

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ**
НАВЧАЛЬНО-НАУКОВИЙ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Система передачі даних для IoT-мереж з обмеженими ресурсами»

на здобуття освітнього ступеня магістра

зі спеціальності 126 Інформаційні системи та технології

освітньо-професійної програми Інформаційні системи та технології

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

(підпис)

Ім'я, ПРІЗВИЩЕ здобувача

Виконав

здобувач вищої освіти Олександр РЕЙНГОЛЬД
група ІСДМ-63

Керівник: Світлана ПОПЕРЕШНЯК

науковий ступінь,

вчене звання

к.ф.-м.н, доц, доцент кафедри ТЦР

Рецензент:

*науковий ступінь, вчене
звання*

Ім'я, ПРІЗВИЩЕ

Київ – 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра	<u>Інформаційних систем та технологій</u>
Ступінь вищої освіти	<u>Магістр</u>
Спеціальність підготовки	<u>Інформаційні системи та технології</u>
Освітньо-професійної програми	<u>Інформаційні системи та технології</u>

ЗАТВЕРДЖУЮ

Завідувач кафедри

Каміла СТОРЧАК

« ____ » _____ 20 ____ р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Рейнгольду Олександрю Юрійовичу

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: Система передачі даних для IoT-мереж з обмеженими ресурсами керівник кваліфікаційної роботи Поперешняк С.В. к.ф.-м.н, доц., доцент кафедри ТЦР

затверджені наказом вищого навчального закладу від «15» жовтня 2024 р. № 320

2. Строк подання кваліфікаційної роботи 27 грудня 2024 р.

3. Вихідні дані до кваліфікаційної роботи

Мета дослідження: дослідження та впровадження оптимальних технологій обміну даними для IoT-систем з обмеженими ресурсами.

Об'єктом дослідження є технології обміну даними в IoT-мережах з обмеженими ресурсами.

Предметом дослідження є методи та підходи до ефективної передачі даних в умовах обмежених ресурсів у IoT-мережах.

Науково-технічна література з питань, пов'язаних з наукою про дані.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Здійснити огляд принципу дії та архітектури Інтернету речей в умовах обмежених ресурсів

2. Проаналізувати переваги та недоліки IoT

3. Проаналізувати технології та протоколи передачі даних IoT на різні відстані з використанням найменших ресурсів

4. Здійснити огляд на актуальність в застосуванні передачі даних в мережі IoT

5. Перелік ілюстрованого матеріалу: *презентація*

1. Мета, об'єкт та предмет дослідження

2. Завдання роботи та розділи магістерської роботи

3. Методологічні підходи до роботи IoT-мережі

4. Огляд та порівняльний аналіз протоколів та технологій передачі даних та повідомлень в мережах Internet of Things
5. Поточний стан та майбутні перспективи розвитку технологій передачі даних в IoT в Україні
6. Висновки та апробація

6. Дата видачу завдання: 15 жовтня 2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	15.10-23.10.24	
2	Вивчення алгоритмів і технологій	24.10-01.11.24	
3	Розробка теоретичної моделі системи	02.11-07.11.24	
4	Реалізація та тестування системи	08.11-16.11.24	
5	Оформлення роботи: вступ, висновки, реферат	12.12-20.12.24	
6	Розробка демонстраційних матеріалів	21.12-22.12.24	

Здобувач вищої освіти _____

Олександр РЕЙНГОЛЬД

Вивчення алгоритмів і технологій
(Ім'я, ПРІЗВИЩЕ)

(підпис)

Керівник

кваліфікаційної роботи _____

Світлана ПОПЕРЕШНЯК

(підпис)

(Ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 68 стор., 20 рис., 0 табл., 20 джерел.

Мета роботи – дослідження та впровадження ефективних технологій передачі даних для IoT-мереж з обмеженими ресурсами. Це передбачає аналіз існуючих технологій та рішень, визначення їх переваг та недоліків, а також розробку рекомендацій щодо оптимального вибору та застосування технологій для забезпечення надійної, енергоефективної та безпечної передачі даних в IoT-мережах.

Об'єкт дослідження – об'єктом дослідження є технології передачі даних у IoT-мережах з обмеженими ресурсами. Це включає як бездротові, так і дротові технології, які використовуються для забезпечення зв'язку між IoT-пристроями та мережевою інфраструктурою. Особлива увага приділяється технологіям, що забезпечують енергоефективність, надійність і безпеку передачі даних в умовах обмежених енергетичних та пропускних можливостей.

Предмет дослідження – Предметом дослідження є методи та підходи до ефективної передачі даних в умовах обмежених ресурсів у IoT-мережах.

Короткий зміст роботи: Тема: Дослідження і впровадження технологій передавання даних для IoT мереж з обмеженими ресурсами.

Метою цього дослідження є розробка та впровадження ефективних технологій передачі даних для IoT-мереж з обмеженими ресурсами. Основний акцент зроблено на забезпеченні надійного, енергоефективного та безпечного передавання даних між пристроями в умовах обмежених ресурсів.

Під час дослідження було вивчено сучасні протоколи передавання даних і технології, такі як LoRaWAN, ZigBee, MQTT і CoAP. Протокол MQTT був обраний через його здатність забезпечувати низьке енергоспоживання і високу швидкість передачі даних. Для підвищення безпеки передачі даних було запропоновано використання криптографічних методів, адаптованих до обмежених можливостей IoT-пристроїв.

Результати дослідження показали, що використання ефективних протоколів у поєднанні з легкими криптографічними алгоритмами дає змогу суттєво знизити енергоспоживання, зберігаючи надійність і безпеку. Однак, застосування сучасних протоколів потребує додаткової оптимізації для зменшення затримок у передачі даних.

Практична новизна дослідження полягає в розробці рекомендацій щодо вибору технологій передавання даних та адаптації наявних протоколів для IoT-мереж з обмеженими ресурсами, що може бути застосовано для створення сучасних систем автоматизації та моніторингу.

КЛЮЧОВІ СЛОВА: IoT-мережі, MQTT, Технології передачі даних, Надійність, Автоматизація

ABSTRACT

Text part of the master's qualification work: ? pages, ? pictures, ? table, ? sources.

The purpose of the work – research and implementation of efficient data transmission technologies for IoT networks with limited resources. This involves analyzing existing technologies and solutions, identifying their advantages and disadvantages, and developing recommendations for the optimal selection and application of technologies to ensure reliable, energy-efficient, and secure data transmission in IoT networks.

Object of research – the object of research is data transmission technologies in IoT networks with limited resources. This includes both wireless and wired technologies that are used to provide communication between IoT devices and network infrastructure. Particular attention is paid to technologies that ensure energy efficiency, reliability and security of data transmission in conditions of limited energy and bandwidth.

Subject of research – The subject of the research is methods and approaches to efficient data transmission in conditions of limited resources in IoT networks.

Summary of the work: Topic: Research and implementation of data transmission technologies for IoT networks with limited resources.

The purpose of this work is to develop and implement efficient data transmission technologies for IoT networks with limited resources. The main emphasis is on ensuring reliable, energy-efficient, and secure data transmission between devices in resource-limited environments.

The study examined modern data transmission protocols and technologies such as LoRaWAN, ZigBee, MQTT, and CoAP. The MQTT protocol was chosen because of its ability to provide low power consumption and high data transfer rate. To improve the security of data transmission, it was proposed to use cryptographic methods adapted to the limited capabilities of IoT devices.

The results of the study showed that the use of efficient protocols in combination with lightweight cryptographic algorithms can significantly reduce power consumption while maintaining reliability and security. However, the use of modern protocols requires additional optimization to reduce data transmission delays.

The practical novelty of the study lies in the development of recommendations for the selection of data transmission technologies and the adaptation of existing protocols for IoT networks with limited resources, which can be used to create modern automation and monitoring systems.

KEYWORDS: IoT networks, MQTT, Data transmission technologies,
Reliability, Automation

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ**

**ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ
КВАЛІФІКАЦІЙНОЇ РОБОТИ на здобуття освітнього ступеня магістр**

Направляється здобувач _____ до захисту кваліфікаційної
роботи за спеціальністю 126 Інформаційні системи та технології
(код, найменування спеціальності)

освітньо-професійної програми Інформаційні системи та технології
на тему: «Дослідження і впровадження технологій передавання даних для IoT-
мереж з обмеженими ресурсами».

Кваліфікаційна робота і рецензія додаються.

Директор ННІ _____ Ім'я ПРІЗВИЩЕ

Висновок керівника кваліфікаційної роботи

Здобувач Ренгольд Олександр Юрійович успішно виконав кваліфікаційну роботу на тему «Система передачі даних для IoT-мереж з обмеженими ресурсами», у процесі виконання роботи здобувач продемонстрував високий рівень теоретичних знань та практичних навичок у використанні сучасних технологій. Перелік використаних джерел свідчить про вміння здобувача розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Рейнольда О.Ю. на оцінку «відмінно» та присвоїти йому кваліфікацію магістр з інформаційних систем та технологій.

Керівник кваліфікаційної роботи _____
(підпис)

Світлана ПОПЕРЕШНЯК
Ім'я ПРІЗВИЩЕ

« ____ » _____ 202_ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Рейнгольд О.Ю. допускається до захисту даної роботи в Експертній комісії.

Завідувач кафедрою _____
(підпис)

Каміла СТОРЧАК
Ім'я ПРІЗВИЩЕ

РЕЦЕНЗІЯ
на кваліфікаційну роботу
на здобуття освітнього ступеня магістра

здобувача вищої освіти Рейнгольда Олександра Юрійовича

(прізвище, ім'я, по батькові)

на тему «Система передачі даних для IoT-мереж з обмеженими ресурсами»

Актуальність.

В умовах сучасного розвитку моя тема є дуже важливою. Розвиток IoT призводить до значного зростання кількості підключених пристроїв, що створює нові виклики в ефективності передачі даних. Враховуючи обмежені ресурси багатьох IoT-пристроїв, як-от мала потужність батарей, невеликий обсяг пам'яті та обмежені можливості процесорів, необхідно розробляти ефективні підходи до забезпечення надійного і ефективного передавання даних. Технології LPWAN, як-от LoRaWAN та NB-IoT, пропонують енергоефективне передавання даних на великі відстані з мінімальним споживанням енергії. Вивчення цих технологій та їх впровадження в IoT-мережі з обмеженими ресурсами є важливим для підвищення ефективності та надійності таких мереж. Дослідження допоможе розширити можливості використання IoT-технологій у різних секторах економіки, забезпечуючи кращу інтеграцію і взаємодію пристроїв, що відкриє нові перспективи для розвитку інноваційних рішень.

Позитивні сторони.

1. Однією сильною стороною роботи є використання сучасних технологій та підходів, таких як LPWAN (LoRaWAN, NB-IoT), які забезпечують ефективне передавання даних на великі відстані з мінімальним енергоспоживанням.

2. Робота включає детальний аналіз основних викликів і переваг впровадження цих технологій, що дозволяє отримати комплексне уявлення про їх можливості та обмеження. Цей підхід сприяє глибшому розумінню проблематики і допомагає знаходити ефективні рішення.

3. Основною позитивною стороною цієї роботи є її актуальність і практичність. З розвитком Інтернету речей (IoT) зростає потреба в ефективних та надійних методах передавання даних, особливо для пристроїв з обмеженими ресурсами. Дослідження цієї теми дозволяє знайти оптимальні рішення для покращення роботи IoT-мереж, що є важливим для подальшого розвитку цієї галузі.

Недоліки.

1. Негативним аспектом є можливі обмеження у збиранні даних і проведенні експериментів. Збір даних може бути ускладнений через обмежений доступ до реальних IoT-пристроїв та мереж, що може вплинути на точність і об'єктивність результатів дослідження.

2. Один з основних недоліків роботи полягає в обмеженій вибірці тестованих технологій і пристроїв. Хоча дослідження охоплює основні технології LPWAN, такі як LoRaWAN і NB-IoT, проте існують інші технології, які можуть також бути релевантними для цієї теми, але не були враховані.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи магістерської.

Висновок: кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "відмінно", а здобувач Рейнгольд Олександр заслуговує присвоєння кваліфікації магістр з інформаційних систем та технологій

Рецензент:

науковий ступінь, вчене звання

(підпис)

Ім'я, ПРІЗВИЩЕ

ЗМІСТ

ВСТУП.....	13
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	12
1. МЕТОДОЛОГІЧНІ ПІДХОДИ ДО РОБОТИ ІОТ-МЕРЕЖІ.....	18
1.1 Основні визначення в мережі IoT.....	18
1.2 Архітектура IoT.....	18-19
1.2.1 Фізичний рівень.....	19-20
1.2.2 Мережевий рівень.....	20-21
1.2.3 Рівень обробки даних.....	21
1.2.4 Рівень застосувань.....	21-22
1.3 Принцип роботи IoT з обмеженими ресурсами.....	22-23
1.3.1 Зчитування інформації за допомогою датчиків.....	23-24
1.3.2 Передача даних від датчиків до хмарних сховищ.....	24
1.3.3 Обробка даних отриманих за допомогою датчиків.....	24-25
1.3.4 Передача даних на інтерфейс користувача.....	25
1.4 Еталонна модель IoT.....	26-27
1.4.1 Прикладний рівень.....	27
1.4.2 Рівень підтримки послуг та додатків.....	28
1.4.3 Мережевий рівень.....	28
1.4.4 Рівень пристроїв.....	28-29
1.4.5 Можливості управління.....	29
1.4.6 Можливості забезпечення безпеки.....	30
1.5 Переваги IoT.....	30-31
1.6 Недоліки IoT.....	31-32
1.7 Висноки до розділу 1.....	32
2. ОГЛЯД ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОТОКОЛІВ ТА ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ ТА ПОВІДОМЛЕНЬ В МЕРЕЖАХ InternetOfThings.....	33
2.1 Технології та протоколи передачі даних на довгі відстані в IoT мережах.....	33-34
2.1.1 LoRaWAN.....	34-36

2.1.2 SigFox.....	36-37
2.1.3 NB-IoT.....	37-39
2.1.4 Weightless-P.....	39-40
2.2 Технології та протоколи передачі даних на короткі відстані в IoT мережах.....	40
2.2.1 Z-Wave.....	40-41
2.2.2 NFC.....	41-42
2.2.3 RFID.....	42-43
2.2.4 Bluetooth Low Energy.....	43-35
2.2.5 Wi-Fi Halow.....	45-47
2.3 Протоколи передачі повідомлень.....	47
2.3.1 Базова топологія, яка використовується для передачі повідомлень в IoT.....	47-49
2.3.2 DDS.....	49-51
2.3.3 XMPP.....	51-52
2.3.4 CoAP.....	52-54
2.3.5 MQTT.....	54-56
2.3.6 STOMP.....	56
2.3.7 SOAP.....	57-58
2.4 Висновки до розділу 2.....	58-59
3. ПОТОЧНИЙ СТАН ТАМ МАЙБУТНІ ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ В ІОТ В УКРАЇНІ.....	60
3.1 Поточний стан технологій передачі даних в Україні.....	60-61
3.2 Перспективи розвитку технологій передачі даних в Україні в умовах блекауту.....	61-62
3.2.1 Безпілотники та дрони.....	62-63
3.2.2 Смарт-місто під час блекауту.....	63-64
3.2.3 Сучасні реалії медицини в Україні.....	64
ВИСНОВКИ.....	66
ПЕРЕЛІК ПОСИЛАНЬ.....	67
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ).....	69-74

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IoT	(Internet of Things)
NFC	(Near Field Communication)
NGN	(Next Generation Network)
RFID	(Radio Frequency identification)
SOAP	(Simple Object Access Protocol)
STOMP	(Simple Text-Oriented Messaging Protocol)
TCP	(Transmission Control Protocol)
XMPP	(Extensible Messaging and Presence Protocol)

ВСТУП

Актуальність теми – Дослідження протоколів і технологій передачі даних для мереж Інтернету речей є надзвичайно важливим через кілька ключових причин. По-перше, стрімке зростання IoT спричиняє значне збільшення кількості підключених пристроїв. По-друге, пристрої IoT мають різні вимоги до передачі даних, залежно від їх особливостей: деякі з них орієнтовані на енергоефективність і низьке споживання енергії, тоді як інші потребують високої пропускної здатності для передачі великих обсягів інформації. По-третє, із розширенням IoT зростає актуальність забезпечення безпеки, оскільки ризик кібератак і витоку конфіденційних даних постійно збільшується. Нарешті, обмежені ресурси IoT-пристроїв, такі як обчислювальна потужність, енергетичні запаси та мережеві можливості, вимагають створення ефективних протоколів передачі даних для забезпечення їх максимальної продуктивності та енергоефективності.

