низька / Середня	Висока / Дуже висока	Дуже низька	Висока / Дуже висока
Затримка	Низька (мс)	Низька (мс)	Висока (с - хв)	Наднизька (URLLC)
Живлення	Від батареї (місяці/роки)	Від мережі (переважно)	Від батареї (роки)	Від мережі / Велика батарея
Вартість модуля	Низька	Середня	Низька / Середня	Висока
Модель витрат	Власна інфраструктура	Власна інфраструктура	Приватна або Операторська	Операторська (SIM)

1.2 Практичні приклади використання кожної технології в IoT

Практичні приклади застосування радіотехнологій дають змогу побачити, як теоретичні характеристики перетворюються на реальні переваги у конкретних проектах. У багатьох випадках саме реальні кейси демонструють, чому одна технологія виявляється оптимальною в певному середовищі, тоді як інша неефективною або надто дорогою. Наприклад, LoRaWAN, як ми вже говорили, чудово зарекомендувала себе у великих розподілених мережах моніторингу, де пристрої розташовані на значній відстані один від одного і передають невеликі обсяги даних.

- *Моніторинг критичної інфраструктури у важкодоступних регіонах (LoRaWAN)*

Яскравим прикладом використання технології LoRaWAN для забезпечення життєво важливих потреб є проект компанії Greencityzen у співпраці з ООН, спрямований на забезпечення доступу до питної води у таборах біженців. Специфіка цих об'єктів полягає у віддаленості та складності доступу, що робить традиційні засоби зв'язку неефективними.

Рішення базується на розгортанні інфраструктури LoRaWAN із використанням шлюзів на сонячних батареях, які передають дані на сервер The Things Stack. Система забезпечує наскрізний моніторинг чотирьохетапного циклу водопостачання: від видобутку води зі свердловин та її хлорування до накопичення у водонапірних вежах і кінцевого розподілу. Це дозволяє в реальному часі відстежувати рівень запасів, якість води, споживання енергії насосами та своєчасно виявляти несправності, що критично важливо для запобігання епідеміям та забезпечення стабільного водопостачання у таких країнах, як Камерун, Бангладеш та Ірак [50].



Рисунок 4.3 – Забезпечення питною водою таборів біженців у 15 країнах

- *Концепція «Розумної лікарні» (Smart Hospital)*

У секторі охорони здоров'я технологія LoRaWAN демонструє ефективність при створенні систем управління інфраструктурою медичних закладів, що було реалізовано іспанською групою Viamed Salud. Головним

викликом було забезпечення централізованого моніторингу 13 лікарень та 15 медичних центрів без проведення масштабних будівельних робіт. Розгортання приватної мережі LoRaWAN дозволило інтегрувати понад 300 пристроїв, які генерують близько 30 000 повідомлень щодня. Система охоплює дев'ять сценаріїв використання, включаючи контроль температурного режиму для зберігання ліків та вакцин (холодовий ланцюг), моніторинг параметрів навколишнього середовища, виявлення протікань води та роботу кнопок екстреного виклику. Впровадження такого рішення значно підвищило ефективність управління об'єктами та гарантію якості медичних послуг завдяки автоматизації процесів контролю [50].

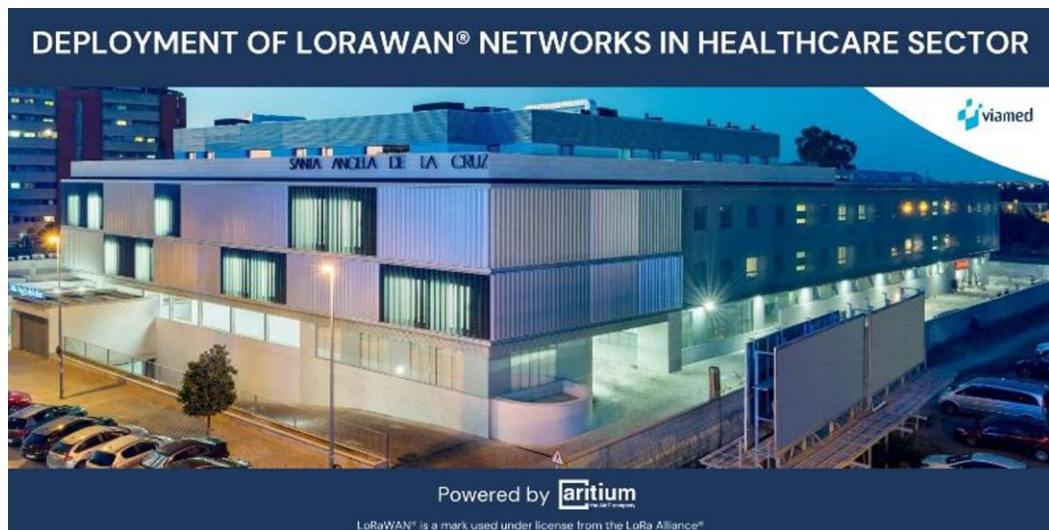


Рисунок 4.4 – Розгортання мереж LoRaWAN® у секторі охорони здоров'я

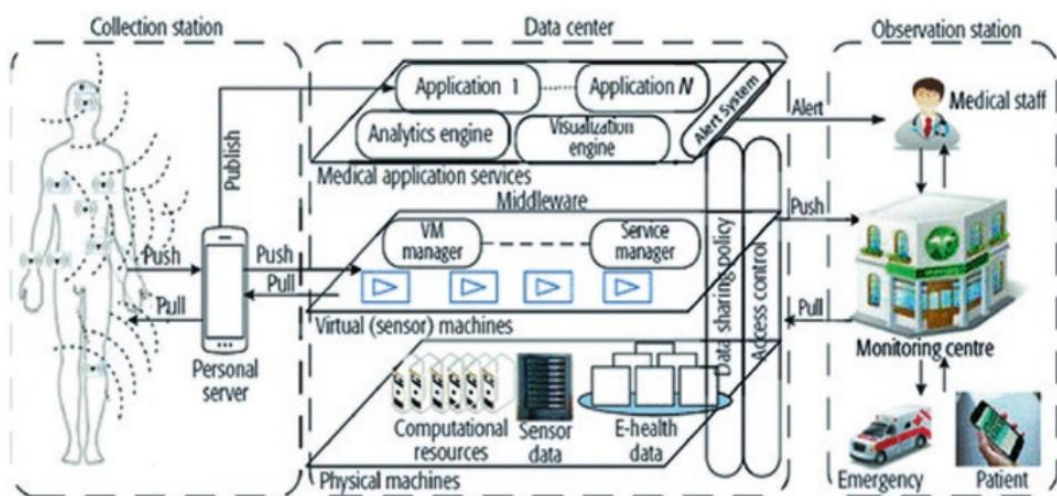


Рисунок 4.5 – Архітектура IoT для розумної охорони здоров'я [11]

