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

Навчально-науковий Інститут телекомунікаційних систем

Кафедра електронних комунікацій та інтернету речей

«До захисту допущено»
ВО завідувача кафедри
_____ В’ячеслав НОСКОВ
«___»_____20__ р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Аналіз технологій та протоколів фізичного та канального рівня мереж Інтернету речей»

Виконала:
студентка IV курсу, групи ТС-12
Семенюк Юлія Сергіївна _____

Керівник:
Доцент кафедри ЕКІР ІТС, доцент
Носков Вячеслав Іванович _____

Рецензент:
Незалежний експерт з телекомунікацій, кандидат
технічних наук, Вахрушев Володимир Платонович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент (-ка) _____

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 – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Освітня програма – «Системи електронних комунікацій та інтернету речей»

ЗАТВЕРДЖУЮ
ВО завідувача кафедри
_____ В’ячеслав НОСКОВ
«___»_____20__ р.

ЗАВДАННЯ
на дипломну роботу студентці
Семенюк Юлії Сергіївні

1. Тема роботи «Аналіз технологій та протоколів фізичного та канального рівня мереж Інтернету речей», керівник роботи Носков Вячеслав Іванович, доцент, затверджені наказом по університету від 26 травня 2025 р. № 1755-С.

2. Термін подання студентом роботи 10 червня 2025 року

3. Вихідні дані до роботи: Матеріали статей та наукових видань, інформаційні ресурси мережі Інтернет, навчально-методичні матеріали. Структурований план порядку розробки матеріалів дипломної роботи.

4. Зміст роботи: Обґрунтувати актуальність теми. Проаналізувати технічні принципи передачі даних в мережах IoT. Виконати класифікацію та аналіз технологій і протоколів фізичного та канального рівня передачі даних. Розробити модель мережі IoT для проведення досліджень параметрів передачі даних. Надати рекомендації щодо використання технологій передачі даних для різних сценаріїв розгортання мереж IoT.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо):

1) Тема та мета роботи; 2) 3) Основні технології та протоколи фізичного та канального рівня мереж IoT; 4) Технічні принципи поширених протоколів

IoT; 5) Порівняльний аналіз технологій IoT; 6) Топологія мережі розумного будинку; 7) Результати моделювання в середовищі Cisco Packet Tracer; 8) Висновки.

6. Дата видачі завдання 31.10.2024 року

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Ознайомлення з темою роботи, підбір джерел інформації	15.12.2024	Виконано
2	Теоретичні засади функіювання мереж IoT	20.01.2025	Виконано
3	Аналіз протоколів канального та фізичного рівня IoT	31.03.2025	Виконано
4	Практичні аспекти використання технологій фізичного та канального рівня в мережах IoT	20.05.2025	Виконано
5	Вступ, Висновки	02.06.2025	Виконано
6	Чистовий варіант дипломної роботи, плакати	10.06.2025	Виконано

Студентка Юлія СЕМЕНЮК

Керівник роботи Вячеслав НОСКОВ

РЕФЕРАТ

Обсяг роботи 102 сторінки, 18 ілюстрацій, 15 таблиць, 18 джерел літератури.

Актуальність дослідження полягає в необхідності ефективного вибору комунікаційних технологій відповідно до специфіки застосування. Різноманіття стандартів, таких як Wi-Fi, Bluetooth, Zigbee, LoRaWAN, NB-IoT та інших, потребує детального аналізу їх характеристик, переваг та обмежень для визначення оптимальних рішень у конкретних сценаріях. Правильний вибір технологій фізичного та канального рівнів дозволяє суттєво підвищити ефективність функціонування IoT-систем, оптимізувати їх енергоспоживання та забезпечити стабільність і якість обміну даними між пристроями.

Мета дослідження: підвищити ефективність побудови та експлуатації IoT-систем шляхом аналізу сучасних технологій і протоколів фізичного та канального рівнів та розробки практичних рекомендацій щодо їх оптимального вибору для різних сценаріїв використання.

Об’єкт дослідження: процеси передавання даних у мережах Інтернету речей на канальному та фізичному рівнях.

Предмет дослідження: методи та протоколи забезпечення зв’язку на канальному та фізичному рівнях мереж Інтернету речей.

Методи дослідження: аналіз наукової та технічної літератури, порівняльний аналіз характеристик фізичних і канальних протоколів, моделювання роботи IoT-мереж, емпіричний аналіз результатів моделювання, метод узагальнення для формування практичних рекомендацій.

Наукова новизна отриманих результатів полягає у систематизації знань про сучасні технології фізичного та канального рівнів, у виявленні залежностей між вибором протоколів і параметрами ефективності IoT-систем, а також у розробці структурованих рекомендацій щодо вибору технологій для різних класів IoT-застосувань.

Практичне значення отриманих результатів полягає у тому, що запропоновані рекомендації можуть бути використані при проектуванні нових

IoT-систем, оптимізації існуючих рішень, а також у навчальному процесі для підготовки фахівців з IoT та мережевих технологій.

КЛЮЧОВІ СЛОВА: Інтернет речей, IoT, фізичний рівень, канальний рівень, протоколи зв’язку, Wi-Fi, ZigBee, LoRaWAN, NB-IoT, BLE, Ethernet, ефективність мережі, енергоспоживання, бездротові мережі, моделювання, Cisco Packet Tracer, розумний будинок, оптимізація IoT-систем, протоколи нижніх рівнів OSI, безпека IoT.

ABSTRACT

The volume of work is 102 pages, 18 illustrations, 15 tables, 18 sources

The relevance of the study lies in the need for effective selection of communication technologies in accordance with the specifics of their application.

The variety of standards, such as Wi-Fi, Bluetooth, Zigbee, LoRaWAN, NB-IoT, and others, requires a detailed analysis of their characteristics, advantages, and limitations to determine the optimal solutions in specific scenarios. The right choice of physical and channel level technologies can significantly improve the efficiency of IoT systems, optimize their energy consumption, and ensure the stability and quality of data exchange between devices.

Research objective: to improve the efficiency of building and operating IoT systems by analyzing modern technologies and protocols at the physical and channel levels and developing practical recommendations for their optimal selection for different usage scenarios.

Research object: data transmission processes in Internet of Things networks at the channel and physical levels.

Subject of the study: methods and protocols for ensuring communication at the channel and physical levels of Internet of Things networks.

Research methods: analysis of scientific and technical literature, comparative analysis of the characteristics of physical and channel protocols, modeling of IoT networks, empirical analysis of modeling results, generalization method for forming practical recommendations.

The scientific novelty of the results obtained lies in the systematization of knowledge about modern technologies at the physical and channel levels, in identifying dependencies between the choice of protocols and the performance parameters of IoT systems, as well as in the development of structured recommendations for the selection of technologies for different classes of IoT applications.

The practical significance of the results obtained lies in the fact that the proposed recommendations can be used in the design of new IoT systems, the

optimization of existing solutions, and in the educational process for training specialists in IoT and network technologies.

KEYWORDS: Internet of Things, IoT, physical layer, channel layer, communication protocols, Wi-Fi, ZigBee, LoRaWAN, NB-IoT, BLE, Ethernet, network efficiency, energy consumption, wireless networks, modeling, Cisco Packet Tracer, smart home, IoT system optimization, lower OSI layer protocols, IoT security.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

IoT	Internet of Things - Інтернет речей
OSI	Open Systems Interconnection - модель взаємодії відкритих систем
PHY	Physical Layer - фізичний рівень
MAC	Medium Access Control - керування доступом до середовища
Wi-Fi	Wireless Fidelity - бездротова мережа стандарту IEEE 802.11
BLE	Bluetooth Low Energy - енергоефективний Bluetooth
NB-IoT	Narrowband Internet of Things = вузькосмуговий Інтернет речей
LoRa	Long Range - радіозв'язок великої дальності
LoRaWAN	Long Range Wide Area Network - широкомережевий протокол LoRa
PLS	Physical Layer Security - безпека фізичного рівня
WPA / WPA2 / WPA3	Wi-Fi Protected Access - протоколи захисту бездротових мереж
SCADA	Supervisory Control and Data Acquisition - системи диспетчерського управління і збору даних
LTE-M	Long Term Evolution for Machines - спрощена мобільна мережа для пристроїв IoT
CRC	Cyclic Redundancy Check - циклічна контрольна сума
TCP/IP	Transmission Control Protocol / Internet Protocol - комплекс протоколів TCP/IP
VPN	Virtual Private Network - віртуальна приватна мережа

ВСТУП

У сучасних умовах бурхливого розвитку технологій Інтернету речей (Internet of Things, IoT) спостерігається стрімке зростання кількості підключених пристроїв у різних сферах — від побутових рішень до промислових систем, транспорту та міської інфраструктури. За оцінками експертів, кількість IoT-пристроїв у світі вже перевищує десятки мільярдів, і ця цифра щороку зростає.

Водночас ефективність роботи IoT-систем значною мірою залежить від вибору технологій і протоколів нижніх рівнів мережевої моделі OSI — фізичного та канального. Саме ці рівні визначають надійність зв’язку, енергоефективність, масштабованість і здатність системи до роботи в реальному часі. Помилки у виборі протоколів або їх невідповідність до вимог сценарію використання можуть призводити до перевитрат енергії, нестабільної роботи мережі або втрати даних.

Актуальність дослідження зумовлена стрімким поширенням IoT у різних сферах та необхідністю ефективного вибору комунікаційних технологій відповідно до специфіки застосування. Різноманіття стандартів, таких як Wi-Fi, Bluetooth, Zigbee, LoRaWAN, NB-IoT та інших, потребує детального аналізу їх характеристик, переваг та обмежень для визначення оптимальних рішень у конкретних сценаріях. Правильний вибір технологій фізичного та канального рівнів дозволяє суттєво підвищити ефективність функціонування IoT-систем, оптимізувати їх енергоспоживання та забезпечити стабільність і якість обміну даними між пристроями.

Мета дослідження: підвищити ефективність побудови та експлуатації IoT-систем шляхом аналізу сучасних технологій і протоколів фізичного та канального рівнів та розробки практичних рекомендацій щодо їх оптимального вибору для різних сценаріїв використання.

Об’єкт дослідження: процеси передавання даних у мережах Інтернету речей на канальному та фізичному рівнях.

Предмет дослідження: методи та протоколи забезпечення зв’язку на канальному та фізичному рівнях мереж Інтернету речей.

Методи дослідження: аналіз наукової та технічної літератури, порівняльний аналіз характеристик фізичних і канальних протоколів, моделювання роботи IoT-мереж, емпіричний аналіз результатів моделювання, метод узагальнення для формування практичних рекомендацій.

Наукова новизна отриманих результатів полягає у систематизації знань про сучасні технології фізичного та канального рівнів, у виявленні залежностей між вибором протоколів і параметрами ефективності IoT-систем, а також у розробці структурованих рекомендацій щодо вибору технологій для різних класів IoT-застосувань.

Практичне значення отриманих результатів полягає у тому, що запропоновані рекомендації можуть бути використані при проектуванні нових IoT-систем, оптимізації існуючих рішень, а також у навчальному процесі для підготовки фахівців з IoT та мережевих технологій.

Задачі дослідження:

1. Проаналізувати архітектуру IoT-мереж та визначити роль фізичного і канального рівнів.
2. Дослідити сучасні технології і протоколи фізичного та канального рівнів.
3. Виконати порівняльний аналіз технологій за ключовими критеріями.
4. Провести моделювання IoT-мережі у Cisco Packet Tracer на прикладі "розумного будинку".
5. Оцінити вплив вибору технологій на параметри роботи мережі.
6. Розробити практичні рекомендації щодо вибору технологій для різних сценаріїв застосування IoT.

Ця робота вносить вклад у наукову сферу через аналіз і структурування критеріїв вибору ефективних технологій для IoT-систем, що дозволяє підвищити їх продуктивність і енергоефективність.

Проведення комплексного аналізу дозволяє ідентифікувати найбільш оптимальні комбінації протоколів для різних сфер застосування IoT — від побутових рішень до промислових і міських мереж.

Практичне значення роботи може бути використане для оптимізації процесів розробки IoT-мереж, підвищення їх надійності, зниження енергоспоживання та забезпечення стабільної якості сервісів.

Застосування розроблених рекомендацій сприятиме підвищенню ефективності управління IoT-інфраструктурою та створенню передумов для впровадження інноваційних послуг і нових моделей взаємодії у цифровій економіці.

1 ТЕОРЕТИЧНІ ЗАСАДИ ФУНКЦІОНУВАННЯ МЕРЕЖ ІОТ

1.1 Архітектура та рівнева модель мереж IoT

Наявність чітко визначеної архітектури IoT значно підвищує шанси на успіх розгортання підключеного до Інтернету речей на підприємстві.

Як повідомляється, корпоративний Інтернет речей зростає приблизно на 20% з року в рік, торкаючись практично кожної галузі та організації. Це означає, що фахівці з корпоративних технологій повинні підготуватися до припливу Інтернету речей у своє середовище.

Але як це зробити? Першим кроком є оцінка бізнес-цілей Інтернету речей в організації. Це може бути збільшення доходів, скорочення витрат, оптимізація бізнес-процесів або просто вписування в загальну технологічну стратегію.

Після того, як роль Інтернету речей стане зрозумілою, наступним кроком буде побудова архітектури. Хоча універсальної архітектури не існує, має сенс побудувати загальну архітектуру, яка охоплює всі компоненти, що можуть бути стандартизовані в організації, а потім розробити специфічні архітектури, налаштовані для досягнення бізнес-потреб.

Чому? Дані показують, що підприємства з архітектурою Інтернету речей значно успішніші, ніж ті, що її не мають. Успішні компанії - ті, що входять до першої третини компаній, коли мова йде про економію коштів, отримання нових доходів або вдосконалення бізнес-процесів за допомогою Інтернету речей - на 34% частіше мають архітектуру Інтернету речей, ніж менш успішні фірми.

Найкраще почати з визначення архітектури. По суті, архітектура - це схема або модель, яка складається з двох частин: ключових технологічних компонентів, які її складають, і взаємозв'язків між цими компонентами.

Іншими словами, архітектура - це більше, ніж перелік необхідних технологічних компонентів, але вона починається з цього переліку. Далі вона визначає, як ці компоненти взаємодіють або взаємодіють один з одним.

Кілька подальших визначень будуть доречними. Технологічний компонент - це система, пристрій або програмне забезпечення, яке забезпечує певну технічну можливість. Хмара не є технологічним компонентом, хоча в ній може знаходитися технологічний компонент, наприклад, хмарний брандмауер. Компоненти можуть бути апаратними, програмними або їх поєднанням, і вони можуть бути визначені на високому рівні (брандмауер) або на гранулярному рівні (фільтрація пакетів на канальному рівні). Визначення компонентів на правильному рівні є частиною завдання розробки архітектури. Наприклад, в архітектурі IoT ці компоненти, швидше за все, включатимуть підключені пристрої, інтелектуальні пристрої, датчики і виконавчі механізми.

На високому рівні архітектура Інтернету речей включає в себе чотири ключові компоненти[2] (Рис. 1.1):

- *Компонент додатків та аналітик:* Цей компонент обробляє та відображає інформацію, зібрану за допомогою Інтернету речей. Він включає в себе інструменти аналітики, штучний інтелект і машинне навчання, а також можливості візуалізації. Технології для цього компонента варіюються від традиційних пакетів аналітики та візуалізації, таких як R, IBM SPSS і SAS, до спеціалізованих інструментів Інтернету речей та інформаційних панелей від хмарних провайдерів, таких як Amazon, Google, Microsoft, Oracle і IBM, а також постачальників пакетів додатків, включаючи SAP, Salesforce та інші.

- *Інтеграційний компонент*: Це компонент, який забезпечує ефективну інтеграцію додатків, інструментів, безпеки та інфраструктури з існуючими ERP-системами та іншими системами управління компанії. Постачальники включають вищезгадані програмні та хмарні гравці, а також ряд продуктів з відкритим вихідним кодом і проміжного програмного забезпечення, таких як Oracle Fusion Middleware, LinkSmart, Apache Kafka і DynThings Open Source IoT Platform.

- *Компонент безпеки та управління:* Безпека IoT включає в себе захист фізичних компонентів системи за допомогою вбудованого програмного забезпечення і вбудованих постачальників послуг безпеки, які включають в

себе як традиційних постачальників послуг безпеки, що мають можливості IoT, так і постачальників, що спеціалізуються на IoT. Приклади включають Armis, Auth0, Cisco, Digicert, Forescout, Ordr, Palo Alto, Rapid7, SimpliSafe і SonicWall.

- *Інфраструктурний компонент:* Сюди входять фізичні пристрої - розумні датчики, які збирають інформацію, та виконавчі механізми, які контролюють навколишнє середовище. Сюди також входить мережа, в якій знаходяться датчики або виконавчі механізми; зазвичай, хоча і не завжди, це бездротова мережа, така як Wi-Fi, Bluetooth, 4G або 5G. З'являються й інші бездротові варіанти, зокрема WAN дальнього радіусу дії та WAN з низьким енергоспоживанням.

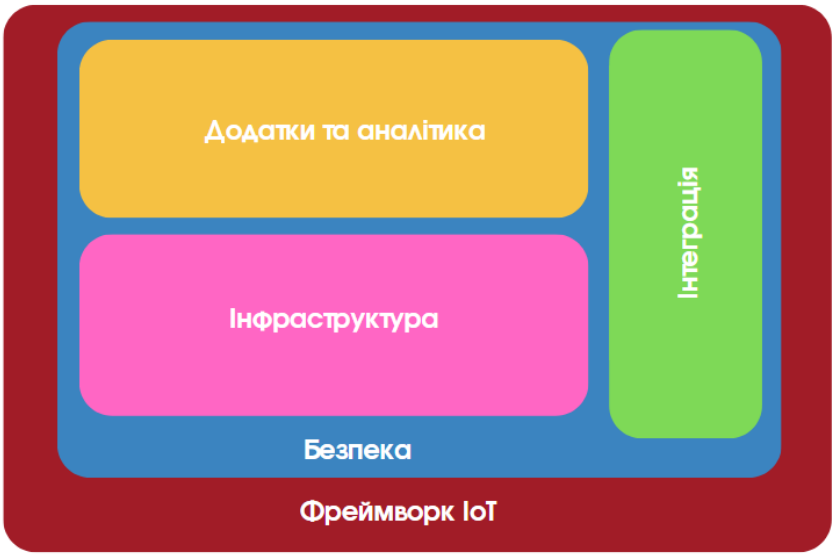

Рисунок 1.1 - Чотири компоненти архітектури IoT[3]

Взаємозв'язок між компонентами - це друга частина архітектури. Під взаємозв'язком між компонентами ми маємо на увазі те, як компоненти взаємодіють один з одним і якою інформацією вони обмінюються. Це може бути потік даних, потік метаданих, керуюча інформація або взагалі ніякої інформації. Програмні компоненти часто взаємодіють через API, а компоненти мережевого рівня зазвичай спілкуються через мережеві протоколи.

Говорячи про шари, архітектори часто думають в термінах компонентних шарів, таких як мережевий рівень, рівень сприйняття, рівень

обробки, фізичний рівень, рівень шлюзу, рівень платформи, рівень пристрою, бізнес-рівень, рівень безпеки, сенсорний рівень і так далі.

Концепція рівня полягає в тому, що він складається з набору можливостей, які взаємодіють один з одним, але для цілей інших компонентів можуть розглядатися як єдине ціле, з єдиною прозорою сутністю.

Так, наприклад, в архітектурі IoT прикладному рівню не потрібно знати, який тип фізичної мережі передає дані. Всі мережеві пристрої складають мережевий рівень, який транспортує трафік відповідно до потреб додатків.

Ми визначаємо шість рівнів архітектури IoT[9], як описано далі - зверніть увагу, що в деяких випадках рівні складаються з підрівнів; це загальна характеристика складних архітектур, таких як архітектура IoT (Рис. 1.2):

1. *Фізичний/пристрійний рівень:* Сюди входять датчики, виконавчі механізми та інші інтелектуальні пристрої, а також підключені пристрої, які складають фізичний рівень і рівень пристроїв. Ці розумні пристрої збирають дані (датчики), виконують дії (виконавчі механізми) або, іноді, і те, і інше.

2. *Мережевий рівень*: До нього входять мережеві пристрої та типи і протоколи зв'язку, наприклад, 5G, Wi-Fi, Bluetooth тощо. Хоча багато архітектур IoT покладаються на мережеві рівні загального призначення, все частіше спостерігається тенденція до переходу на спеціалізовані мережі, призначені для IoT.

3. *Рівень даних/бази даних:* Сюди також входить рівень платформи бази даних. Існує цілий ряд баз даних, що використовуються для архітектур IoT, і багато організацій витрачають досить багато часу на вибір і архітектуру правильних баз даних IoT для них.

Разом фізичний рівень/рівень пристроїв, мережевий рівень і рівень даних/бази даних складають інфраструктурний компонент, про який йшлося вище.

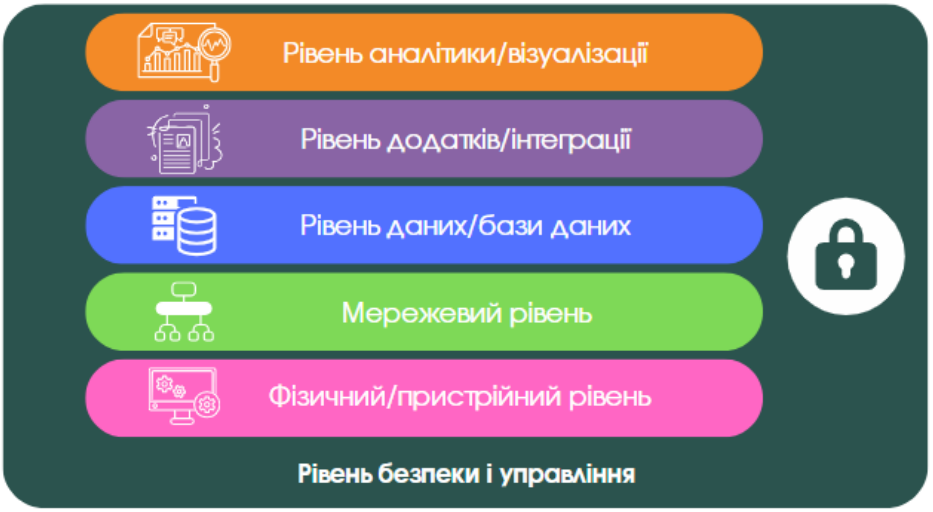

Рисунок 1.2 - Шість рівнів архітектури IoT

4. *Рівень аналітики/візуалізації:* Цей рівень складається з рівня аналітики, рівня візуалізації та рівня сприйняття. По суті, цей рівень зосереджений на аналізі даних, наданих Інтернетом речей, і наданні їх користувачам і додаткам для осмислення.

5. *Рівень додатків/інтеграції:* Це рівень додатків і платформ, які працюють разом, щоб забезпечити функціональність інфраструктури Інтернету речей для бізнесу. Іншими словами, рівень додатків, рівень платформи і рівень інтеграції - це те, що забезпечує цінність інфраструктури Інтернету речей для бізнесу. Рівень обробки та бізнес-рівень є частиною більшого рівня додатків/інтеграції.