Мета роботи – дослідження та впровадження ефективних технологій передачі даних для IoT-мереж з обмеженими ресурсами. Це передбачає аналіз існуючих технологій та рішень, визначення їх переваг та недоліків, а також розробку рекомендацій щодо оптимального вибору та застосування технологій для забезпечення надійної, енергоефективної та безпечної передачі даних в IoT-мережах.

Завдання дослідження – у ході дослідження виконано такі завдання: проаналізовано наявні протоколи, досліджено вимоги мереж Інтернету речей, розроблено нові або вдосконалено існуючі протоколи, проведено експериментальне моделювання та оцінювання їхньої ефективності, здійснено аналіз безпеки, а також виконано валідацію та порівняльний аналіз протоколів.

Об'єкт дослідження – об'єктом дослідження є технології передачі даних у IoT-мережах з обмеженими ресурсами. Це включає як бездротові, так і дротові технології, які використовуються для забезпечення зв'язку між IoT-пристроями та мережевою інфраструктурою. Особлива увага приділяється технологіям, що

забезпечують енергоефективність, надійність і безпеку передачі даних в умовах обмежених енергетичних та пропускних можливостей.

Предмет дослідження – Предметом дослідження є методи та підходи до ефективної передачі даних в умовах обмежених ресурсів у IoT-мережах.

Методи дослідження – у даному дослідженні використовуються різні методи, включаючи аналіз літератури, експериментальні дослідження, порівняльний аналіз, моделювання та симуляцію, статистичний аналіз і методи оптимізації. Аналіз літератури охоплює вивчення наукових статей, книг та технічних документів, пов'язаних з технологіями передачі даних у IoT-мережах. Експериментальні методи включають лабораторні експерименти для вимірювання енергоспоживання, пропускної здатності та надійності передачі даних. Порівняльний аналіз дозволяє оцінити ефективність різних технологій за заданими критеріями. Моделювання та симуляція використовуються для створення комп'ютерних моделей IoT-мереж і аналізу результатів симуляції. Статистичний аналіз допомагає обробляти та оцінювати отримані експериментальні дані за допомогою статистичних методів. Нарешті, методи оптимізації розробляються для мінімізації енергоспоживання та покращення надійності передачі даних.

Наукова новизна та практична значущість отриманих результатів – Наукова новизна дослідження полягає в інноваційному підході до аналізу технологій передачі даних для IoT-мереж з обмеженими ресурсами, розробці нових методів оптимізації передачі даних для зниження енергоспоживання та підвищення надійності, а також використанні комп'ютерного моделювання для вивчення поведінки IoT-мереж. Експериментальні дослідження проводяться з використанням різних технологій передачі даних в реальних умовах експлуатації, що дозволяє отримати нові дані про їх практичну ефективність.

Практична значущість дослідження виражається у розроблених рекомендаціях для впровадження ефективних технологій передачі даних, що можуть бути використані для оптимізації роботи IoT-мереж у різних галузях. Запропоновані рішення та методи сприяють значному зниженню

енергоспоживання IoT-пристроїв, підвищенню надійності та безпеки передачі даних, що критично важливо для систем, де відмови можуть мати серйозні наслідки. Отримані результати сприяють розвитку IoT-інфраструктури та забезпечують ефективне використання існуючих технологій і створення нових рішень.

Апробація – II міжнародна науково-практична конференція «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії»

Структура кваліфікаційної магістерської роботи – магістерська робота складається з наступних структурних елементів:

1. Титульна сторінка:

Відображає назву роботи, автора, наукового керівника, навчальний заклад та рік виконання (1 сторінка).

2. Завдання на кваліфікаційну роботу включає в себе такі пункти:

- Тему кваліфікаційної роботи
- Строк подання
- Вихідні дані для роботи
- Перелік питань, які потрібно розробити
- Перелік демонстраційного матеріалу
- Дату видачі завдання
- Календарний план

3. Анотація на українській та англійській мовах:

Призначена для експрес-ознайомлення з кваліфікаційною роботою. Включає в себе відомості про обсяг кваліфікаційної роботи, кількість рисунків, таблиць, джерел згідно із списком використаних джерел (? сторінки).

4. Подання голові екзаменаційної комісії:

Включає інформацію, яка характеризує магістерську роботу та студента, а також містить рекомендації щодо допуску до захисту (? сторінка).

5. Рецензія на кваліфікаційну роботу:

Офіційний документ, у якому незалежний експерт оцінює якість виконаної роботи. Включає в себе загальну інформацію, актуальність теми, позитивні сторони, недоліки та висновок (? сторінка).

6. Зміст кваліфікаційної роботи:

Включає перелік усіх розділів, підрозділів, із зазначенням номерів сторінок.

7. Перелік умовних позначень:

У кваліфікаційній магістерській роботі є розділом, у якому перелічуються всі скорочення, аббревіатури, спеціальні символи та терміни, що використовуються в тексті роботи.

8. Вступ:

Цей розділ знайомить читача з контекстом дослідження. У ньому визначаються актуальність теми, мета, завдання, об'єкт і предмет дослідження, методи, наукова новизна та практична значущість отриманих результатів. Окрім того, вказується на апробацію роботи та наводиться структура магістерської кваліфікаційної роботи.

9. Перший розділ:

Перший розділ здебільшого має теоретичний характер. У ньому аналізуються ключові категорії та поняття, розвиток теми, розкривається суть проблеми, наводяться різні наукові підходи і власний критичний аналіз. Обґрунтовується вибір методів дослідження. Сучасний стан проблеми ілюструється практичними даними у вигляді таблиць, графіків та діаграм із посиланнями на джерела.

10. Другий розділ:

Другий розділ є аналітичним і містить системний аналіз проблеми з використанням обраних методів дослідження. Результати оформлюються у вигляді таблиць, графіків, діаграм тощо. Цей розділ є основою для формулювання рекомендацій і розробки третього розділу роботи.

11. Третій розділ:

Третій розділ підсумовує результати дослідження, виявлені проблеми та розробляє конкретні пропозиції, рекомендації і заходи для їх вирішення.

12. Висновки:

Підсумовують основні результати дослідження та роблять узагальнення щодо досягнутих цілей і виконаних завдань. Вони дають чітке розуміння того, що було отримано під час роботи, та можуть включати рекомендації для подальших досліджень чи практичного застосування.

13. Перелік посилань:

Розділ, у якому наведено список усіх джерел інформації, використаних під час написання роботи.

РОЗДІЛ 1. МЕТОДОЛОГІЧНІ ПІДХОДИ ДО РОБОТИ ІОТ-МЕРЕЖІ

1.1 Основні визначення в мережі IoT

Основи IoT включають ключові поняття і терміни, які визначають основні компоненти цієї технології. Пристрої Інтернету речей - це фізичні об'єкти, оснащені датчиками та виконавчими механізмами, які підключаються до Інтернету для збору та обміну даними. Датчики зчитують такі параметри, як температура, вологість або тиск, і перетворюють їх в електричні сигнали для подальшої обробки.

Для підключення пристроїв IoT до центральних систем використовуються як дротові (Ethernet), так і бездротові (Wi-Fi, Bluetooth, LoRa) мережі. Такі протоколи, як MQTT, CoAP і Zigbee, стандартизують обмін даними, забезпечуючи ефективність і сумісність між пристроями.

Хмарні платформи відіграють важливу роль у зберіганні та обробці великих обсягів даних, що надходять від пристроїв IoT. Це дозволяє використовувати аналітичні інструменти для прийняття обґрунтованих рішень.

Захист мереж IoT надзвичайно важливий через можливу вразливість пристроїв до кібератак. Для цього використовуються методи шифрування, аутентифікації та контролю доступу.

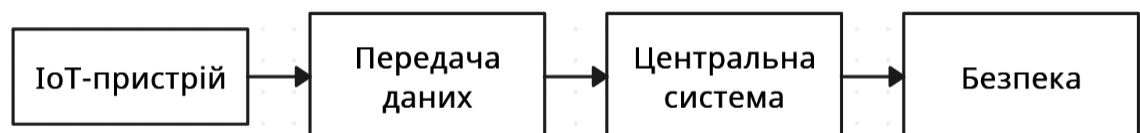


Рис. 1.1 – Процес роботи IoT-системи

Ці поняття є фундаментальними для розуміння роботи систем Інтернету речей, які використовуються в різних галузях для підвищення ефективності, безпеки та якості життя. [1]

1.2 Архітектура IoT

Архітектура Інтернету речей (IoT) складається з декількох рівнів, які забезпечують функціональність і надійність системи:

1. Фізичний рівень охоплює пристрої та датчики, що збирають дані з навколишнього середовища, як-от температура, вологість або рух.

2. Мережевий рівень відповідає за передачу даних між пристроями та центральними системами через бездротові (Wi-Fi, Zigbee) або провідні (Ethernet) мережі.

3. Рівень обробки даних займається аналізом і обробкою інформації, отриманої від датчиків, як на локальних серверах, так і в хмарних платформах.

4. Рівень застосунків надає користувачам доступ до опрацьованих даних через мобільні застосунки, веб-інтерфейси або системи моніторингу.

5. Рівень безпеки реалізує методи захисту даних і пристроїв, зберігаючи їхню конфіденційність і цілісність.

У сукупності ці рівні формують гнучку архітектуру IoT, що забезпечує безпечну та надійну роботу систем у різних сферах.

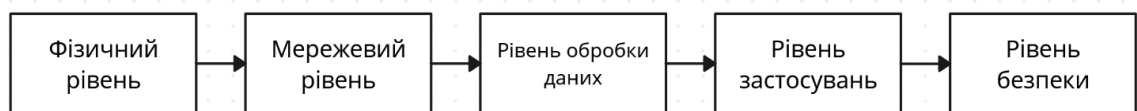


Рис. 1.2 – Архітектура IoT-системи

1.2.1 Фізичний рівень

Фізичний рівень є основною складовою архітектури Інтернету речей (IoT), оскільки саме тут відбувається взаємодія з реальним світом. На цьому рівні знаходяться різні пристрої та датчики, які збирають дані про фізичні параметри, такі як температура, вологість, тиск, освітлення, рух тощо.

Пристрої на фізичному рівні можуть варіюватися від простих сенсорів, що виконують одне конкретне завдання, до комплексних багатофункціональних систем, здатних одночасно вимірювати кілька параметрів. Наприклад, у сільському господарстві використовують датчики для моніторингу вологості ґрунту, температури повітря і рівня освітленості, що допомагає оптимізувати процес вирощування. У промисловості такі пристрої дають змогу відстежувати стан обладнання, виявляти несправності та запобігати аваріям.

Датчики генерують електричні сигнали у відповідь на зміни фізичних умов. Ці сигнали можуть бути як аналоговими, так і цифровими, залежно від конструкції пристроїв. Зібрані дані перетворюються у формати, придатні для

передавання на інші рівні IoT-систем для подальшого опрацювання. Наприклад, аналогові сигнали можуть бути оцифровані для зручності зберігання і передавання мережею.

Для передачі даних на мережевий рівень IoT-пристрої оснащуються комунікаційними модулями. Передача може здійснюватися за допомогою різних технологій і протоколів зв'язку, таких як Wi-Fi, Bluetooth, Zigbee або LoRa. Вибір конкретної технології залежить від потреб системи, включно з вимогами до пропускної здатності, енергоспоживання, радіусу дії та надійності з'єднання.

Енергоефективність є ключовим критерієм для фізичного рівня, особливо для пристроїв із живленням від батарей з обмеженим ресурсом. Для мінімізації енергоспоживання застосовуються низькоенергетичні мікропроцесори, оптимізовані протоколи зв'язку та методи зменшення частоти передачі даних. Це дає змогу значно подовжити термін автономної роботи пристроїв.

Крім того, фізичний рівень охоплює механізми калібрування і самодіагностики, які забезпечують збереження точності та надійності вимірювань. Багато сучасних датчиків здатні самостійно виконувати калібрування під час експлуатації, що забезпечує стабільну якість вимірювань протягом усього терміну служби.

Фізичний рівень IoT є джерелом даних, необхідних для подальшого опрацювання, аналізу та прийняття рішень на інших рівнях архітектури. Завдяки цьому рівню IoT-системи можуть ефективно взаємодіяти з реальним світом.

1.2.2 Мережевий рівень

Мережевий рівень в архітектурі IoT забезпечує зв'язок між пристроями, центральними системами та хмарними сервісами. Він об'єднує різні мережеві технології, такі як дротові (наприклад, Ethernet) і бездротові (Wi-Fi, Bluetooth, Zigbee, LoRa, NB-IoT) рішення. Завдяки цьому рівню дані надійно передаються від фізичних пристроїв до систем для подальшої обробки та аналізу.

Для стандартизації обміну даними між пристроями використовуються протоколи зв'язку, такі як MQTT, CoAP і Zigbee. Вони оптимізують передачу

інформації, беручи до уваги особливості IoT-систем, зокрема обмежену пропускну здатність та енергоспоживання.

Одним із ключових завдань мережевого рівня є забезпечення якості обслуговування (QoS), яка гарантує стабільність передачі даних навіть за умов обмежених ресурсів. Цей рівень також включає функції безпеки передачі інформації та управління мережею, що є важливим для надійної роботи IoT-систем.

Важливим аспектом мережевого рівня є управління криптографічними ключами, зокрема симетричними. Автоматизація цього процесу дозволяє уникнути помилок, спрощує захист інформації та забезпечує безпеку обміну даними навіть через різні захищені канали.

1.2.3 Рівень обробки даних

Рівень обробки даних в архітектурі IoT виконує функцію перетворення та аналізу інформації, зібраної з фізичних пристроїв. Основні завдання цього рівня включають фільтрацію, агрегацію та трансформацію даних для їх підготовки до подальшого використання.

Обробка може виконуватися як на локальних пристроях (наприклад, за допомогою вбудованих модулів обробки), так і на хмарних платформах. Локальна обробка зменшує обсяг переданих даних і знижує затримки, що є важливим для завдань реального часу. Використання хмарних сервісів дає можливість масштабувати обчислювальні ресурси та зберігати великі обсяги інформації.

Результатом роботи рівня обробки даних є отримання цінної аналітичної інформації, яка може використовуватися для прийняття рішень, автоматизації процесів та підвищення ефективності роботи IoT-систем. Наприклад, аналіз даних може сприяти прогнозуванню несправностей обладнання, оптимізації енергоспоживання або створенню інтелектуальних систем управління.

1.2.4 Рівень застосувань

Рівень застосувань в IoT-архітектурі дозволяє кінцевим користувачам взаємодіяти із системою через зручні інтерфейси та інструменти. Сюди входять

мобільні додатки, веб-платформи та інтерактивні системи управління, що забезпечують доступ до зібраних та оброблених даних.

Цей рівень дає змогу користувачам виконувати такі функції, як моніторинг стану пристроїв, отримання сповіщень про події, налаштування параметрів системи та віддалене управління. Наприклад, у розумному будинку додатки можуть дозволяти регулювати температуру, вмикати освітлення або відстежувати споживання енергії.

Основна мета рівня застосувань — підвищити зручність, доступність та ефективність використання IoT-рішень. Він дозволяє отримувати корисну аналітику, автоматизувати рутинні процеси та швидко реагувати на зміни в системі. [2]

1.3 Принцип роботи IoT з обмеженими ресурсами

Функціонування IoT-систем з обмеженими ресурсами ґрунтується на чотирьох основних етапах, які сприяють енергоефективності та оптимальному використанню ресурсів:

1. Збір даних

Датчики збирають інформацію з навколишнього середовища або внутрішніх параметрів пристрою. Для економії енергії використовуються низькоенергетичні сенсори та технології, які підтримують мінімальне споживання енергії під час простою.

2. Передача даних

Зібрані дані передаються до хмарних сховищ або локальних серверів. На цьому етапі застосовуються енергоефективні протоколи зв'язку (наприклад, LoRa, Zigbee, MQTT), які знижують частоту передачі даних і мінімізують обсяг переданої інформації.