- *Точне землеробство та оптимізація ресурсів (Precision Farming)*

Говорячи про LoRaWAN не можна забути про аграрний сектор. У сільському господарстві LoRa дозволяє досягти значних економічних показників, що підтверджується досвідом вирощування яблук у регіоні Кашмір (Індія). Впровадження комплексного рішення від EnthuTech, яке включає датчики вологості ґрунту, температури, рН та електропровідності, дозволило перейти до моделі точного землеробства. Дані передаються через шлюзи LoRaWAN навіть у складних ландшафтних умовах, забезпечуючи автоматизоване керування системами зрошення. Результати впровадження демонструють високу ефективність технології: споживання води знизилося на 10–12%, операційні витрати зменшилися на 20–25% за рахунок автоматизації ручної праці, а якість врожаю зросла на 7–8% завдяки підтримці ідеальних умов навколишнього середовища [50].



Рисунок 4.6 – Вирощування яблук за допомогою мереж LoRaWAN

- *5G URLLC у промисловій автоматизації (Industry 4.0)*

Одним із показових прикладів впровадження новітніх стільникових

технологій у виробничому секторі є спільний проект компаній Ericsson та Audi, спрямований на автоматизацію «розумних фабрик». Головним викликом для сучасної промисловості є потреба у гнучкості та мобільності виробничих ліній, що традиційно обмежується використанням дротових з'єднань для керування роботами. Використання технології 5G URLLC (Ultra-Reliable Low-Latency Communication) дозволило подолати ці обмеження, забезпечуючи критично важливі параметри надійності та затримки, які раніше були доступні виключно через кабельні мережі [51]. Практична демонстрація технології, яка зображена на рисунку 4.7, була реалізована на базі роботизованої комірки, що виконує монтаж подушок безпеки в рульові колеса. Система працює з використанням стандартних промислових протоколів автоматизації PROFINET RT та PROFIsafe безпосередньо через мережу 5G.



Рисунок 4.7 – Використання 5G URLLC при монтажі подушок безпеки

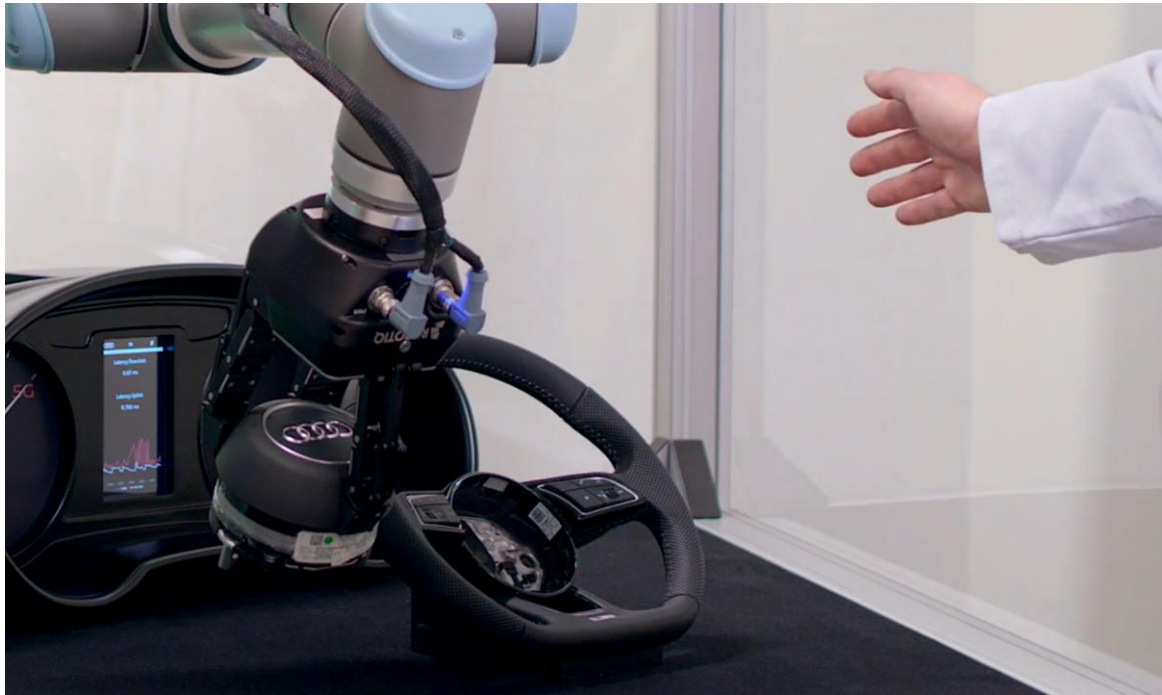


Рисунок 4.8 – Демонстрація наднизької затримки при перетині бар'єру

Ключовим досягненням стала реалізація механізмів безпеки: завдяки гарантованій наднизькій затримці 5G URLLC, система миттєво зупиняє робота при перетині людиною захисного лазерного бар'єру, це зображено на рисунку 4.8. Така швидкість реакції є критичною для безпечної взаємодії людини та машини і не могла бути реалізована на базі Wi-Fi або мобільних мереж попередніх поколінь через неможливість гарантувати суворі межі затримок [51].

Перехід на 5G URLLC відкриває шлях до створення повністю бездротових виробничих цехів, де роботизовані комплекси потребують лише підключення до електроживлення. Це радикально підвищує ефективність підприємства, дозволяючи вільно переміщувати обладнання та змінювати конфігурацію виробничих ліній щодня залежно від поточних потреб, що є фундаментальною основою концепції фабрики майбутнього.