6. *Рівень безпеки і управління:* Як випливає з назви, цей рівень охоплює як рівень безпеки, так і рівень управління. Строго кажучи, це не рівень, оскільки він з'єднується з усіма іншими рівнями для забезпечення безпеки та управління. Але це важливий компонент, який варто враховувати на кожному рівні.

Ці шари йдуть знизу вгору, як у моделі взаємозв'язку відкритих систем, яка була першоджерелом концепції шаруватості (Рис. 1.3).

Рисунок 1.3 - Огляд моделі архітектури IoT

1.2 Особливості передавання даних на фізичному та канальному рівнях

Фізичний рівень та рівень каналу передачі даних складається з об'єктів Інтернету речей (IoT) та фізичних мереж, що з'єднують їх з іншими об'єктами або мережею. На цьому рівні біти вихідних даних або інформації кодуються і декодуються та обмінюються через дротовий або бездротовий фізичний канал зв'язку. Існує багато протоколів і стандартних технологій, визначених різними органами та організаціями для протоколів фізичного та мережевого доступу. Ці протоколи і технології підходять для різних додатків і мережевих сайтів. Деякі з популярних протоколів і стандартів фізичного та рівня каналу передачі даних[14] такі: Ethernet, Bluetooth Low Energy, Wi-Fi, Wi-Fi Direct, WPA, Wireless HART, Zigbee, Z-wave, RFID, IEEE 802.11.ah, IEEE 802.15.4e, LoRaWAN, DASH7, Weightless, HomePlug, G.9959, LTE-A, DECT/ULE, ISA 100.11a, ANT, NFC, EPC Global, EddyStone, EnOcean, WiMax, NB-IoT, EC-GSM-IoT (Extended Coverage GSM-IoT), RPMA, LTE-MTC (LTE-Machine Type Communication), Cellular (GPRS/2G/3G/4G/5G), CDMA, Thread, INSTEON, DigiMesh.

Представлені стандарти та протоколи, які сьогодні активно застосовуються для з’єднання комп’ютерів і мобільних пристроїв. Їх широке впровадження пояснюється тим, що вони повсюдно використовуються в міських умовах і мегаполісах. До таких протоколів належать: 1) Ethernet, 2) Bluetooth 4.0, 3) Wi-Fi, 4) Wi-Fi Direct, 5) WPA/WPA2/WPA3.[17]

1) Ethernet - Ethernet є найпопулярнішою дротовою мережевою технологією. Вона широко використовується для з'єднання комп'ютерів у персональну мережу (PAN), домашню мережу (HAN), локальну мережу (LAN), глобальну мережу (WAN) і міську мережу (MAN). Він заснований на стандарті IEEE 802.3.[12] У системі IoT Ethernet можна використовувати для підключення стаціонарних або фіксованих IoT-пристроїв. Наприклад, він може бути використаний для з'єднання сенсорних мереж в промисловості, ланцюгів управління приладами в системі домашньої автоматизації або IoT-пристроїв в системі автоматизації офісу.

Швидкість передачі даних в Ethernet може досягати 10 гігабіт на секунду (Гбіт/с) для кабелів категорії 6.[8] Швидкість передачі даних через Ethernet залежить від типу кабелю і може бути обмежена адміністратором мережі. Для побудови мережі Ethernet можуть використовуватися оптоволоконні, коаксіальні кабелі або вита пара. Ethernet має дуже низьку затримку, що робить його придатним для критично важливих додатків IoT, де пристрої можуть бути розташовані спільно або на великій відстані.

2) Bluetooth Low Energy (BLE) – Bluetooth це стандарт бездротової технології для обміну даними на коротких відстанях між стаціонарними та мобільними пристроями, створюючи персональну мережу (PAN) з високим рівнем безпеки. Bluetooth Low Energy[6], також відомий як Bluetooth Smart, розроблений і запропонований Bluetooth Special Interest Group. BLE - це версія з низьким енергоспоживанням оригінального Bluetooth 2,4 ГГц. BLE був представлений як Bluetooth 4.0 у 2011 році.

BLE був розроблений для передачі невеликих обсягів даних на високій швидкості (1 Мбіт/с), коли один пристрій може бути з'єднаний з декількома пристроями в топології «зірка».[13] Радіус дії BLE обмежений 100 метрами, тому він зазвичай підходить для персональних мереж (PAN). Пристрої, підключені через BLE, переходять у сплячий режим, коли не передають дані. Час з'єднання між пристроями BLE може становити лише кілька мілісекунд, порівняно з середнім часом у 100 мілісекунд у класичному Bluetooth. Завдяки короткому часу з'єднання та високій швидкості передачі даних, BLE є надзвичайно енергоефективним у порівнянні з будь-якими іншими конкуруючими протоколами.

Рисунок 1.4 - Зображення, що демонструє архітектуру протоколу Bluetooth Low Energy (BLE)

BLE розроблений для IoT-пристроїв, які можуть працювати кілька років від невеликої батареї. На Bluetooth Low Energy реалізовані як фізичний, так і канальний рівні моделі OSI. Стек протоколу BLE складається з двох частин - контролера та хоста. В архітектурі фізичний і канальний рівні реалізовані в частині контролера. Контролер, як правило, являє собою SOC (System on Chip - система на кристалі) з радіопристроєм Bluetooth. Решта речей, таких як GAP, сервіси GATT, менеджер безпеки, включені в хост-частину. Як мінімум, служба GAP (Generic Access Profile - загальний профіль доступу) в Bluetooth

дозволяє BLE-пристрою спостерігати за іншими BLE-пристроями і підключатися до них (тільки коли це необхідно). Служба GATT (Generic Attribute Profile - загальний профіль атрибутів) в Bluetooth LE дозволяє іншим пристроям отримати доступ до сервісів і характеристик, які присутні в цьому Bluetooth-пристрої.

Стек протоколу BLE схожий на стек, який використовується для класичної технології Bluetooth, але BLE не сумісний з класичним Bluetooth. Основна відмінність полягає в тому, що BLE не підтримує потокову передачу даних. Замість цього він підтримує лише швидку передачу невеликих пакетів даних (розмір пакетів невеликий) зі швидкістю передачі даних 1 Мбіт/с.

У BLE є два типи пристроїв - головний і підлеглий. Майстер виступає в ролі центрального пристрою, який може підключатися до різних підлеглих. Розглядаючи сценарій IoT, телефон або ПК може слугувати головним пристроєм, а смарт-замок із вбудованим BLE - підлеглим пристроєм. Головний пристрій керує підлеглим на основі поданих ним команд. У таких випадках підлеглий пристрій повинен бути дуже енергоефективним.

Тоді як у класичному Bluetooth з'єднання залишається увімкненим весь час, навіть якщо передача даних не відбувається. Крім того, класичний Bluetooth підтримує 79 каналів передачі даних (з пропускною здатністю 1 МГц), тоді як BLE підтримує 40 каналів з пропускною здатністю 2 МГц (вдвічі більше, ніж класичний Bluetooth).

Стек протоколів BLE також підтримує зв'язок на основі IP.

Таблиця 1.1 - Перелік частот і діапазонів протоколу BLE

Частота	2,4 ГГц
Діапазон	1–100 м
Приклади	Гарнітури гучного зв'язку, брелоки, фітнес-трекери

3) Wi-Fi - запропонований Wi-Fi Alliance, Wireless Fidelity (Wi-Fi) є стандартом для бездротових локальних мереж (WLAN). Він базується на

стандарті IEEE 802.11 з різними номерами версій, позначеними як a, b, c, g, n і т.д., де від a до n - останні версії. Wi-Fi використовує діапазони радіочастот 2.4, 3.6, 5 і 60 ГГц і може мати швидкість передачі даних від 2 Мбіт/с (для застарілого 802.11) до 1.73 Гбіт/с (для 802.11ac хвиля 2). Досить поширений 802.11 n має швидкість передачі даних до 450 Мбіт/с.[11]

Через Wi-Fi пристрій підключається до роутера, налаштованого як точка доступу або точка доступу до мережі, а інші пристрої з підтримкою Wi-Fi підключаються до пристрою через точку доступу. Основними недоліками мережі Wi-Fi є затримка і низький рівень безпеки. Легше зламати точку доступу Wi-Fi і отримати доступ до фізичного середовища зв'язку. Однак, мережу Wi-Fi можна захистити, використовуючи типи WPA та управління маячковими пакетами.

Wi-Fi також дозволяє здійснювати зв'язок ad-hoc, коли пристрої з підтримкою Wi-Fi можуть безпосередньо взаємодіяти без точки доступу або маршрутизатора. Для цього пристроям потрібно надати спільний доступ до Інтернету за допомогою ad hoc і налаштувати себе як хот-спот або віртуальну точку доступу. Wi-Fi широко використовується для об'єднання в мережу комп'ютерів, ноутбуків і мобільних пристроїв. У системах IT його можна використовувати для створення персональних мереж (PAN), локальних мереж (LAN) і глобальних мереж (WAN).

Радіус дії будь-якої точки доступу Wi-Fi може становити до 100 метрів. Зона покриття мережі Wi-Fi може бути розширена за допомогою багатохопової маршрутизації. При багатоточковій маршрутизації один вузол (точка доступу) може використовувати інший вузол (точку доступу) як ретранслятор, збільшуючи таким чином загальну зону покриття мережі.

Таблиця 1.2 - Перелік частот і діапазонів Wi-Fi

Протокол Wi-Fi та безпека	802.11 a/b/g/n/af
Частота	Діапазони 2.4 ГГц, 3.6 ГГц і 4.9/5.0 ГГц

Продовження таблиці 1.2

Діапазон	Звичайна дальність дії - до 100 м, але може бути збільшена.
Приклади	Роутери, планшети тощо.

4) Wi-Fi Direct - це версія стандарту Wi-Fi «груша-груша». Він дозволяє двом пристроям встановити зв'язок без роутера або точки доступу.[8] Wi-Fi Direct - це стандарт з одним стрибком, тому його радіус дії не може бути розширений. Сьогодні Wi-Fi Direct широко використовується в ноутбуках, мобільних пристроях, камерах, телевізорах та ігрових приставках. Саме Wi-Fi Direct у смартфонах дозволяє їм налаштовуватися як точка доступу до Інтернету і надавати спільний доступ до Інтернету. Радіус дії Wi-Fi Direct обмежений 100 метрами.

5) WPA/WPA2/WPA3 - Wireless Protected Access (WPA) - протокол безпеки для стандарту Wi-Fi. Він був запропонований з огляду на вразливість мереж Wi-Fi. Він базується на стандарті IEEE 802.11i і використовує 64-бітний або 128-бітний ключ шифрування для захисту даних. За стандартом WPA послідував WPA2, а на зміну WPA2 прийде WPA3[9], який буде використовувати 192-бітове шифрування для захисту даних в мережі Wi-Fi. У той час як Wi-Fi Direct дозволяв використовувати стандарт Wi-Fi для додатків Personal Area Network (PAN), стандарти WPA зробили мережі Wi-Fi достатньо безпечними для використання в додатках IoT на базі WLAN.

Ці стандарти і протоколи є найбільш поширеними серед усіх інших і широко використовуються для з'єднання комп'ютерів, побутової техніки та мобільних пристроїв між собою.

1.3 Основні виклики та обмеження технологій та протоколів цих рівнів

1.3.1 Фізичний рівень:

У добу стрімкого розвитку комунікацій та застосунків Інтернет речей (IoT) стає необхідністю для задоволення зростаючих потреб користувачів.

Безпека зв'язку в IoT критично важлива, і значну увагу привертає безпека фізичного рівня (PLS), що забезпечує доказову та вимірювану секретність. Водночас особливості IoT — масовість, низька вартість, широке покриття — ускладнюють розробку PLS-протоколів.

Дослідження безпеки фізичного рівня можна простежити до теорії секретного зв'язку, створеної Шенноном [11]. Згідно з теорією Шеннона, система вважається такою, що перебуває в ідеальній секретності, якщо виконується наступна умова:

$$H(M|X) = H(M), \tag{1.1}$$

де $H(M)$ і $H(M|X)$ - ентропія повідомлення M і умовна ентропія M, обумовлена спостереженням підслуховувача X, відповідно. Для досягнення ідеальної секретності код, який використовується для кодування повідомлення, повинен бути незалежним від самого повідомлення. Одним з можливих підходів до реалізації цього є шифрування «одноразовим блокнотом», де кожен біт секретного ключа об'єднується XOR з кожним бітом повідомлення для отримання переданого кодового слова X. Ця вимога є надто складною для багатьох застосувань. На відміну від роботи Шеннона, Аарон Вайнер у 1975 році запропонував модель зашумленого каналу прослуховування [12]. Канал зашумленого прослуховування складається з одного законного передавача (Аліса), одного законного приймача (Боб) і одного підслуховувача (Єва). Для цієї моделі Вайнер сформулював умову безпечної передачі, тобто передача є інформаційно теоретично безпечною, якщо ймовірність помилки декодування на законному приймачі може бути як завгодно малою, а підслуховувач не може отримати жодної вихідної інформації. Максимальна швидкість, при якій може бути виконана вищезгадана умова, називається завадостійкістю, яка характеризує межі продуктивності для захищеної передачі в зашумлених каналах. У гауссівських каналах прослуховування завадостійкість Cs дорівнює різниці потужностей Шеннона між легальним (Аліса-Боб) і підслуховуючим (Аліса-Єва) каналами, тобто,

$$C_s = [\log(1 + \mathrm{SNR_B}) - \log(1 + \mathrm{SNR_E})]^+, \quad (1.2)$$

де $[x]^+ = \max(x, 0)$, $\mathrm{SNR_B}$ і $\mathrm{SNR_E}$ - прийняте відношення сигнал/шум (SNR) у Боба і Єви відповідно. Виходячи з мітки (2), безпечний зв'язок без ключів може бути реалізований до тих пір, поки якість каналу легітимного зв'язку є кращою за якість каналу для підслуховування. Таким чином, в роботі [12] було закладено основу для створення безпечного безключового зв'язку.

Однак, протягом тривалого періоду з моменту публікації роботи Вайнера, техніка PLS не привертала до себе особливої уваги. Це пов'язано з наступними причинами: по-перше, досяжність секретності залежить від використання стохастичного кодування. Однак побудувати практичні стохастичні коди з прийнятною складністю надзвичайно складно. По-друге, щоб досягти позитивного потенціалу секретності, отриманий SNR у законного користувача повинен бути строго вищим, ніж у підслуховувача, що важко гарантувати в бездротових середовищах. І останнє, але не менш важливе: незабаром після того, як була запропонована концепція секретності, Діффі і Хеллман розробили криптографію з відкритим ключем, яка спирається на математичні функції, що вважаються важкими для обчислення, і з моменту своєї появи домінує в дослідженнях безпеки.

Методи PLS[16] для IoT:

- *Введення штучного шуму*:

Одним з перспективних методів забезпечення інформаційної безпеки в системах Інтернету речей є введення штучного шуму (ШШ). Принцип методу полягає в одночасній передачі корисного сигналу та навмисно створеного шуму з метою зниження якості прийому інформації у зловмисника при мінімальному впливі на легітимного отримувача. Штучний шум зазвичай спрямовується у нульовий простір каналу законного користувача, що дозволяє ефективно зберігати конфіденційність.

Хоча така стратегія є дієвою, її реалізація зазвичай потребує використання кількох антен на передавачі, що не відповідає вимогам низької вартості та компактності IoT-пристроїв. У зв’язку з цим дослідники

пропонують кооперативну введення ШШ із залученням сторонніх пристроїв-джамерів, які допомагають формувати перешкоди для зловмисників.

Серед реалізацій цього підходу можна відзначити:

- використання енергонезалежних джамерів із протоколом harvest-then-jam (спочатку накопичення енергії, потім генерація шуму);
- оптимізацію розподілу потужності для одночасного забезпечення секретності й підтримки енергетичного балансу;
- інтеграцію введення ШШ з іншими техніками, такими як фонтанне кодування або стиснене зондування, що дозволяє підвищити рівень безпеки та зменшити затримки передачі й накладні витрати.

Ці підходи відкривають перспективи для побудови захищених IoT-систем, які враховують обмеження ресурсів і високі вимоги до ефективності зв’язку.

- *Компресійне зондування:*

Компресійне зондування (CS, compressed sensing) — це метод, який дозволяє стискати розріджені сигнали зі швидкістю нижчою за частоту Найквіста, що робить його привабливим для ресурсозалежних IoT-пристроїв. Останнім часом CS застосовується також як інструмент підвищення безпеки на фізичному рівні.

Суть підходу полягає в застосуванні лінійного перетворення до сигналу шляхом множення на вимірювальну матрицю. Безпека забезпечується тим, що ця матриця відома лише легітимним вузлам і недоступна зловмисникам. Наприклад, у деяких схемах вона генерується на основі випадкового насіння, отриманого з RSSI-показників каналів зв’язку між довіреними пристроями, що унеможливлює її відтворення підслуховувачем.

Також застосовуються комбінації CS з введенням штучного шуму, який передається разом із повідомленням і вибірково впливає лише на зловмисника, не порушуючи прийому легітимним одержувачем. У низці робіт запропоновано криптосистеми на основі CS, які демонструють обчислювальну стійкість навіть при застосуванні циркулярних матриць.

Окрім того, CS-техніка використовується у багатовузлових кооперативних IoT-системах. У таких мережах матриця каналів між джерелами та ретрансляторами слугує матрицею вимірювання, що дозволяє досягти високого рівня секретності. Зокрема, в багатохопових конфігураціях можливе досягнення безпечної передачі без використання криптографічних ключів.[15]

- *Перекидання біта:*

Метод перекидання бітів (bit flipping) застосовується для підвищення безпеки передачі даних у великих сенсорних мережах, особливо при взаємодії між сенсорами та легітимним центром злиття (ЛЦЗ). Згідно з цим підходом, сенсорні вузли класифікуються на сильні та слабкі групи залежно від якості їхнього каналу зв'язку. Датчики з кращими каналами (сильна група) передають правдиві дані, а датчики зі слабшими каналами – навмисно спотворені, інверсовані біти, щоб ускладнити прослуховування з боку центру злиття для підслуховування (ЦЗП).

Оскільки канали ЛЦЗ і ЦЗП статистично незалежні, спотворення даних значно погіршує якість прийому саме у зловмисника. У рамках досліджень запропоновано схеми з двома та трьома пороговими значеннями SNR, які використовуються для автономного визначення належності сенсорів до певної групи. Трипороговий варіант передбачає також наявність «мовчазної» групи датчиків, що додатково знижує енергоспоживання та покращує захищеність передачі.

Таким чином, метод перекидання бітів є ефективною стратегією фізичного рівня для захисту інформації[18] в багатовузлових IoT-системах за умов обмежених енергетичних і обчислювальних ресурсів.

- *Кооперативна таємниця:*

Кооперативна таємниця — це метод підвищення безпеки на фізичному рівні, що базується на використанні довірених проміжних вузлів (ретрансляторів), які допомагають легітимному відправнику забезпечити надійну й захищену передачу даних до приймача в умовах потенційної

присутності зловмисника.

Основна ідея полягає в тому, що кооперативні вузли беруть участь у передачі даних, посилюючи сигнал для легітимного приймача та/або створюючи перешкоди для підслуховувача. Залежно від стратегії, ретранслятори можуть:

- підсилювати і передавати (Amplify-and-Forward),
- перехоплювати і передавати (Decode-and-Forward),
- генерувати штучний шум (Cooperative Jamming),
- або поєднувати ці підходи.

У мережах IoT кооперативна таємниця дозволяє ефективно долати виклики, пов’язані з обмеженим енергоживленням та обчислювальними можливостями кінцевих пристроїв. На відміну від традиційної криптографії, такий підхід не потребує обміну ключами або складних обчислень — захист ґрунтується на фізичних характеристиках каналу.

Ключовою перевагою методу є адаптивність до топології мережі: у випадку слабкого прямого каналу між відправником і приймачем ретранслятори можуть формувати надійні кооперативні маршрути. Крім того, метод забезпечує захист навіть у динамічних умовах, коли зловмисник не має доступу до інформації про вибір ретрансляторів або їхню конфігурацію.

- *Шифрування фізичного рівня:*

Шифрування фізичного рівня - це метод захисту даних, який реалізується безпосередньо в процесі фізичної передачі сигналу, до моменту обробки протоколами вищих рівнів.[19] На відміну від класичного криптографічного захисту, який працює на прикладному або транспортному рівні, PLE спрямований на перетворення самого сигналу таким чином, щоб зробити його незрозумілим для неавторизованих отримувачів.

Методи шифрування фізичного рівня зазвичай базуються на модифікації базових параметрів сигналу:

- фази, амплітуди або частоти модуляції,
- часових затримок сигналу,

- порядку передачі бітів або символів.

У контексті мереж Інтернету речей PLE є перспективним, оскільки дозволяє зменшити залежність від складних програмних криптографічних схем, які можуть бути надто ресурсоємними для малопотужних пристроїв. Зокрема, в IoT часто застосовують легкі PLE-механізми, які забезпечують початковий рівень секретності з мінімальними накладними витратами.

Одним із підходів до реалізації PLE є використання сеансових параметрів модуляції, які змінюються з кожною передачею і є відомими лише легітимним сторонам. Іншим варіантом є інтеграція PLE з характеристиками каналу — наприклад, використання змін фазового зсуву відповідно до коефіцієнтів каналу, які складно відтворити зловмиснику.

Загалом, PLE є дієвим доповненням до класичних заходів безпеки і може використовуватись у багатошаровій архітектурі IoT для забезпечення базової конфіденційності даних на рівні фізичної передачі.

Аналіз переваг і недоліків існуючих методів PLS

Кожна з вищезгаданих методик PLS має свої переваги та недоліки. Введення AN є легкою для реалізації, оскільки штучні шуми можуть бути створені за допомогою генератора псевдовипадкових чисел, для якого можна безпосередньо використовувати багато існуючих алгоритмів. Однак, підвищення секретності, яке забезпечує метод введення AN, досягається за рахунок додаткового споживання енергії, яка використовується для надсилання штучного шумового сигналу. Порівняно з методом введення AN, метод захищеної передачі на основі CS не потребує витрат додаткової енергії і, таким чином, є більш енергоефективним. Однак, матриця вимірювань повинна бути спільною для легальних приймачів і зберігатися в таємниці від підслуховування, що вимагає узгоджених знань про CSI у різних сторін. Це призводить до значних накладних витрат при розробці протоколу. Техніка перекидання бітів може значно зменшити складність реалізації і подолати недоліки підходу, заснованого на CS. Однак, в методі перекидання бітів датчики в слабкій групі повинні передавати неправдиві дані, щоб збити з

пантелику підслуховувача, що призводить до марної трати енергії та пропускної здатності. Кооперативна секретність може бути найбільш поширеним підходом до PLS. Впровадження механізму співпраці дозволяє малопотужним пристроям боротися з потужними підслуховуючими пристроями з меншим споживанням ресурсів.Проте, основним недоліком методу кооперативного шифрування є те, що для координації роботи різних пристроїв в мережі необхідна додаткова сигналізація, що також ускладнює розробку протоколу. Шифрування на фізичному рівні - це, по суті, міжшаровий підхід, який поєднує генерацію секретного ключа на фізичному рівні та шифрування на прикладному рівні. Найбільшою перевагою цього підходу є те, що він може бути легко інтегрований з існуючими протоколами мережевої безпеки, які базуються на криптографічних методах на прикладному рівні. Однак, з іншого боку, ефективність шифрування на фізичному рівні сильно залежить від того, чи можуть сторони, що спілкуються, досягти згоди щодо згенерованих ключів, що є досить складним завданням у бездротових середовищах.