3. Обробка даних

Для аналізу та отримання цінної інформації використовуються оптимізовані алгоритми та методи машинного навчання. Обробка даних може виконуватись локально або на хмарних платформах із низьким споживанням

ресурсів, що забезпечує ефективність та точність навіть при обмежених обчислювальних потужностях.

4. Інтерфейс користувача

Оброблені дані передаються до інтерфейсу користувача, де вони можуть моніторитися, аналізуватися та використовуватися для управління IoT-пристроями. При цьому рівень енерговитрат залишається оптимальним завдяки використанню легких та швидкодіючих інтерфейсів.

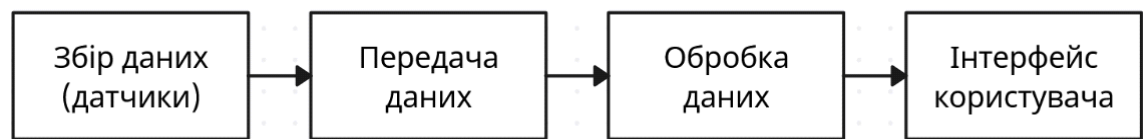


Рис. 1.3 – Основні етапи роботи IoT з обмеженими ресурсами

Ці чотири етапи забезпечують ефективну роботу IoT-систем в умовах обмежених ресурсів, сприяючи максимальній продуктивності та енергоефективності. [2]

1.3.1 Зчитування інформації за допомогою датчиків

Зчитування даних за допомогою датчиків є початковим етапом у функціонуванні IoT-систем. При роботі в умовах обмежених ресурсів важливо забезпечити енергоефективність і мінімальні витрати пристроїв. Датчики, розроблені для таких умов, зазвичай характеризуються низьким рівнем енергоспоживання і підтримують сплячі режими для зменшення енерговитрат у періоди неактивності.

Для оптимізації передачі інформації датчики можуть використовувати механізми фільтрації, які дозволяють передавати тільки важливі або значущі дані. Наприклад, передача даних може відбуватися лише при виявленні значних змін або подій, що допомагає зменшити навантаження на мережу і заощадити енергію.

Ключову роль у таких системах відіграють енергоефективні протоколи зв'язку, такі як MQTT або Zigbee. Ці протоколи оптимізують обмін даними, знижуючи обсяг переданої інформації і частоту комунікацій між пристроями.

Для подальшого зменшення обсягу даних, які потрібно передавати на центральний сервер або в хмарне сховище, попередня обробка інформації може виконуватися безпосередньо на датчику. Це може включати базову фільтрацію шумів або агрегацію зібраних даних.

1.3.2 Передача даних від датчиків до хмарних сховищ

Процес передачі даних від датчиків до хмарних сховищ вимагає ретельної оптимізації для зменшення енергоспоживання та ефективного використання пропускної здатності мережі. Дані, зібрані датчиками, передаються за допомогою енергоефективних протоколів, таких як MQTT або CoAP, які знижують обсяг переданої інформації та частоту передачі.

Щоб зменшити кількість даних для передачі, пристрої можуть виконувати попередню обробку інформації на місці. Це включає фільтрацію шумів і передачу тільки значущих змін або подій, що дозволяє уникнути передачі зайвої інформації.

Такий підхід знижує навантаження на мережу, оптимізує витрати енергії і забезпечує надійну передачу даних до хмарних сховищ. У хмарі дані проходять подальшу обробку і аналіз, що створює основу для прийняття ефективних рішень у системах IoT.

1.3.3 Обробка даних, отриманих за допомогою датчиків

Обробка даних, зібраних датчиками з обмеженими ресурсами, вимагає ефективного використання як енергії, так і обчислювальних потужностей. Початковий етап обробки виконується безпосередньо на датчику або мікроконтролері, де проводяться прості операції, такі як фільтрація шумів або нормалізація сигналів. Це зменшує обсяг даних, які потрібно передавати далі, що знижує енергоспоживання та навантаження на мережу.

Після початкової обробки дані можуть бути передані до локальних обчислювальних вузлів або хмарних сервісів для складнішого аналізу. У хмарі використовуються потужні аналітичні інструменти, алгоритми штучного інтелекту та машинного навчання для виявлення шаблонів, прогнозування і

прийняття рішень. Хмарна обробка дозволяє масштабувати ресурси відповідно до потреб, забезпечуючи високу продуктивність і точність.

Поєднання локальної та хмарної обробки забезпечує ефективність та гнучкість IoT-систем, зберігаючи енергію, оптимізуючи використання обчислювальних потужностей і забезпечуючи оперативну обробку даних для прийняття обґрунтованих рішень і автоматизації процесів.

1.3.4 Передача інформації на інтерфейс користувача

Передача інформації на інтерфейс користувача в умовах обмежених ресурсів потребує використання енергоефективних методів і технологій для забезпечення оптимальної взаємодії. Спочатку зібрані датчиками дані обробляються локально, щоб зменшити їх обсяг. Потім ці дані передаються до хмарних сервісів або центральних систем через протоколи, що мінімізують енергоспоживання.

Користувач отримує доступ до обробленої інформації через мобільні додатки або веб-інтерфейси, які дозволяють ефективно моніторити та керувати IoT-системами. Сповіщення про критичні події, такі як перевищення температури або інші важливі параметри, надсилаються через текстові повідомлення або електронну пошту, забезпечуючи швидке інформування користувача.

Автоматизація деяких процесів дозволяє системі виконувати певні дії без втручання користувача, що сприяє економії ресурсів. Це включає автоматичне коригування параметрів, таких як температура, або відправку сповіщень службам безпеки про підозрілу активність без необхідності постійного моніторингу.

Таким чином, передача інформації на інтерфейс користувача в умовах обмежених ресурсів здійснюється з акцентом на ефективність, енергозбереження та надійний доступ до необхідних даних для прийняття обґрунтованих рішень і управління системами. [3]

1.4 Еталонна модель IoT

Еталонна модель IoT для умов обмежених ресурсів спрямована на оптимізацію використання енергетичних, обчислювальних і комунікаційних ресурсів пристроїв, забезпечуючи максимальну ефективність. Модель включає кілька ключових компонентів:

- Використання енергоефективних датчиків, які працюють у сплячому режимі для зниження енергоспоживання і активуються лише під час зчитування та передачі даних.
- Локальна обробка зібраних датчиками даних для зменшення їх обсягу, що дозволяє знизити навантаження на мережу і заощадити ресурси. [4]

Передача даних здійснюється за допомогою енергоефективних протоколів зв'язку, таких як MQTT, CoAP або LoRaWAN, оптимізованих для передачі малих обсягів даних на великі відстані. Після цього дані надсилаються до хмарних сервісів, де відбувається їх подальша обробка, прогнозування і прийняття рішень завдяки потужним аналітичним інструментам та алгоритмам штучного інтелекту. Це дозволяє масштабувати ресурси відповідно до потреб.

Інтерфейси користувачів розробляються з урахуванням мінімального споживання енергії, а сповіщення про критичні події надсилаються економічними методами, такими як текстові повідомлення чи електронні листи. Система також передбачає автоматизацію деяких процесів, щоб зменшити потребу у втручанні користувача. [5] Це може включати автоматичне регулювання параметрів пристроїв або сповіщення служб безпеки.

Такий підхід дозволяє забезпечити ефективну та економічну роботу IoT-систем в умовах обмежених ресурсів, гарантуючи надійність, масштабованість і безпеку. Модель досягає балансу між функціональністю та оптимізацією ресурсів, що є критичним для IoT-систем в умовах з обмеженими можливостями.

Згідно з рекомендацією Y.2060, еталонна модель Інтернету речей (IoT) складається з чотирьох основних рівнів і двох додаткових, що охоплюють управління та безпеку. Розглянемо кожен із цих рівнів:

- Прикладний рівень
- Рівень підтримки послуг та додатків
- Мережевий рівень
- Рівень пристроїв

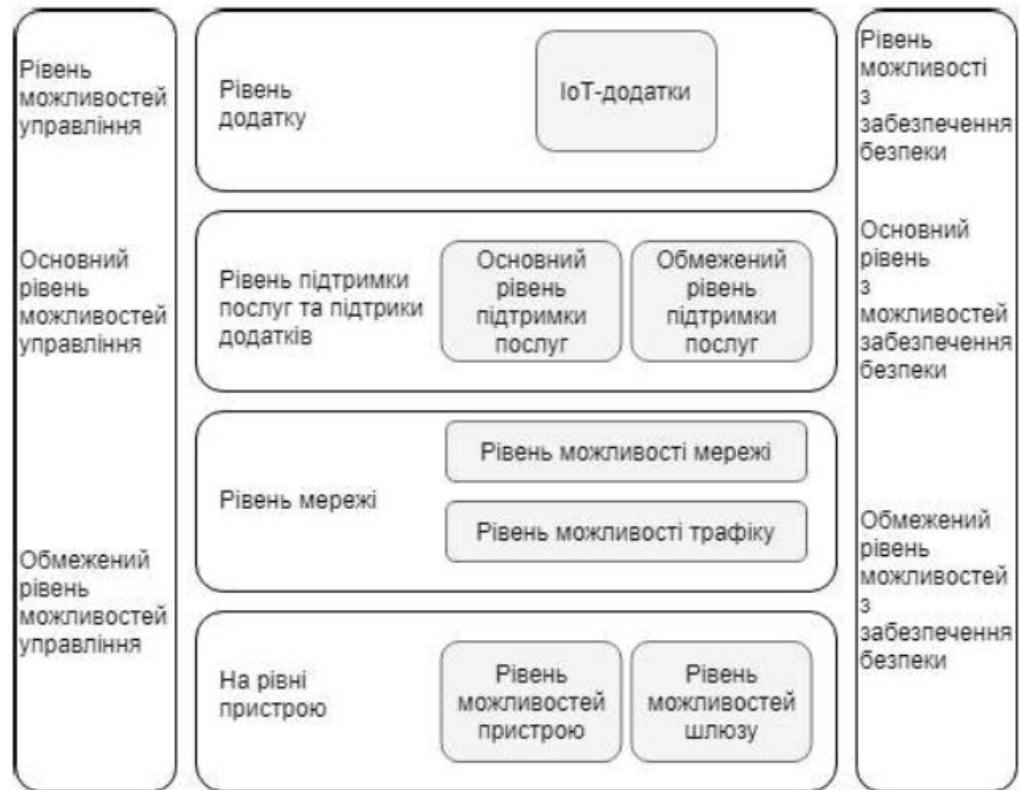


Рис. 1.4 – Еталонна модель IoT

1.4.1 Прикладний рівень

Прикладний рівень орієнтований на створення додатків, що максимально ефективно використовують ресурси. Це досягається завдяки оптимізації програмного коду, що знижує енергоспоживання та потребу в обчислювальних потужностях, а також впровадженню подієво-орієнтованої архітектури, яка активує обробку даних лише при виникненні певних подій.

Використання кешування та локального зберігання даних зменшує навантаження на мережу. Додатки повинні мати здатність автоматично відновлюватися після збоїв та забезпечувати ефективний процес оновлення, що забезпечує надійну та ефективну роботу IoT-систем. [6]

1.4.2 Рівень підтримки послуг та додатків

Рівень підтримки послуг та додатків націлений на ефективну роботу сервісів при мінімальних витратах ресурсів. Для цього необхідно оптимізувати процеси для економії енергії та обчислювальних потужностей. Використовуються легкі протоколи зв'язку, що зменшують навантаження на мережу. Основні завдання цього рівня включають обробку запитів, зберігання та доступ до даних, а також управління додатками.

Всі ці процеси повинні враховувати обмеження ресурсів для забезпечення стабільної та надійної роботи системи. Таким чином, рівень підтримки послуг забезпечує ефективність IoT-систем навіть в умовах обмежених можливостей. [4]

1.4.3 Мережевий рівень

Мережевий рівень передбачає використання оптимізованих методів для ефективного обміну даними між пристроями. Для збереження енергії та ресурсів застосовуються легкі протоколи зв'язку, такі як MQTT або CoAP, що зменшують обсяг переданих даних. Важливим аспектом є локальна обробка даних, яка дозволяє агрегувати та попередньо фільтрувати інформацію перед її передачею, що суттєво знижує навантаження на мережу.

Мережевий рівень має забезпечувати стабільний і надійний зв'язок, мінімізуючи енергоспоживання. Це включає використання механізмів управління якістю обслуговування (QoS) для надання пріоритету важливим даним. Безпека переданих даних також є критично важливою, тому застосовуються легкі алгоритми шифрування для захисту інформації без значного збільшення навантаження на ресурси пристроїв. [5]

1.4.4 Рівень пристроїв

Рівень пристроїв, що працює в умовах обмежених ресурсів, зосереджений на ефективній роботі різних IoT-пристроїв при мінімальних витратах енергії та ресурсів. Цей рівень включає всі пристрої, які здійснюють збір, передачу та іноді попередню обробку даних. Вони повинні бути розроблені для роботи в

економному режимі, використовуючи енергоефективні процесори та протоколи зв'язку.

Датчики, актуатори, мікроконтролери та інші пристрої часто працюють від батарейок, тому важливо мінімізувати їхнє енергоспоживання. Для цього використовуються різні методи, такі як сплячий режим, коли пристрій активується тільки на короткий час для збору або передачі даних.

Також пристрої повинні мати достатню потужність для виконання необхідних завдань, але не бути надмірно складними, щоб уникнути перевантаження системи та не витратити зайві ресурси. Важливо забезпечити їхню надійність та тривалість роботи, що включає використання міцних матеріалів і компонентів, які легко обслуговуються.

Отже, рівень пристроїв в умовах обмежених ресурсів вимагає збалансованого підходу до їхнього дизайну та функціонування, щоб вони могли ефективно виконувати свої завдання, використовуючи мінімальну кількість енергії та інших ресурсів. Це критично для стабільної роботи IoT-систем у різних умовах. [4]

1.4.5 Можливості управління

Загальні можливості управління в IoT включають керування пристроями, такими як віддалене ввімкнення/вимкнення, діагностика стану, оновлення прошивки або програмного забезпечення, а також контроль робочого стану пристроїв. До цього також входить управління топологією локальної мережі, що передбачає налаштування з'єднань між пристроями та керування комунікаційними шляхами. Управління трафіком і перевантаженнями охоплює виявлення перевантажень, пріоритизацію критичних потоків, резервування ресурсів і ефективний розподіл трафіку в мережі IoT. [5]

Спеціалізовані можливості управління залежать від конкретних вимог додатків або сценаріїв використання. Наприклад, управління розумними енергомережами може включати контроль ліній передачі електроенергії, моніторинг споживання та оптимізацію розподілу ресурсів.

1.4.6 Можливості забезпечення безпеки

Можливості забезпечення безпеки в IoT можна поділити на загальні та спеціалізовані. Загальні можливості включають кілька рівнів захисту. Наприклад, на прикладному рівні це авторизація, автентифікація, захист конфіденційності та цілісності даних, захист приватного життя, аудит безпеки і антивірусне програмне забезпечення. На мережевому рівні також важливими є авторизація, автентифікація, захист конфіденційності даних і сигналізації, а також забезпечення цілісності даних сигналізації. На рівні пристроїв акцент робиться на автентифікацію, авторизацію, перевірку цілісності пристрою, управління доступом і захист конфіденційності та цілісності даних.

Спеціалізовані можливості безпеки залежать від конкретних додатків чи сценаріїв. Наприклад, для мобільних платежів необхідні додаткові заходи, такі як шифрування даних, механізми аутентифікації користувачів і захист від шахрайства. [6]

1.5 Переваги IoT

Переваги IoT в умовах обмежених ресурсів дійсно вражають, особливо з точки зору ефективності та економії. Найголовнішою перевагою є енергоефективність. Завдяки використанню IoT-пристроїв можна значно знизити споживання енергії, оптимізуючи роботу пристроїв та застосовуючи енергоефективні протоколи зв'язку. Протоколи як MQTT або CoAP мінімізують обсяг переданої інформації, що дозволяє економити енергію.

Іншою важливою перевагою є зниження навантаження на мережу. Локальна обробка даних дозволяє скоротити обсяг інформації, яку необхідно передавати в хмарні сервіси, що підвищує швидкість і ефективність системи. Це особливо важливо у випадках з обмеженою пропускнуою здатністю мережі.