- *Smart Parking на базі NB-IoT*

Проблема перевантаженості міського трафіку значною мірою спричинена водіями, що шукають місця для паркування. Для вирішення цього завдання компанія Deutsche Telekom спільно з Huawei реалізувала

пілотний проект «розумного паркування» в місті Бонн (Німеччина) та Нідерландах. Технічне рішення базується на використанні ультразвукових датчиків, вмонтованих безпосередньо в дорожнє покриття або паркомісце. Ці сенсори детектують наявність автомобіля та передають статус («вільно/зайнято») через мережу NB-IoT на хмарний сервер, звідки інформація потрапляє у мобільний додаток для водіїв.

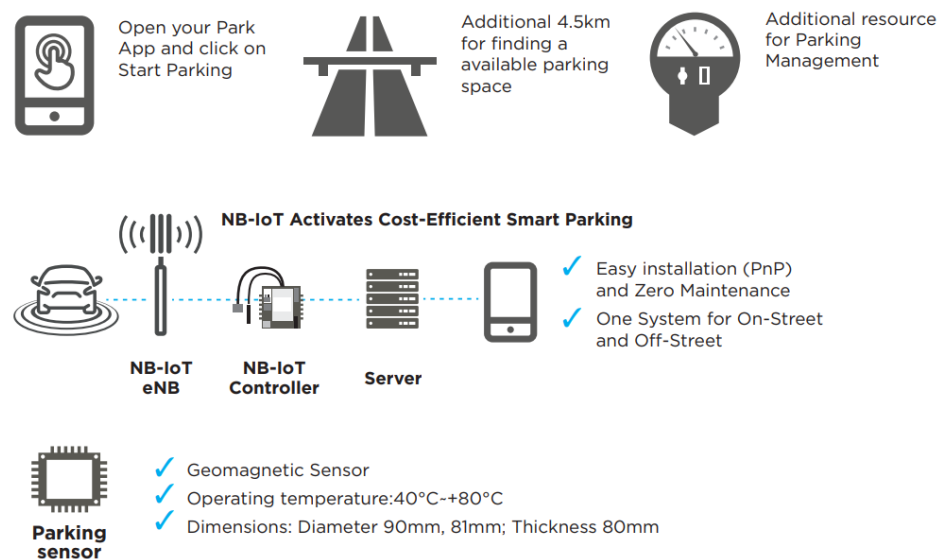


Рисунок 4.9 – Розумне паркування на базі NB-IoT

Вибір технології NB-IoT (Narrowband IoT) для цього завдання обумовлений її унікальними характеристиками, критично важливими для міської інфраструктури. По-перше, технологія забезпечує підсилення сигналу на 20 дБ порівняно зі звичайними стільниковими мережами, що дозволяє передавати дані навіть з підземних паркінгів або через товсті стіни будівель. По-друге, низьке енергоспоживання дозволяє датчикам працювати від однієї батареї до 10 років, що мінімізує витрати на обслуговування (OPEX) [52].

- *Екологічний моніторинг та відстеження біорізноманіття*

Окрім урбаністичних застосувань, технології LPWA відкривають нові можливості для збереження дикої природи. Показовим є проект, реалізований оператором Vodafone спільно з Підрозділом досліджень морських ссавців (SMRU) у Шотландії, метою якого є дослідження причин

різкого скорочення популяції звичайних тюленів. Традиційні супутникові системи відстеження мали суттєві обмеження: вони передавали лише приблизні координати і лише кілька разів на добу, що не давало повної картини поведінки тварин.



Рисунок 4.10 – Використання мобільного IoT для моніторингу тварин

Використання нових телеметричних міток з підтримкою мобільного IoT дозволило вивести моніторинг на новий рівень. Спеціальні безпечні датчики, прикріплені до тварин, збирають та передають деталізовані дані про їхнє місцезнаходження, глибину занурення, температуру води та навіть рівень солоності. Ключовою перевагою LPWA у цьому сценарії є розширений радіус дії та енергоефективність, що дозволяє відстежувати переміщення тварин далеко у відкритому морі протягом тривалого часу без необхідності заміни джерела живлення. Отримані масиви даних (Big Data) дозволяють науковцям будувати точні моделі поведінки популяції та розробляти ефективні стратегії її захисту [53].

- *Агрометеорологічний моніторинг у віддалених зонах (NB-IoT/LTE-M)*

Ще одним прикладом застосування ліцензованих технологій LPWAN

для потреб точного землеробства є рішення μ METOS - автономної метеостанції, спроектованої спеціально для роботи у віддалених та важкодоступних локаціях, де раніше розгортання систем моніторингу було економічно недоцільним. Ключовою особливістю системи є універсальність комунікаційного модуля, який підтримує стандарти LTE-M (Cat M1) та NB-IoT (Cat NB1), а також має опцію резервного перемикання на мережі 2G (fallback). Це забезпечує максимальну гнучкість покриття та гарантує передачу телеметрії навіть в умовах слабого сигналу стільникової мережі.



Рисунок 4.11 – Метеостанція μ METOS та API

Функціональність станції охоплює моніторинг критично важливих для агрономії параметрів: температури повітря, кількості опадів, сонячної радіації, а також характеристик ґрунту (вологість, температура, електропровідність). Система реалізує енергоефективний алгоритм роботи: збір даних відбувається з інтервалом у 15 хвилин, а передача на хмарну платформу FieldClimate – щогодини. Важливим аспектом надійності є механізм буферизації: у разі відсутності підключення станція зберігає дані за останні кілька днів у внутрішній пам'яті та автоматично синхронізує їх після відновлення мережі. Це дозволяє фермерам отримувати безперервні ряди даних для побудови моделей захворювань рослин, планування польових робіт та інтеграції з технікою (наприклад, John Deere) через API [54].

- *Дистанційний моніторинг пацієнтів з хронічними захворюваннями (Remote Patient Monitoring)*

У сфері охорони здоров'я технології Інтернету речей відіграють ключову роль у трансформації підходів до лікування хронічних захворювань, таких як діабет, серцева недостатність, хвороба Альцгеймера та гіпертонія. Традиційні методи лікування часто є реактивними, тоді як IoT дозволяє перейти до проактивної моделі через системи дистанційного моніторингу здоров'я (Remote Health Monitoring). Використання носимих пристроїв, які підтримують BLE та домашнього медичного обладнання, підключеного до мережі, забезпечує безперервний збір фізіологічних показників пацієнта поза межами клініки, що дозволяє лікарям отримувати об'єктивну картину перебігу хвороби в динаміці, а не лише під час візитів.