Проблеми проектування протоколу PLS для Інтернету речей

Як згадувалося раніше, дослідження методів PLS[21] сформувало великий масив літератури, починаючи від фундаментальних інформаційно-теоретичних досліджень і закінчуючи практичною розробкою протоколів PLS. Однак, як розробити стратегії PLS, які б добре відповідали унікальним особливостям IoT, все ще залишається відкритою проблемою. Більшість існуючих методів PLS мають наступні недоліки, які забороняють їх пряме застосування в IoT.

По-перше, пристрої Інтернету речей характеризуються «низькою вартістю», що означає, що ці пристрої зазвичай мають дуже обмежену пам'ять і можливості обробки даних. Крім того, пристрої Інтернету речей зазвичай живляться від батарей, що накладає значні енергетичні обмеження. Низька вартість і низьке енергоспоживання вимагають, щоб стратегії PLS були дуже енергоефективними і могли бути реалізовані з дуже низькою складністю.

Однак більшість існуючих схем PLS забезпечують безпеку за рахунок додаткового енергоспоживання або підвищеної складності апаратного забезпечення. Наприклад, підходи PLS на основі AN покладаються на введення штучних шумових сигналів, що призводить до додаткового енергоспоживання; безпечні методи формування/перекодування променя зазвичай базуються на багатоантенній структурі передавача, що неможливо з огляду на розмір і вартість пристроїв Інтернету речей; схеми PLS на основі кооперації вимагають наявності дружніх перешкод, які посилають сигнали, що заважають, що також ускладнює дизайн протоколу і збільшує енергоспоживання. З практичної точки зору, протоколи PLS, орієнтовані на IoT, повинні враховувати обмеження ресурсів пристроїв IoT, а також знаходити компроміс між безпекою, складністю та енергоспоживанням.

По-друге, з точки зору мережевої перспективи, очікується, що IoT підтримуватиме передачу даних на великі відстані. Наприклад, у бездротових сенсорних мережах, які є втіленням Інтернету речей, локальні дані, зібрані датчиками, повинні бути доставлені до віддаленого центру управління для подальшої обробки. Однак, відстань передачі даних в IoT за один стрибок досить обмежена через низьку потужність пристроїв IoT. Тому, щоб задовольнити вимогу широкого покриття, мережеві протоколи передачі повинні включати багато нових функцій, таких як багатоходова маршрутизація, кооперативна ретрансляція, когнітивна передача і т.д. Це, в свою чергу, вимагає, щоб стратегії PLS були достатньо «розумними», щоб адаптуватися до складних мережевих середовищ. Наприклад, пристрої IoT повинні співпрацювати з багатьма ненадійними безпосередніми вузлами. Хоча ці ненадійні вузли можуть не бути зловмисниками, цілком можливо, що вони не пройшли аутентифікацію і мають нижчий рівень безпеки, ніж пристрої IoT. Як ми можемо використовувати ненадійні вузли, щоб допомогти в доставці інформації, зберігаючи при цьому конфіденційність вмісту даних для них? Як кількість ненадійних ретрансляторів впливає на безпеку мережі? Ці питання ще не до кінця зрозумілі і потребують більш глибоких досліджень.

По-третє, IoT націлений на забезпечення масового підключення, яке може вмістити мільйони пристроїв на квадратний кілометр для обміну інформацією. Більше того, пристрої Інтернету речей, вироблені різними корпораціями, є гетерогенними вузлами з абсолютно різними типами послуг, моделями трафіку та режимами передачі даних. Ці особливості роблять IoT великомасштабною гетерогенною мережею, для якої питання масштабованості є першочерговим. Однак існуючі схеми PLS в основному розроблені для невеликих мереж, для яких важливими є лише показники продуктивності на рівні каналу, наприклад, рівень секретності, ймовірність перехоплення інформації тощо. Кілька фундаментальних проблем безпечної передачі даних у великих мережах не вирішуються належним чином. Наприклад, як залежить ступінь секретності системи від кількості вузлів у мережі? Як ми можемо перетворити величезну кількість з'єднань у мережі на потужний ресурс проти прослуховування? Щоб відповісти на ці питання, необхідно розробити нові математичні інструменти та інноваційні мережеві протоколи передачі даних.

По-четверте, очікується, що майбутній IoT буде підтримувати різні сценарії застосування з диверсифікованими бездротовими послугами. Різні типи послуг мають абсолютно різні вимоги до безпеки, затримки, пропускної здатності та надійності передачі. Однак більшість існуючих протоколів PLS просто спрямовані на оптимізацію рівня секретності або ймовірності втрати секретності. Таким чином, неможливо забезпечити комплексну гарантію QoS для додатків IoT. Щоб подолати цю складність, дизайн протоколу PLS повинен враховувати різні аспекти вимог користувача, включаючи затримку, надійність, пропускну здатність і секретність.

Перспективні рішення PLS[15] для Інтернету речей:

1. Агрегація шуму та самошифрування (Noise Aggregation and Self-Encryption)

Цей підхід поєднує інжекцію штучного шуму (AN) з вбудованим шифруванням даних, яке виконується самим пристроєм або групою пристроїв

без участі зовнішніх криптографічних систем.

Основні компоненти:

- Агрегація шуму: декілька пристроїв або ретрансляторів генерують штучний шум, який додається до інформаційного сигналу, створюючи перешкоди для зловмисника.
- Самошифрування: дані шифруються на рівні фізичного сигналу (наприклад, змінюється порядок бітів або модуляція), і цей процес повністю виконується вузлом IoT без складних криптографічних обчислень.

Переваги:

- Низьке енергоспоживання — метод не вимагає складних алгоритмів.
- Незалежність від ключової інфраструктури — шифрування реалізується без обміну ключами.
- Стійкість до аналізу сигналу — агрегація шуму ускладнює зворотне відновлення переданих даних.

Застосування:

- Масивні сенсорні мережі, де є велика кількість вузлів з обмеженою потужністю.
- Мережі, що працюють у складних або ворожих умовах (наприклад, військові або аварійні IoT-системи).

2. Розробка сигналу проти підслуховування за допомогою обертання сузір'я

У цьому підході забезпечення безпеки досягається за рахунок обертання сигнального сузір’я (наприклад, у модуляції QAM або PSK), що використовується для передачі даних.

Сигнальне сузір’я — це набір точок на комплексній площині, які відповідають різним комбінаціям бітів. При обертанні сузір’я координати кожної точки змінюються, і це ускладнює правильне декодування сигналу для стороннього отримувача.

Основні принципи:

- Відправник застосовує випадкове або квазівипадкове обертання сузір’я, яке

відоме лише легітимному приймачу.

- Зловмисник, не знаючи кута обертання, не може правильно визначити, який біт закодовано кожною точкою.
- Інколи також використовується динамічне обертання — кут змінюється з кожною передачею.

Переваги:

- Сумісність з існуючими модуляціями — метод легко інтегрується у системи з QAM, PSK.
- Висока стійкість до атак без потреби у шифруванні.
- Низька складність реалізації на пристроях з базовою обробкою сигналу.

Застосування:

- IoT-пристрої, які працюють у відкритих мережах із ризиком прослуховування.
- Бездротові мережі, де критична конфіденційність (медицина, фінанси).

3. Безпечна передача на основі фонтанного кодування

Фонтанне кодування (LT-коди, Raptor-коди) — це стохастичне джерело надлишкових кодованих блоків, з яких отримувач може відновити вихідне повідомлення після отримання достатньої кількості блоків (не обов’язково всіх).

У PLS цей механізм використовується для:

- розпорошення інформації у великій кількості надлишкових блоків,
- зниження ймовірності перехоплення — зловмисник отримує лише частину блоків, які не дають змоги відновити вихідне повідомлення.

Додаткові засоби безпеки:

- Поєднання з інжекцією шуму або канально-орієнтованим вибором блоків (на основі CSI).
- Випадковий порядок або таймінг передачі блоків, що ускладнює збір повної інформації стороннім приймачем.

Переваги:

- Гнучкість — отримувач може відновити дані при втраті частини пакунків.

- Надійність — добре працює в умовах з високим рівнем втрат.
- Вбудована стійкість до перехоплення без додаткового шифрування.

Застосування:

- Сенсорні мережі в агресивних середовищах (індустріальний IoT, військові об'єкти).
- Сценарії, де неможливо гарантувати стабільний канал або потрібно забезпечити “відкладене відновлення” повідомлення.

У таблиці 1.3 та 1.4 узагальнено переваги та недоліки методів забезпечення безпеки на фізичному рівні (PLS). Особливу увагу приділено таким критеріям, як енергоспоживання та складність реалізації, які мають вирішальне значення для пристроїв Інтернету речей із обмеженими ресурсами. Крім того, наведено типові сценарії застосування, де кожен із методів виявляє найбільшу ефективність. Дана таблиця може слугувати орієнтиром для інженерів та розробників при виборі відповідного PLS-рішення для конкретних завдань у сфері IoT.

Таблиця 1.3 - Переваги та недоліки методів безпеки фізичного рівня

Техніка PLS	Переваги	Недоліки
Введення AN	Покоління AN можна легко реалізувати	Додаткове споживання енергії
Компресійне зондування	Не потребує додаткового живлення	Матриця вимірювань має бути спільною
Перекидання бітів	Процес обробки сигналу на передавачі простий	Потрібна додаткова пропускна здатність та енергія
Кооперативна таємниця	Висока гнучкість та краща безпека	Зчначне сигнальне навантаження
Шифрування фізичного рівня	Легко інтегрується з існуючими протоколами безпеки	Потрібне зондування каналу та узгодження секретного ключа
Агрегація шуму	Легко впроваджується	Потрібен зворотний зв'язок щодо каналу
Обертання сузір'їв	Ступінь свободи каналів може бути повністю використаний	Потрібен CSIT
Фонтанне кодування	Комплексна гарантія якості обслуговування (QoS)	Потрібен зворотний зв'язок щодо каналу

Таблиця 1.4 - Порівняння методів безпеки фізичного рівня

Техніка PLS	Складність впровадження	Споживання енергії	Потенційні сценарії застосування
Введення AN	Помірний	Високий	Телемедицина
Компресійне зондування	Високий	Низький	Бездротові локальні мережі
Перекидання бітів	Низький	Високий	Сенсорні мережі
Кооперативна таємниця	Високий	Помірний	Безпілотні літальні апарати (БПЛА)
Шифрування фізичного рівня	Високий	Низький	Дистанційний коучинг
Агрегація шуму	Низький	Низький	Імерсивні системи, відеоспостереження
Обертання сузір'їв	Помірний	Помірний	Зв'язок між пристроями (D2D)
Фонтанне кодування	Низький	Низький	Промисловий Інтернет речей

На основі аналізу, поданого в таблицях 1.3 та 1.4, можна зробити висновок, що кожен із методів забезпечення безпеки фізичного рівня (PLS) в IoT має свої переваги й обмеження, що визначають доцільність його використання в певному контексті. Методи з низьким енергоспоживанням і невеликою складністю впровадження — як-от компресійне зондування, агрегація шуму та фонтанне кодування — є найбільш придатними для масового використання в енергообмежених IoT-середовищах, наприклад, у сенсорних мережах чи промислових системах. Водночас методи з вищим рівнем захисту, як-от інжекція AN або обертання сузір’їв, можуть бути доцільними у критичних сферах, де безпека є пріоритетом, незважаючи на додаткові витрати ресурсів.

Таким чином, вибір оптимального PLS-рішення повинен базуватись на балансі між енергетичними можливостями пристрою, складністю реалізації методу та рівнем загроз у конкретному сценарії застосування. Представлені в таблицях характеристики можуть слугувати практичним орієнтиром для проєктування IoT-систем із відповідним рівнем фізичної безпеки, що враховує

реальні обмеження й вимоги середовища.

1.3.2 Канальний рівень

Канальний рівень (Data Link Layer, DLL) - це другий рівень в моделі OSI від ISO, який відіграє найважливішу роль в комп'ютерних мережах. Канальний рівень відіграє ключову роль в управлінні кодуванням, передачею та прийомом пакетів даних у фізичних мережах. Він забезпечує надійний зв'язок між вузлами мережі за допомогою методів виявлення, виправлення та кадрування помилок.[18]

Розуміння та оптимізація канального рівня допомагає забезпечити надійну роботу мережі. Виправлення помилок проектування на цьому рівні впливає на продуктивність мережі, спричиняючи помилки передачі, втрату даних, збільшення затримок і зниження ефективності. Далі ми розглянемо такі ключові поняття, як керування доступом до середовища (Medium Access Control, MAC), методи контролю помилок і механізми керування потоком.

Рисунок 1.5 - Шари моделі OSI

Канальний рівень, який позиціонується як другий рівень у моделі OSI (Open Systems Interconnection), є фундаментальним для мережевого зв'язку. Розроблена на початку 1980-х років, модель OSI забезпечила стандартизовану

основу, яка революціонізувала мережу, розбивши складні комунікаційні системи на керовані рівні.

Канальний рівень з'єднує фізичний і мережевий рівні, забезпечуючи надійну передачу даних через фізичне середовище. Цей рівень відповідає за фреймінг, який передбачає поділ даних на керовані одиниці, що називаються кадрами даних.[19] Він також допомагає у фізичній адресації за допомогою апаратних адрес, відомих як MAC-адреси (Media Access Control). Виявлення та виправлення помилок є критично важливими функціями канального рівня, які виявляють і виправляють помилки під час передачі контрольної суми.

Модель OSI (Open Systems Interconnection) - це концептуальна основа для розуміння та реалізації мережевих протоколів на семи рівнях, а саме: фізичному, канальному, мережевому, транспортному, сеансовому, представницькому та прикладному. Канальний рівень, розташований над фізичним і під мережевим рівнями, відіграє вирішальну роль у забезпеченні зв'язку між цими рівнями. Він приймає необроблені біти з фізичного рівня, організовує їх у кадри і гарантує, що ці кадри не містять помилок і мають правильну послідовність, перш ніж передавати їх на мережевий рівень. Цей рівень відповідає за управління логічним з'єднанням (LLC), яке керує синхронізацією кадрів і управлінням потоком, а також за управління доступом до середовища (MAC), яке визначає, як пристрої спільно використовують середовище передачі даних. З практичної точки зору, розглянемо, як Ethernet і Wi-Fi, дві повсюдно поширені мережеві технології, покладаються на протоколи канального рівня для безперебійного функціонування, обробляючи все - від організації пакетів даних до виявлення та уникнення колізій. Сервісний інтерфейс, що надається цим рівнем, є важливим для належного функціонування верхніх рівнів.

Ключові функції та обов'язки

Канальний рівень виконує кілька важливих функцій[21] для забезпечення надійного та ефективного мережевого зв'язку:

- Кадрування: Поділ потоку даних на керовані одиниці, які

називаються кадрами. Кожен кадр включає заголовок і трейлер, які містять керуючу інформацію для адресації та виявлення помилок. Початок і кінець кадру можна визначити на основі певної послідовності бітів. Ця послідовність бітів додається у кадр для позначення його меж. Цей метод називається бітовим заповненням. Бітове заповнення реалізовано на багатьох канальних рівнях, в тому числі на канальному рівні популярного протоколу USB (Universal Serial Bus).

- Керування потоком: Керування швидкістю передачі даних між відправником і одержувачем, щоб запобігти перевантаженню пристрою-одержувача. Такі протоколи, як механізм ковзного вікна, широко використовуються у сценаріях надійної передачі даних, наприклад, у мережах TCP/IP. Ці механізми є життєво важливими для повільних одержувачів і швидких відправників.
- Виявлення та виправлення помилок: Впроваджує такі методи, як CRC (циклічна перевірка на надлишковість) для виявлення та виправлення помилок під час передачі даних, забезпечуючи їхню цілісність. Удосконалені методи виправлення помилок, такі як коди Ріда-Соломона, стають все більш важливими у високонадійних додатках, включаючи супутниковий зв'язок і зв'язок у далекому космосі.
- Фізична адресація: Використовує MAC-адреси для ідентифікації пристроїв у мережі. Ці апаратні адреси гарантують, що дані будуть доставлені на правильний пристрій або комп'ютер призначення. У мережі Wi-Fi MAC-адреси допомагають безперешкодно скеровувати дані на відповідні бездротові пристрої.
- Контроль доступу: Регулює доступ до спільного середовища передачі, використовуючи такі протоколи, як CSMA/CD (Carrier Sense Multiple Access with Collision Detection), щоб уникнути колізій і забезпечити ефективний зв'язок. Нові технології, такі як Інтернет речей (IoT), створюють нові виклики і можливості для контролю доступу до середовища, вимагаючи інноваційних рішень для ефективного управління численними підключеними

пристроями.

Розуміючи ці основоположні концепції та їхнє реальне застосування, мережеві інженери можуть краще оцінити складність проектування канального рівня і критично важливу роль, яку він відіграє в забезпеченні ефективного і надійного мережевого зв'язку.

У моделі OSI канальний рівень знаходиться між фізичним і мережевим рівнями. Отже, він отримує біти від фізичного рівня і зобов'язується доставити їх у належному форматі на мережевий рівень. При надсиланні даних повідомлення спочатку використовують сервіси мережевого рівня, потім звертаються до сервісів канального рівня і в кінцевому підсумку надсилають дані через фізичний рівень. На стороні прийому відбувається зворотний шлях: біти з фізичного рівня передаються на канальний рівень, який потім доставляє повідомлення на мережевий рівень. Таким чином, канальний рівень є проміжною ланкою між фізичним і мережевим рівнями, забезпечуючи надійність доставки шляхом структурування даних у чітко визначені кадри.

Канальний рівень гарантує, що мережевий рівень отримає дані відправника без втрат. Він також може встановити логічний канал зв'язку між відправником і одержувачем повідомлення, відстежуючи віртуальне з'єднання між ними. Віртуальними з'єднаннями керує канальний рівень. У цьому контексті канальний рівень надає мережевому рівню наступні типи послуг:

- Послуга без розпізнавання підключень: Ця послуга забезпечує доставку даних без помилок. Однак кадри даних, що передаються, не залежать один від одного і не підлягають підтвердженню з боку комп'ютера-одержувача щодо їх належної доставки. Послуга характеризується як «без з'єднання», оскільки канальний рівень не встановлює жодного віртуального з'єднання між відправником і одержувачем. Крім того, послуга є непідтвердженою, тобто, у випадку втрати кадру, не передбачено жодних заходів для виявлення втрати та її відновлення. По суті, послуга без з'єднання не передбачає контролю помилок і управління потоком. Найяскравішим прикладом протоколу канального рівня без встановлення з'єднання є популярний протокол Ethernet.

- Послуга з підтвердженням відсутності з'єднання: Як і у випадку з попередньою службою, ця служба не встановлює і не відстежує віртуальне з'єднання між відправником і одержувачем. Проте, на відміну від попередньої послуги, одержувач підтверджує доставку пакета. Таким чином, відправник знає, що дані, які він передав, надійно і безпечно отримані. Оскільки між відправником і одержувачем немає віртуального з'єднання, різні кадри підтверджуються окремо. Якщо протягом визначеного інтервалу часу підтвердження не отримано, відправник повторно надсилає кадр даних. Таким чином, ця послуга забезпечує підвищену надійність у порівнянні з послугою без квитування. Послуги без підтвердження з'єднання зазвичай використовуються на ненадійних фізичних каналах, таких як широкосмугові мережі Wi-Fi.
- Служба, орієнтована на підтверджене з'єднання: Ця послуга встановлює логічне з'єднання між сервером і приймачем. Встановлення відбувається перед передачею будь-яких даних. Відповідно, дані передаються через встановлене логічне з'єднання. Крім того, в рамках цієї послуги кадри маркуються відповідними номерами, щоб гарантувати, що кожен з них буде отриманий тільки один раз, а також засвідчити їх належний порядок і послідовність.

На практиці канальний рівень надає мережевому рівню послуги кадрування, тобто інкапсулює передану інформацію у кадри. Останні приймаються на приймальній стороні і передаються на мережевий рівень. Крім того, канальний рівень пропонує функції адресації, що базуються на використанні апаратних адрес, які є унікальними для мережевого каналу. Такі адреси кодуються в мережевих пристроях (наприклад, комутаторах, мережевих інтерфейсних картах) їхніми OEM-виробниками (Original Equipment Manufacturer). Крім того, канальний рівень забезпечує синхронізацію відправників і одержувачів і пропонує це як послугу для мережевого рівня, тобто він запобігає необхідності мережевого рівня вирішувати проблеми синхронізації.

Вирішення проблем проектування: основні проблеми проектування канального рівня

Канальний рівень стикається з кількома проблемами при проектуванні, які можуть вплинути на загальну продуктивність мережі. Ці виклики розвивалися разом з мережевими технологіями, підкреслюючи постійну потребу в інноваціях у високопродуктивних мережах. Деякі з них включають:

- Виявлення та виправлення помилок
- Керування потоком
- Контроль доступу до середовища (MAC)
- Масштабованість
- Інтероперабельність

Виявлення та виправлення помилок

У високопродуктивних мережах підтримка цілісності даних має вирішальне значення для забезпечення надійного зв'язку та ефективної роботи. Механізми виявлення та виправлення помилок є фундаментальними для досягнення цієї мети. Оскільки дані передаються різними фізичними середовищами, вони схильні до пошкодження через шум, перешкоди та інші фактори навколишнього середовища. Тому надійні методи обробки помилок необхідні для виявлення і виправлення цих помилок, гарантуючи, що передані дані залишаються точними і надійними.

Розширені методи виявлення та виправлення помилок

Для покращення можливостей виявлення та виправлення помилок у мережах було розроблено кілька передових методів. Історично ці методи розвивалися, щоб відповідати зростаючій складності та вимогам сучасних систем зв'язку.

- Коди Хеммінга: Запроваджені Річардом Хеммінгом у 1950-х роках, коди Хеммінга - це набір кодів для виправлення помилок, які можуть виявляти до двох одночасних бітових помилок і виправляти однобітові помилки. Ці коди додають надлишкові біти до вихідних даних, що дозволяє виявляти і виправляти помилки за допомогою перевірки на парність. Коди

Хеммінга широко використовуються в системах комп'ютерної пам'яті та ранніх системах зв'язку, забезпечуючи баланс між простотою та ефективністю.