Також не можна забувати про автоматизацію. IoT дозволяє автоматизувати багато процесів, зменшуючи потребу у людському втручанні і дозволяючи

пристроєм працювати автономно. Це економить не лише енергію, але й час — важливий ресурс.

Ще однією ключовою перевагою є масштабованість. IoT-системи можна легко розширювати, додаючи нові пристрої та сенсори без значних додаткових витрат на ресурси. Це дозволяє швидко адаптуватися до нових вимог і завдань.

І нарешті, слід підкреслити покращення якості життя. Використання IoT у різних сферах — від розумного дому до промислових застосувань — підвищує комфорт, безпеку та зручність, дозволяючи людям більше часу присвячувати важливим для них справам. [7]

Таким чином, переваги IoT в умовах обмежених ресурсів включають ефективність, економію, автоматизацію, масштабованість та покращення якості життя. Ці фактори роблять IoT технологією, яка здатна змінити підходи до повсякденних завдань та викликів.

1.6 Недоліки IoT

Незважаючи на численні переваги IoT, існують певні виклики, особливо в умовах обмежених ресурсів.

Перший значний недолік — це енергоспоживання. Незважаючи на використання енергоефективних протоколів, пристрої все одно потребують живлення, а процес заміни батарей або підзарядки може бути неприємним і затратним, особливо коли пристроїв багато або вони знаходяться у важкодоступних місцях.

Інший важливий аспект — це безпека. Величезна кількість пристроїв, які взаємодіють між собою, створює численні точки вразливості. Злам одного пристрою може призвести до компрометації всього мережевого середовища. Це особливо небезпечно в умовах обмежених ресурсів, коли впровадження надійних систем захисту може бути надто дорогим або складним.

Ще одним недоліком є обмеження мережевих можливостей. У багатьох випадках обмежена пропускна здатність мережі або нестабільний доступ до інтернету можуть негативно вплинути на ефективність передачі даних, що знижує загальну роботу IoT-системи.

Не можна оминати складність налаштування та управління великою кількістю пристроїв. Це вимагає значних ресурсів, як людських, так і технічних, що ускладнює підтримку та обслуговування таких систем.

Зрештою, ще однією проблемою є надійність і довговічність пристроїв. Вони часто піддаються впливу зовнішніх чинників, таких як погодні умови чи фізичні пошкодження, що може призвести до скорочення терміну служби пристроїв і потреби у частій заміні або ремонті. [7]

Отже, недоліки IoT в умовах обмежених ресурсів включають енергоспоживання, проблеми з безпекою, обмеження в мережевих можливостях, складність управління та надійність пристроїв. Ці аспекти необхідно враховувати при проектуванні та впровадженні IoT-систем.

1.7 Висновки до розділу 1

Висновок з цього розділу полягає в тому, що, попри виклики, переваги IoT в умовах обмежених ресурсів можуть значно перевищити недоліки за умови правильного впровадження та управління. Ефективне використання ресурсів і енергоефективні технології дозволяють IoT-системам забезпечувати надійну та економічну роботу, підвищуючи зручність і ефективність у різних сферах життя.

РОЗДІЛ 2. ОГЛЯД І ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОТОКОЛІВ І ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ ТА ПОВІДОМЛЕНЬ У МЕРЕЖАХ ІОТ

2.1 Технології та протоколи передачі даних на довгі відстані в IoT мережах

Передача даних на великі відстані в IoT мережах при обмежених ресурсах, особливо під час блекауту, потребує застосування ефективних технологій та протоколів, що забезпечують надійність та стабільність роботи системи. Однією з ключових технологій є LoRaWAN (Long Range Wide Area Network), який відрізняється низьким енергоспоживанням і здатністю передавати дані на великі відстані. LoRaWAN використовує незарезервовані частоти, що дозволяє уникнути високих витрат на ліцензії та забезпечує великий радіус дії — до кількох десятків кілометрів у сільській місцевості. Завдяки цьому протоколу можна забезпечувати роботу в умовах відсутності постійного доступу до електромережі або для моніторингу віддалених об'єктів та середовищ. [8]

Іншою популярною технологією є Sigfox, яка також характеризується низьким енергоспоживанням і здатністю працювати на великих відстанях. Sigfox використовує глобальну мережу для передачі даних і відома своєю здатністю передавати невеликі обсяги даних на значні відстані з мінімальними витратами енергії. Це робить її ідеальною для застосувань, де потрібно передавати короткі повідомлення, як-от трекери для логістичних компаній чи сенсори для моніторингу стану навколишнього середовища. [10]

Технологія NB-IoT (Narrowband IoT) є ще однією важливою складовою для передачі даних в умовах обмежених ресурсів. NB-IoT використовує існуючу інфраструктуру стільникових мереж, що забезпечує високу надійність та широке покриття. Цей протокол оптимізований для передачі невеликих обсягів даних на низьких швидкостях при високій енергоефективності. Оскільки NB-IoT підтримується операторами мобільного зв'язку, він може використовуватися навіть під час блекауту, коли інші види зв'язку можуть бути недоступні.

Також варто згадати протокол MQTT (Message Queuing Telemetry Transport), який широко застосовується для передачі даних між датчиками і хмарними сервісами. MQTT відзначається своєю легкістю та здатністю працювати при низькій пропускну здатності мережі. Він використовує принцип "публікації/підписки", що дозволяє ефективно управляти потоками даних і знижувати навантаження на мережу. В умовах обмежених ресурсів MQTT дозволяє передавати дані з мінімальними витратами енергії та забезпечує високу надійність з'єднання. [14]

Крім того, важливо враховувати використання автономних джерел енергії, таких як сонячні батареї або генератори, для забезпечення роботи IoT пристроїв під час блекауту. Це дозволяє зберегти працездатність системи навіть при відсутності централізованого енергопостачання. Використання акумуляторних батарей з високою ємністю та ефективних енергозберігаючих технологій також сприяє довготривалій роботі пристроїв без потреби у постійній підзарядці.

2.1.1 LoRaWAN

LoRaWAN (Long Range Wide Area Network) — це комунікаційний протокол та система мережі, розроблена для пристроїв IoT, що потребують передачі даних на великі відстані з низьким енергоспоживанням. LoRaWAN використовує радіочастоти з невисокою пропускну здатністю, але з великою дальністю дії, що дозволяє пристроям обмінюватися даними навіть на відстанях до кількох десятків кілометрів у сільській місцевості або кілька кілометрів у міських умовах. [8]

Основні характеристики LoRaWAN:

- Низьке енергоспоживання: Пристрої, що використовують LoRaWAN, можуть працювати від батарейок протягом багатьох років без потреби у заміні.
- Велика дальність дії: Завдяки використанню незарезервованих частот (ISM band), дані можуть передаватись на великі відстані, що робить цю технологію ідеальною для сільських і віддалених областей.

- **Масштабованість:** LoRaWAN мережі здатні підтримувати одночасну роботу великої кількості пристроїв, що є важливим для реалізації великих IoT проектів.
- **Безпека:** Протокол підтримує два рівні шифрування даних — один на рівні мережі і один на рівні програми, що забезпечує високу безпеку передачі даних.
- **Адаптивна швидкість передачі даних:** LoRaWAN автоматично регулює швидкість передачі даних залежно від якості з'єднання, що допомагає знизити енергоспоживання і підвищити надійність зв'язку.

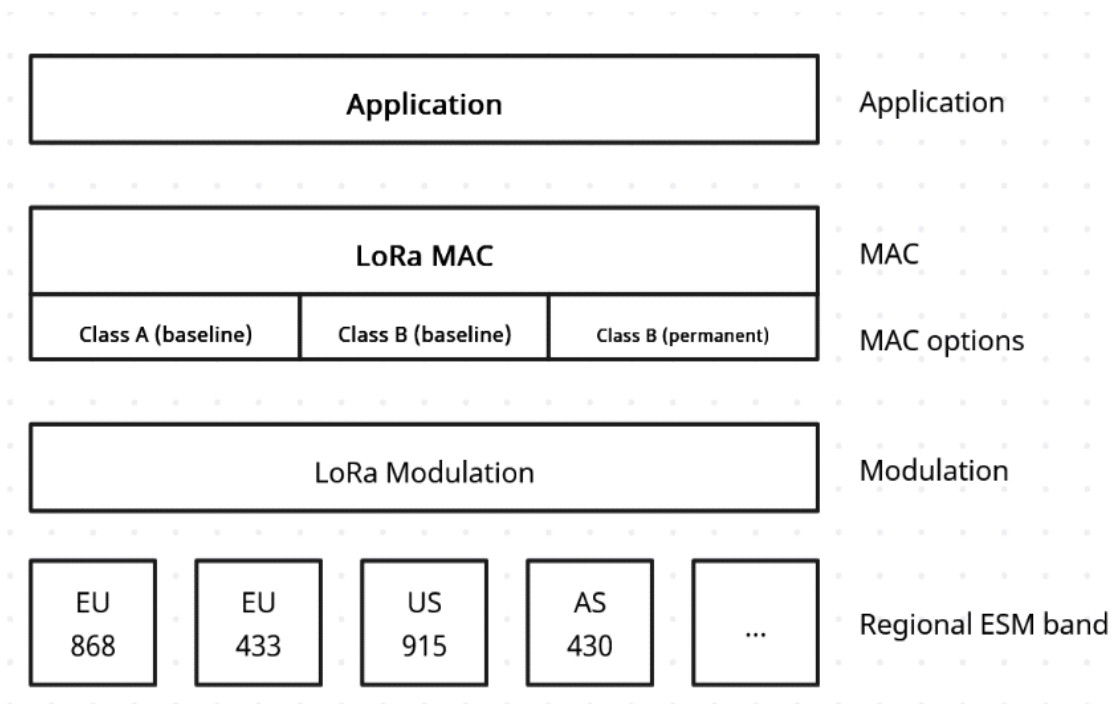


Рис. 2.1 – Типи пристроїв LoRaWAN

Завдяки своїм характеристикам, LoRaWAN знаходить широке застосування в різних галузях, таких як сільське господарство (моніторинг стану ґрунту, погоди), розумні міста (управління вуличним освітленням, моніторинг трафіку), промисловість (контроль обладнання, управління ресурсами) і багатьох інших.

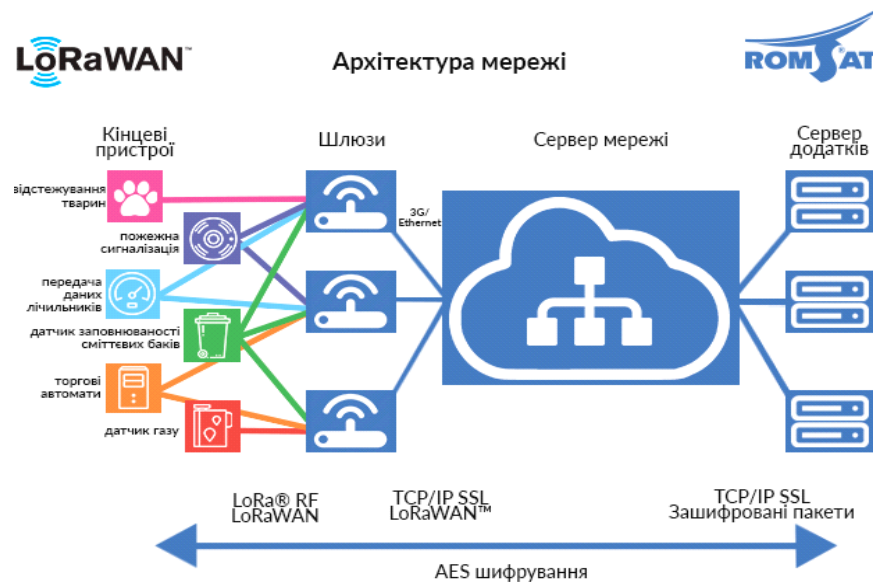


Рис. 2.2 – Архітектура мережі LoRaWAN [9]

2.1.2 SigFox

SigFox — це технологія далекодійного зв'язку, яка використовується для передачі даних з низьким енергоспоживанням, що робить її особливо цінною в умовах блекауту. Під час відключення електроенергії, де багато систем можуть втратити функціональність, SigFox продовжує працювати завдяки своїй незалежності від центральної енергомережі. Це досягається завдяки низькому споживанню енергії пристроями, що використовують цю технологію. Вони можуть працювати від батарей протягом кількох років без необхідності в частій заміні або підзарядці. [10]

SigFox використовує вузькополосний діапазон частот, що дозволяє передавати дані на великі відстані, досягаючи десятків кілометрів у сільській місцевості. Це ідеально підходить для розгортання у віддалених регіонах або у випадках, коли відсутній надійний доступ до електромережі. Завдяки простій архітектурі та низьким витратам на впровадження, SigFox може бути швидко розгорнутий і забезпечити стабільний зв'язок між великими обсягами пристроїв, навіть під час блекауту.

Що робить SigFox ще більш ефективним в умовах блекауту, це його здатність працювати в умовах обмежених ресурсів, зберігаючи при цьому високу надійність передачі даних. Це досягається за рахунок використання простих повідомлень з невеликим обсягом даних, що знижує навантаження на мережу і

дозволяє економити енергію. Таким чином, навіть у найскладніших умовах SigFox забезпечує безперервну роботу IoT пристроїв, що особливо важливо для критичних застосувань, таких як моніторинг стану навколишнього середовища, управління інфраструктурою чи надзвичайні служби. [11]

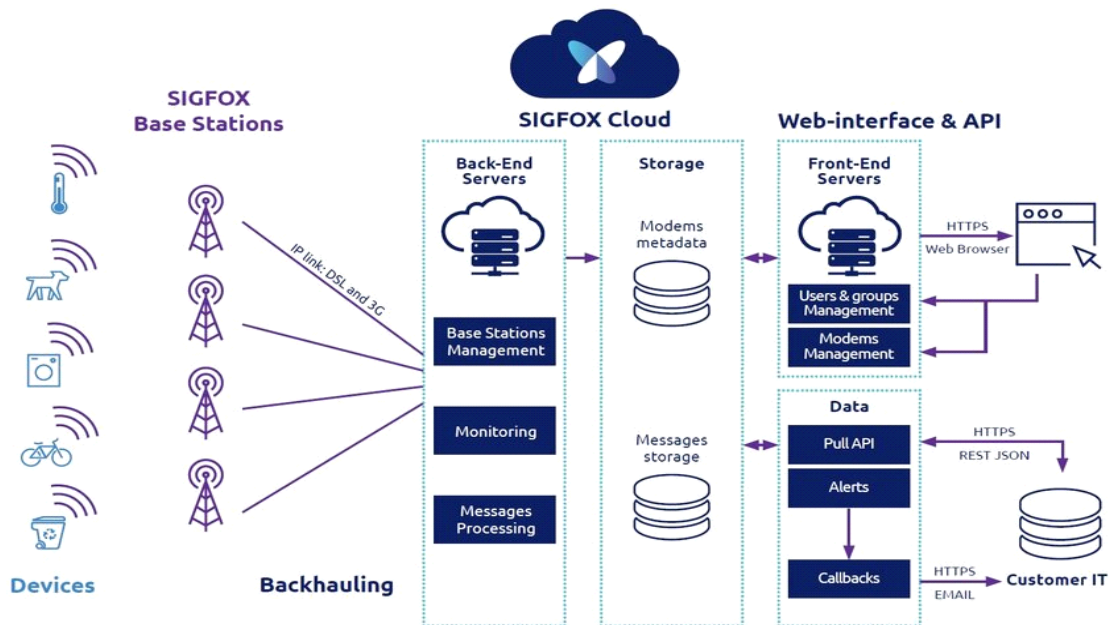


Рис. 2.2 – Архітектура мережі SigFox

Отже, завдяки своїм характеристикам SigFox є надійним рішенням для забезпечення безперервного зв'язку та передачі даних в умовах блекауту, дозволяючи IoT системам залишатися функціональними і ефективними навіть за відсутності стабільного енергопостачання.