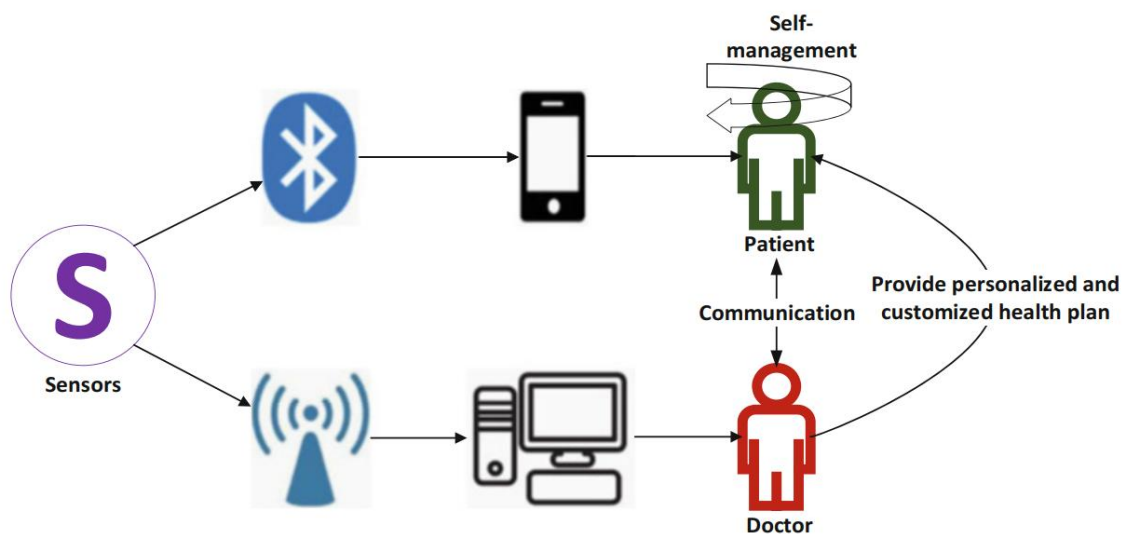


Рисунок 4.12 – Дистанційний моніторинг здоров'я пацієнтів

Технічна архітектура таких рішень зазвичай включає три основні компоненти: сенсори для збору даних, технології передачі інформації та програмне забезпечення для аналізу та виявлення аномалій. Прикладом реалізації такого підходу є платформа Personal Care Connect (PCC) – стандартизована відкрита система, що дозволяє інтегрувати пристрої та додатки від різних виробників. На відміну від телемедицини, що вимагає

інтерактивного аудіо-відео зв'язку, системи моніторингу фокусуються на автоматичній передачі даних, що дозволяє своєчасно коригувати плани лікування, запобігати критичним станам та уникати непотрібних госпіталізацій.

1.3 Вибір оптимальних технологій для різних типів IoT-додатків

Процес вибору радіотехнології для побудови системи Інтернету речей є багатофакторною задачею, яка не має єдиного правильного рішення для всіх випадків. Як було продемонстровано у попередніх розділах, кожна сфера, від побутової автоматизації до важкої промисловості, висуває свій унікальний набір вимог до пропускної здатності, енергоефективності, дальності зв'язку та вартості.

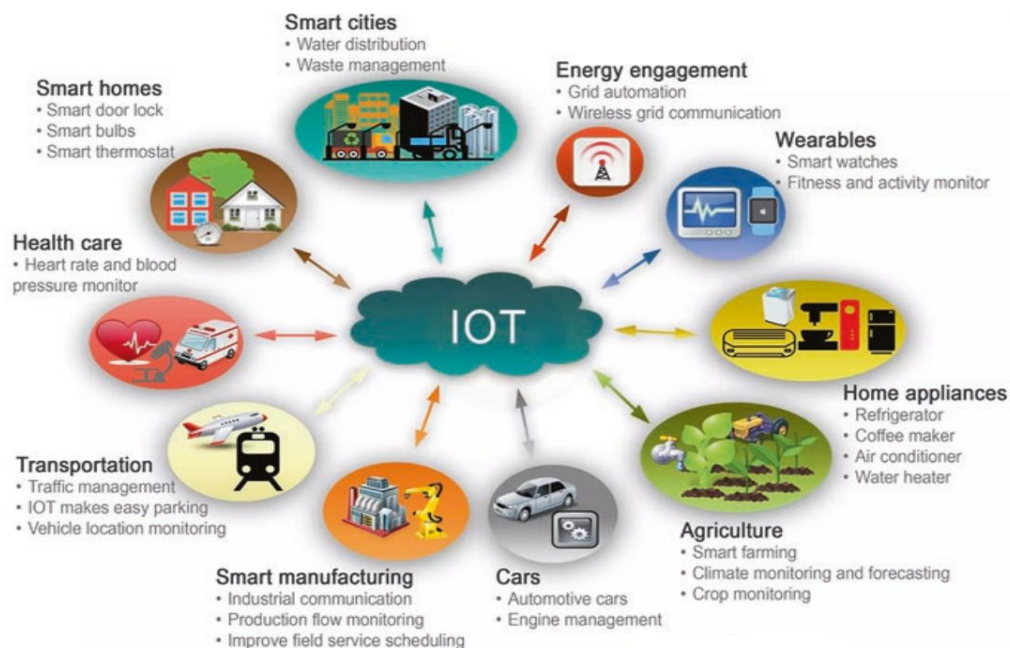


Рисунок 4.13 – Застосування Інтернету речей у сучасну епоху

В цілому, нічого не заважає обрати будь-яку технологію, яку ви забажаєте, але не завжди це буде доцільно, в першу чергу, як з точки зору вартості, так і з точки зору надмірності. Тому вибір оптимального стандарту має базуватися на чіткому розумінні профілю трафіку та умов експлуатації

кінцевих пристроїв. Для систематизації підходів до вибору доцільно згрупувати технології за основними класами задач:

Високошвидкісні локальні системи (Smart Home та відеоспостереження)

Для застосунків, що вимагають передачі великих обсягів даних (потоків відео, голосовий трафік) або забезпечення швидкого відгуку в межах обмеженого простору, безумовним лідером є технологія Wi-Fi. Вона є оптимальною для стаціонарних систем із постійним живленням, таких як камери відеоспостереження або мультимедійні хаби розумного будинку. Однак для сценаріїв, де необхідно поєднати високу швидкість із збільшеним радіусом дії та кращим проникненням крізь стіни, перспективною альтернативою є стандарт Wi-Fi HaLow (IEEE 802.11ah). Працюючи в суб-гігагерцовому діапазоні, він дозволяє розгортати мережі відеоспостереження на великих територіях (кампуси, склади) без необхідності встановлення численних репітерів.