- Коди Ріда-Соломона: Це блокові коди, що виправляють помилки, які працюють шляхом передискретизації полінома, побудованого на основі даних. Розроблені в 1960 році Ірвінгом С. Рідом і Густавом Соломоном, коди Ріда-Соломона особливо ефективні для виправлення пакетних помилок, коли кілька бітів пошкоджуються послідовно. Вони широко використовуються в цифрових системах зв'язку та зберігання даних, таких як CD, DVD та QR-коди. Їх стійкість до помилок робить їх ідеальними для носіїв, які вимагають високої надійності.
- Згорткові коди: На відміну від блокових кодів, згорткові коди обробляють біти даних послідовно і використовують регістри зсуву для генерації бітів парності. Ці коди, розроблені в 1950-х і 1960-х роках, є високоефективними для виправлення помилок у реальному часі і широко використовуються в таких додатках, як мобільний зв'язок і супутниковий зв'язок. Алгоритм Вітербі, запропонований Ендрю Вітербі в 1967 році, зазвичай використовується для ефективного декодування згорткових кодів, що робить їх основними в сучасних системах зв'язку.

Таблиця 1.5 - Порівняння методів виявлення помилок

Техніка	Можливість виявлення помилок	Можливість виправлення помилок	Обчислювальна складність	Застосування
Коди Хеммінга	Однобітові та двобітові помилки	Однобітові помилки	Низький	Комп'ютерна пам'ять, ранні системи зв'язку
Коди Ріда-Соломона	Багатобітові (надлишкові) помилки	Багатобітові помилки	Помірний	Цифрове сховище, оптичні носії, QR-коди
Згорткові коди	Безперервні бітові потоки	Багатобітові помилки	Високий	Мобільний зв'язок, супутникові канали

Виявлення та виправлення помилок є невід'ємною частиною забезпечення надійності та ефективності передачі даних у високопродуктивних мережах. Використовуючи передові методи, такі як коди Хеммінга, коди Ріда-Соломона та згорткові коди, мережі можуть досягти вищого рівня цілісності даних, підтримуючи надійний та ефективний зв'язок навіть у складних умовах. З появою нових технологій ці методи обробки помилок будуть продовжувати розвиватися, задовольняючи постійно зростаючі вимоги сучасних мережевих систем.

Забезпечення ефективного управління потоком

Було розроблено кілька механізмів управління потоком для забезпечення ефективної передачі даних і запобігання перевантажень в різних умовах роботи мережі:

- Зупинка та очікування ARQ: протокол автоматичного повторного запиту (ARQ) - один з найпростіших механізмів керування потоком. У цьому методі відправник передає один кадр, а потім чекає на підтвердження від одержувача, перш ніж надсилати наступний кадр. Це гарантує, що одержувач обробляє кожен кадр перед тим, як отримати наступний, запобігаючи переповненню буфера. Однак, протокол зупинки і очікування може бути неефективним у мережах з високою затримкою, оскільки відправник витрачає значну кількість часу на очікування підтвердження.
- Протокол ковзного вікна: Протокол ковзного вікна є більш ефективним, ніж ARQ із зупинкою та очікуванням. Він дозволяє відправнику передавати декілька кадрів до того, як буде потрібне підтвердження, до певного розміру вікна. Цей розмір вікна представляє кількість непідтверджених кадрів, які можуть перебувати в дорозі. Після отримання підтверджень вікно пересувається вперед, дозволяючи надсилати нові кадри. Цей метод покращує пропускну здатність і зменшує час очікування, що робить його придатним для мереж з високою затримкою. Протокол можна тонко налаштувати, щоб збалансувати компроміс між пропускною здатністю і використанням пам'яті, регулюючи розмір вікна. Він працює в одному з

наступних двох режимів:

- Go-Back-N ARQ (автоматичний запит на повтор): У цьому режимі відправник передає пакети без необхідності чекати на пакет ACK. Кількість пакетів, які можуть бути надіслані без ACK, вказується розміром вказаного вікна (N). Якщо помилок не виявлено, і відправник відправив пакети вікна розміром N у правильному порядку, відправник повинен дочекатися підтвердження, перш ніж відправляти наступні пакети.
- Вибіркове повторення ARQ: Цей режим зосереджений на повторній передачі потенційно пошкоджених або втрачених даних. Передача даних від відправника до одержувача відбувається безперервно і не обмежується жодним вікном. Відправник повторно передає лише ті кадри, які не були підтверджені. Отже, цей режим зазвичай призводить до меншої кількості ретрансляцій і більшої пропускної здатності, ніж попередній.
- Алгоритм «дірявого відра»: Алгоритм «дірявого відра» - це механізм формування трафіку, який контролює потік даних у мережі зі сталою швидкістю. Він працює шляхом буферизації вхідних даних і вивільнення їх з постійною швидкістю, незалежно від інтенсивності вхідного трафіку. Аналогія з дірявим відром допомагає зрозуміти цей механізм: дані надходять у відро з різною швидкістю, але витікають з нього з фіксованою швидкістю. Це допомагає згладжувати сплески трафіку і підтримувати постійний потік даних, що особливо корисно для запобігання перевантаженню мережі в середовищах зі змінним навантаженням.

Приклади та аналіз ефективності

- Stop-and-Wait ARQ у мережах з низькою затримкою: У локальній мережі (LAN) з мінімальною затримкою протокол зупинено-очікувального ARQ може працювати адекватно. Оскільки час передачі підтверджень в обидва кінці невеликий, відправник не відчуває значних простоїв, а простота протоколу забезпечує мінімальні накладні витрати.
- Протокол ковзного вікна в глобальних мережах (WAN): Для середовищ з високою затримкою, таких як глобальні мережі, протокол

ковзного вікна пропонує значні покращення продуктивності порівняно з ARQ із зупинкою та очікуванням. Дозволяючи декільком кадрам перебувати в дорозі, протокол зберігає мережеву трубу заповненою, максимізуючи пропускну здатність. Наприклад, у системі супутникового зв'язку з великим часом передачі даних в обидва кінці, відповідне налаштування розміру вікна може допомогти підтримувати високу швидкість передачі даних, не перевантажуючи приймач.

- Алгоритм «дірявого відра» в умовах змінного трафіку: Алгоритм «дірявого відра» особливо ефективний у мережах з мінливим трафіком, наприклад, у мережах інтернет-провайдерів. Згладжуючи сплески даних і підтримуючи постійний потік, він допомагає запобігти раптовим сплескам трафіку, що спричиняють затори. Наприклад, під час пікових навантажень алгоритм leaky bucket може ефективніше керувати потоком даних, забезпечуючи стабільну якість обслуговування користувачів.

Розуміння та впровадження цих механізмів управління потоком є важливими для мережевих інженерів, щоб забезпечити ефективну та надійну передачу даних, адаптовану до конкретних умов та вимог їхніх мереж.

Контроль доступу до середовища (MAC) - це важливий компонент мережі, який керує передачею пакетів даних через спільне середовище зв'язку. У середовищах, де кілька пристроїв повинні взаємодіяти через один канал, рівень MAC відповідає за регулювання доступу, щоб уникнути колізій і забезпечити ефективне використання середовища. Цей рівень знаходиться на канальному рівні моделі OSI і відіграє життєво важливу роль у координації процесу передачі даних.

Для ефективної комунікації в мережевих середовищах спільного користування необхідно вирішити кілька проблем:

- Зіткнення: Коли два або більше пристроїв намагаються одночасно надсилати дані по одному каналу, виникає колізія, що призводить до пошкодження даних. Ефективні MAC-протоколи мають важливе значення для виявлення та пом'якшення колізій для збереження цілісності даних.

- Конкуренція: Це відбувається, коли кілька пристроїв конкурують за доступ до середовища зв'язку. Належне управління конкуренцією допомагає уникнути затримок і забезпечити справедливий доступ для всіх пристроїв.
- Розподіл каналів: Ефективний розподіл каналів між численними пристроями є складним завданням. Рівень MAC повинен динамічно розподіляти канали, щоб максимізувати пропускну здатність і мінімізувати перешкоди.

Для вирішення цих проблем були розроблені різні MAC-протоколи, кожен зі своїми технічними характеристиками та варіантами використання:

1. CSMA/CD (множинний доступ з визначенням несучої та виявленням колізій)

Технічні характеристики: Пристрої прослуховують мережу перед передачею. Якщо середовище вільне, вони передають дані. Якщо виявлено колізію, пристрої припиняють передачу, чекають випадковий проміжок часу, а потім повторюють спробу.

Застосування: Широко використовується в традиційних мережах Ethernet.

2. CSMA/CA (множинний доступ зі збереженням несучої та уникненням колізій)

Технічні характеристики: Пристрої прослуховують мережу перед передачею і використовують підтвердження для підтвердження успішної передачі. Цей протокол мінімізує колізії за рахунок використання алгоритму резервування і є особливо ефективним у бездротових мережах, де колізії важче виявити.

Застосування: Стандарт в мережах Wi-Fi (IEEE 802.11).

3. Передача токенів

Технічні характеристики: Токен циркулює по мережі, і тільки пристрій, що має токен, може передавати дані. Цей метод усуває колізії і забезпечує організований доступ до середовища.

Застосування: Використовується в мережах токен-кілець та деяких

промислових мережевих протоколах, таких як ARCNET.

Ефективний контроль доступу до середовища має важливе значення для забезпечення надійного та ефективного зв'язку в загальному мережевому середовищі. Розуміючи та впроваджуючи відповідні MAC-протоколи, мережеві інженери можуть подолати проблеми, пов'язані з колізіями, суперечками та розподілом каналів, тим самим підвищуючи продуктивність та стабільність мережі.

Швидкий розвиток мережевих технологій призвів до значного прогресу у вирішенні питань проектування канального рівня. Ці інновації є результатом передових досліджень і розробок нових алгоритмів, апаратних реалізацій і галузевих стандартів, кожен з яких сприяє підвищенню надійності сучасних мереж.

Дві помітні інновації у виявленні та виправленні помилок - це коди LDPC (Low-Density Parity-Check-Check - перевірка на парність низької щільності) та турбо-коди:

- LDPC-коди: Коди LDPC - це високоефективні коди для виправлення помилок, які забезпечують продуктивність, близьку до пропускної здатності. Вони широко використовуються в таких додатках, як цифрове телебачення, стандарти бездротового зв'язку (наприклад, 5G) і системи зберігання даних. Ці коди використовують розріджені матриці для створення довгих кодових слів, що забезпечує надійне виявлення та виправлення помилок з відносно низькою обчислювальною складністю. Впровадження LDPC-кодів у сучасних системах значно підвищило надійність та ефективність передачі даних.
- Турбо-коди: Турбо-коди - це ще один потужний клас кодів, що виправляють помилки, відомий своєю високою продуктивністю. Вони поєднують два або більше згорткових кодів з інтерлейвером для покращення можливостей виправлення помилок. Турбо-коди широко використовуються в глибокому космічному зв'язку, 4G LTE та інших системах бездротового зв'язку. Їх здатність наближатися до межі Шеннона - теоретичної

максимальної ефективності виправлення помилок - робить їх критично важливим компонентом у досягненні високої швидкості передачі даних і низького рівня помилок.

Вирішення ширших проблем: масштабованість та сумісність

Оскільки мережеві середовища стають дедалі складнішими, виникають ширші проблеми, такі як масштабованість та інтероперабельність, що впливають на ефективність проектування канального рівня. Ці виклики виходять за рамки конкретних технічних питань і вимагають комплексного підходу.

Масштабованість є критично важливою проблемою для канального рівня, особливо в міру того, як мережі збільшуються в розмірах і ускладнюються. Зі збільшенням кількості пристроїв, що підключаються, і зростанням трафіку даних канальний рівень повинен ефективно керувати цим зростанням для підтримання оптимальної продуктивності. Історичний розвиток інтернету створює фон для цих викликів. Перші мережі, такі як ARPANET, повинні були швидко адаптуватися, оскільки кількість підключених пристроїв зростала в геометричній прогресії, що призвело до створення більш надійних протоколів та ієрархічних мережевих структур.

- Проблеми масштабування: Однією з головних проблем є збільшення кількості пристроїв, які повинні одночасно обмінюватися даними. Це вимагає від канального рівня обробки більших обсягів трафіку і більш складних моделей зв'язку без шкоди для швидкості і надійності. Крім того, мережеві топології стають все більш динамічними, пристрої часто підключаються до мережі і відключаються від неї, що може призвести до перенапруження пропускної здатності канального рівня. Реальні приклади включають різке зростання кількості пристроїв Інтернету речей, що вимагає від мереж підтримки мільйонів одночасних з'єднань.
- Ієрархічний дизайн: Це передбачає структурування мережі на шари або рівні, де кожен рівень керує підмножиною пристроїв. Це зменшує навантаження на окремі вузли і підвищує загальну ефективність мережі.

Наприклад, ієрархічна структура стільникових мереж дозволяє ефективно керувати великими базами користувачів.

- Розподілені протоколи: Ці протоколи забезпечують децентралізоване управління мережевими ресурсами, що дозволяє мережі більш ефективно масштабуватися. Приклади включають алгоритми розподіленого планування та методи балансування навантаження, які рівномірно розподіляють трафік по мережі. Такі технології, як блокчейн, також пропонують децентралізовані рішення, які можуть підвищити масштабованість певних мережевих додатків.

1.4 Висновки до розділу 1

У першому розділі дипломної роботи було проведено глибокий теоретичний аналіз архітектури, протоколів та особливостей функціонування фізичного та канального рівнів мереж Інтернету речей (IoT).

У пункті 1.1 розглянуто багаторівневу архітектуру IoT-систем, зокрема описано шість ключових рівнів: фізичний/пристрійний, мережевий, рівень даних/бази даних, рівень аналітики/візуалізації, рівень додатків/інтеграції та рівень безпеки і управління. Детально представлено взаємодію компонентів архітектури IoT, що створює основу для розуміння ролі фізичного та канального рівнів у загальній структурі системи.

У пункті 1.2 здійснено огляд сучасних протоколів і технологій фізичного та канального рівнів, які застосовуються у практичних IoT-системах. Проведено докладний аналіз таких технологій, як Ethernet, Bluetooth Low Energy (BLE), Wi-Fi, Wi-Fi Direct, WPA/WPA2/WPA3, із наведенням технічних характеристик, архітектурних особливостей та сценаріїв використання. Було підкреслено важливість вибору відповідної технології залежно від вимог до енергоспоживання, швидкості, дальності та безпеки передачі даних.

У пункті 1.3 розглянуто основні виклики та обмеження технологій фізичного та канального рівнів. Окрему увагу приділено питанням безпеки

фізичного рівня (PLS), зокрема розглянуто такі методи, як введення штучного шуму, компресійне зондування, перекидання бітів, кооперативна таємниця, шифрування фізичного рівня та новітні підходи до забезпечення стійкості каналів зв’язку. Також детально проаналізовано функціонування канального рівня — управління доступом до середовища, контроль помилок, управління потоком та масштабованість у великих IoT-мережах.

Таким чином, перший розділ заклав ґрунтовну теоретичну основу для подальшого аналізу практичних аспектів побудови IoT-мереж, які розглядаються у наступних розділах. Отримані теоретичні висновки дозволяють зрозуміти специфіку роботи фізичного та канального рівнів у різних IoT-сценаріях і слугують базою для розробки практичних рекомендацій щодо вибору відповідних технологій у розділі 3.

2 АНАЛІЗ ТЕХНОЛОГІЙ ТА ПРОТОКОЛІВ КАНАЛЬНОГО ТА ФІЗИЧНОГО РІВНЯ ІОТ

2.1 Технології та стандарти фізичного рівня

Фізичний рівень мереж Інтернету речей (IoT) відповідає за передачу бітів інформації через середовище передачі — дротове або бездротове. У контексті IoT найбільш поширеними є бездротові технології, які забезпечують енергоефективну та далекодійну комунікацію між пристроями. Одним із ключових напрямів фізичного рівня є технології LPWAN (Low Power Wide Area Network), до яких належать NB-IoT, LoRaWAN та Sigfox. Їх популярність пояснюється здатністю забезпечувати зв’язок на великі відстані при низькому енергоспоживанні, що є критично важливим для автономних пристроїв з живленням від батарей.

NB-IoT

NB-IoT (Narrowband Internet of Things) - це технологія на основі стільникового зв'язку, яка використовує низькочастотні радіохвилі для зв'язку з малопотужними пристроями.[14]

Вона працює в стільникових мережах 4G/LTE і забезпечує широкий діапазон покриття з низькою затримкою і високою надійністю.

NB-IoT підходить для додатків, які вимагають передачі даних на великі відстані, наприклад, для інтелектуального обліку або відстеження активів у міських умовах.

Технологія підтримує до 10 000 пристроїв на одну базову станцію, що робить її ідеальною для широкомасштабного розгортання.

Переваги NB-IoT[17]:

- Висока масштабованість: Поєднання низької вартості підключення пристроїв до мережі та зниження складності робить NB-IoT ідеальним рішенням для високої масштабованості.
- Економічна ефективність: NB-IoT працює з невеликими обсягами даних, що призводить до низького споживання енергії, а пристрої більшу

частину часу залишаються в режимі енергозбереження.

- Широке покриття: Високе проникнення NB-IoT в будівлі робить його ідеальним для передачі даних всередині будівель, де доступ до існуючої внутрішньої мережевої інфраструктури може бути обмежений.

Недоліки NB-IoT:

- Дані: NB-IoT пропонує нижчу швидкість передачі даних - приблизно 250 Кбіт/с на завантаження і 20 Кбіт/с на вивантаження порівняно з LTE Cat-M1, що робить його непридатним для великих проектів.
- Передача мови: Voice Over LTE (VoLTE) не підтримується NB-IoT для передачі голосу, що робить передачу голосу неможливою.
- Роумінг: На даний момент NB-IoT не підтримує роумінг, на відміну від LTE-M та Sigfox. Однак очікується, що він буде підтримуватися найближчим часом.

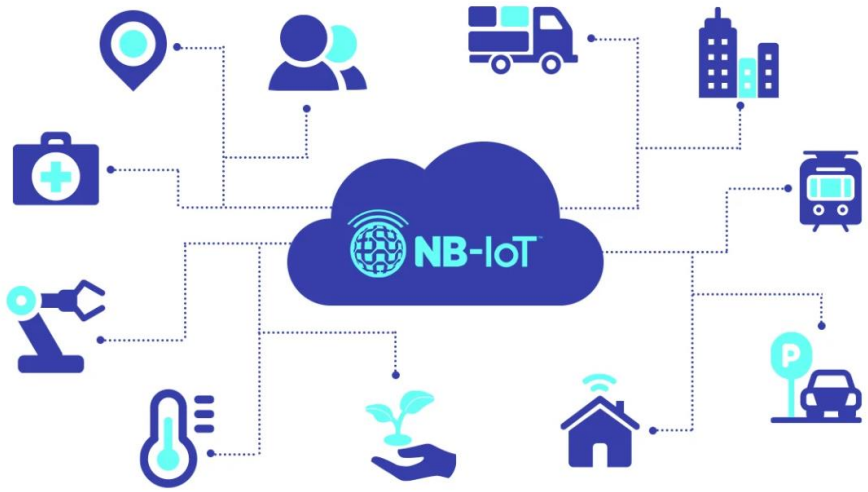

Рисунок 2.1 - Приклади застосування технології NB-IoT у різних сферах

LoRa

LoRa — це пропрієтарна бездротова технологія фізичного рівня, розроблена компанією Semtech, яка використовується для енергоефективної передачі даних на великі відстані у мережах IoT.

Вона застосовує chirp spread spectrum (CSS) — тип модуляції, яка

забезпечує високу стійкість до завад і здатність прийому слабких сигналів, що є критично важливим для сенсорних мереж з обмеженим енергоспоживанням.

LoRa підтримує адаптивне налаштування параметрів передавання[12], що дозволяє балансувати між дальністю зв'язку, енергоспоживанням і швидкістю передачі. Зокрема, параметр Spreading Factor (SF) впливає на тривалість сигналу: чим вищий SF, тим більша дальність передачі, але нижча швидкість. Bandwidth (ширина смуги) може становити 125, 250 або 500 кГц, впливаючи на загальну пропускну здатність каналу. Крім того, Coding Rate забезпечує виявлення і корекцію помилок, змінюючись у межах від 4/5 до 4/8 для підвищення надійності зв'язку.

Оскільки LoRa реалізує лише фізичний рівень і відповідає за модуляцію та передачу сигналів, для створення повноцінної IoT-мережі необхідна надбудова у вигляді LoRaWAN. Цей протокол додає канальний рівень (MAC), забезпечує адресацію пристроїв, шифрування трафіку для безпеки, а також визначає архітектуру мережі, яка включає пристрої-клієнти, шлюзи (gateways), мережеві сервери та сервери додатків. Завдяки такій модульній структурі LoRa та LoRaWAN дозволяють будувати масштабовані, енергоефективні IoT-системи з великою зоною покриття.

Переваги LoRa:

- Низьке енергоспоживання – пристрої можуть працювати на батареї кілька років без підзарядки.
- Велика дальність зв'язку – до 15 км у сільській місцевості та 2–5 км у місті.
- Стійкість до завад – завдяки модуляції chirp spread spectrum LoRa може працювати в шумному середовищі.
- Висока чутливість приймача – здатна приймати сигнали навіть на рівні -137 dBm.
- Робота в незастережених діапазонах ISM – не потребує ліцензії на частоти, що зменшує витрати на розгортання.
- Гнучкість конфігурації – можливість адаптації параметрів зв'язку

для оптимізації за енергією, дальністю або швидкістю.

- Проста архітектура – використання мережевих шлюзів і центрального сервера дозволяє легко масштабувати мережу.

Недоліки LoRa:

- Низька швидкість передачі даних – максимум до 50 Кбіт/с, що обмежує обсяги інформації.
- Висока затримка – не підходить для застосунків із вимогами до реального часу.
- Непридатна для великого трафіку – неефективна для передачі великих пакетів або потоків даних.
- Необхідність використання LoRaWAN для повноцінної мережі – LoRa сам по собі не забезпечує логіку мережі.
- Потенційні колізії при великій кількості пристроїв – у мережах із багатьма вузлами можуть виникати конфлікти через просту схему доступу (ALOHA).
- Обмежена надійність у щільних міських середовищах – перешкоди багатошляхове затухання можуть впливати на якість сигналу.

Рисунок 2.2 - Приклад побудови мережі LoRaWAN для моніторингу сенсорів

Sigfox

Sigfox - ще один протокол LPWA. Він використовує неліцензійні ISM-діапазони для зв'язку між пристроями та шлюзами, розташованими в різних регіонах або містах.[8]

Він призначений для підтримки зв'язку на великі відстані з низьким енергоспоживанням. Це робить його ідеальним для таких застосувань, як відстеження активів або віддалений моніторинг у сільській місцевості.

На відміну від інших технологій, Sigfox не вимагає додаткової апаратної інфраструктури, такої як антени або ретранслятори.

Це робить його привабливим вибором для підприємств, які прагнуть розгорнути великомасштабні мережі Інтернету речей швидко та економічно ефективно.