2.1.3 NB-IoT

NB-IoT (Narrowband Internet of Things) є стандартом мобільного зв'язку, створеним для пристроїв телеметрії з низьким обсягом передачі даних. Розроблений 3GPP (3rd Generation Partnership Project) і вперше представлений у 2016 році, цей стандарт також відомий як LTE-CAT.M2. Його головні переваги включають низьке енергоспоживання, що дозволяє пристроям працювати до 10 років від однієї батареї, а також широке покриття, яке забезпечує зв'язок навіть для віддалених пристроїв. Це дозволяє NB-IoT бути ефективним навіть в умовах блекауту, забезпечуючи стабільний зв'язок і високу надійність мережі. [11]

NB-IoT відрізняється тим, що може працювати на тих самих частотах, що й технології 2G/3G/4G, включаючи діапазони 800 МГц, 900 МГц і 1800 МГц. Це

знижує витрати на впровадження, оскільки можна використовувати існуючу інфраструктуру. В умовах блекауту NB-IoT продовжує забезпечувати зв'язок завдяки низькому енергоспоживанню, що дозволяє пристроям працювати тривалий час на акумуляторних батареях.

Для забезпечення ефективної роботи NB-IoT використовуються три методи виділення частотного ресурсу: Stand-Alone (автономний), In Band (у середині смуги) і Guard Band (у захисному інтервалі). Автономний режим передбачає виділення окремого каналу шириною 200 кГц, що мінімізує інтерференцію і покращує стабільність.

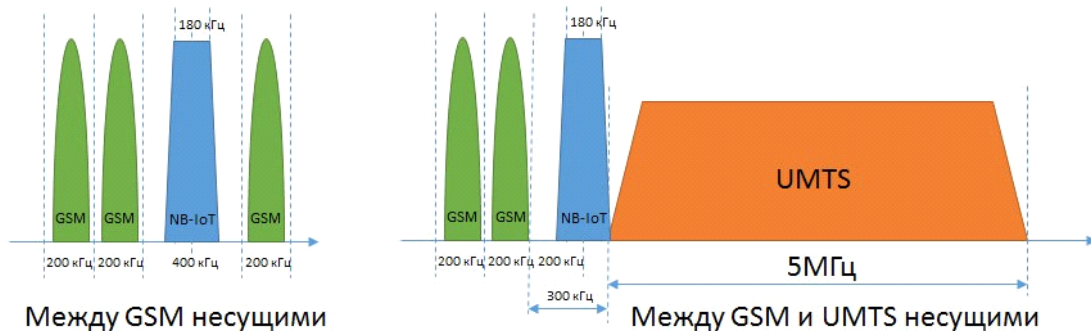


Рис. 2.3 – Варіанти розміщення NB-IoT в режимі Stand – Alone

Режим In Band використовує ресурси всередині існуючої несучої LTE, що дозволяє економити частотний ресурс, проте може спричинити інтерференцію з LTE мережею.

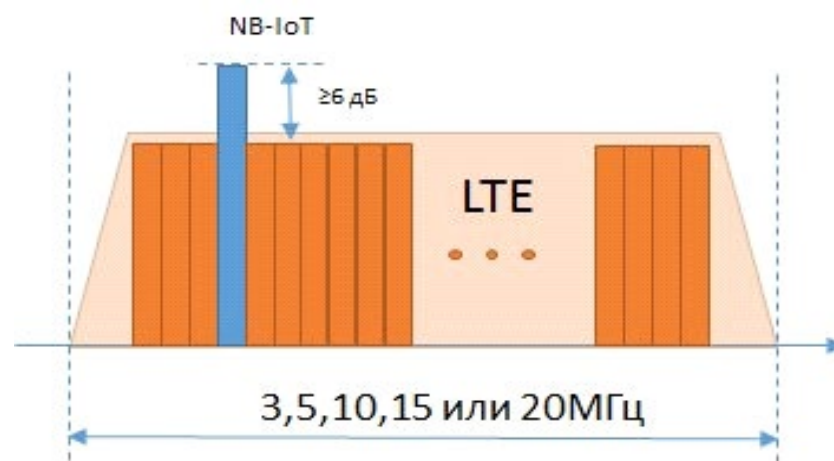


Рис. 2.4 – Розміщення Nb IoT в режимі in Band

Guard Band працює у захисному інтервалі в межах існуючої полоси LTE, що дозволяє знизити витрати частотного ресурсу і зменшити взаємний вплив з LTE.

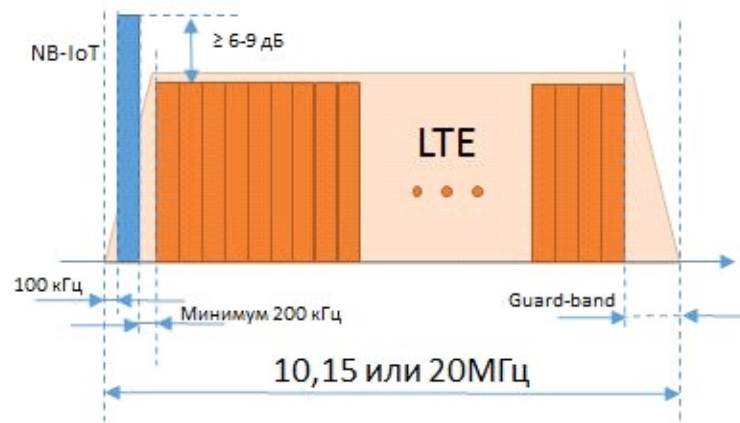


Рис. 2.5 – Розміщення NB-IoT в режимі Guard Band

Завдяки своїм перевагам, таким як низьке енергоспоживання, велике покриття і висока надійність, NB-IoT стає привабливим рішенням для забезпечення зв'язку в умовах обмежених ресурсів, особливо під час блекауту. Він знаходить застосування в різних галузях, включаючи розумні міста, сільське господарство і промисловість, де важливо підтримувати надійний зв'язок навіть у найскладніших умовах. [12]

2.1.4 Weightless-P

Weightless-P — це технологія LPWAN, яка чудово підходить для використання в умовах блекауту завдяки своїй здатності працювати тривалий час від однієї зарядки. Вона забезпечує двонаправлений зв'язок та високу щільність кінцевих пристроїв, що робить її надзвичайно надійною. Технологія включає широке покриття, масштабованість мережі та довготривалу роботу батареї, водночас зберігаючи високий рівень безпеки.

Weightless-P підтримує обмежений набір модуляцій і забезпечує надійність зв'язку завдяки можливості двонаправленого зв'язку. Її базова станція має повний контроль над мережею і пристроями в будь-який момент, що відрізняє її від інших технологій, як-от LoRa та SigFox. Це гарантує доставку повідомлень без потреби повторної передачі, що сприяє економії заряду батареї.

Додатковою перевагою є метод адаптивної швидкості передачі даних, який збільшує термін служби батареї та підвищує продуктивність мережі. Швидкість передачі даних регулюється залежно від відстані між вузлами та базовою станцією: чим ближче вузли, тим швидше передача даних, що зменшує ефірний час і знижує вихідну потужність. [13]

Weightless-P є компактною та оптимізованою системою протоколів, що знижує вартість і спрощує експлуатацію в порівнянні з NB-IoT та іншими стільниковими системами M2M. Ця технологія ефективно використовується для моніторингу, здоров'я, розумних пристроїв та інших IoT-застосувань, забезпечуючи надійний зв'язок навіть під час блекаутів.

2.2 Технології та протоколи передачі даних на короткі відстані в IoT мережах

2.2.1 Z-Wave

Z-Wave — це бездротова радіотехнологія з низьким енергоспоживанням, спеціально оптимізована для передачі простих команд управління з мінімальними затримками. Використання частотного діапазону до 1 ГГц дозволяє уникнути перешкод, що часто виникають у більш поширених частотах, таких як 2,4 ГГц, яку використовує Wi-Fi. Завдяки цьому, Z-Wave забезпечує стабільний зв'язок і надійне функціонування IoT пристроїв у будь-яких умовах. [15]

В умовах блекауту Z-Wave показує себе як надзвичайно ефективне рішення. Система з низьким енергоспоживанням дозволяє забезпечити автономну роботу пристроїв від акумуляторів протягом тривалого часу, що є критично важливим під час відключення електропостачання. Завдяки дистанційному керуванню і використанню радіохвиль низької потужності, Z-Wave дозволяє мати повний контроль над домашньою безпекою та енергоспоживанням з мінімальними зусиллями. Ви можете створити власну систему домашньої автоматизації, програмуючи такі елементи будинку, як освітлення, опалення, кухонні прилади, охолодження та систему безпеки, що значно підвищує комфорт і безпеку в умовах відсутності електрики.

Технологія Z-Wave також має переваги у простоті використання та енергоефективності. Вона дозволяє заощаджувати енергію, знижуючи витрати на електроенергію, а також економить час, що важливо в умовах блекауту. Мережа з подібною до сітки структурою дозволяє сигналам проходити через стіни, поверхи та меблі, забезпечуючи надійне підключення у всіх частинах будинку. Це

особливо корисно, коли немає світла, оскільки підтримується стабільний зв'язок між пристроями, навіть якщо деякі з них тимчасово виходять з ладу. [16]

2.2.2 NFC

NFC (Near Field Communication) — це технологія, розроблена компаніями Sony та NXP Semiconductors, яка поєднує безконтактні технології зв'язку та радіочастотну ідентифікацію. NFC дозволяє обмінюватися різними типами інформації, такими як зображення, музичні файли, номери телефонів або цифрові ключі, між двома пристроями, які знаходяться поруч один з одним і підтримують NFC. Приклади таких пристроїв включають смарт-картки, різноманітні портативні пристрої та зчитувачі RFID. NFC також може використовуватися для доступу до даних або послуг, таких як електронні замки або безготівкові платежі. [18]

Однією з відмінних рис NFC є можливість обміну даними між двома активними пристроями, на відміну від інших технологій безконтактного зв'язку, де дані передаються лише від активного пристрою до пасивного. NFC активно використовується для взаємодії з пристроями RFID. Для забезпечення сумісності між RFID-картками та мобільними телефонами різних виробників проводяться перевірки цифрових протоколів та вимірювання всіх важливих характеристик радіочастотного сигналу, таких як часові параметри, чутливість і амплітуда приймача в активному режимі, а також частота несучої амплітуди сигналу. [17]

В умовах блекауту технологія NFC стає надзвичайно корисною. Вона дозволяє здійснювати безконтактні мобільні платежі, ідентифікацію та автентифікацію навіть без центрального електропостачання. Наприклад, за допомогою смартфона можна отримати доступ до важливих приміщень або активувати аварійне освітлення. Завдяки низькій вартості впровадження та простоті використання, NFC дозволяє швидко і ефективно взаємодіяти з пристроями, забезпечуючи надійний зв'язок навіть в умовах відключення електрики. Ця технологія забезпечує простоту та зручність користування, що особливо важливо в критичних ситуаціях.

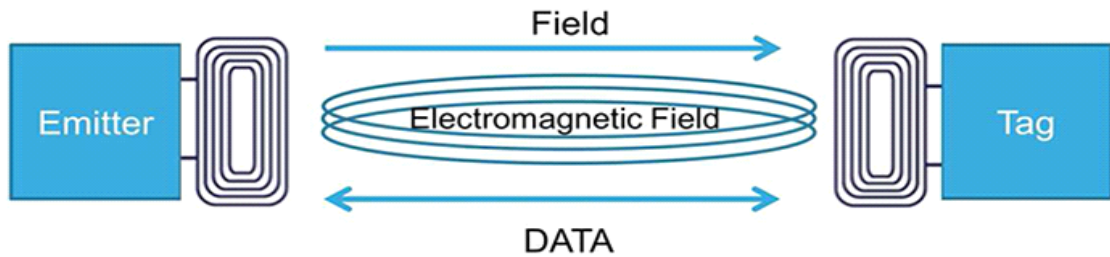


Рис. 2.6 – Принцип роботи NFC [17]

2.2.3 RFID

RFID (Radio Frequency Identification) — це метод автоматичної ідентифікації об'єктів, який використовує радіосигнали для зчитування або запису даних, що зберігаються у спеціальних мітках, відомих як RFID-мітки. Будь-яка система RFID складається зі зчитувача (рідера) та транспондера (RFID-мітки або тегу). Більшість RFID-міток мають інтегральну схему для обробки та зберігання інформації, модулювання та демодулювання радіосигналу, а також антену для передачі та отримання сигналу. Для роботи з такими мітками потрібне відповідне програмне забезпечення, яке забезпечує аналіз та збір інформації.

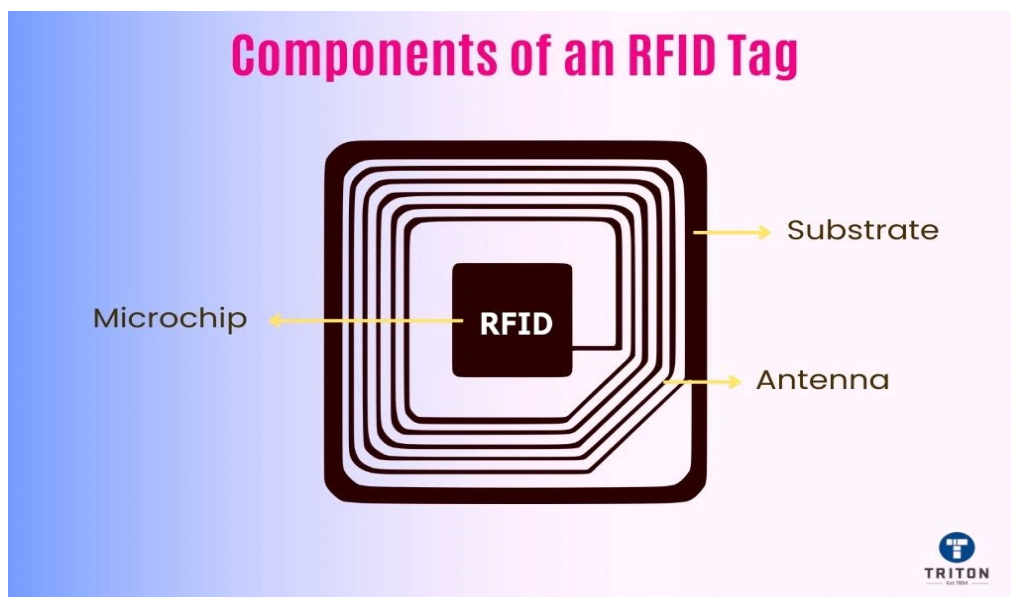


Рис. 2.7 – Будова RFID-мітки

Існує два типи RFID-міток: активні та пасивні. Активні мітки мають власне джерело живлення, що дозволяє їм самостійно передавати сигнал на великі відстані. Пасивні мітки не мають власного джерела живлення і активуються лише після отримання сигналу від зчитувача, передаючи збережену в них інформацію. [19]

В умовах блекауту RFID-технологія має багато переваг. Вона дозволяє ефективно управляти товарними запасами або відстежувати час на спортивних змаганнях навіть без постійного електроживлення. Пасивні RFID-мітки, які не потребують власного джерела живлення, є особливо корисними в таких умовах, оскільки вони активуються зчитувачем і не залежать від централізованого живлення. Наприклад, RFID-мітки можуть бути використані для маркування великої рогатої худоби з метою запису інформації про проходження ветеринарного огляду. У транспортній галузі RFID допомагає ідентифікувати автомобілі, навіть якщо вони рухаються на великій швидкості.

Деякі авіалінії використовують RFID-мітки для ефективного відстеження багажу, що є критично важливим в умовах обмеженого електропостачання. RFID також вбудовується у біометричні паспорти та кредитні картки для забезпечення безпечного доступу до захищених зон. Навіть за відсутності прямої видимості зчитувача, RFID-мітки можуть бути прочитані на відстані кількох метрів, що забезпечує їх ефективність у різних сценаріях. [19]

2.2.4 Bluetooth Low Energy

Bluetooth Low Energy (BLE) вперше з'явилася в специфікації Bluetooth 4.0 і продовжується до версії Bluetooth 5.0. Ця технологія відзначається значно меншим енергоспоживанням порівняно з попередніми версіями Bluetooth, що дозволяє багатьом пристроям працювати протягом року або навіть довше, використовуючи невелику кнопкову батарею без необхідності заряджання. Це відкриває можливості для застосування невеликих датчиків, які можуть постійно функціонувати та взаємодіяти з іншими пристроями.