Персональні мережі та автоматизація будівель

У сегменті носимих пристроїв (wearables), таких як фітнес-трекери, смарт-годинники та медичні сенсори, домінуючою технологією залишається Bluetooth Low Energy (BLE). Його ключовою перевагою є надзвичайно низьке енергоспоживання та нативна інтеграція зі смартфонами, що дозволяє створювати персональні екосистеми моніторингу здоров'я. Для задач автоматизації будівель (керування освітленням, замками, кліматом) більш доцільним є використання ZigBee або Z-Wave. Ці технології підтримують комірчасту топологію (mesh), що підвищує надійність мережі та дозволяє покривати великі приміщення, використовуючи пристрої (наприклад, розумні розетки) як ретранслятори сигналу.

Розподілені мережі моніторингу (Massive IoT)

Для сценаріїв, де тисячі датчиків розподілені на значних територіях (розумне місто, точне землеробство) і передають невеликі пакети даних, критичними є автономність та дальність дії. Тут оптимальним вибором є

LoRaWAN, що працює в неліцензованому спектрі. Це ідеальне рішення для агросектору та моніторингу навколишнього середовища, де важлива низька вартість розгортання приватної мережі. Натомість для стаціонарних об'єктів у міській забудові, таких як розумні лічильники в підвалах, краще підходить NB-IoT. Використання ліцензованого спектру забезпечує гарантовану якість обслуговування та глибоке проникнення сигналу, хоча і передбачає операційні витрати на оплату послуг оператора.

Критичні додатки та мобільні об'єкти

Окрему нішу займають задачі, що вимагають підтримки мобільності або наднизьких затримок. Для відстеження рухомих активів (логістика, телематика) перевагу слід надати технології LTE-M, яка, на відміну від NB-IoT, підтримує безшовний хендовер між вежами та передачу голосу. Для найбільш вимогливих промислових сценаріїв (Industry 4.0), де необхідне керування роботами в реальному часі або забезпечення роботи автономного транспорту, безальтернативним є використання мереж 5G. Завдяки режиму URLLC (Ultra-Reliable Low-Latency Communication) вони забезпечують затримки на рівні мілісекунд та найвищу надійність з'єднання.

1.4 Висновки до розділу 4

У четвертому розділі магістерської дисертації було розроблено практичні рекомендації щодо застосування радіотехнологій у сучасних мережах Інтернету речей. На основі аналізу реальних кейсів впровадження у таких сферах, як агросектор, промисловість, охорона здоров'я та розумні міста, було підтверджено тезу про те, що ефективність системи залежить не від пошуку універсального стандарту, а від вибору технології, яка найкраще відповідає специфічним вимогам конкретної задачі.

Було систематизовано ключові критерії вибору, розподіливши їх на технічні (швидкість, затримка, дальність), експлуатаційні (енергоефективність, мобільність) та економічні (CAPEX/OPEX). Детальний

розгляд прикладів, таких як використання 5G URLLC для промислової робототехніки або LoRaWAN для моніторингу водних ресурсів у віддалених регіонах, наочно продемонстрував, як теоретичні переваги стандартів трансформуються у реальну бізнес-цінність та соціальний ефект.

Узагальнюючи результати розділу, для зручності прийняття рішень, зведемо всю отриману інформацію в одну матрицю рекомендацій щодо вибору технологій представлена та представимо її в таблиці 4.2, яка дозволяє чітко розмежувати сфери застосування: від високошвидкісних локальних мереж до енергоефективних глобальних рішень. Це створює методичну основу для проектування надійних та рентабельних IoT-систем, забезпечуючи баланс між функціональними можливостями мережі та витратами на її розгортання і підтримку.

Таблиця 4.2 – Вибір оптимальної радіотехнології для типових IoT-задач

Сфера застосування / Задача	Основні вимоги	Рекомендована технологія
Розумний будинок (Відео)	Висока швидкість, живлення від мережі	Wi-Fi 6/7
Розумний будинок (Сенсори)	Mesh-мережа, низьке енергоспоживання	ZigBee, Z-Wave, Thread
Носимі пристрої (Медицина)	Персональна зона, зв'язок зі смартфоном	BLE (Bluetooth)
Відеоспостереження (Периметр)	Середня дальність, проникнення крізь стіни	Wi-Fi HaLow
Агросектор (Поля)	Велика дальність, автономність, дешевизна	LoRaWAN
Комунальні послуги (Лічильники)	Глибоке проникнення (підвали), стабільність	NB-IoT
Логістика (Трекінг)	Мобільність, роумінг, передача голосу	LTE-M
Промисловість (Робототехніка)	Наднизька затримка, надійність	5G URLLC

ВИСНОВКИ

У даній магістерській дисертації було проведено комплексне дослідження радіотехнологій Інтернету речей, проаналізовано їхні технічні характеристики, методи моделювання та особливості практичного застосування. Основні результати роботи та висновки полягають у наступному:

- ♦ Проаналізовано концепцію та архітектуру сучасних мереж IoT. Встановлено, що ефективність функціонування Інтернету речей залежить від коректної взаємодії всіх рівнів його архітектури – від сенсорів та виконавчих пристроїв до мережеских шлюзів та хмарних платформ. Виявлено, що основними викликами для подальшого розвитку галузі є забезпечення масштабованості мереж в умовах масового підключення пристроїв (Massive IoT), гарантування енергоефективності автономних вузлів та захист даних у гетерогенних середовищах.