Переваги Sigfox:

- Має низьке енергоспоживання: Ідеально підходить для простих пристроїв, які передають дані нечасто, оскільки може передавати невеликі обсяги даних у повільному темпі.
- Забезпечує широке покриття в тих районах, де є. Простий в налаштуванні, не потребує кабелів чи складних процедур встановлення.
- Він простий в налаштуванні і не вимагає кабелів або складних процедур встановлення.
- Sigfox може значно зменшити споживання енергії та витрати, пов'язані з підключеними пристроями.
- Ця платформа ідеально підходить для малопотужних додатків, які передають невеликі обсяги даних через нерегулярні проміжки часу на великі відстані.

Недоліки Sigfox:

- Він розгорнутий не скрізь, тому наразі не буде працювати для великої кількості випадків використання.
- Зв'язок краще направляти вгору від кінцевої точки до базової станції. Вона має двонаправлену функціональність, але її пропускна здатність від

базової станції до кінцевої точки обмежена, і ви матимете менший бюджет на канал зв'язку, якщо він буде спрямований вниз, ніж вгору.

- З пристроями Sigfox складно забезпечити мобільність.

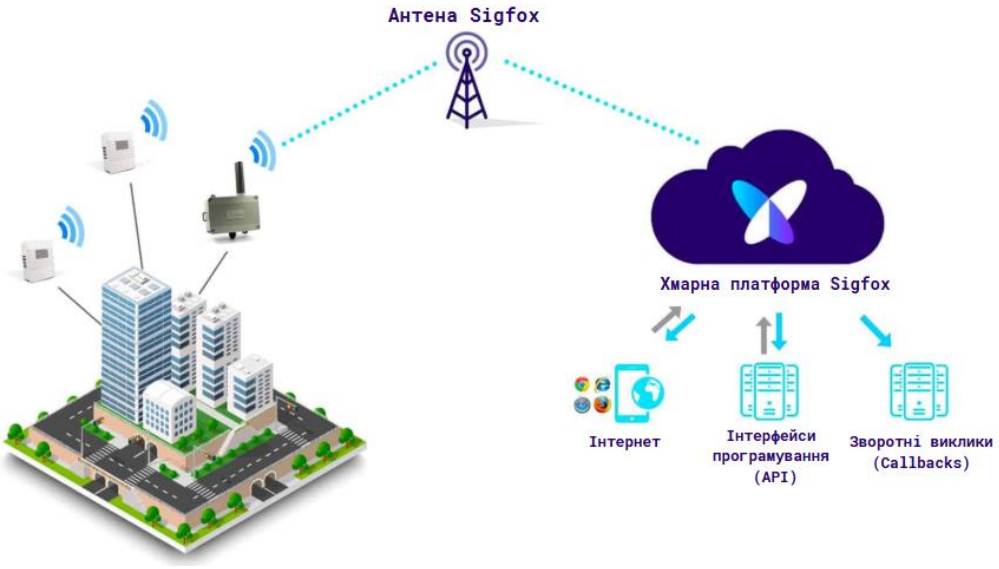

Рисунок 2.3 - Архітектура мережі Sigfox для міських IoT-систем[9]

Вибір між технологіями NB-IoT, LoRaWAN та Sigfox повинен базуватися на специфіці бізнес-завдань та характеристиках цільових IoT-додатків. Оскільки кожна з цих технологій має власні переваги та обмеження, доцільно здійснити комплексну оцінку технічних і функціональних вимог перед прийняттям рішення щодо впровадження.

Таблиця 2.1 - Порівняння фізичних протоколів IoT

Параметр	NB-IoT	LoRa	Sigfox
Покриття (Coverage)	+20 дБ порівняно з LTE, до 22 км	До 15 км у сільській місцевості, 2–5 км у місті	Менше ніж 17 км
Частотний спектр	LTE: вбудований (In-band), захисний (Guard band), окремий (Standalone)	Неліцензований ISM спектр: 868 МГц (Європа), 915 МГц (США)	Неліцензований спектр

Продовження таблиці 2.1

Смуга сигналу (Signal Bandwidth)	180 кГц	125, 250 або 500 кГц	0,1 кГц
Швидкість передачі (Data Rate)	200 кбіт/с	0.3 – 50 кбіт/с залежно від SF і Bandwidth	100 біт/с
Термін служби батареї	10 років	10 років (при енергозберігаючому налаштуванні)	10 років

Підсумуючи, якщо необхідна надійна мережа з широким діапазоном покриття, але при цьому передбачається використання додаткової апаратної інфраструктури, доцільним варіантом є використання NB-IoT. У випадках, коли пріоритетом є простота розгортання та мінімальні витрати на обладнання, доцільніше розглядати Sigfox. Вибір технології має ґрунтуватися на конкретних вимогах проєкту та попередньому аналізі умов впровадження.

2.2 Технології та протоколи канального рівня

Канальний рівень відіграє ключову роль в архітектурі мереж Інтернету речей, оскільки відповідає за встановлення та підтримку надійного з'єднання між фізичними пристроями, керування доступом до середовища передавання, виявлення та виправлення помилок, а також фрагментацію кадрів.

Далі ми проаналізуємо найпоширеніші технології та протоколи канального рівня, які використовуються в IoT-рішеннях:

IEEE 802.15.4 MAC

Протокол Medium Access Control (MAC) у стандарті IEEE 802.15.4 визначає правила доступу пристроїв до бездротового середовища, формат кадрів, адресацію, виявлення колізій та механізми управління енергоспоживанням.[10]

MAC-рівень працює поверх фізичного рівня, який у цьому стандарті

використовує частоти 868 МГц (Європа), 915 МГц (США) та 2,4 ГГц (глобально).

MAC-рівень стандарту IEEE 802.15.4 виконує ключові функції керування доступом до бездротового середовища, що дозволяє забезпечити ефективну та енергоощадну роботу IoT-пристроїв. Він підтримує два режими доступу: beacon-enabled, де координатор періодично розсилає маяки (beacons) і визначає структуру суперфрейму, та non-beacon mode, в якому використовується несинхронізований алгоритм CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). У цьому режимі пристрій спочатку "прослуховує" ефір: якщо він вільний — відбувається передача, якщо зайнятий — пристрій чекає випадковий інтервал часу (backoff). Передача даних відбувається через чотири типи MAC-кадрів: data, acknowledgment, command та beacon, а адресація може бути 16- або 64-бітною, що дозволяє масштабувати мережу до тисяч пристроїв.

Протокол також реалізує механізми енергозбереження, зокрема можливість переходу пристроїв у "сплячий" режим і передачу даних лише в активні часові слоти при beacon-синхронізації. Для забезпечення безпеки MAC-рівень підтримує шифрування за алгоритмом AES-128, автентифікацію пристроїв та перевірку цілісності кадрів. Завдяки такій структурі IEEE 802.15.4 MAC забезпечує ефективну взаємодію IoT-пристроїв у мережах з низьким енергоспоживанням, надаючи гнучкі інструменти керування трафіком і захисту даних.

Переваги IEEE 802.15.4 MAC:

- Низьке енергоспоживання – завдяки сплячим режимам і ефективному доступу до середовища.
- Підтримка великої кількості вузлів – до 65 000 пристроїв у мережі завдяки 16- та 64-бітній адресації.
- Можливість роботи в двох режимах – beacon та non-beacon, що дозволяє адаптувати мережу до різних сценаріїв.
- Підтримка топологій mesh, зірка, peer-to-peer – гнучкість побудови

мереж.

- Інтегрована підтримка безпеки – MAC-контроль шифрування і цілісності.
- Широке використання – використовується як основа в Zigbee, Thread, 6LoWPAN тощо.

Недоліки IEEE 802.15.4 MAC:

- Низька пропускна здатність – до 250 Кбіт/с, що обмежує сценарії з великою кількістю трафіку.
- Обмежена надійність у режимі non-beacon – складніше контролювати колізії без централізованого розкладу.
- Складність реалізації beacon-mode – вимагає синхронізації, що може бути складним у великих мережах.
- Необхідність надбудов для повноцінного мережевого стеку – сам IEEE 802.15.4 MAC не забезпечує повної мережевої логіки (тому використовуються Zigbee, Thread тощо).
- Обмежена дальність – порівняно з LoRa чи NB-IoT, дальність передавання вища лише в рамках кімнати чи будівлі.

LoRaWAN

LoRaWAN (Long Range Wide Area Network) — це відкритий протокол, розроблений LoRa Alliance, який визначає правила побудови енергоефективних, довготривалих бездротових мереж IoT з великою площею покриття.[12] На відміну від LoRa, який відповідає лише за фізичний рівень (модуляцію сигналу), LoRaWAN реалізує канальний рівень (MAC): керує доступом до середовища, адресацією пристроїв, автентифікацією та організацією мережі.

Протокол LoRaWAN реалізує канальний рівень у мережах Інтернету речей, визначаючи правила обміну даними між пристроями та центральним сервером через проміжні шлюзи. Він побудований за зіркоподібною архітектурою: сенсорні вузли передають повідомлення до найближчих gateway, які далі передають дані до мережевого сервера через IP-мережу.

LoRaWAN підтримує три класи пристроїв (A, B, C), що дозволяє збалансувати між енергоспоживанням і затримками. Найекономніший — клас A — відкриває приймальні вікна лише після передачі, у той час як клас C забезпечує постійний прийом, але витрачає більше енергії. Доступ до середовища організовано за принципом ALOHA — без потреби в синхронізації, що спрощує реалізацію, але водночас збільшує ризик колізій у навантажених мережах.

Кожен пристрій має унікальний ідентифікатор (DevEUI) і проходить процедуру приєднання до мережі (Join), під час якої формуються ключі безпеки. LoRaWAN забезпечує високий рівень захисту даних завдяки двошаровій криптографії — окремі ключі використовуються для автентифікації у мережі та шифрування даних на рівні застосунку. Крім того, протокол підтримує адаптивну зміну параметрів передавання (Spreading Factor) через механізм ADR (Adaptive Data Rate), що дозволяє оптимізувати зв’язок залежно від умов середовища та навантаження. Завдяки цим функціям LoRaWAN забезпечує масштабовану, енергоефективну та безпечну платформу для IoT-рішень із великою зоною покриття.

Переваги LoRaWAN:

- Дуже низьке енергоспоживання – особливо у класі A, дозволяє пристроям працювати до 10 років на батареї.
- Велика дальність передачі – до 15 км у відкритому просторі.
- Робота в незастережених діапазонах ISM – немає витрат на ліцензування частот.
- Підтримка масштабованих мереж – завдяки централізованому мережевому серверу та використанню gateway.
- Гнучкість пристроїв (класи A, B, C) – дає змогу балансувати між енергоефективністю і затримками.
- Вбудована безпека – двошарова криптографія з ключами для мережі й застосунку.
- Підходить для широкого спектра IoT-застосунків – смарт-міста,

агронагляд, лічильники, екологічний моніторинг.

Недоліки LoRaWAN:

- Обмежена пропускна здатність – максимум 50 Кбіт/с, не підходить для відео чи великих даних.
- Висока затримка (latency) – через ALOHA-доступ і асинхронну передачу.
- Можливість колізій при великій кількості пристроїв – особливо без використання ADR.
- Залежність від центрального сервера – точка відмови в архітектурі.
- Немає гарантії доставки – немає вбудованого механізму підтвердження (ack) для кожного кадру за замовчуванням.
- Потребує LoRa-сумісного обладнання – шлюзи, модулі, сервіси.

Wi-Fi MAC (IEEE 802.11 MAC)

Wi-Fi MAC — це частина стандарту IEEE 802.11, яка реалізує канальний рівень бездротової локальної мережі. Вона забезпечує управління з’єднанням, доступом до бездротового середовища, передачу та прийом кадрів, контроль помилок і базову безпеку. На відміну від Ethernet (який використовує CSMA/CD), Wi-Fi працює з CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), оскільки в бездротовому середовищі колізії не можна виявити напряму.

Wi-Fi MAC (IEEE 802.11) забезпечує ключові функції доступу до бездротового середовища, використовуючи алгоритм CSMA/CA для уникнення колізій. Перед передачею даних пристрій прослуховує ефір: якщо він вільний, ініціюється передача; якщо зайнятий — застосовується механізм випадкової затримки (backoff). Основним механізмом доступу є DCF, який працює децентралізовано, хоча також передбачено централізований режим PCF із плануванням трафіку, однак останній використовується рідко. MAC-рівень керує встановленням з'єднань, автентифікацією та асоціацією пристроїв, передачею службових Beacon-кадрів і підтримкою стабільного з'єднання між клієнтами та точкою доступу.

Крім того, MAC-протокол у Wi-Fi відповідає за фрагментацію, агрегацію, повторну передачу кадрів, виявлення дублікатів і контроль послідовності. Він реалізує базову безпеку — спочатку через застарілий WEP, а згодом через WPA/WPA2/WPA3, які працюють у тісному зв’язку з вищими рівнями. Wi-Fi MAC забезпечує як унікаст, так і широкомовну передачу, підтримує QoS (у стандарті 802.11e), а також дозволяє динамічну зміну швидкості залежно від якості каналу. Завдяки гнучкості й масштабованості цей протокол став основою більшості сучасних бездротових локальних мереж.

Переваги Wi-Fi MAC:

- Висока швидкість передачі даних – до 9,6 Гбіт/с (Wi-Fi 6)
- Гнучкість – підтримка різних типів трафіку (реальний час, фонова передача)
- Широка підтримка пристроями – стандартизована технологія з глобальним поширенням
- Підтримка мобільності – можливість плавного переходу між точками доступу (roaming)
- QoS та приоритезація трафіку – для VoIP, відео, критичних даних (802.11e)
- Вбудована безпека – WPA3 та аутентифікація EAP

Недоліки Wi-Fi MAC:

- Високе енергоспоживання – у порівнянні з LPWAN або BLE
- Низька ефективність у навантажених мережах – CSMA/CA може призводити до затримок і колізій
- Обмежена дальність дії – зазвичай до 100 метрів
- Перешкоди у бездротовому середовищі – вплив інших мереж, пристроїв, об'єктів
- Складність управління великими мережами – потребує налаштування контролерів, VLAN, безпечного роумінгу
- Низька надійність у реальному часі – нестабільна затримка в середовищі з багатьма користувачами

Bluetooth MAC

Bluetooth MAC (Medium Access Control) — це частина протоколу Bluetooth, яка визначає, як пристрої встановлюють з’єднання, синхронізуються, обмінюються кадрами, керують черговістю передавання і забезпечують логіку взаємодії на рівні "мастер-підлеглий" або в mesh-мережах (BLE 5.0+). Вона працює поверх фізичного рівня (PHY), що використовує частоти в ISM-діапазоні 2.4 ГГц.[6]

MAC-рівень Bluetooth відповідає за встановлення з’єднань між пристроями, обмін службовими кадрами та управління доступом до каналу за допомогою TDMA-таймінгу.[11] Класична модель передбачає фіксовану ієрархію: один пристрій (master) ініціює і контролює зв’язок з підлеглими (slave). У BLE моделі реалізовано також асинхронну модель передачі, де пристрої передають "рекламні пакети" (advertising), на які сканери відповідають запитами про з'єднання. Після встановлення зв’язку MAC-рівень координує передачу даних у фіксованих часових слотах, уникаючи колізій.

Також Bluetooth MAC забезпечує частотне перестрибування (FHSS) — техніку, що підвищує стійкість сигналу до завад. Формат кадру містить службові поля, CRC та адресацію.[13] MAC-рівень виконує енергозберігаючі функції, дозволяючи пристроям переходити в неактивні стани, що особливо важливо для сенсорів і носимих пристроїв. Починаючи з BLE 5.0, MAC підтримує mesh-мережі, де всі вузли рівноправні, що дозволяє масштабувати IoT-мережі на основі Bluetooth без необхідності постійної участі центрального вузла.

Переваги Bluetooth MAC:

- Низьке енергоспоживання (BLE) – ідеально підходить для живлення від батарей
- Часовий поділ доступу (TDMA) – гарантує відсутність колізій
- Частотне перестрибування (FHSS) – висока стійкість до завад
- Глобальна підтримка – всі смартфони, більшість мікроконтролерів мають Bluetooth

- Підтримка mesh-топології – з BLE 5.0 можливе створення розгалужених IoT-мереж
- Простота реалізації – багато мікросхем мають вбудовану MAC-реалізацію

Недоліки Bluetooth MAC:

- Обмежена дальність – до 10–100 м (BLE), хоча BLE 5.0 може більше
- Обмежена кількість з’єднань у Classic Bluetooth – максимум 7 slave-пристроїв на master
- Низька швидкість у BLE – від 125 Кбіт/с до 2 Мбіт/с, але зменшення швидкості збільшує дальність
- Не підходить для великих пакетів даних – краще для періодичних коротких повідомлень
- Залежність від середовища – ефективність роботи погіршується в багатоповерхових приміщеннях
- Classic Bluetooth має вищу затримку і більше енергоспоживання – порівняно з BLE

У контексті мереж Інтернету речей ефективність обміну даними значною мірою залежить від протоколів канального рівня, які регулюють доступ до середовища, формат кадрів, управління енергоспоживанням і безпекою. У таблиці 2.2 наведено порівняння розглянутих вище протоколів, які використовуються у сучасних IoT-системах.

Таблиця 2.2 - Порівняння канальних протоколів IoT

Параметр	IEEE 802.15.4 (Zigbee, Thread)	LoRaWAN	Wi-Fi MAC (IEEE 802.11)	Bluetooth MAC (BLE)
Тип доступу до середовища	CSMA/CA (в non-beacon), TDMA (у beacon-режимі)	ALOHA (асинхронний доступ)	CSMA/CA (DCF), іноді PCF	TDMA (тайм-слоти), FHSS

Продовження таблиці 2.2

Архітектура мережі	Зірка, mesh, peer-to-peer	Зірка через шлюзи (gateway), star-of-stars	Інфраструктурна (з точкою доступу)	Зірка (BLE), Mesh (BLE 5.0+)
Класи енергоспоживання / режим	Перехід у сплячий режим, передача в активних слотах	Класи A, B, C (енергозбереження залежно від класу)	Постійна активність або режим енергозбереження (Wi-Fi HaLow)	Рекламний режим, періодична активність, сплячий режим
Швидкість обробки кадрів	До 250 Кбіт/с	До 50 Кбіт/с	До 9.6 Гбіт/с (Wi-Fi 6)	До 2 Мбіт/с (BLE 5.0)
Безпека	AES-128, контроль цілісності та автентифікація	Двошарове шифрування (Network + Application Session Keys)	WPA2, WPA3, 802.1X	AES-CCM, pairing, authentication
Складність реалізації	Середня, потребує синхронізації для beacon-режиму	Висока (потрібен мережевий сервер, gateway)	Висока, складна інфраструктура та управління	Низька, реалізовано у багатьох чипах
Підтримка IoT-застосувань	Сенсорні мережі, автоматизація, розумні будівлі	Смарт-міста, лічильники, агронагляд	Відеоспостереження, VoIP, промислова автоматизація	Фітнес-браслети, трекери, побутові сенсори

Отже, зведене порівняння канальних протоколів IoT демонструє, що кожна технологія має власний баланс між енергоспоживанням, швидкістю передачі, дальністю зв’язку та складністю реалізації. LoRaWAN вирізняється великим покриттям і тривалим часом автономної роботи, але поступається в швидкості. IEEE 802.15.4 забезпечує гнучку топологію та помірне енергоспоживання, що робить його зручним для сенсорних мереж. Bluetooth Low Energy є лідером за енергоефективністю в короткодистанційних застосунках, а Wi-Fi надає високу швидкість обміну даними, проте потребує більше енергії та має меншу дальність. Таким чином, вибір канального протоколу має ґрунтуватися на конкретних вимогах до IoT-системи.

2.3 Порівняльний аналіз технологій та протоколів фізичного та канального рівня

Проведений аналіз показав, що технології фізичного та канального рівня в IoT-системах мають суттєві відмінності за рядом ключових параметрів: архітектурною побудовою, енергоспоживанням, пропускною здатністю, дальністю передавання сигналу, здатністю масштабуватись і вимогами до реалізації. Кожен рівень — як фізичний, так і канальний — виконує унікальні функції, але їх поєднання визначає функціональність, ефективність і надійність кінцевої IoT-мережі.

Фізичний рівень		Канальний рівень	
LoRa (Long Range Radio)	Далекобійна, малопотужна радіотехнологія. Працює на частотах 433 МГц, 868 МГц. Використання декількох частот.	LoRaWAN	Спеціалізований MAC-протокол, розроблений LoRa Alliance. Доступ до середовища передачі - проста ALOHA. Протокол включає специфікацію MAC поверх LoRa (фізичний рівень)
Sigfox	Ультранизька швидкість передачі, але велика дальність та висока енергоефективність	Пропрієтарний протокол	Доступ до середовища передачі – проста ALOHA. Довжина кадру – 12 байт Uplink; 8 байт Downlink. Переважно знаходиться у режимі сну.
NB-IoT (Narrowband IoT)	Технологія, що працює в рамках мобільних мереж LTE, спеціально розроблена для IoT.	NB-IoT MAC/RLC	Використовує адаптовані протоколи з мобільної мережі для роботи з IoT- пристроями.
Zigbee	Бездротова технологія з низьким енергоспоживанням, коротким радіусом дії	IEEE 802.15.4	Доступ до середовища передачі – CSMA/CA. Надає механізми доступу до середовища передачі (MAC).
Bluetooth Low Energy (BLE)	Адаптований Bluetooth для IoT (зниження споживання енергії)	Bluetooth MAC	Визначає процес з'єднання та передавання кадрів у BLE
Wi-Fi (IEEE 802.11)	Використовується для пристроїв з живленням від електромережі (не енергоощадний).	Wi-Fi MAC (IEEE 802.11 MAC)	MAC-рівень для Wi-Fi з розширеннями для QoS

Рисунок 2.4 - Основні технології та протоколи фізичного та канального рівня IoT[1]

На фізичному рівні основна увага приділяється характеристикам радіосигналу: модуляції, смузі частот, потужності передавача, чутливості приймача та типу спектра. LoRa, зокрема, забезпечує надзвичайно велику дальність дії — до 15 км — навіть у складних радіоумовах, завдяки використанню розширеного спектра модуляції (Chirp Spread Spectrum). Це робить її ідеальною для розподілених мереж з великою площею покриття, наприклад, у сільському господарстві або екологічному моніторингу. IEEE 802.15.4 забезпечує помірну дальність і стабільність сигналу при низькому

енергоспоживанні, що дозволяє використовувати його у побудові сенсорних мереж із високою щільністю вузлів, таких як розумні будинки або індустріальні системи. Bluetooth Low Energy (BLE) розрахований на дуже короткі відстані, але забезпечує рекордно низьке енергоспоживання, що є критично важливим для автономних пристроїв із живленням від батарей. Натомість Wi-Fi, хоча й пропонує високу пропускну здатність (до кількох гігабітів на секунду), має високе енергоспоживання та обмежене покриття, тому краще підходить для сценаріїв з наявним живленням і вимогами до швидкої передачі великих обсягів даних.