Енергоефективність BLE значно розширює можливості для його використання в різних галузях, включаючи Інтернет речей (IoT) та носимі пристрої. Завдяки низькому енергоспоживанню, пристрої можуть безперервно відстежувати, моніторити та обмінюватися даними з іншими пристроями, що сприяє розширенню автоматизації та бездротового зв'язку. У цілому, BLE відіграє важливу роль у вдосконаленні бездротових комунікацій, забезпечуючи низьке

енергоспоживання, тривалий термін роботи на батареї та ефективний зв'язок між пристроями. [20]

BLE складається з кількох рівнів, які забезпечують функціональність і взаємодію між пристроями. Основні рівні BLE включають:

Рівень додатків: реалізує корисну логіку роботи для кінцевого користувача.

Рівень хоста: забезпечує верхні рівні стеку протоколів Bluetooth, включаючи Generic Access Profile (GAP), Generic Attribute Profile (GATT), Attribute Protocol (ATT), Security Manager (SM), Logical Link Control and Adaptation Protocol (L2CAP) та Host Controller Interface (HCI).

Рівень контролера: відповідає за обробку нижніх рівнів стеку протоколів Bluetooth і включає Link Layer (LL) та фізичний рівень (PHY).

В умовах блекауту BLE є ідеальним рішенням завдяки своїй здатності забезпечувати надійний зв'язок між компактними пристроями з мінімальним енергоспоживанням. Наприклад, у порівнянні з класичними Bluetooth-рішеннями, BLE споживає в 10-20 разів менше енергії і може передавати дані на відстань понад 100 метрів. Це робить його особливо корисним для пристроїв, які не можуть вмістити повноцінний акумулятор або велику батарею, але потребують тривалого терміну роботи без заряджання.

Окрім цього, BLE забезпечує високу безпеку, надійність, низьку затримку при підключенні та низьку споживчу потужність. Важливою особливістю є його здатність до адаптивного переналаштування частоти, що допомагає уникати помилок передачі сигналу, перешкод та інтерференції.

З випуском специфікації Bluetooth 5.0 BLE став ще більш придатним для Інтернету речей. Новий стандарт пропонує значне підвищення швидкості передачі даних, наближаючись до швидкостей HSPA та LTE, зберігаючи при цьому низьке енергоспоживання. Це робить BLE перспективним вибором для побудови мереж IoT, особливо в умовах обмежених ресурсів та під час блекауту, де енергоефективність є критично важливою. Навіть якщо Bluetooth 5.0 поки не є повсюдним, очікується, що в майбутньому всі мобільні пристрої будуть підтримувати цей стандарт.

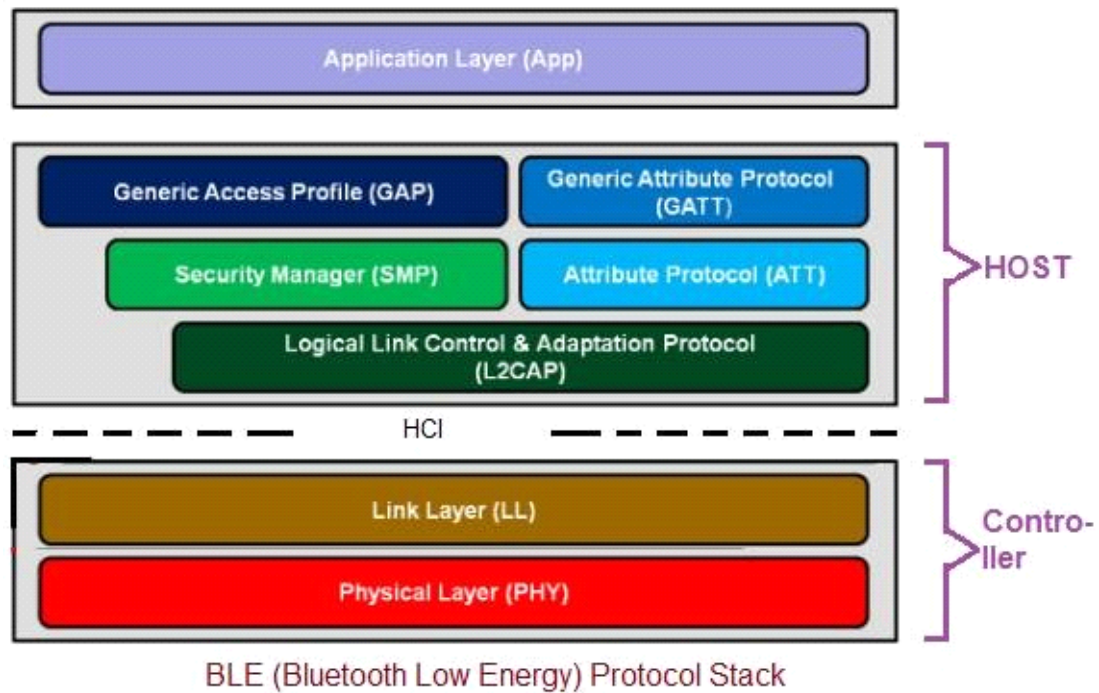


Рис. 2.8 – Архітектура BLE

Таким чином, BLE має значні переваги, такі як низьке енергоспоживання, швидкість передачі даних, висока безпека та здатність до адаптивного переналаштування частоти, що робить його ідеальним вибором для різноманітних застосувань в IoT та інших областях, особливо в умовах блекауту.

2.2.5 Wi-Fi HaLow

Wi-Fi HaLow є розширенням стандарту бездротових мереж IEEE 802.11, представленим у 2017 році. Цей протокол використовує діапазон частот 900 МГц, який не потребує ліцензування, що забезпечує більшу дальність дії порівняно зі звичайними Wi-Fi мережами, які працюють на частотах 2,4 ГГц та 5 ГГц. Однією з ключових переваг Wi-Fi HaLow є його низьке енергоспоживання, що дозволяє створювати великі групи станцій або датчиків, які взаємодіють між собою для забезпечення зв'язку та підтримки концепції Інтернету речей (IoT). Порівняно з Bluetooth, Wi-Fi HaLow забезпечує нижче енергоспоживання, вищу швидкість передачі даних та більший діапазон покриття. Ці особливості роблять Wi-Fi HaLow привабливим вибором для застосувань в IoT та інших галузях, де потрібна далека дія мережі та мінімальне енергоспоживання.

Wi-Fi HaLow розширює можливості енергоефективних сценаріїв використання у розумних будинках, автомобілях, торгівлі, промисловості,

сільському господарстві та інших сферах. Цей протокол дозволяє з'єднувати пристрої малої потужності, такі як датчики та портативні комп'ютери, в діапазоні 900 МГц. Wi-Fi HaLow успадковує позитивні якості попередніх версій Wi-Fi, такі як надійний захист інформації, широку сумісність обладнання та простоту встановлення.

Пристрої, що підтримують Wi-Fi HaLow, можуть також працювати в діапазонах 2,4 ГГц та 5 ГГц, що дозволяє їх інтегрувати у вже існуючу екосистему, яка нараховує понад 7 мільярдів пристроїв. Крім того, Wi-Fi HaLow підтримує підключення по протоколу IP, що сприяє роботі з хмарними сервісами, що є важливим для Інтернету речей. До однієї точки доступу можуть підключатися близько 1000 пристроїв, що значно розширює його потенціал для створення масштабних мереж IoT.

В умовах блекауту Wi-Fi HaLow є особливо цінним завдяки своїй здатності забезпечувати стабільний зв'язок з мінімальним енергоспоживанням. Наприклад, його можна використовувати для моніторингу стану сільськогосподарських угідь або управління розумними пристроями в будинку. Завдяки своїй ефективності та низькому енергоспоживанню, Wi-Fi HaLow дозволяє підтримувати зв'язок між пристроями протягом тривалого часу навіть за відсутності централізованого електропостачання.

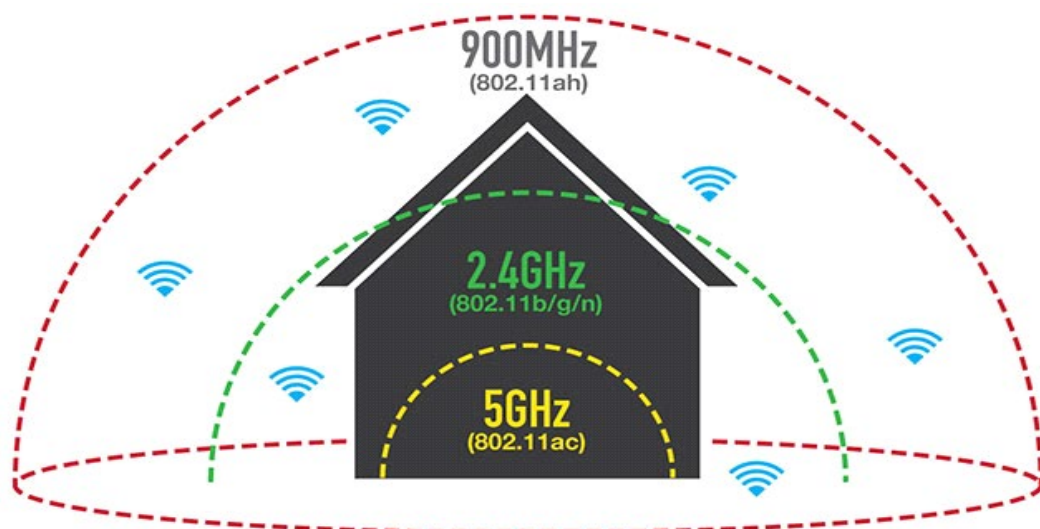


Рис. 2.9 – Порівняння різних протоколів Wi-Fi за зоною покриття

Отже, Wi-Fi HaLow є потужним інструментом для забезпечення зв'язку в IoT мережах, особливо в умовах блекауту. Його характеристики, такі як низьке

енергоспоживання, великий діапазон покриття та висока швидкість передачі даних, роблять його ідеальним вибором для широкого спектра застосувань в Інтернеті речей та інших галузях.

2.3 Протоколи передачі повідомлень

Передача повідомлень у мережах Інтернету речей (IoT) стикається з певними викликами. Незважаючи на те, що кожен окремий сенсорний вузол може генерувати невелику кількість даних, більшість IoT-сервісів залежить від обробки інформації з великої кількості таких вузлів. Це значно відрізняється від традиційних мережевих архітектур, таких як телефонні мережі або класичні клієнт-серверні системи.

У зв'язку з цим виникає нова архітектура, де існує багато джерел і багато одержувачів, а обсяг трафіку з сенсорних вузлів може значно варіюватися — від дуже малих до дуже великих значень. Звичайні прикладні протоколи передачі повідомлень не підходять для такого типу використання.

Отже, існує потреба у розробці нових протоколів та архітектур, які враховуватимуть особливості мереж IoT, такі як масштабованість, ефективне управління трафіком, оптимізація енергоспоживання та забезпечення безпеки передачі даних. Це важливий аспект для успішного впровадження IoT та побудови ефективних і надійних мереж з численними пристроями.

2.3.1 Базова топологія, яка використовується для передачі повідомлень в IoT

Шаблон проектування передачі повідомлень, відомий як "видавець-підписник" (Publisher-Subscriber, або pub/sub). У цій моделі існують два ключові елементи: видавець (publisher), який генерує та розповсюджує інформацію, і передплатник (subscriber), який отримує цю інформацію.

В понятті "підписка" йдеться про процес, який виконують учасники для отримання інформації від певного видавця. Підписка дозволяє передплатнику вказати, яку саме інформацію він хоче отримувати та в якому форматі. Крім цього, вона дає змогу встановити параметри частоти отримання інформації та

інші налаштування, що регулюють збір і передачу даних від видавця до передплатника.

Цей підхід ефективно організовує передачу повідомлень у мережах IoT, забезпечуючи гнучкість і масштабованість. Він дозволяє передплатникам отримувати тільки потрібну їм інформацію та налаштовувати параметри її отримання відповідно до своїх потреб. Це сприяє ефективному управлінню трафіком та ресурсами мережі, що є критично важливим для успішної реалізації проєктів IoT.

Розглянемо ситуацію, коли сенсорний вузол збирає дані від багатьох датчиків і передає їх відповідно до параметрів підписки, за запитом або автоматично через певні інтервали часу. Датчики, зазвичай, прості та постійно передають оновлювані дані про вимірювані параметри. Для ефективної передачі цих даних, їх об'єднують у вузли з мікроконтролерами, які забезпечують зчитування даних та їх відправлення на сервер за певними алгоритмами.

Для взаємодії з системою клієнт використовує програму, встановлену на персональному пристрої. Ця програма відображає отримані дані від датчиків або вже оброблену сервером інформацію і дозволяє керувати системою.

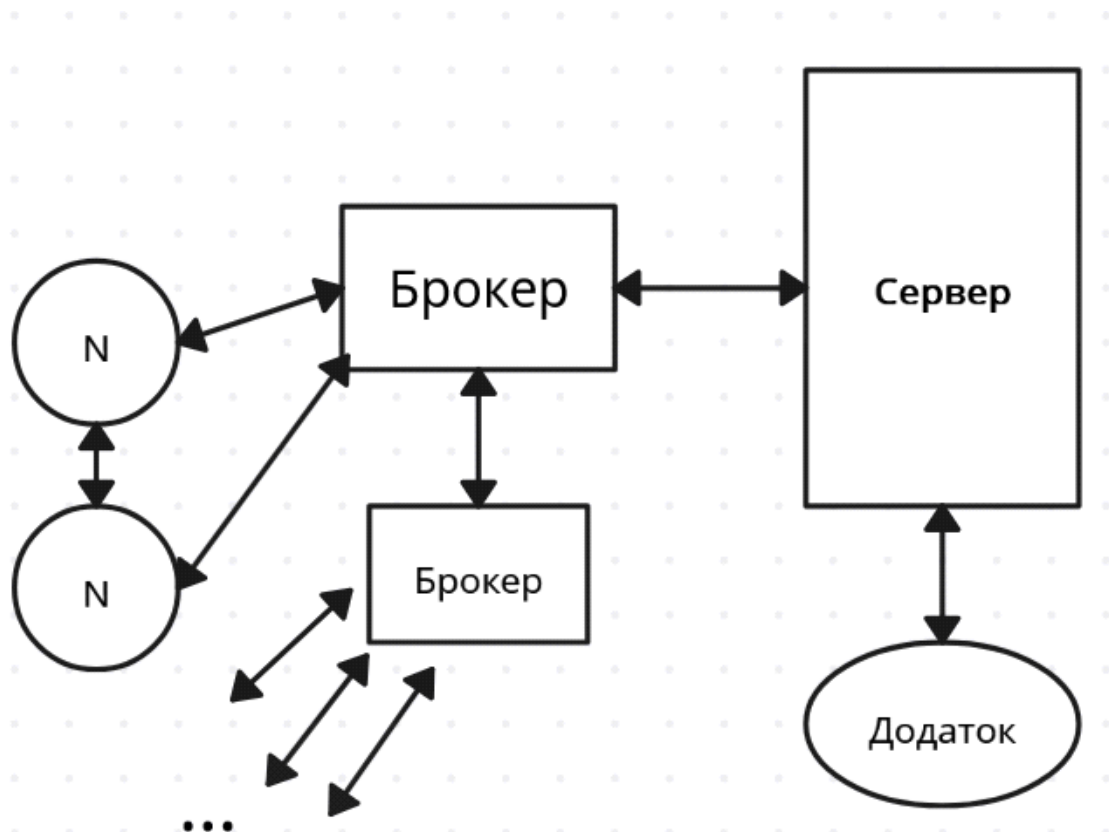


Рис. 2.10 – Топологія системи, яка виконує передачу даних між різними вузлами мережі IoT

У цій топології також використовується брокер (Broker) — сервер, що отримує інформацію від видавців (сенсорних вузлів) і передає її передплатникам. У складних системах брокер може виконувати різні операції, пов'язані з аналізом і обробкою даних. Він встановлює пріоритети з'єднань і створює черги для передачі повідомлень. Черга повідомлень — це контейнер, де зберігаються повідомлення під час їх передачі. Якщо ресурси каналу зв'язку обмежені або одержувач недоступний, черга зберігає повідомлення до тих пір, поки вони не будуть доставлені.