- ♦ Виконано порівняльний аналіз ключових радіотехнологій. Досліджено характеристики технологій ближнього (Bluetooth, ZigBee, Wi-Fi HaLow) та дальнього радіусу дії (LoRaWAN, NB-IoT, LTE-M, 5G). З'ясовано, що не існує універсального стандарту для всіх задач IoT, тоді як:

- Технології LPWAN (LoRaWAN, NB-IoT) є оптимальними для побудови енергоефективних мереж з великим радіусом покриття, але мають обмеження щодо швидкості передачі даних.
- Стільникові технології нового покоління (5G URLLC, RedCap) вирішують проблеми затримок та надійності, що критично важливо для промислової автоматизації та автономного транспорту.
- Технології WPAN (ZigBee, BLE) залишаються стандартом для локальних рішень, таких як «розумний будинок», завдяки підтримці mesh-топологій та низькій вартості.

- ♦ Розроблено методику дослідження радіотехнологій на основі імітаційного моделювання. Обґрунтовано, що комп'ютерне моделювання є

найбільш доцільним методом оцінки ефективності масштабних мереж. Проведено порівняльний огляд симуляторів NS-3 та OMNeT++, в результаті якого визначено, що NS-3 забезпечує вищу точність моделювання фізичного рівня стільникових мереж (LTE/NB-IoT), тоді як OMNeT++ вирізняється гнучкістю архітектури та кращими засобами візуалізації. Сформовано методологічний алгоритм постановки задачі моделювання, який включає вибір сценарію (топологія, трафік), визначення метрик (PDR, затримка, енергоспоживання та ін.) та опис програмної архітектури моделі. Що дозволить прогнозувати поведінку мережі ще на етапі проектування.

- ◆ Сформовано практичні рекомендації щодо застосування радіотехнологій. На основі аналізу реальних кейсів (Smart City, агромоніторинг, охорона здоров'я) розроблено матрицю вибору оптимальних технологій. Визначено, що для розподілених сенсорних мереж (лічильники, датчики ґрунту) економічно та технічно доцільним є використання LoRaWAN або NB-IoT, тоді як для задач відеоспостереження та керування роботами необхідно застосовувати високошвидкісні канали Wi-Fi або 5G.

Загалом, результати роботи підтверджують, що побудова надійної мережі Інтернету речей вимагає системного підходу до вибору радіотехнологій, які базуються на балансі між вимогами до дальності дії, автономності, пропускну здатності та вартості розгортання. Запропоновані у роботі методичні підходи та практичні рекомендації можуть бути використані при проектуванні сучасних інфокомунікаційних систем різного призначення. Крім того, вони можуть стати основою для подальших наукових досліджень у сфері IoT, зокрема для вдосконалення алгоритмів імітаційного моделювання з метою вибору оптимальної технології під конкретні сценарії експлуатації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cirani, S., Ferrari, G., Picone, M., & Veltri, L. (2019). Internet of Things: Architectures, Protocols and Standards. Wiley. [https://aitskadapa.ac.in/e-books/CSE/IOT/Internet%20of%20Things_%20Architectures,%20Protocols%20and%20Standards%20\(%20PDFDrive%20\).pdf](https://aitskadapa.ac.in/e-books/CSE/IOT/Internet%20of%20Things_%20Architectures,%20Protocols%20and%20Standards%20(%20PDFDrive%20).pdf)
2. Domínguez-Bolaño, T., Campos, O., Barral, V., Escudero, C. J., & García-Naya, J. A. (2022). An overview of IoT architectures, technologies, and existing open-source platforms. Internet of Things. <https://doi.org/10.1016/j.iot.2022.100626>
3. Технології інтернету речей. Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 12,5 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с
4. Архітектура та технології Інтернету речей: навч. посіб. / І.В. Пулеко, А.А. Єфіменко. – Електронні дані. – Житомир: Державний університет «Житомирська політехніка», 2022. – 234 с.
5. Guth, J., Breitenbücher, U., Falkenthal, M., Leymann, F., & Reinfurt, L. (2016). Comparison of IoT platform architectures: A field study based on a reference architecture. Proc. 2016 Cloudification of the Internet of Things (CIoT), 1–6. <https://www.iaas.uni-stuttgart.de/publications/INPROC-2016-48-Comparison-of-IoT-Platform-Architectures.pdf>
6. IEEE Standard for an Architectural Framework for the Internet of Things (IoT), IEEE Std 2413-2019, 2019. <https://ieeexplore.ieee.org/document/9032420>
7. ITU Telecommunication Standardization Sector. (2012). Overview of the Internet of Things, Rec. ITU-T Y.4000/Y.2060. <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060>

8. Носков , В. І. ., & Кузьмінський, А. Р. . (2025). ПОРІВНЯЛЬНИЙ АНАЛІЗ РАДІОТЕХНОЛОГІЙ МЕРЕЖ ІОТ . Збірник матеріалів Міжнародної науково-технічної конференції «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ», 85–87.
<https://conferenc-journal.its.kpi.ua/article/view/330926/320259>
9. Кузьмінський, А. Р., Носков, В. І., & Бондарчук, А. П. (2025). Гібридний підхід поєднання NB-IoT з LoRa. Телекомунікаційні та інформаційні технології, (2 (87)), 134–148.
<https://doi.org/10.31673/2412-4338.2025.029573>
10. Milenkovic, M. (2020). Internet of Things: Concepts and System Design. – Cham: Springer. – 323 p. – ISBN 978-3-030-41345-3.
<https://doi.org/10.1007/978-3-030-41346-0>
11. Mohanty, S., Chatterjee, J. M., & Satpathy, S. M. (Eds.). (2021). Internet of Things and Its Applications. – 562 p.
<https://doi.org/10.1007/978-3-030-77528-5>
12. García Márquez, F. P., & Lev, B. (Eds.). (2021). Internet of Things: Cases and Studies. – Cham: Springer. – 304 p.
<https://doi.org/10.1007/978-3-030-70478-0>
13. Grizhnevich, A. IoT Systems Classification with Examples. ScienceSoft Blog. May, 2018. – [Електронний ресурс]. – Режим доступу: <https://www.scnsoft.com/blog/iot-systems-classification>
14. «Інтернет речей в сільському господарстві» / Agrilab.ua. – [Електронний ресурс]. – Режим доступу: <https://www.agrilab.ua/internet-rechey-iot-v-silskomu-gospodarstvi-9-prykladiv-vykorystannya-tehnologij-dlya-tochnogo-zemlerobstva-i-vyklyky-yaki-slid-vrahuvaty/>
15. «Інтернет речей у сільському господарстві: 8 варіантів використання технологій для розумного землеробства» / Global X-UA. – лютий 2022. – [Електронний ресурс]. – Режим доступу: <https://globalx-ua.com/internet-veschey-v-selskom-hozyaystve>
16. Peixiong He, Yi Zhou, Xiao Qin (2024). A Survey on Energy-Aware