На канальному рівні (MAC) головну роль відіграє організація обміну даними між пристроями: розподіл доступу до середовища, синхронізація передавання, управління колізіями, форматування кадрів, а також безпека та адресація. LoRaWAN, як MAC-протокол для LoRa, реалізує просту модель на основі ALOHA-доступу: кожен пристрій передає дані без узгодження з іншими, що знижує складність реалізації і споживання енергії, але збільшує ймовірність колізій при зростанні кількості пристроїв. IEEE 802.15.4 MAC пропонує більш гнучкий підхід — підтримує як асинхронний CSMA/CA-доступ, так і синхронізований beacon-режим, що дозволяє досягти балансу між ефективністю та точністю синхронізації. Це робить його придатним для масштабованих мереж із передбачуваним трафіком. Bluetooth MAC (BLE) використовує TDMA-доступ у поєднанні з частотним перестрибуванням (FHSS), що гарантує мінімальні завади й високу ефективність навіть у насиченому радіоефірі, а також дозволяє реалізувати складні топології, зокрема mesh у BLE 5.0. Wi-Fi MAC, базуючись на CSMA/CA з підтримкою QoS і фрагментації кадрів, надає гнучкість для мультимедійних та високонавантажених мереж, проте не призначений для систем із обмеженими ресурсами.

Таким чином, вибір технологій і протоколів на фізичному та канальному рівнях має базуватися на пріоритетах конкретного IoT-застосування. Якщо головною вимогою є максимальна енергоефективність — найкращими

варіантами будуть BLE або LoRaWAN. Якщо необхідна висока швидкість передачі даних — варто звернутися до Wi-Fi. Для гнучких сенсорних мереж середньої складності, які потребують баланс між масштабованістю та стабільністю — доцільним є IEEE 802.15.4 у поєднанні з Zigbee або Thread. Важливо також пам’ятати, що жоден рівень не працює ізольовано: ефективна IoT-мережа — це результат вдалої інтеграції PHY і MAC, яка повинна враховувати архітектуру мережі, тип трафіку, потребу в мобільності, безпеку, а також обмеження за енергоспоживанням і пропускною здатністю.

Ретельне вивчення характеристик фізичних і канальних технологій дає змогу сформувати обґрунтовані підходи до їх застосування у різних прикладних сценаріях. Оскільки жодне технічне рішення не є універсальним, вибір відповідної комбінації протоколів залежить від конкретного середовища, типу пристроїв, обсягів передаваних даних, вимог до енергоспоживання та очікуваного терміну служби. Нижче наведено узагальнену таблицю з рекомендованими технологіями для типових задач IoT, де враховано ключові переваги кожного підходу та доцільність їх застосування у відповідних умовах.

Таблиця 2.3 - Рекомендації щодо вибору технологій для різних сценаріїв IoT

Сценарій застосування	Рекомендована технологія	Обґрунтування
Моніторинг навколишнього середовища в полі	LoRa + LoRaWAN	Велика дальність, довгий термін автономності
Розумний дім / сенсорні мережі	IEEE 802.15.4 + Zigbee / Thread	Mesh-топологія, низьке енергоспоживання
Носимі пристрої (фітнес-браслети, трекери)	BLE	Енергоощадний режим, підтримка смартфонами
Відеоспостереження, потокові дані	Wi-Fi (802.11)	Висока пропускна здатність
Промислові IoT-системи (індустрія 4.0)	IEEE 802.15.4 / Wi-Fi HaLow	Надійність, можливість побудови автономних мереж
Трекінг об’єктів у місті	NB-IoT (поза межами цієї таблиці)	Стільникове покриття, інтеграція з LTE

Оскільки фізичний та канальний рівні працюють у зв’язці, їх поєднання визначає технічні можливості, архітектуру та поведінку IoT-систем у

реальному середовищі. Саме комбінація PHY і MAC-рівнів формує готове мережеве рішення з конкретними властивостями: дальністю зв’язку, швидкістю обміну, стабільністю, енергоспоживанням та здатністю до масштабування. Нижче подано узагальнену таблицю, яка порівнює популярні комбінації фізичного та канального рівнів за ключовими технічними параметрами. Вона дозволяє швидко зорієнтуватися у перевагах кожної технології та її доцільності для різних типів IoT-сценаріїв.

Таблиця 2.4 - Порівняння комбінацій PHY + MAC у IoT

Технологія	Покриття	Швидкість	Енергоспоживання	Ключові особливості
LoRa + LoRaWAN	До 15 км	0.3 – 50 Кбіт/с	Дуже низьке	Проста архітектура, ALOHA, класи A/B/C
IEEE 802.15.4 + Zigbee	До 500 м	До 250 Кбіт/с	Низьке	Beacon/non-beacon режими, mesh-топологія
BLE (Bluetooth 5.0)	До 100 м	До 2 Мбіт/с	Дуже низьке	TDMA, FHSS, підтримка смартфонів
Wi-Fi (802.11)	До 100 м	До 9,6 Гбіт/с (Wi-Fi 6)	Високе	QoS, CSMA/CA, WPA3, роумінг

Отже, наведена таблиця демонструє, що вибір комбінації PHY + MAC протоколів має здійснюватися на основі компромісу між дальністю зв’язку, швидкістю передавання, енергоспоживанням і топологією мережі. LoRa + LoRaWAN найкраще підходить для широкомасштабних, малодинамічних IoT-систем із низькими вимогами до швидкості, тоді як Wi-Fi орієнтований на високошвидкісну передачу великих обсягів даних у локальному середовищі. IEEE 802.15.4 з Zigbee забезпечує гнучкість топології та баланс між енергозбереженням і пропускною здатністю, а BLE є ідеальним рішенням для мобільних і носимих пристроїв з обмеженим живленням. Такий порівняльний підхід дозволяє чітко зорієнтуватися у виборі технології відповідно до потреб конкретного IoT-проєкту.

2.4 Висновки до розділу 2

У другому розділі дипломної роботи було здійснено комплексний аналіз сучасних технологій і протоколів фізичного та канального рівнів, які застосовуються у різних сферах Інтернету речей. Розгляд було проведено як з точки зору технічних параметрів, так і практичної придатності до реальних IoT-сценаріїв.

У пункті 2.1 детально розглянуто найбільш актуальні технології фізичного рівня: NB-IoT, LoRa, Sigfox. Проведено глибокий аналіз їх архітектури, механізмів модуляції, параметрів передачі даних, енергоспоживання та обмежень. Підкреслено, що NB-IoT забезпечує високу надійність і проникнення сигналу у міських умовах, LoRaWAN оптимально підходить для великих розподілених систем з тривалим часом автономної роботи, а Sigfox є економічно ефективним рішенням для передачі малих обсягів даних у віддалених регіонах.

У пункті 2.2 було проаналізовано протоколи канального рівня, що забезпечують ефективний доступ до середовища передачі та управління кадрами: IEEE 802.15.4 MAC, LoRaWAN, Wi-Fi MAC, Bluetooth MAC. Для кожної технології наведено переваги і недоліки, визначено найбільш ефективні сценарії застосування. Показано, що IEEE 802.15.4 MAC дозволяє будувати енергоефективні сенсорні мережі, LoRaWAN забезпечує широке покриття, Wi-Fi MAC — високу швидкість для мультимедійного трафіку, а BLE MAC — низьке енергоспоживання для мобільних пристроїв.

У пункті 2.3 виконано порівняльний аналіз фізичних і канальних технологій у контексті практичного застосування в різних IoT-системах. Окреслено ключові критерії вибору протоколів: дальність, енергоспоживання, пропускна здатність, топологія, гнучкість масштабування. Наведені узагальнюючі таблиці дозволяють зрозуміти оптимальні комбінації PHY + MAC для різних прикладних задач — від моніторингу довкілля до промислових систем і персональних пристроїв.

У результаті проведеного аналізу сформовано обґрунтовані підходи до вибору технологій фізичного та канального рівнів, які будуть використані як база для розробки практичних рекомендацій у наступному розділі роботи. Зроблено висновок, що ефективна IoT-система неможлива без грамотної інтеграції фізичного і канального рівнів, причому вибір протоколів має чітко відповідати конкретним вимогам сценарію використання.

3 ПРАКТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ФІЗИЧНОГО ТА КАНАЛЬНОГО РІВНЯ В ІОТ

3.1 Методика дослідження та вибір тестового середовища

У рамках дослідження було обрано середовище Cisco Packet Tracer, яке є потужним інтерактивним інструментом для моделювання комп'ютерних мереж, зокрема з підтримкою технологій Інтернету речей (IoT). Починаючи з версії 7.0, Cisco Packet Tracer[17] містить функціонал для створення, налаштування та тестування віртуальних IoT-мереж, що дозволяє відтворити поведінку реальних пристроїв та їхню взаємодію у симульованому середовищі без потреби у фізичному обладнанні.

Цей інструмент надає користувачу можливість додавати до мережевої топології різноманітні смарт-пристрої, зокрема датчики руху, температури, диму, електронні замки, освітлювальні прилади, камери спостереження, елементи клімат-контролю та інші актуатори. Усі ці пристрої можуть бути з'єднані за допомогою стандартного протоколу Wi-Fi (IEEE 802.11) або через спеціальні IoT-шлюзи, які моделюють взаємодію з іншими бездротовими технологіями, такими як ZigBee чи Bluetooth (в обмеженому вигляді).

Крім того, Cisco Packet Tracer підтримує автоматизацію дій пристроїв через просту візуальну мову програмування Blockly, а також через середовище JavaScript, що дозволяє задавати складну логіку реакції пристроїв на певні події. Наприклад, у середовищі легко реалізувати сценарій: «якщо сенсор руху активовано, то ввімкнути світло й надіслати сповіщення на мобільний додаток».

Середовище також містить інструменти для моніторингу та управління пристроями: інтерфейс IoT Monitor, налаштування властивостей мережі, перегляд статусу та взаємодії об'єктів у режимі реального часу. Це робить Cisco Packet Tracer зручним не лише для вивчення архітектури IoT-систем, а й для оцінки їх поведінки в різних умовах експлуатації.

Переваги Cisco Packet Tracer у контексті даного дослідження включають:

- можливість побудови повноцінної моделі IoT-мережі без додаткового апаратного забезпечення;
- підтримку симуляції протоколів фізичного та канального рівнів (Wi-Fi, ZigBee, Ethernet);
- інтуїтивно зрозумілий графічний інтерфейс;
- доступність як навчального ресурсу в рамках програми Cisco Networking Academy.

Також варто зазначити, що Cisco Packet Tracer, на відміну від багатьох інших симуляційних середовищ (наприклад, NS-3, OMNeT++ або Cooja), має суттєві переваги в контексті навчального процесу. Він не потребує програмування «з нуля», складної компіляції чи тривалого налаштування мережевих стеків. Завдяки цьому середовище дозволяє студентам і дослідникам швидко зосередитися на логіці функціонування IoT-систем, тестуванні протоколів, оцінці взаємодії пристроїв та формуванні сценаріїв реального використання — без зайвих технічних бар’єрів.

Ще однією важливою перевагою є вбудована підтримка інтеграції рівнів OSI: у Cisco Packet Tracer можна одночасно моделювати фізичний зв’язок, логіку на канальному рівні, маршрутизацію та взаємодію з транспортними протоколами, такими як MQTT або CoAP, які працюють поверх моделі. Це забезпечує багаторівневе представлення роботи IoT-мережі, що особливо важливо для комплексного аналізу ефективності та продуктивності протоколів нижчих рівнів.

Крім того, у Packet Tracer реалізована візуалізація мережевих подій, що допомагає виявити проблеми з підключенням, конфігурацією пристроїв або затримкою реакції на події. Завдяки цьому дослідник може проводити імітаційні експерименти, змінюючи в реальному часі параметри мережі, конфігурації протоколів або логіку обробки подій.

Таблиця 3.1 - Порівняльна таблиця середовищ для симуляції IoT-мереж

Параметр / Середовище	Cisco Packet Tracer	Cooja (Contiki OS)	NS-3	OMNeT++	Tinkercad Circuits
Рівень складності	Низький	Високий	Високий	Високий	Низький
Потреба у програмуванні	Ні (Blockly / JS)	Так (C / nesC)	Так (C++)	Так (C++)	Ні (візуально)
Підтримка IoT-протоколів	Wi-Fi, ZigBee (симуляція)	6LoWPAN, RPL	6LoWPAN, UDP, MQTT	6LoWPAN, MQTT, TCP/IP	Обмежена
Сценарії «розумного будинку»	Так (вбудовано)	Так (ручна реалізація)	Так (з модулями)	Так	Частково
Графічний інтерфейс	Так	Частково	Ні	Так	Так
Рівень деталізації	Середній	Високий	Високий	Високий	Низький
Платформа	Windows, Linux	Linux, Windows	Linux, Windows	Linux, Windows	Веб-браузер

Виходячи з порівняльного аналізу, Cisco Packet Tracer є найоптимальнішим середовищем для моделювання IoT-мереж у навчальних та демонстраційних цілях, оскільки поєднує зручний графічний інтерфейс, базову підтримку протоколів фізичного та канального рівнів (Wi-Fi, ZigBee), просту логіку автоматизації без необхідності глибокого програмування, а також повну офлайн-роботу. На відміну від більш складних інструментів, таких як Cooja, NS-3 або OMNeT++, які орієнтовані на академічні дослідження з високим рівнем деталізації, Packet Tracer дозволяє швидко створювати сценарії типу «розумний будинок» та досліджувати принципи побудови IoT-мереж без потреби у спеціалізованих знаннях у сфері низькорівневого програмування чи мережевого моделювання.

З огляду на вищевикладене, Cisco Packet Tracer забезпечує найкращий баланс між функціональністю, простотою, наочністю та відповідністю освітнім цілям дослідження. Саме тому його було обрано як основне середовище для моделювання IoT-мережі в рамках даної роботи.

Модель дослідження — розумний будинок

Для реалізації практичної частини дослідження було обрано модель розумного будинку (Smart Home) як типову прикладну IoT-систему, що

дозволяє продемонструвати роботу пристроїв фізичного та канального рівнів у контексті побутового середовища.[17] Така модель є однією з найпоширеніших архітектур в IoT-мережах, оскільки передбачає взаємодію великої кількості сенсорів, виконавчих пристроїв та шлюзів, які функціонують автономно, але при цьому координуються єдиною системою керування.

У моделі розумного будинку, реалізованій у середовищі Cisco Packet Tracer, змодельовано наступну структуру:

- Інфраструктурна частина: бездротовий маршрутизатор, IoT-шлюз (Home Gateway), що забезпечує централізоване з’єднання пристроїв і передачу даних.
- Сенсори (пристрої збору даних): датчик руху (Motion Detector), датчик диму (Smoke Detector), датчик температури (Temperature Sensor).
- Актуатори (виконавчі пристрої): смарт-лампа (Smart Lamp), електронний дверний замок (Smart Door Lock), вентилятор (Smart Fan), система освітлення.
- Засоби автоматизації: інтегровані сценарії на Blockly або JavaScript, які визначають поведінку пристроїв у відповідь на певні події (наприклад, "при активації сенсора руху — увімкнути світло").

Уся система функціонує в рамках локальної мережі з використанням протоколу Wi-Fi (IEEE 802.11) як базового каналу зв’язку на фізичному та канальному рівнях. Усі пристрої підключені до одного маршрутизатора, який забезпечує бездротове покриття у межах симульованого середовища. Передача даних між пристроями та їх керування здійснюються через IoT-шлюз, який виступає аналогом центрального контролера системи.

Розумний будинок як модель дозволяє реалізувати типові сценарії взаємодії в IoT-системах, такі як:

- автоматичне вмикання освітлення при вході до приміщення;
- блокування дверей при виявленні диму або загрози;
- запуск вентилятору при підвищенні температури;
- дистанційне управління пристроями через мобільний інтерфейс

(умовно реалізований у Cisco Packet Tracer через інтерфейс "IoT Monitor").

Ця модель є зручною для тестування принципів децентралізованого керування, обробки подій на рівні пристроїв, оцінки стабільності зв’язку та реакції системи в режимі реального часу. Оскільки мережа не передбачає складної маршрутизації або великого навантаження, обрана топологія дозволяє зосередитись саме на функціонуванні фізичного та канального рівнів, які й становлять основний предмет аналізу в цій роботі.

Це дослідження дозволить краще зрозуміти, як працюють технології фізичного та канального рівня в умовах реального сценарію використання, зокрема на прикладі розумного будинку — одного з найпоширеніших і найпрактичніших застосувань Інтернету речей. Саме така модель дає змогу детально дослідити, як саме встановлюється з’єднання між пристроями, якими каналами передаються дані, як реагує система на події та як обираються протоколи зв’язку залежно від функції пристрою (сенсор, актуатор, шлюз). Модель включає різноманітні типи пристроїв, які працюють у єдиній локальній мережі, але виконують різні завдання — від моніторингу до автоматизації дій. Це дозволяє побачити, в яких умовах краще працюють ті чи інші технології (наприклад, Wi-Fi для камер, ZigBee для сенсорів, дротове з’єднання для шлюзу) та які протоколи забезпечують найкраще співвідношення між енергоспоживанням, стабільністю зв’язку і затримками передачі.

Таким чином, дослідження на прикладі розумного будинку надає практичну базу для рекомендацій щодо вибору протоколів у різних IoT-сценаріях.

3.2 Моделювання роботи мережі IoT у Cisco Packet Tracer

На рисунку 3.1 представлено концептуальну схему розумного будинку, яка була взята за основу для подальшого моделювання в середовищі Cisco Packet Tracer. Ілюстрація демонструє типовий склад IoT-інфраструктури, що

включає як сенсорні пристрої (Temperature Meter, Smoke Detector, Motion Detector), так і виконавчі елементи (Smart Lamp, Smart Fan, Smart Coffee Maker, Smart Door), а також мережеві компоненти (Home Gateway, Wireless Router, Cable Modem).

Цей приклад відображає інтегровану систему розумного середовища, в якій усі пристрої об'єднані єдиною локальною мережею, керуються централізовано через шлюз, і взаємодіють між собою на основі заданих сценаріїв. Візуалізація охоплює різні зони будинку — житлову частину, гараж, садову ділянку, басейн — і дозволяє чітко уявити, як IoT-рішення можуть бути впроваджені для забезпечення автоматизації, безпеки, енергоефективності та комфорту. Саме ця структура лягла в основу побудови та тестування симуляційної моделі в Packet Tracer, що детально описується далі у цьому розділі.

Крім того, дана візуалізація дозволяє наочно простежити розподіл ролей пристроїв у IoT-екосистемі: сенсори слугують джерелами даних про стан навколишнього середовища (температура, дим, рух), актуатори відповідають за виконання певних дій (відкривання дверей, вмикання вентилятора, освітлення), а мережеві елементи забезпечують транспорт даних та координацію подій. Особливу увагу в схемі приділено зв’язності компонентів: усі пристрої об’єднані бездротовою мережею з виходом в Інтернет через домашній шлюз, що відповідає сучасним підходам до побудови розумного будинку.[18] Така архітектура дозволяє реалізувати як локальні, так і хмарно-орієнтовані сценарії керування пристроями, що особливо актуально в умовах розвитку мереж IoT.

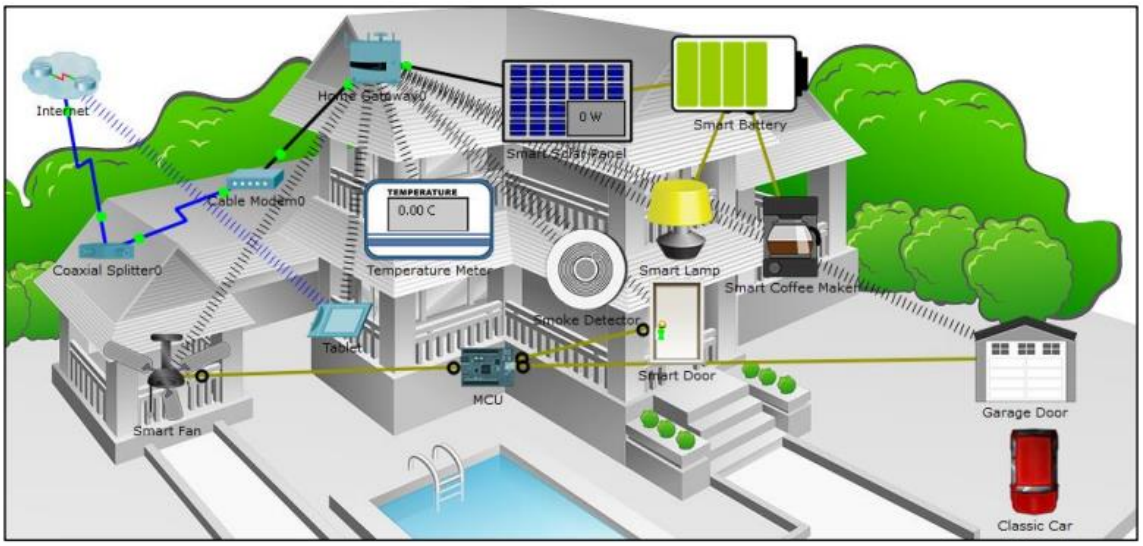

Рисунок 3.1 - Концептуальна схема «розумного будинку»

У рамках побудови симульованої IoT-мережі було використано низку віртуальних пристроїв, які доступні в бібліотеці середовища Cisco Packet Tracer. Кожен із них виконує окрему функцію в моделі розумного будинку та взаємодіє з іншими компонентами через бездротову інфраструктуру. Нижче подано опис ключових елементів моделі, їхніх логічних ролей та функціонального призначення відповідно до завдань, покладених на систему автоматизації.