Таким чином, ця топологія ефективно підтримує взаємодію між різними вузлами мережі IoT, забезпечуючи надійну передачу даних і гнучке управління ресурсами.

2.3.2 DDS

DDS (Direct Digital Synthesis), або прямий цифровий синтез, є методом генерування точних і стабільних частот із єдиної довідкової частоти. Цей метод широко використовується в комунікаційних системах, вимірювальних приладах і обробці сигналів. Основна ідея DDS полягає у використанні цифрового фазового акумулятора для створення хвильової форми, яка потім перетворюється в аналоговий сигнал за допомогою ЦАП (цифро-аналоговий перетворювач).

DDS працює наступним чином: фазовий акумулятор накопичує фазову інформацію на кожному тактовому циклі і оновлюється шляхом додавання частотного контрольного слова до його поточного значення. Вихід фазового акумулятора використовується як адреса для таблиці пошуку, яка зберігає зразки хвильової форми, наприклад, значення синусоїдальної хвилі. Отримані цифрові значення потім перетворюються в аналоговий сигнал за допомогою ЦАП.

Однією з головних переваг DDS є висока точність і стабільність генерованих частот. Гнучкість цієї технології дозволяє легко змінювати частоту шляхом коригування частотного контрольного слова. Крім того, DDS забезпечує

швидке перемикання частот і модуляцію, що робить його особливо корисним для застосувань, де потрібна висока точність і надійність.

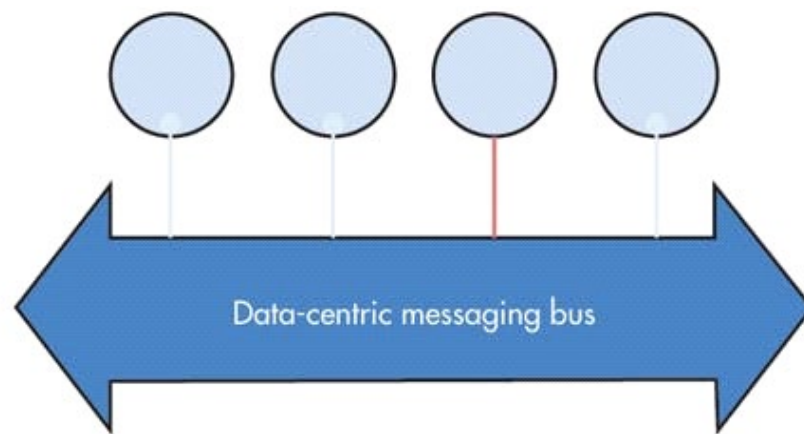


Рис. 2.11 – Принцип з'єднання пристроїв за допомогою протоколу DDS в IoT

В умовах блекауту забезпечення безперебійної роботи систем DDS може бути складним завданням, однак існує кілька рішень, які можуть допомогти. Наприклад, використання джерела безперебійного живлення (UPS) може забезпечити резервне живлення для DDS системи, дозволяючи їй працювати під час відключення електрики. Також можна інтегрувати резервне живлення від батарей, яке дозволить підтримувати роботу DDS протягом обмеженого часу. Крім того, можна впровадити механізми захисту від збоїв, які дозволять плавно вимикати DDS систему або переключатися на безпечний режим під час зникнення живлення. Використання резервних джерел живлення також може забезпечити безперервну роботу системи навіть у разі відмови одного з джерел.

DDS часто застосовується в критичних системах, де надійність і точність є важливими, таких як аерокосмічна галузь, медичні прилади і промислова автоматизація. Забезпечення здатності цих систем працювати під час відключення електрики є важливим для підтримання їх функціональності та безпеки.

Отже, DDS є потужним інструментом для генерування точних і стабільних частот, і його використання в умовах блекауту потребує додаткових заходів для забезпечення безперебійної роботи та захисту системи.

2.3.3 XMPP

XMPP (Extensible Messaging and Presence Protocol) — це протокол, який забезпечує обмін повідомленнями та інформацією про статус користувачів у реальному часі. Він був розроблений на основі технології Jabber і призначений для використання в децентралізованих мережах, забезпечуючи гнучкість і надійність у передачі даних.

Основна структура XMPP складається з кількох ключових компонентів. Клієнти — це програми, які користувачі використовують для надсилання та отримання повідомлень. Сервери обробляють ці повідомлення, передаючи їх від одного клієнта до іншого, та забезпечують підтримку таких функцій, як присутність, що показує статус користувачів (наприклад, онлайн або відсутній). Протокол XMPP визначає набір правил для передачі та обробки повідомлень, що робить його сумісним з різними форматами даних, включаючи текст, файли, аудіо та відео.

- XMPP підтримує різні можливості, серед яких:
- Відправка та отримання текстових повідомлень.
- Показування статусу користувача (присутність).
- Передача файлів між користувачами.
- Створення та участь у групових чатах.
- Інтеграція з іншими протоколами, такими як HTTP або SMTP, для розширення функціональності.

У умовах блекауту XMPP може стати важливим інструментом для підтримання зв'язку. Оскільки цей протокол може працювати в децентралізованих мережах, він не залежить від єдиного центрального сервера. Це дозволяє забезпечити зв'язок навіть тоді, коли звичні канали комунікації недоступні. Під час стихійних лих або технічних несправностей, XMPP може допомогти організувати зв'язок між різними групами або організаціями.

Окрім того, XMPP можна використовувати у автономних або локальних мережах, які не залежать від зовнішнього інтернет-з'єднання. Це забезпечує

додаткову надійність і стійкість системи в умовах, коли зв'язок із зовнішнім світом може бути перерваний.

Отже, XMPP є ефективним і гнучким протоколом, який забезпечує надійний зв'язок у будь-яких умовах, включаючи блекаут. Завдяки своїй здатності працювати у децентралізованих мережах та підтримці різних форматів повідомлень, XMPP є важливим інструментом для організації зв'язку та координації дій у надзвичайних ситуаціях.

2.3.4 CoAP

CoAP (Constrained Application Protocol) — це спеціалізований протокол, розроблений робочою групою IETF-CORE для використання в мережах і пристроях з обмеженими ресурсами, зокрема для машинно-машинних (M2M) додатків. Протокол CoAP можна розглядати як легшу версію HTTP, адаптовану для роботи в умовах обмежених ресурсів. Він використовує транспортний протокол UDP, що забезпечує ефективну передачу даних з мінімальними затримками.

CoAP використовує невелику кількість повідомлень, що складаються переважно з запитів і відповідей. Основні типи повідомлень включають GET (отримання інформації про ресурс), PUT (встановлення нового завдання для ресурсу), POST (зміна дій над ресурсом), DELETE (видалення можливостей ресурсу) та CONNECT (встановлення з'єднання). Ці повідомлення дозволяють клієнтам (користувачьким додаткам) керувати та спостерігати за ресурсами. Особливо корисною є функція спостереження, коли сервер продовжує надсилати відповіді після початкового повідомлення, дозволяючи організувати потокову передачу даних про зміни стану датчиків.

У мережах, що складаються з сенсорних вузлів і брокерів, які забезпечують зв'язок, для реєстрації, конфігурації та передачі інформації часто використовуються два основні протоколи — XMPP та CoAP. Вибір конкретного протоколу залежить від умов роботи мережі. XMPP зазвичай використовується в системах освітлення та клімату, а також для адресації пристроїв у невеликих персональних мережах. З іншого боку, CoAP призначений для роботи в умовах

обмежених ресурсів і низького енергоспоживання, що робить його ідеальним для застосування в системах датчиків температури та інших пристроях у розумних будинках.

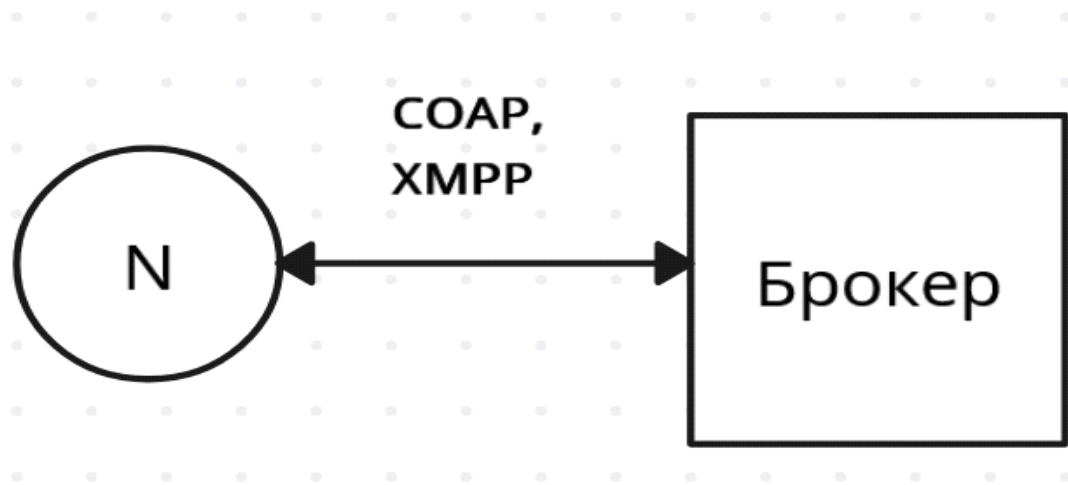


Рис. 2.12 – Сегмент мережі де використовується протокол CoAP та XMPP

В умовах блекауту CoAP виявляється надзвичайно корисним завдяки своїй здатності працювати в умовах низької енергії та обмежених ресурсів. Пристрої, що використовують CoAP, можуть працювати від акумуляторів або інших автономних джерел живлення, забезпечуючи стабільний зв'язок і контроль навіть за відсутності центрального електропостачання. Це дозволяє забезпечити безперервну роботу критично важливих систем, таких як моніторинг температури, управління освітленням і безпекою, навіть у випадках зникнення електроживлення.

Таким чином, CoAP є ефективним протоколом для використання в умовах обмежених ресурсів і блекауту, забезпечуючи надійний зв'язок і управління в системах з низьким енергоспоживанням. Він дозволяє зберегти функціональність і безпеку IoT пристроїв, навіть у найскладніших умовах.

2.3.5 MQTT

MQTT (Message Queue Telemetry Transport) є відкритим протоколом обміну даними, що відзначається своєю легкістю та компактністю. Він спеціально розроблений для передачі даних у віддалених мережах з обмеженою пропускну здатністю та обмеженим об'ємом коду. Цей протокол широко використовують у системах M2M (машина-машина) для забезпечення ефективного зв'язку між пристроями.

Окрім основного протоколу, існує також його варіант — MQTT-SN (MQTT для мереж датчиків), раніше відомий як MQTT-S. Цей варіант розроблений для бездротових вбудованих пристроїв, які не підтримують мережі TCP/IP.

Повідомлення в протоколі MQTT структуровані таким чином, що містять два основні заголовки. Перший, фіксованої довжини, включає основну інформацію про повідомлення, а другий, змінної довжини, залежить від типу повідомлення і містить додаткові параметри. Саме корисне навантаження повідомлення також має змінну довжину і містить дані, що передаються.

Основний заголовок повідомлення складається з таких компонентів: тип повідомлення, прапор дублювання, рівень якості обслуговування (QoS), прапор збереження повідомлення та залишкова довжина. Тип повідомлення визначає його функціональну роль, наприклад, чи це публікація, підписка або підтвердження. Прапор дублювання вказує, чи є повідомлення дублікатом, що забезпечує надійність доставки. Рівень якості обслуговування визначає ступінь гарантії доставки повідомлення, з трьома можливими рівнями: QoS 0, QoS 1 та QoS 2. Прапор збереження вказує, чи потрібно зберігати останнє повідомлення на брокері, щоб нові підписники отримали його при підписці на тему. Залишкова довжина вказує загальну довжину повідомлення, що включає заголовки та корисне навантаження.

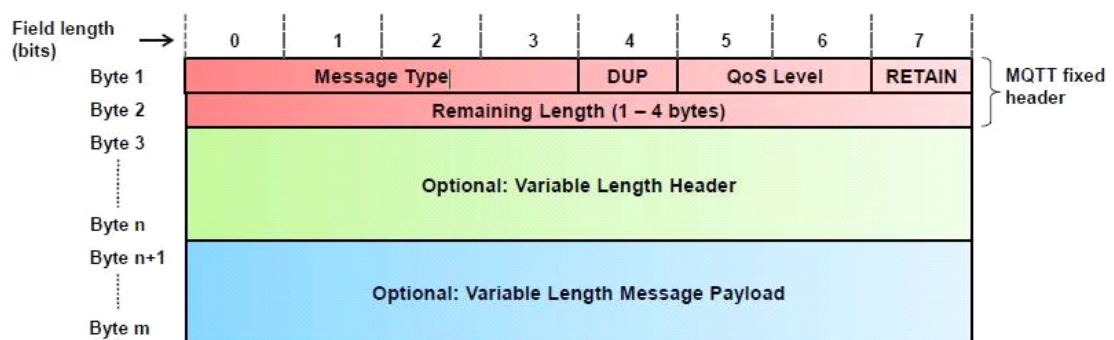
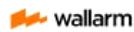


Рис. 2.13 – Загальний формат повідомлення протоколу MQTT

Принцип роботи MQTT можна описати через взаємодію видавця (публікуючого клієнта) та брокера. Видавець відправляє повідомлення з даними на брокер. Це повідомлення може містити інформацію від датчиків, як-от дані про вологість, і має певну тему, до якої належить ця інформація. Брокер отримує

повідомлення, аналізує, які передплатники підписані на цю тему, і пересилає повідомлення з інформацією до відповідних передплатників. Кожен передплатник отримує повідомлення, що містить потрібну йому інформацію.



MQTT Protocol

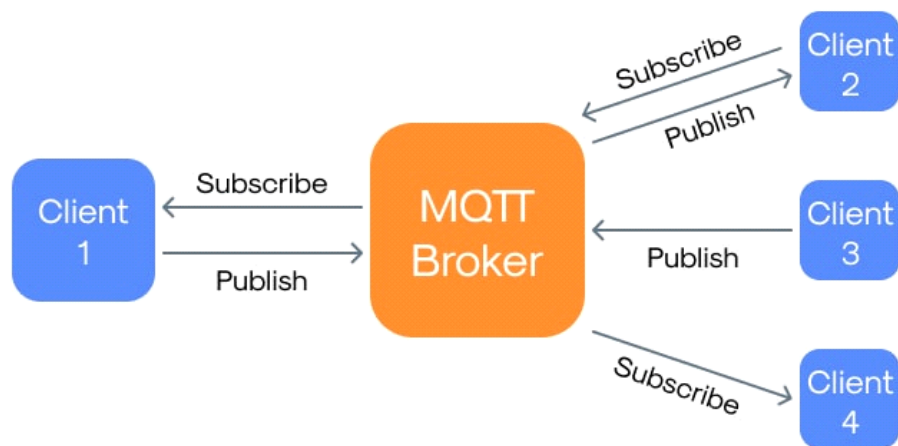


Рис. 2.14 – Принцип роботи протоколу MQTT

В умовах блекауту MQTT виявляє свої переваги завдяки низькому енергоспоживанню та здатності працювати в обмежених мережових середовищах. Пристрої, що використовують MQTT, можуть продовжувати комунікацію навіть за відсутності основного електропостачання, оскільки їхні вимоги до ресурсів мінімальні. Це дозволяє забезпечити безперебійне управління та моніторинг систем у критичних умовах, таких як відключення електроенергії.

Таким чином, MQTT є ефективним інструментом для організації надійного зв'язку в умовах обмежених ресурсів та блекауту. Його здатність забезпечувати комунікацію між багатьма пристроями з мінімальним енергоспоживанням робить його важливим компонентом у побудові стабільних і безпечних IoT систем.

2.3.6 STOMP

STOMP (Simple Text Oriented Messaging Protocol) є текстовим протоколом, який використовується для комунікації між клієнтами та брокерами в системах,

що базуються на повідомленнях. Цей протокол є легким, зворотно сумісним та підтримує різні мови програмування та платформи¹.

У умовах блекауту, STOMP може бути дуже корисним завдяки своїй простоті та ефективності. При відсутності основного електропостачання, системи, що базуються на STOMP, можуть продовжувати функціонувати, оскільки вони вимагають мінімальних ресурсів для передачі повідомлень¹. Це дозволяє забезпечити надійну комунікацію між пристроями, навіть у випадку відключення електроенергії.