- Security Mechanisms for the Internet of Things.
<https://doi.org/10.3390/fi16040128>
17. Cheikh, I., Roy, S., Sabir, E., & Aouami, R. (2025). Energy, Scalability, Data and Security in Massive IoT: Current Landscape and Future Directions. – 5 травня 2025. <https://doi.org/10.48550/arXiv.2505.03036>
 18. Кузьмінський, А. Р. Аналіз стандартів IEEE 802.15 побудови мереж Інтернету речей : дипломна робота ... бакалавра : 172 Телекомунікації та радіотехніка / Кузьмінський Артем Ростиславович. – Київ, 2024. – 98 с.
 19. Qahhar Muhammad Qadir, Tarik A. Rashid, Nawzad K. Al-Salihi, Birzo Ismael, Alexander A. Kist, Zhongwei Zhang (2020). Low Power Wide Area Networks: A Survey of Enabling Technologies, Applications and Interoperability Needs. <https://arxiv.org/abs/2008.08639>
 20. Koulouras, Grigorios; Katsoulis, Stylianos; Zantalis, Fotios (2025). Evolution of Bluetooth Technology: BLE in the IoT Ecosystem. Sensors, 25(4), 996. [Електронний ресурс]. – Режим доступу: <https://www.mdpi.com/1424-8220/25/4/996>
 21. P. Bhoyar, P. Sahare, S.B. Dhok, R.B. Deshmukh, Communication Technologies and Security Challenges for Internet of Things: A Comprehensive Review, International Journal of Electronics and Communications (2018). <https://doi.org/10.1016/j.aeue.2018.11.031>
 22. Bishnu Kumar Maharjan, Ulf Witkowski, Reza Zandian (2014). Tree network based on Bluetooth 4.0 for wireless sensor network applications.: <https://doi.org/10.1109/EDERC.2014.6924382>
 23. Marksteiner, Stefan; Juan Expósito Jiménez, Víctor; Vallant, Heribert (2018). An Overview of Wireless IoT Protocol Security in the Smart Home Domain. <https://doi.org/10.48550/arXiv.1801.07090>
 24. Vaezi, Mojtaba; Azari, Amin; Khosravirad, Saeed R.; Shirvanimoghaddam, Mahyar; Azari, M. Mahdi; Chasaki, Danai; Popovski, Petar (2021). Cellular, Wide-Area, and Non-Terrestrial IoT: A Survey on 5G Advances and the

- Road Towards 6G. <https://doi.org/10.48550/arXiv.2107.03059>
25. LTE-M – the new form of IoT technology. [Электронный ресурс]. – Режим доступа: <https://powunity.com/en/lte-m-the-new-form-of-iot-technology>
 26. Abou El Hassan, A.; El Mehdi, A.; Saber, M. (2021). NB-IoT and LTE-M towards massive MTC: Complete performance evaluation for 5G mMTC. Indonesian Journal of Electrical Engineering and Computer Science, 23(1), 308-320. DOI:10.11591/ijeecs.v23.i1.pp308-320
 27. Bahalul Haque, A.K.M., Oahiduzzaman Mondol Zihad, M., Rifat Hasan, M. (2023). 5G and Internet of Things–Integration Trends, Opportunities, and Future Research Avenues. https://doi.org/10.1007/978-981-99-3668-7_11
 28. 5G RedCap for IoT: The Perfect Balance of 5G Capabilities [Электронный ресурс] / Telenor IoT. – Режим доступа: <https://iot.telenor.com/technologies/connectivity/5g-redcap/>
 29. Introduction to 5G Reduced Capability (RedCap) Devices Previously known as NR-Lite / NR-Light [Электронный ресурс] / 3G4G Ltd.– Режим доступа: <https://www.3g4g.co.uk/Training/beginners0039.pdf>
 30. Industry’s First 802.11ah (HaLow) Wireless Module for IoT Devices [Электронный ресурс]. – Режим доступа: <https://www.silextechnology.com/unwired/industrys-first-802.11ah-halow-wireless-module-for-iot-devices>
 31. Gomathi, R. M.; Satya Krishna, G. Hari; Prince, Brumancia; Dhas, Y. Mistica (2018). A Survey on IoT Technologies, Evolution and Architecture. DOI: 10.1109/ICCCSP.2018.8452820
 32. Ding, Jie; Nemati, Mahyar; Ranaweera, Chathurika; Choi, Jinho (2020). IoT Connectivity Technologies and Applications: A Survey. DOI: 10.1109/ACCESS.2020.2985932
 33. Bang, Ankur; Rao, Udai Pratap; Visconti, Andrea; Brighente, Alessandro (2022). An IoT Inventory Before Deployment: A Survey on IoT Protocols, Communication Technologies, Vulnerabilities, Attacks, and Future Research