Таблиця 3.2 - Опис кожного із використаних елементів

№	Тип пристрою	Назва в Packet Tracer	Функціональне призначення
1	Смарт-лампа	Smart Light	Вмикається при спрацюванні сенсора руху
2	Датчик руху	Motion Detector	Виявляє наявність руху у приміщенні
3	Смарт-замок	Smart Door Lock	Блокує або розблокує доступ до приміщення
4	Смарт-вентилятор	Smart Fan	Автоматично вмикається при підвищенні температури
5	Датчик диму	Smoke Detector	Активує тривогу при виявленні диму
6	Камера спостереження	Wireless Camera	Слідкує за приміщенням, може бути активована за подією
7	IoT-шлюз	Home Gateway	Централізований контролер усіх IoT-пристроїв
8	Маршрутизатор Wi-Fi	Wireless Router	Забезпечує бездротове підключення пристроїв до мережі

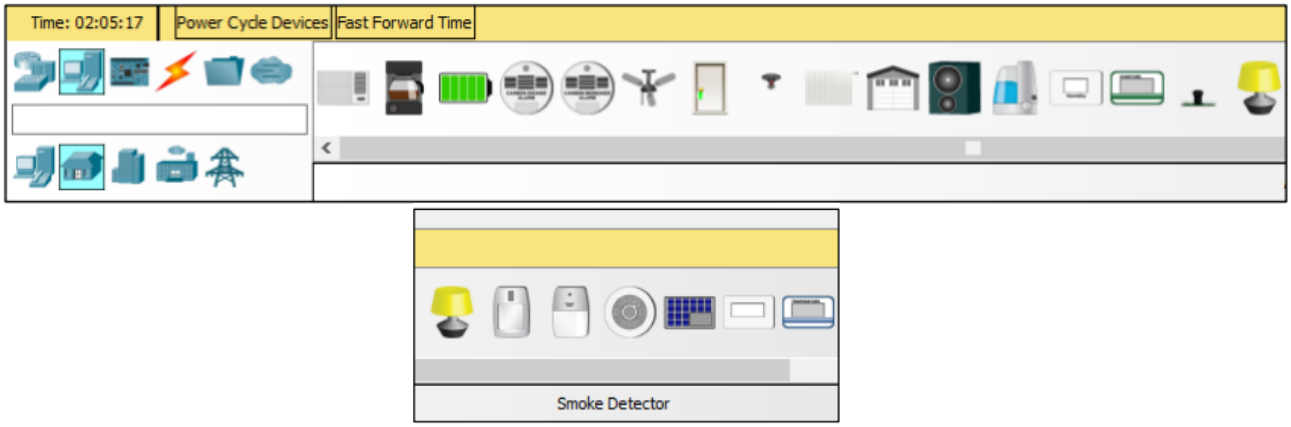

Рисунок 3.2 - Позначки елементів у Cisco Packet Tracer

Усі ці пристрої були розміщені на віртуальному полі Cisco Packet Tracer і з’єднані в одну логічну мережу з використанням бездротового з’єднання за протоколом IEEE 802.11 (Wi-Fi).

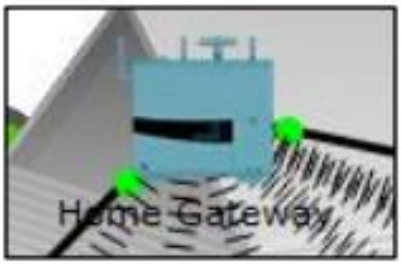

Рисунок 3.3 - Позначка елементу Home Gateway у Cisco Packet Tracer

Перед підключенням кожного пристрою необхідно виконати базову конфігурацію Wi-Fi-з’єднання, а також здійснити авторизацію через центральний контролер — Home Gateway.

1. Налаштування Wi-Fi-з’єднання

Кожен IoT-пристрій, який підтримує бездротове підключення, потребує введення таких параметрів:

- SSID мережі (наприклад, *HomeNet*);
- Authentication Mode: WPA2-PSK;
- Password: задається користувачем (наприклад, *smart123*);
- IP-адреса: автоматично призначається маршрутизатором (DHCP) або задається вручну.

Ці параметри вносяться на вкладці Config пристрою → підрозділ Wireless Settings.

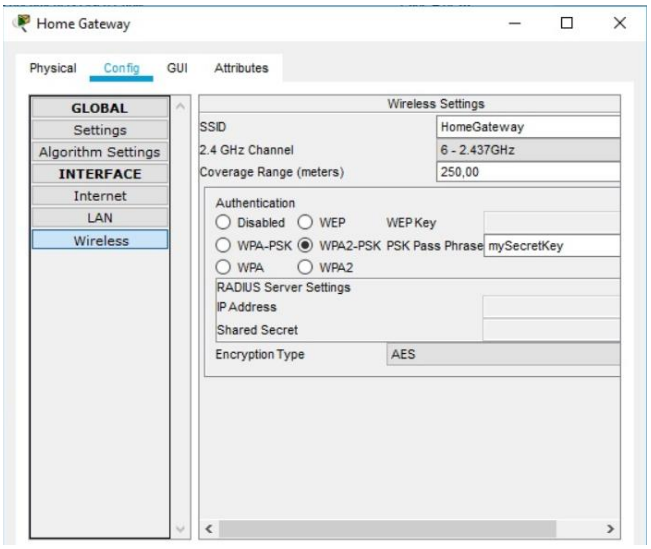

Рисунок 3.3 - Вкладка Config пристрою Home Gateway із внесеними даними

2. Додавання пристрою до Home Gateway

Після підключення до Wi-Fi необхідно «зареєструвати» пристрій у системі керування IoT.

Для цього потрібно:

1. Відкрити інтерфейс Home Gateway.
2. Перейти на вкладку IoT Registration Server.
3. Внести логін/пароль для пристрою (за замовчуванням admin / admin або створені вручну).

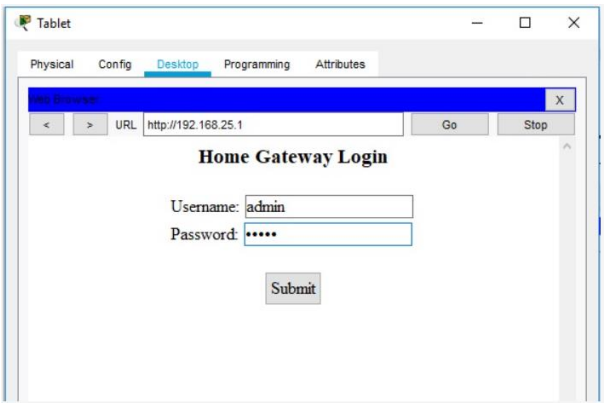

Рисунок 3.4 - Вкладка для реєстрації пристрою Home Gateway

4. Після успішної аутентифікації пристрій з’явиться у списку підключених об’єктів у вкладці Device List.

Ця процедура моделює централізований контроль і захист доступу до системи — важливий елемент безпеки IoT-мереж.

3. Перевірка підключення

Після завершення налаштування можна протестувати:

- Зв’язок між пристроєм і маршрутизатором (ping через вкладку Desktop → Command Prompt).

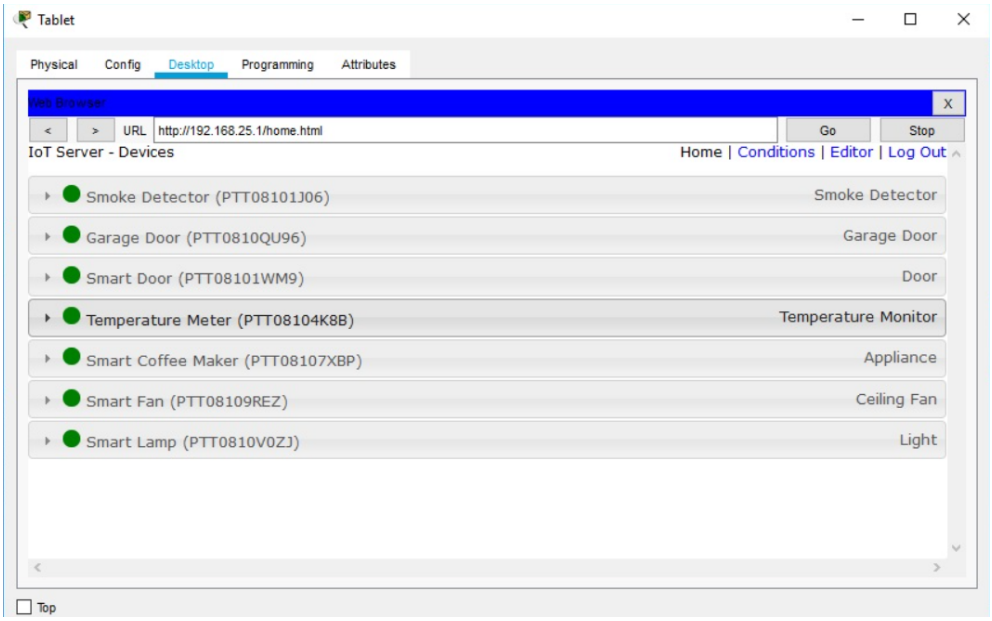

Рисунок 3.5 - Вкладка для перевірки зв’язоку між пристроєм і маршрутизатором

- Взаємодію між пристроєм та IoT Gateway (через інтерфейс IoT Monitor).
- Готовність пристрою до отримання автоматизованих інструкцій (вкладка Programming має бути активною).

Наступним етапом моделювання реалізовано сценарій автоматичного зрошення газону, який ілюструє типову IoT-взаємодію між сенсором і виконавчим пристроєм. В даному випадку використовується сенсор вологості (Soil Moisture Sensor), який при виявленні низького рівня вологи активує зрошувач (Lawn Sprinkler).

Покрокове налаштування сценарію:

1. *Розміщення пристроїв на полі симуляції*

До віртуального середовища було додано два пристрої з категорії IoT:

- Soil Moisture Sensor – датчик, що фіксує рівень вологості ґрунту.
- Lawn Sprinkler – автоматичний зрошувач, який вмикається при потребі.

2. *Підключення до Wi-Fi та реєстрація*

Обидва пристрої були підключені до мережі Wi-Fi з використанням SSID, встановленим у маршрутизаторі (наприклад, HomeNet). Після підключення пристрої були зареєстровані у Home Gateway, що дозволило керувати ними централізовано.

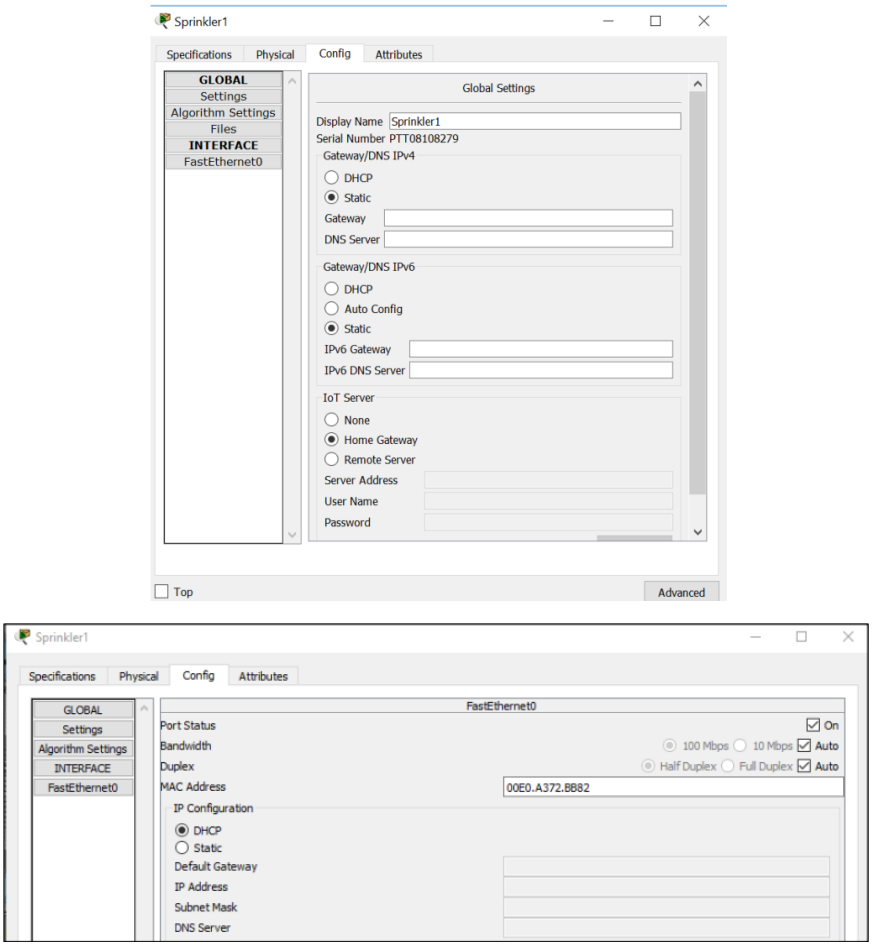

Рисунок 3.6 - Вкладка Config пристрою Lawn Sprinkler із внесеними даними

3. *Програмування сценарію у Blockly*

Вкладка Programming пристрою Soil Moisture Sensor була використана для створення логіки за допомогою Blockly:

a. Подія: when moisture changes

b. Умова: if moisture < 30

c. Дія: Sprinkler.on = true

Це означає, що якщо рівень вологості в ґрунті опускається нижче 30%, зрошувач автоматично вмикається.

4. *Тестування сценарію*

Значення вологості можна змінити вручну у вкладці Config → Environment, або під час симуляції в режимі реального часу. При падінні рівня вологості нижче порогового значення, пристрій Lawn Sprinkler змінює свій стан на активний (вмикається).

Рисунок 3.7 - Вкладка Environment пристрою Lawn Sprinkler для тестування та кінцевий візуальний вигляд

Заключними етапами побудови моделі розумного будинку здійснено інтеграцію бездротових IoT-пристроїв до локальної Wi-Fi-мережі з подальшою реєстрацією у системі керування Home Gateway. Цей процес дозволяє забезпечити зв’язок між фізичними пристроями та мережею, а також централізоване управління їхньою поведінкою.

До вже змодельованого середовища було додано ще кілька пристроїв із підтримкою Wi-Fi-з’єднання, зокрема:

- Smart Lamp
- Smart Door Lock
- Smart Fan

- Smoke Detector
- Motion Detector
- Camera

Кожен пристрій був підключений до мережі Wi-Fi, створеної за допомогою маршрутизатора. Після успішного з’єднання з мережею, кожен пристрій потребує реєстрації у шлюзі Home Gateway.

Після додавання пристроїв до мережі, вони доступні для:

- Програмування поведінки (через вкладку Programming),
- Віддаленого моніторингу та керування (через IoT Monitor або сам Gateway),
- Побудови сценаріїв автоматизації у моделі "розумного будинку".

Таким чином, завершено формування повноцінного набору бездротових IoT-пристроїв, які взаємодіють між собою в межах єдиної Wi-Fi-мережі. Це створює основу для реалізації сценаріїв автоматизації, аналізу протоколів нижнього рівня та дослідження особливостей функціонування IoT-мереж у побутовому середовищі.

Для оцінки результатів моделювання було проведено тестування роботи IoT-пристроїв у симульованій мережі. Зокрема, перевірено поведінку пристроїв до та після запуску подієво-орієнтованих сценаріїв, реалізованих за допомогою Blockly.

Таблиця 3.3 - Змін станів пристроїв до/після сценарію

Пристрій	Подія	Стан до сценарію	Стан після запуску сценарію
Motion Detector	Виявлення руху	Активний	Активний
Smart Lamp	Реакція на рух	OFF	ON
Smoke Detector	Виявлення диму	Немає	Виявлено
Smart Door Lock	Реакція на дим	Розблоковано	Заблоковано
Soil Moisture Sensor	Низька вологість	50%	25%
Lawn Sprinkler	Зрошення газону	OFF	ON
Smart Fan	Температура > 28°C	OFF	ON

Сценарії було протестовано у режимі симуляції:

- Було вручну змінено значення сенсорів (наприклад, зменшення вологості, натискання кнопки "Detect Motion").
- У відповідь виконавчі пристрої (лампа, замок, зрошувач) змінювали стан відповідно до закладеної логіки.
- Усі зміни були відображені в IoT Monitor, де можна відстежити активні події та зміну станів пристроїв у режимі реального часу.

Таблиця 3.4 - Пристрої, IP-адреси та логічні імена у моделі IoT-мережі

№	Назва пристрою	Тип пристрою	Ім’я в моделі (Device Name)	Призначена IP-адреса	Протокол зв’язку
1	Smart Lamp	Актуатор	`Lamp1`	192.168.0.101	Wi-Fi (802.11)
2	Motion Detector	Сенсор	`MotionSensor1`	192.168.0.102	Wi-Fi (802.11)
3	Smart Door Lock	Актуатор	`DoorLock1`	192.168.0.103	Wi-Fi (802.11)
4	Smoke Detector	Сенсор	`SmokeSensor1`	192.168.0.104	Wi-Fi (802.11)
5	Smart Fan	Актуатор	`Fan1`	192.168.0.105	Wi-Fi (802.11)
6	Soil Moisture Sensor	Сенсор	`SoilSensor1`	192.168.0.106	Wi-Fi (802.11)
7	Lawn Sprinkler	Актуатор	`Sprinkler1`	192.168.0.107	Wi-Fi (802.11)
8	Wireless Camera	Камера спостереження	`Cam1`	192.168.0.108	Wi-Fi (802.11)
9	Home Gateway	IoT-шлюз	`IoT-Gateway`	192.168.0.1	LAN
10	Wireless Router	Маршрутизатор	`Router1`	192.168.0.254	—

Таким чином, моделювання підтвердило функціональність мережі IoT, а також ефективність реалізованих сценаріїв автоматизації. Це дозволяє вважати побудовану модель релевантною до реальних IoT-розгортань на побутовому рівні.

У результаті поетапного моделювання було побудовано повнофункціональну мережу IoT-системи «розумний будинок», зображену на рисунку. Дана топологія охоплює як сенсорні компоненти (датчики

температури, диму), так і виконавчі пристрої (смарт-лампа, двері, вентилятор, кавоварка, гаражні ворота), а також джерела живлення (сонячна панель, батарея) і мережеву інфраструктуру (маршрутизатор, шлюз, модем).

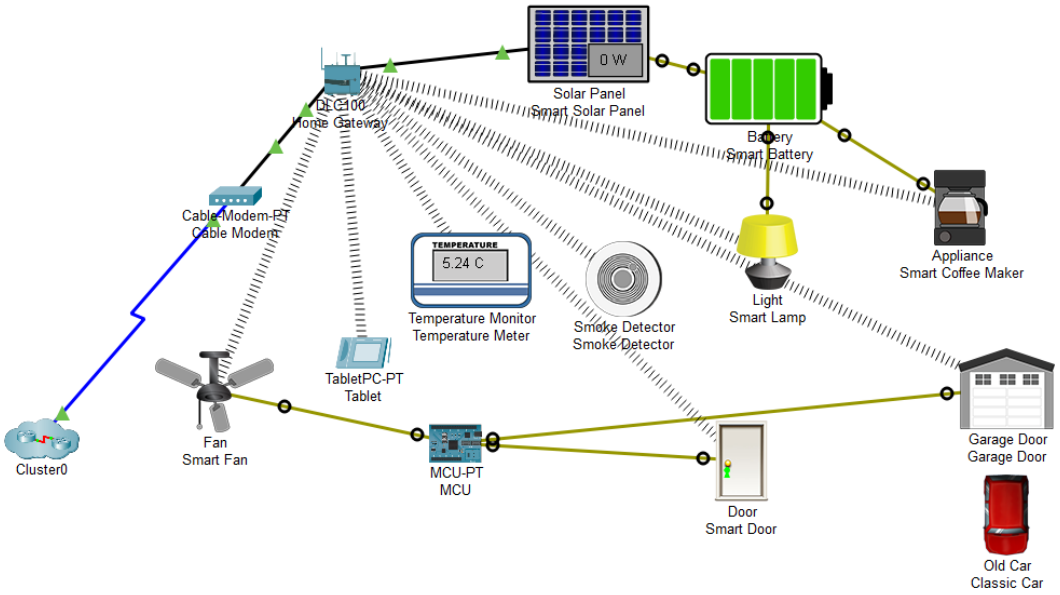

Рисунок 3.8 - Завершена топологія мережі «розумного будинку»

На основі зображеної топології моделі розумного будинку в Cisco Packet Tracer можна детально описати взаємодію пристроїв на фізичному та канальному рівнях моделі OSI наступним чином:

На фізичному рівні пристрої обмінюються сигналами через різні середовища передавання, основним з яких у цій моделі є бездротове середовище Wi-Fi (IEEE 802.11).

- Маршрутизатор Wi-Fi (Home Gateway) виконує функцію точки доступу (Access Point), забезпечуючи передавання радіохвиль для підключення сенсорів, актуаторів, камери, кавоварки, лампи та інших пристроїв.
- Пристрої типу Smart Lamp, Smoke Detector, Smart Fan, Smart Coffee Maker, Smart Door, Tablet PC, MCU, тощо підключені до спільної бездротової мережі, використовуючи вбудовані Wi-Fi-інтерфейси, які фізично передають інформацію у вигляді цифрових імпульсів.
- Сонячна панель і батарея в цій моделі умовно подають живлення

на виконавчі пристрої, однак їхній облік має більше символічний характер у симуляторі.

Усе передавання інформації на фізичному рівні базується на радіохвилях, які розповсюджуються від точки доступу до пристроїв у межах зони покриття.

На канальному рівні відбувається організація доступу до середовища передавання, адресація та контроль помилок:

- Технологія доступу до середовища – CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), характерна для Wi-Fi. Перед передачею даних пристрій «прислухається» до каналу та передає тільки у разі його вільності, щоб уникнути колізій.
- MAC-адресація використовується для унікальної ідентифікації пристроїв у мережі. Кожен сенсор чи актуатор має свій власний MAC-адрес, за яким відбувається взаємодія в межах бездротової мережі.
- Формування кадрів: на цьому рівні дані упаковуються у Wi-Fi фрейми з заголовками, які включають адреси відправника і отримувача, контрольну суму (CRC) для виявлення помилок, та інші службові поля.
- Обробка подій: наприклад, при виявленні руху або диму, сенсор формує кадр і передає його до шлюзу або безпосередньо до пристрою-отримувача (наприклад, лампи чи замка), використовуючи механізми канального рівня.

Таким чином, модель розумного будинку наочно демонструє, як на фізичному рівні відбувається передача сигналів між пристроями через бездротове середовище (Wi-Fi), а на канальному рівні — забезпечується організація доступу до мережі, адресація, контроль помилок та уникнення колізій за допомогою протоколу CSMA/CA. Завдяки цьому забезпечується стабільна, координована робота сенсорів, актуаторів і контролерів у межах локальної IoT-мережі, що дозволяє ефективно реагувати на події та підтримувати надійний обмін даними між пристроями.

Також у випадку пристроїв, які працюють постійно (наприклад, сенсори або камери), помітно, що Wi-Fi потребує більше енергії, ніж, наприклад, ZigBee або BLE (хоч ці протоколи не реалізовані в цій моделі, їхня відсутність дає підставу для порівняння). Віддалені пристрої або ті, що опинилися поза зоною дії (наприклад, Garage Door) вимагають сильнішого сигналу або ретрансляції, що також впливає на стабільність з'єднання.

Завдяки таким спостереженням стало очевидно, що вибір технології зв'язку має бути адаптований до функціонального навантаження, розміщення та критичності пристрою, що й лягло в основу розробки рекомендацій у наступному підрозділі.

3.3 Розробка рекомендацій щодо вибору технологій та протоколів для різних сценаріїв використання

Вибір відповідної технології передачі даних у системах Інтернету речей є одним із ключових рішень, що напряму впливає на ефективність, стабільність і життєвий цикл IoT-мережі. Особливо це актуально на фізичному та канальному рівнях моделі OSI, де визначається тип середовища передачі, спосіб доступу до каналу, енергетична модель взаємодії пристроїв і здатність мережі до масштабування.

Зважаючи на це, доцільно виокремити основні критерії, які слід враховувати під час вибору технологій фізичного та канального рівнів для будь-якого IoT-сценарію:

Топологія мережі:

Тип топології мережі (зірка, деревоподібна, коміркова, mesh) впливає на вибір технології:

- Для централізованих архітектур (наприклад, розумний будинок) з єдиним шлюзом підходять Wi-Fi або Ethernet, де всі пристрої зв'язуються із центральним вузлом.
- У розподілених або масштабованих системах (розумні міста,

аграрні IoT) доцільно застосовувати LoRa, ZigBee, або mesh-протоколи, які дозволяють багатоступеневу маршрутизацію.