- Directions. DOI: 10.1016/j.cose.2022.102914
34. Prakash, Ramya; Jyoti, Neeli; Manjunatha, S. (2024). A survey of security challenges, attacks in IoT. E3S Web of Conferences, 491, 04018.
DOI: 10.1051/e3sconf/202449104018
 35. Ugwuanyi, S., Paul, G., & Irvine, J. (2021). Survey of IoT for Developing Countries: Performance Analysis of LoRaWAN and Cellular NB-IoT Networks. Electronics, 10(18), 2224.
<https://doi.org/10.3390/electronics10182224>
 36. Koulouras, G., Katsoulis, S., & Zantalis, F. (2025). Evolution of Bluetooth Technology: BLE in the IoT Ecosystem. Sensors, 25(4), 996.
<https://doi.org/10.3390/s25040996>
 37. Silicon Laboratories Inc. (2025). AN1142: Mesh Network Performance Comparison. – Application Note. Режим доступа:
<https://www.silabs.com/documents/public/application-notes/an1142-mesh-network-performance-comparison.pdf>
 38. Klima, Matej; Rechtberger, Vaclav; Bures, Miroslav; Bellekens, Xavier; Hindy, Hanan; Ahmed, Bestoun S. (2020). Quality and Reliability Metrics for IoT Systems: A Consolidated View.
DOI: 10.48550/arXiv.2011.10865
 39. Network Simulation Tools. Network Simulator Projects. – Электронный ресурс. – Режим доступа: <https://networksimulationtools.com/network-simulator-projects/>
 40. Patel, Ronit L.; Pathak, Maharshi J.; Nayak, Amit J. (2018). Survey on Network Simulators. International Journal of Computer Applications, 182(21), 23–30.
DOI: 10.5120/ijca2018917974
 41. Sharma, Pramod (2014). A Comparative Study of NS-2 and NS-3. Indian Journal of Scientific Research, 2(3), 428–431. – Электронный ресурс. – Режим доступа:
https://www.researchgate.net/publication/359649322_A_Comparative_Study_of_NS-2_and_NS-3

y of NS-2 and NS-3

42. Manzoor, Sohaib; Manzoor, Mahak; Manzoor, Hira; Adan, Durr E. (2023). Which Simulator to Choose for Next Generation Wireless Network Simulations? NS-3 or OMNeT++. DOI: 10.3390/engproc2023046036
43. List of IoT Simulator. MATLABSimulation.com – Электронный ресурс. – Режим доступа: <https://matlabsimulation.com/list-of-iot-simulator/>
44. Wehner, P., Göhringer, D. (2017). Internet of Things Simulation Using OMNeT++ and Hardware in the Loop. In: Keramidas, G., Voros, N., Hübner, M. (eds) Components and Services for IoT Platforms. Springer, Cham. https://doi.org/10.1007/978-3-319-42304-3_4
45. Khan, Atta ur Rehman; Bilal, Sardar M.; Othman, Mazliza (2013). A Performance Comparison of Network Simulators for Wireless Networks. DOI: 10.48550/arXiv.1307.4129
46. Difference Between OMNeT++ and NS3 Projects. PhDProposal.org – Электронный ресурс. – Режим доступа: <https://www.phdproposal.org/Difference-Between-OMNet++-&-Ns3-projects.html>
47. Ugwuanyi, Stephen; Paul, Greig; Irvine, James (2021). Survey of IoT for Developing Countries: Performance Analysis of LoRaWAN and Cellular NB-IoT Networks. Electronics, 10(18), 2224. <https://doi.org/10.3390/electronics10182224>
48. Abou El Hassan, Adil; El Mehdi, Abdelmalek; Saber, Mohammed (2021). NB-IoT and LTE-M towards massive MTC: Complete performance evaluation for 5G mMTC. Indonesian Journal of Electrical Engineering and Computer Science, 23(1), 308–320. DOI: 10.11591/ijeecs.v23.i1.pp308-320
49. Ugwuanyi, Stephen; Paul, Greig; Irvine, James (2021). Survey of IoT for Developing Countries: Performance Analysis of LoRaWAN and Cellular NB-IoT Networks. Electronics, 10(18), 2224. DOI: 10.3390/electronics10182224

50. Use Cases and Case Studies of Live LoRaWAN Deployments. LoRa Alliance – Электронный ресурс. – Режим доступа:
<https://resources.lora-alliance.org/use-cases>
51. 5G URLLC – Achieving industrial automation. Ericsson.com – Электронный ресурс. – Режим доступа:
<https://www.ericsson.com/en/cases/2020/accelerate-factory-automation-with-5g-urllc>
52. LPWA: Making Parking Smarter. GSMA Mobile IoT Case Study – Электронный ресурс. – Режим доступа: https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/gsma_resources/lpwa-making-parking-smarter/
53. LPWA: Enabling Extreme Wildlife Tracking. GSMA Mobile IoT Case Study – Электронный ресурс. – Режим доступа:
<https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/wp-content/uploads/2017/08/LPWA-Enabling-Extreme-Wildlife-Tracking.pdf>
54. µMETOS NB-IoT/CLIMA. METOS.global – Электронный ресурс. – Режим доступа: <https://metos.global/en/micrometos-nbiot/>
55. NS-3 LTE Module Documentation – Электронный ресурс. – Режим доступа: <https://www.nsnam.org/docs/models/html/lte.html>
56. Piro, Giuseppe; Baldo, Nicola; Miozzo, Marco (2011). An LTE module for the ns-3 network simulator. DOI: 10.4108/icst.simutools.2011.245571
57. Magrin, Davide; Capuzzo, Martina; Romagnolo, Stefano; Luvisotto, Michele. LoRaWAN ns-3 module – Электронный ресурс. – Режим доступа: <https://github.com/signetlabdei/lorawan>
58. Yang, Shun-Ren; Chou, Tzu-Hsiang. Simulating Narrow Band Internet of Things: Scheduler: Using ns-3 – Электронный ресурс. – Режим доступа:
<https://drive.google.com/file/d/1qAG6mTjKeFjokdqFP5QDan21bhWGXEJY/view>
59. Lin, Kuan-Yu; Yang, Shun-Ren. Simulating NB-IoT Random Access:

Using ns-3 as an Example – Электронный ресурс. – Режим доступа: <https://drive.google.com/file/d/1RO6PNewPiJe7ZAKegtAKxc5VUhM--pPT/view>

60. INET Framework for OMNeT++: Users Guide Электронный ресурс. – Режим доступа: <https://inet.omnetpp.org/docs/users-guide/>
61. Slabicki, Mariusz; PremSankar, Gopika; Di Francesco, Mario (2018). Adaptive configuration of LoRa networks for dense IoT deployments. DOI: 10.1109/NOMS.2018.8406255