Тип пристроїв та їх призначення:

Різні типи IoT-пристроїв мають різні вимоги до пропускної здатності, стабільності з'єднання і енергоспоживання:

- Сенсори (руху, диму, температури) передають невеликі пакети даних з інтервалами, отже потребують енергоощадних технологій, як-от ZigBee, BLE, LoRa.
- Актуатори (реле, замки, вентилятори) мають мати мінімальні затримки при отриманні команд — для них важлива стабільність та швидкість каналу.
- Мультимедійні пристрої (камери, мікрофони) потребують високої пропускної здатності та стійкості, що забезпечується лише Wi-Fi або дротовими рішеннями (Ethernet).

Споживання енергії:

Оскільки більшість IoT-пристроїв працюють автономно, вибір технології має враховувати енергоспоживання модуля зв'язку:

- Протоколи Wi-Fi забезпечують хорошу швидкість, але споживають найбільше енергії.
- ZigBee, BLE, LoRaWAN створені з урахуванням енергозбереження та дозволяють пристроям працювати від батареї роками.

Частота обміну даними:

IoT-системи можуть бути поділені за частотою обміну:

- Нерегулярні/подієві пристрої (наприклад, детектори диму) можуть працювати з великими інтервалами.
- Періодичні сенсори (температура, вологість) передають дані раз на декілька хвилин або годин.
- Потокові пристрої (камери, монітори) потребують постійного високошвидкісного з'єднання.

Цей фактор є вирішальним при виборі між низькошвидкісними

енергоощадними та високошвидкісними, але витратними технологіями.

Відстань між пристроями та середовище експлуатації:

- У межах приміщення (до 30 м) ефективно працює Wi-Fi, Bluetooth, ZigBee.
- Для відкритих майданчиків (сади, ферми, парковки) кращими будуть LoRaWAN, NB-IoT, здатні передавати сигнал на кілометри.
- У складних умовах (стіни, метал, перешкоди) краще застосовувати дротові протоколи або радіозв'язок із високою проникністю (нижчі частоти).

Надійність зв'язку та відмовостійкість:

Критичні IoT-системи, пов'язані з безпекою (замки, сигналізації, відеоспостереження), повинні функціонувати без збоїв:

- Рекомендується використання дублюючих каналів зв'язку (наприклад, Wi-Fi + LTE або дріт + ZigBee).
- У випадках з високими вимогами до QoS — протоколи з вбудованими механізмами повторної передачі, перевірки помилок, пріоритезації кадрів (наприклад, 802.11e для Wi-Fi).

У контексті Інтернету речей вибір технологій фізичного та канального рівнів не є універсальним і потребує урахування конкретних умов експлуатації, функціональних вимог пристроїв і особливостей середовища передачі даних. Відповідність протоколів певному сценарію визначається низкою факторів: необхідною дальністю дії, щільністю пристроїв, рівнем енергоспоживання, швидкістю передачі даних, допустимими затримками та надійністю з'єднання. Технології, що добре функціонують у компактному середовищі з доступом до електромережі, можуть виявитися неефективними у віддалених або мобільних системах.

На фізичному рівні важливими параметрами є тип середовища (дротове чи бездротове), частотний діапазон, модуляція та потужність передавача. На канальному рівні критичну роль відіграють методи доступу до середовища (CSMA/CA, TDMA, FDMA), механізми виявлення помилок, підтримка адресації та здатність до формування топології (зірка, mesh, деревоподібна

структура тощо). Наприклад, протоколи, побудовані на основі технологій IEEE 802.15.4 (як-от ZigBee), забезпечують низьке енергоспоживання та самоорганізовану мережу з великою кількістю пристроїв, що ідеально підходить для домашньої автоматизації.

Натомість для систем, де пріоритетом є висока пропускна здатність (наприклад, передача відеопотоку з камер або контроль промислових механізмів у реальному часі), варто обирати дротові інтерфейси (Ethernet) або сучасні версії Wi-Fi (802.11ac, ax), які здатні забезпечити стабільну, високошвидкісну передачу без істотних затримок. Аналіз різних сценаріїв використання дозволяє сформувати узагальнені рекомендації щодо вибору відповідних технологій, адаптованих до конкретних потреб IoT-системи, що й відображено у таблиці нижче.

Таблиця 3.5 - Відповідність технологій фізичного та канального рівнів до сценаріїв IoT-застосування

Сценарій використання	Пристрої/вимоги	Рекомендовані технології	Обґрунтування вибору
Розумний будинок	Сенсори руху, диму, смарт-лампи, двері, камери	Wi-Fi, ZigBee, BLE	Невелика територія, потреба у швидкому реагуванні, наявність джерел живлення, підтримка мобільних додатків
Розумне сільське господарство	Вологоміри, термодатчики, сонячні панелі	LoRaWAN, NB-IoT	Велика площа, низька частота передачі, необхідність тривалої автономної роботи
Системи відеоспостереження	IP-камери, сховища, детектори руху	Ethernet, Wi-Fi	Потреба у високій пропускній здатності, низька затримка, стабільне з’єднання
Міський транспорт / Smart Parking	Датчики місць, лічильники, камери, дисплеї	NB-IoT, LTE-M, Wi-Fi	Покриття мобільними мережами, потреба у геолокації, середній трафік

Продовження таблиці 3.5

Медичні носимі пристрої	Фітнес-трекери, монітори стану, пульсометри	BLE, ZigBee	Мала дальність, низьке енергоспоживання, безпечне з’єднання
Промислові системи контролю	Роботи, датчики навантаження, лічильники	Ethernet, Wi-Fi + Modbus	Висока стабільність, промислові протоколи, суворі вимоги до точності

Як свідчить аналіз у таблиці 3.5, вибір технологій фізичного та канального рівнів напряму залежить від характеру середовища, типу переданих даних, вимог до енергоспоживання та надійності зв’язку. Наприклад, для компактних побутових систем доцільно використовувати Wi-Fi або ZigBee, тоді як у розподілених мережах на відкритих територіях — LoRaWAN або NB-IoT. У сценаріях з великим потоком даних (відео, контроль обладнання) безальтернативними залишаються Ethernet або високошвидкісний Wi-Fi. Таким чином, універсального рішення не існує — кожен тип IoT-системи вимагає індивідуального підходу до вибору протоколів зв’язку, що й зумовлює потребу у комплексному аналізі умов експлуатації.

Один із ключових аспектів під час проєктування IoT-систем полягає у розумінні того, як вибір протоколу фізичного та канального рівнів безпосередньо впливає на роботу всієї мережі. Технології передачі даних істотно відрізняються за затримкою, енергоспоживанням, надійністю з'єднання та здатністю масштабування (тобто кількістю пристроїв, які можуть стабільно взаємодіяти в межах однієї мережі). Наприклад, ZigBee або BLE дозволяють пристроям працювати автономно роками завдяки мінімальному енергоспоживанню, але мають обмежену швидкість передачі. Натомість Wi-Fi забезпечує високу пропускну здатність, але швидко витрачає акумулятор. Такі нюанси особливо важливі для систем, які працюють без постійного підключення до джерел живлення або потребують наднизької затримки, як у випадку охоронних систем.

Таблиця 3.6 - Вплив вибраних технологій на ключові параметри роботи IoT-мережі

Технологія	Середня затримка	Енергоспоживання	Надійність з'єднання	Кількість підтримуваних пристроїв
Wi-Fi	Низька (~10–20 мс)	Високе	Висока	Обмежено (~30 50/роутер)
ZigBee	Середня (~50 мс)	Низьке	Висока (mesh-топологія)	До 65 000
LoRaWAN	Висока (>1000 мс)	Дуже низьке	Середня	До 100 000 (в межах області покриття)
BLE	Середня (~100 мс)	Низьке	Середня	До 7–10 (в одному сеансі)
Ethernet	Дуже низька (<1 мс)	Постійне живлення	Дуже висока	Залежить від мережевої інфраструктури

Як показано у таблиці 3.6, жодна технологія не є універсальною — кожна має свої переваги та обмеження. Наприклад, для систем з критичними вимогами до затримки або стабільності (відеоспостереження, автоматика) найкращим вибором буде Ethernet або Wi-Fi. У сценаріях, де важливіша енергоефективність, лідерами залишаються LoRaWAN, BLE та ZigBee. Також варто враховувати масштаб: якщо необхідно підключити тисячі пристроїв, ZigBee або LoRaWAN будуть оптимальними. Таким чином, правильний вибір технології напряму визначає не лише якість зв’язку, а й життєвий цикл пристроїв, масштабованість і загальну стабільність роботи IoT-системи.

У сфері Інтернету речей (IoT) використовуються різноманітні технології фізичного та канального рівнів, кожна з яких має свою специфіку, переваги та обмеження. Знання цих характеристик дозволяє обрати найдоцільніше рішення залежно від задачі, середовища розгортання та технічних обмежень. Зараз розглянемо найбільш поширені технології, що застосовуються в практиці побудови IoT-систем.

Wi-Fi (IEEE 802.11) є однією з найпоширеніших технологій бездротової передачі даних, яка активно використовується в системах IoT, особливо в побутових умовах. Основною перевагою є висока швидкість передачі (до кількох сотень мегабіт за секунду), що дозволяє обслуговувати мультимедійний трафік та реальні додатки з високими вимогами до

пропускної здатності. Крім того, Wi-Fi підтримується великою кількістю пристроїв і забезпечує прямий вихід до мережі Інтернет. Серед недоліків варто виокремити значне енергоспоживання, що обмежує використання в автономних пристроях на батарейках, а також обмеження щодо кількості одночасно підключених пристроїв у межах одного маршрутизатора.

ZigBee (на основі IEEE 802.15.4) позиціонується як енергоефективна технологія для створення малопотужних бездротових мереж з великою кількістю вузлів. Вона ідеально підходить для побудови «розумного будинку» завдяки підтримці mesh-топології, яка забезпечує надійність і самовідновлення мережі. Однією з головних переваг є здатність працювати з тисячами пристроїв при наднизькому енергоспоживанні. До недоліків можна віднести обмежену швидкість передачі (до 250 кбіт/с) та необхідність використання окремого шлюзу для з’єднання з Інтернетом.

Bluetooth Low Energy (BLE) розроблений спеціально для малопотужних короткочасних з’єднань, що робить його ідеальним рішенням для носимих пристроїв, трекерів та інших персональних IoT-гаджетів. Перевагами є дуже низьке енергоспоживання, мала вартість модулів та сумісність з більшістю мобільних пристроїв. Слабкими сторонами є обмежена кількість підключень (до 7–10 пристроїв у рамках одного майстра), невелика дальність дії (до 30 м) та невисока пропускна здатність.

LoRaWAN вирізняється наддалекою дальністю передачі даних (до 15–20 км у сільській місцевості), що робить її особливо привабливою для застосування в агропромисловості, екологічному моніторингу та інфраструктурних рішеннях. До переваг відносяться: наднизьке енергоспоживання, велика кількість пристроїв на одному шлюзі та підтримка широких територій. Основні обмеження стосуються низької швидкості передачі (до 50 кбіт/с), високої затримки та обмеженого застосування в сценаріях реального часу.

Ethernet залишається еталонною технологією для побудови надійних дротових мереж у промислових та комерційних системах. Серед головних

переваг — наднизька затримка, стабільне з’єднання, висока пропускна здатність та захищеність від електромагнітних завад. Ethernet не залежить від радіосередовища, що робить його ідеальним для систем відеоспостереження, автоматизації та SCADA. Основним недоліком є відсутність мобільності, необхідність прокладання кабелів та підключення до живлення, що обмежує його використання в автономних і розподілених IoT-сценаріях.

NB-IoT та LTE-M — це вузькосмугові технології, розроблені на базі стільникових мереж спеціально для пристроїв Інтернету речей. Їх головною перевагою є можливість використання вже існуючої інфраструктури мобільних операторів, що значно спрощує масштабування. Вони підтримують низьке енергоспоживання (завдяки режимам PSM/DRX), мають хороше покриття навіть у важкодоступних місцях (наприклад, підвалах або лічильниках під землею). Проте, серед недоліків слід згадати залежність від оператора зв’язку, необхідність оплати послуг зв’язку, наявність SIM-карт або eSIM, а також високу змінність затримок у перевантажених мережах.

На основі проведеного дослідження, моделювання IoT-системи розумного будинку в Cisco Packet Tracer, а також порівняльного аналізу характеристик фізичних і канальних технологій, можна сформулювати низку практичних рекомендацій, які доцільно враховувати при проєктуванні IoT-мереж для різних умов використання.

1. Для невеликих побутових IoT-систем (розумний будинок), де критичними є компактність, енергоефективність і надійність, доцільно застосовувати ZigBee або BLE. ZigBee забезпечує стабільну мережу з можливістю масштабування завдяки mesh-архітектурі, а BLE чудово підходить для простих пристроїв на батарейках із коротким діапазоном передачі.

2. Для сценаріїв, де пріоритетом є висока швидкість та мала затримка (відеоспостереження, автоматизація процесів, охоронні системи), оптимальним вибором буде Wi-Fi або Ethernet. Перший варіант забезпечує гнучкість та високу швидкість у бездротовому режимі, другий — максимальну

стабільність, але вимагає дротової інфраструктури.

3. У великих розподілених системах моніторингу з вимогою до великої дальності передачі та тривалого терміну автономної роботи (наприклад, в аграрному секторі, екології, смарт-містах), доцільно використовувати LoRaWAN або NB-IoT. Вони забезпечують покриття на великі відстані та мінімальне енергоспоживання, однак не підходять для задач із реальним часом через високу затримку.

4. Для систем, які потребують гнучкого масштабування з підключенням великої кількості пристроїв (до десятків тисяч), найкращим варіантом є ZigBee, LoRaWAN або Thread, які підтримують динамічне управління топологією та надають гнучкість при розвитку мережі.

5. З погляду безпеки, при роботі з чутливими даними доцільно віддавати перевагу технологіям, що підтримують сучасні алгоритми шифрування (AES, TLS, WPA3), як-от Wi-Fi, ZigBee, а також стільникові протоколи з вбудованою SIM-ідентифікацією (NB-IoT, LTE-M).

Узагальнюючи, можна зазначити, що вибір технології не повинен ґрунтуватися лише на технічних параметрах, а має враховувати специфіку середовища, джерела живлення, критичність затримки, обсяг трафіку, необхідний рівень безпеки та бюджет проєкту. Рекомендується також поєднувати кілька технологій у межах однієї IoT-системи, утворюючи гібридну мережу, що дозволить р еалізувати сильні сторони кожної з них.

3.3 Висновки до розділу 3

У третьому розділі дипломної роботи було здійснено практичне моделювання роботи IoT-мережі на прикладі системи «розумний будинок» із використанням інструменту Cisco Packet Tracer. Було обґрунтовано вибір цього середовища для дослідження завдяки його підтримці симуляції фізичного та канального рівнів, наочності інтерфейсу та можливості реалізації сценаріїв реального використання IoT-пристроїв.

У пункті 3.1 детально описано методику дослідження та обґрунтовано вибір моделі «розумного будинку» як найбільш наочного та поширеного прикладу побутового сценарію IoT. Побудована топологія включала як сенсорні пристрої (датчики руху, температури, диму), так і виконавчі елементи (лампи, вентилятори, замки), що взаємодіють у єдиній локальній мережі Wi-Fi із централізованим керуванням через шлюз Home Gateway.

У пункті 3.2 було здійснено поетапне моделювання роботи IoT-мережі, реалізовано автоматизовані сценарії управління пристроями з використанням мови Blockly (наприклад, автоматичне зрошення, вмикання освітлення при виявленні руху). Проведено тестування реакції системи на події у режимі реального часу, що дозволило оцінити роботу технологій фізичного та канального рівнів на практиці.

У пункті 3.3 на основі отриманих результатів моделювання та теоретичного аналізу було сформовано рекомендації щодо вибору технологій та протоколів для різних IoT-сценаріїв. Проведено порівняльний аналіз характеристик різних технологій (Wi-Fi, ZigBee, BLE, LoRaWAN, Ethernet, NB-IoT) за критеріями затримки, енергоспоживання, масштабованості та надійності. Узагальнено, що вибір протоколів повинен базуватись на вимогах до конкретного середовища застосування та типу задачі (побутової, промислової, міської або аграрної IoT-системи).

Загалом практична частина підтвердила важливість правильного вибору технологій нижніх рівнів для забезпечення ефективної та стабільної роботи IoT-систем. Досвід моделювання на прикладі розумного будинку надав практичне підґрунтя для рекомендацій, які можуть бути використані для подальшого проєктування та впровадження IoT-мереж у різних сферах.

ВИСНОВКИ

У дипломній роботі на тему «Аналіз технологій та протоколів фізичного та канального рівня мереж Інтернету речей» було всебічно досліджено теоретичні, аналітичні та практичні аспекти вибору й використання технологій нижніх рівнів моделі OSI у сучасних IoT-системах.

У ході виконання роботи були реалізовані поставлені завдання:

- Проаналізовано архітектуру та рівневу модель мереж Інтернету речей, визначено місце і роль фізичного та канального рівнів у загальній структурі IoT-систем (розділ 1).
- Досліджено особливості передавання даних на фізичному та канальному рівнях, зокрема ключові протоколи та стандарти, що застосовуються у практиці: NB-IoT, LoRaWAN, Sigfox, IEEE 802.15.4 (ZigBee), BLE, Wi-Fi, Ethernet (розділ 2).
- Виконано аналіз викликів і обмежень технологій цих рівнів, зокрема питань безпеки фізичного рівня та ефективності управління доступом до середовища (пункт 1.3, 2.3).
- Проведено практичне моделювання роботи IoT-мережі на прикладі «розумного будинку» всередовищі Cisco Packet Tracer, реалізовано автоматизовані сценарії роботи IoT-пристроїв, протестовано взаємодію пристроїв на фізичному та канальному рівнях (розділ 3).
- Розроблено практичні рекомендації щодо вибору технологій і протоколів для різних сценаріїв використання IoT-систем, сформовано узагальнюючі таблиці вибору технологій залежно від умов експлуатації, типу даних, енергоспоживання та топології мережі (пункт 3.3).

Основними результатами роботи є:

- Систематизовано знання про сучасні технології фізичного та канального рівнів для IoT, що дозволяє ефективно орієнтуватися у виборі протоколів залежно від задачі.
- Підтверджено вплив вибору технології PHY та MAC-рівнів на

ключові параметри роботи IoT-системи — енергоспоживання, затримки, надійність зв’язку, масштабованість.

- Доведено ефективність застосування інструменту Cisco Packet Tracer для моделювання та дослідження роботи IoT-мереж, що дозволяє на практиці апробувати сценарії реального використання IoT-пристроїв.
- Сформульовано рекомендації для практичного застосування, що мають цінність для розробників IoT-систем як побутового, так і промислового призначення.

Таким чином, поставлена мета дипломної роботи — на основі аналізу існуючих технологій та протоколів фізичного та канального рівня мереж Інтернету речей розробити рекомендації щодо їх використання — досягнута у повному обсязі.

Результати дослідження мають практичне значення і можуть бути використані при проєктуванні нових IoT-систем у різних галузях: від побутової автоматизації до промислового моніторингу і розумної міської інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Семенюк Ю.С., Носков В.І. АНАЛІЗ ТЕХНОЛОГІЙ ТА ПРОТОКОЛІВ ФІЗИЧНОГО ТА КАНАЛЬНОГО РІВНЯ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ//XIX Міжнародна науково-технічна конференція “Перспективи телекомунікацій” ПТ-2025: Збірник матеріалів конференції. – К.: КПІ ім. Ігоря Сікорського, 2025. – с. 333.

2. Пулеко І. В. Єфіменко А. А. П88 Архітектура та технології Інтернету речей: навч. посіб. / І.В. Пулеко, А.А. Єфіменко. – Електронні дані. – Житомир: Державний університет «Житомирська політехніка», 2022. – 234 с.

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. Harari, Y. N. Homo Deus: A Brief History of Tomorrow / Yuval Noah Harari. – London: Vintage, 2017. – 513 c.

5. Gislason, D. Zigbee Wireless Networking / Drew Gislason. – Burlington: Newnes, 2008. – 344 c.

6. Heydon, R. Bluetooth Low Energy: The Developer's Handbook / Robin Heydon. – Upper Saddle River: Prentice Hall, 2013. – 368 c.

7. Hillar, G. C. MQTT Essentials: A Lightweight IoT Protocol / Gastón C. Hillar. – Birmingham: Packt Publishing, 2017. – 178 c.

8. Hersent, O., Boswarthick, D., Elloumi, O. The Internet of Things: Key Applications and Protocols / Olivier Hersent, David Boswarthick, Omar Elloumi. – Chichester: Wiley, 2012. – 360 c.

9. Cirani, S., Ferrari, G., Picone, M., Veltri, L. Internet of Things: Architectures, Protocols and Standards / Simone Cirani, Gianluigi Ferrari, Marco Picone, Luca Veltri. – Chichester: Wiley, 2018. – 250 c.

10. IEEE. IEEE Standard for Low-Rate Wireless Networks. IEEE Std 802.15.4.

11. IEEE. IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11.

12. LoRa Alliance. LoRaWAN Specification. [Електронний ресурс]. URL: https://lora-alliance.org/resource_hub/lorawan-specification-v1-0-4/

13. Bluetooth SIG. Bluetooth Core Specification. [Електронний ресурс]. URL: https://www.bluetooth.com/specifications/bluetooth-core-specification/

14. 3GPP. Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Narrowband IoT (NB-IoT). 3GPP TS 36.xxx.

15. Shannon C. E. Communication Theory of Secrecy Systems. Bell System Technical Journal. 1949. Vol. 28, no. 4. с. 656–715.

16. Wyner A. D. The Wire-Tap Channel. Bell System Technical Journal. 1975. Vol. 54, no. 8. с. 1355–1387.

17. Cisco Networking Academy. Packet Tracer – Adding IoT Devices to Smart Homes. [Електронний ресурс]. URL:https://contenthub.netacad.com/legacy/I2PT/1.1/en/course/files/5.1.1.2%20Packet%20Tracer%20-%20Adding%20IoT%20devices%20to%20Smart_Homes.pdf

18. Roman R., Najera P., Lopez J. Securing the Internet of Things. Computer. 2011. Vol. 44(9). с. 51–58.

19. Raza S., Wallgren L., Voigt T. Security Measures for the Industrial IoT: State of the Art and Future Directions. IEEE Communications Magazine. 2017. Vol. 55(1). с. 42–47.

20. Hossain M. S., Muhammad G. Cloud-assisted Industrial Internet of Things (IIoT) – Framework and Future Directions. IEEE Communications Magazine. 2016. Vol. 54(12). с. 66–73.

21. Granjal J., Monteiro E., Silva J. S. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Communications Surveys & Tutorials. 2015. Vol. 17(3). с. 1294–1312.