Крім того, STOMP підтримує бі-прямову комунікацію, що дозволяє клієнтам не лише отримувати повідомлення, але й надсилати їх. Це особливо корисно в умовах блекауту, коли необхідно забезпечити двосторонню передачу інформації між пристроями для координації дій та забезпечення безперебійної роботи систем.

Таким чином, STOMP є ефективним інструментом для забезпечення надійної комунікації в умовах обмежених ресурсів та блекауту, дозволяючи системам продовжувати функціонувати навіть при відсутності основного електропостачання.

2.3.7 SOAP

SOAP (Simple Object Access Protocol) — це протокол обміну повідомленнями, який використовується для обміну структурованою інформацією в розподілених комп'ютерних мережах. Він був розроблений для забезпечення інтероперабельності між різними системами та додатками, дозволяючи їм взаємодіяти один з одним незалежно від платформи або мови програмування.

Протокол SOAP базується на XML (Extensible Markup Language), що дозволяє описувати повідомлення у вигляді структурованих документів. Основними елементами SOAP є конверт, що містить заголовок та тіло повідомлення. Заголовок використовується для передачі метаданих про

повідомлення, такої як маршрут передавання, безпека та управління транзакціями. Тіло повідомлення містить фактичні дані, які передаються між учасниками.

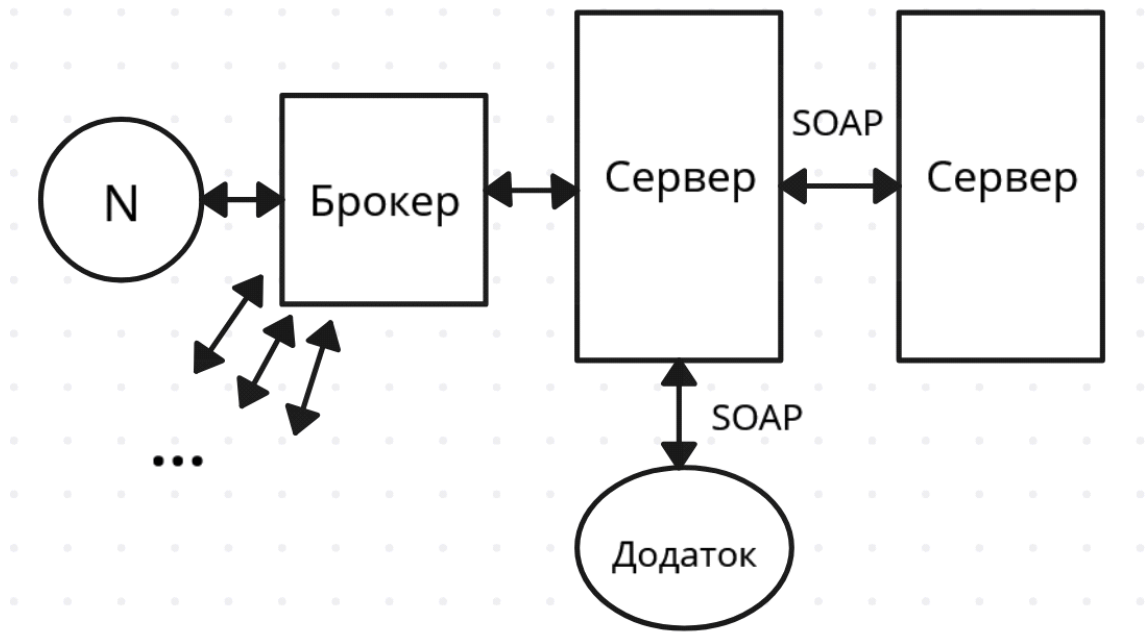


Рис. 2.15 – Сегмент мережі де використовується протокол SOAP

Однією з ключових особливостей SOAP є його здатність працювати через різні транспортні протоколи, включаючи HTTP, SMTP та інші. Це дозволяє використовувати SOAP у різних середовищах та забезпечує гнучкість у виборі транспортного шару.

В умовах блекауту SOAP може бути корисним завдяки своїй здатності забезпечувати надійний обмін повідомленнями між системами, навіть якщо мережеві ресурси обмежені або нестабільні. Наприклад, SOAP підтримує механізми надійної передачі повідомлень та управління помилками, що дозволяє повторно відправляти повідомлення у випадку їх втрати або пошкодження. Це забезпечує високу надійність і стійкість системи, що є критично важливим у умовах відключення електропостачання.

Крім того, SOAP підтримує розширені функції безпеки, такі як аутентифікація, авторизація та шифрування даних. Це дозволяє захищати передавані дані від несанкціонованого доступу та забезпечувати конфіденційність і цілісність інформації. В умовах блекауту, коли існує ризик

порушення безпеки та стабільності мережі, ці функції забезпечують додатковий рівень захисту.

2.4 Висновки до розділу

На основі розглянутих протоколів та технологій передачі даних, можна зробити висновки щодо їх ефективності в умовах блекауту. Розглянуті нами протоколи, такі як XMPP, CoAP, MQTT, STOMP і SOAP, демонструють різні підходи до організації зв'язку та обміну даними, кожен з яких має свої унікальні переваги і може знайти своє застосування в Україні під час відключень електроенергії.

XMPP відзначається своєю здатністю працювати в децентралізованих мережах, що дозволяє підтримувати зв'язок навіть за обмеженого доступу до інтернету. Це робить його корисним для організації комунікації між різними групами або організаціями у надзвичайних ситуаціях.

CoAP, завдяки своїй компактності та ефективності, є ідеальним для пристроїв з обмеженими ресурсами та мереж з низьким енергоспоживанням. Він дозволяє забезпечити стабільний зв'язок між сенсорними вузлами та брокерами, що особливо важливо для систем моніторингу та автоматизації в розумних будинках.

MQTT, завдяки своїй легкості та компактності, є оптимальним для використання у віддалених мережах з обмеженою пропускнуою здатністю. Його здатність забезпечувати ефективний обмін даними між пристроями з мінімальним енергоспоживанням робить його надзвичайно корисним в умовах блекауту.

STOMP забезпечує надійний обмін повідомленнями між клієнтами та брокерами завдяки своїй простоті та здатності підтримувати двосторонню комунікацію. Це дозволяє підтримувати зв'язок та координацію дій між пристроями навіть при обмежених ресурсах.

SOAP, завдяки використанню XML для опису повідомлень, забезпечує структурованість даних і можливість передачі складної інформації. Його здатність працювати через різні транспортні протоколи та підтримка механізмів

надійної передачі повідомлень роблять його важливим інструментом для побудови стійких і безпечних комунікаційних систем, особливо в умовах нестабільного електропостачання.

Таким чином, найкращими протоколами для використання в Україні під час блекаутів є CoAP та MQTT. Вони забезпечують стабільний та ефективний обмін даними між пристроями з низьким енергоспоживанням, що є критично важливим для підтримання функціональності систем у складних умовах. Використання XMPP, STOMP і SOAP може доповнювати ці рішення, забезпечуючи надійний зв'язок та безпеку передачі даних.

Завдяки своїй гнучкості, надійності та безпеці, SOAP є ефективним рішенням для організації обміну повідомленнями в розподілених системах, особливо в умовах обмежених ресурсів та нестабільного електропостачання. Його здатність працювати через різні транспортні протоколи та забезпечувати високу надійність передачі даних робить його важливим інструментом для побудови стійких і безпечних комунікаційних систем у будь-яких умовах.

РОЗДІЛ 3. ПОТОЧНИЙ СТАН ТАМ МАЙБУТНІ ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ В ІОТ В УКРАЇНІ

3.1 Поточний стан технологій передачі даних в Україні

На сьогодні в Україні найбільші телекомунікаційні компанії активно впроваджують технології IoT, серед яких найпоширенішими є LoRaWAN та NB-IoT. Ці технології використовуються для передачі даних на великі відстані, причому LoRaWAN працює в неліцензованому спектрі, а NB-IoT використовує ліцензований спектр на частотах, що застосовуються мережами 4G.

Компанія Lifecell обрала LoRaWAN для створення нової мережі IoT. Це рішення прийнято через те, що протокол LoRa, на якому базується LoRaWAN, функціонує на нижчих частотах і охоплює більші території порівняно з NB-IoT, який використовує частоти 1800 МГц. Lifecell використовує частоту 868 МГц, що

дозволяє здійснювати зв'язок між пристроями на відстані до 15 км з мінімальним енергоспоживанням. Разом з IoT Ukraine компанія вже встановила понад 80 базових станцій у Києві, Львові та Кропивницькому, покриваючи 90% території цих міст.

Під час реалізації проєкту були протестовані рішення для "розумних" міст, моніторингу довкілля, логістичних сервісів, "розумних" будинків та інших застосувань. Найбільшу популярність серед компаній здобули послуги обліку витрат на водопостачання, газ та електроенергію, розумне освітлення, моніторинг відкриття дверей, а також контроль вологості та температури в приміщеннях. Наразі понад 10 бізнес-компаній різних галузей користуються технологіями IoT.

Vodafone Україна також випробувала технологію NB-IoT у найбільших містах країни. Пристрої NB-IoT здатні обмінюватися даними на частоті 1800 МГц, забезпечуючи стабільний доступ до мережі навіть у важкодоступних місцях, таких як ліфтові шахти та підвали. Оскільки NB-IoT працює на базі мережі LTE, користувачі отримують високий рівень безпеки завдяки шифруванню та автентифікації на основі SIM-картки. Ця технологія оптимізує енергоспоживання та збільшує термін служби батареї пристроїв до 10 років, а також має високу ємність та легко масштабовується.

В умовах блекауту впровадження та використання цих технологій є надзвичайно важливим. Використання LoRaWAN дозволяє забезпечити безперебійний зв'язок між пристроями на великих відстанях з мінімальним енергоспоживанням, що є критично важливим у разі відключення електропостачання. Технологія NB-IoT, завдяки своїм перевагам у стабільності та безпеці зв'язку, також є незамінною у таких умовах, оскільки дозволяє підтримувати зв'язок навіть у важкодоступних місцях, зберігаючи енергію та забезпечуючи довготривалу роботу пристроїв. Це дозволяє забезпечити безпеку, моніторинг та контроль різноманітних систем і пристроїв навіть у складних умовах.

3.2 Перспективи розвитку технологій передачу даних в Україні в умовах блекауту

Перспективи розвитку технологій передачі даних в Україні в умовах блекауту є багатообіцяючими, зважаючи на сучасні виклики та необхідність забезпечення надійного зв'язку в екстремальних умовах. Впровадження технології 5G забезпечить значно більшу пропускну здатність та зниження затримок, що сприятиме підвищенню стабільності та швидкості передачі даних, особливо важливої в умовах блекауту. Використання супутникових мереж також матиме велике значення, оскільки супутниковий інтернет дозволить забезпечити доступ до мережі в регіонах з обмеженим доступом до традиційних інфраструктур, що є критично важливим під час відключень електроенергії.

Розвиток технологій Інтернету речей (IoT) відкриває великі можливості для підвищення ефективності управління різними системами та обладнанням. Це дозволить створювати інтелектуальні системи моніторингу та контролю, здатні функціонувати навіть в умовах обмеженого електропостачання. Використання технологій з низьким енергоспоживанням, таких як LoRaWAN та NB-IoT, допоможе забезпечити стабільний зв'язок та моніторинг, що є критично важливим в умовах блекауту. Ці технології дозволяють пристроям працювати протягом тривалого часу без потреби в заряджанні, що забезпечує безперебійне функціонування критичних систем.

Підвищення рівня кібербезпеки також залишається одним із пріоритетних напрямків розвитку. Забезпечення захисту від кібератак та збереження цілісності даних є надзвичайно важливими, особливо в умовах нестабільного електропостачання, коли ризик порушення безпеки мереж зростає. Крім того, розвиток автономних джерел живлення, таких як акумулятори та сонячні батареї, дозволить забезпечити безперебійне функціонування систем передачі даних навіть під час відключень електроенергії.

Не менш важливим є розвиток резервних мереж, які можуть працювати незалежно від основних інфраструктур. Такі мережі сприятимуть підвищенню надійності зв'язку в умовах блекауту, дозволяючи зберегти зв'язок та

координацію дій у надзвичайних ситуаціях. Отже, впровадження нових мережевих рішень, підвищення енергоефективності, зміцнення кібербезпеки та розвиток автономних джерел живлення є ключовими аспектами для забезпечення надійного зв'язку та стабільного функціонування критичних систем в Україні в умовах блекауту.

3.2.1 Безпілотники та дрони

Інтернет речей (IoT) відіграє надзвичайно важливу роль у безпілотниках, забезпечуючи їх автономну роботу та ефективний зв'язок з операторами та іншими пристроями. Завдяки IoT безпілотники оснащуються різноманітними сенсорами та датчиками, які збирають дані про навколишнє середовище, наприклад, GPS-координати, температурні показники, відеозображення та багато іншого. Ці дані передаються через IoT-платформи для аналізу та прийняття рішень, що дозволяє безпілотникам функціонувати автономно та виконувати складні завдання без безпосереднього втручання оператора.

Інтернет речей також забезпечує постійний зв'язок безпілотників з базовими станціями, серверами та іншими пристроями, використовуючи мобільні мережі або спеціалізовані протоколи. Це дозволяє операторам моніторити стан безпілотника в режимі реального часу, отримуючи інформацію про його місцезнаходження, рівень заряду батареї, та інші критичні параметри. Така зв'язковість є ключовою для забезпечення безпеки та ефективності роботи безпілотників, особливо в умовах складних місій або аварійних ситуацій.

Автономна робота безпілотників, забезпечена IoT, досягається за допомогою алгоритмів машинного навчання та штучного інтелекту, які аналізують зібрані дані та приймають обґрунтовані рішення. Це дозволяє безпілотникам адаптуватися до змінних умов навколишнього середовища та виконувати завдання з високою точністю.

Інтернет речей також дозволяє безпілотникам взаємодіяти з іншими системами та пристроями, такими як смарт-доми або системи безпеки. Це розширює функціональні можливості безпілотників, дозволяючи їм виконувати

більш складні завдання, наприклад, автоматизоване доставлення вантажів або моніторинг території в реальному часі.

3.2.2 Смарт-місто під час блекауту

В умовах блекауту смарт-місто стикається з низкою серйозних викликів, однак завдяки технологіям Інтернету речей (IoT) вдається ефективно боротися з цими проблемами. Смарт-міста використовують мережі сенсорів та датчиків для моніторингу стану критично важливих інфраструктурних об'єктів, таких як електричні мережі, водопостачання та системи безпеки. Ці сенсори в реальному часі передають дані про стан об'єктів, що дозволяє оперативно реагувати на перебої в електропостачанні та вживати необхідні заходи для мінімізації їх впливу.

Автоматизація управління електромережею та іншими системами смарт-міста значно підвищує їхню стійкість до блекаутів. Наприклад, у разі виявлення перебою, системи автоматично включають резервні джерела живлення, такі як акумулятори або генератори, для забезпечення безперебійної роботи критичних об'єктів. Цей підхід допомагає запобігти збоям у роботі інфраструктури та зменшити негативні наслідки для населення.

Крім того, розподілене виробництво енергії є важливою частиною стратегії боротьби з блекаутами в смарт-містах. Використання джерел відновлюваної енергії, таких як сонячні панелі та вітрові турбіни, дозволяє забезпечувати стабільне електропостачання навіть за відсутності централізованої мережі. Це зменшує залежність міста від зовнішніх джерел енергії та підвищує його енергетичну незалежність.

Інформування населення про стан електромережі та можливі перебої також є важливою складовою управління смарт-містом в умовах блекауту. Завдяки мобільним додаткам та повідомленням, мешканці можуть швидко отримувати інформацію про перебої в електропостачанні та вживати заходів для зменшення їхнього впливу, таких як вимкнення непотрібних електроприладів або підготовка до використання альтернативних джерел живлення.

Після відновлення електропостачання, системи смарт-міста допомагають швидко оцінити стан інфраструктури та виявити можливі пошкодження. Це дозволяє оперативно реагувати на проблеми та забезпечувати нормальну роботу міста. Таким чином, технології IoT відіграють ключову роль у підтриманні стабільності та безпеки смарт-міст в умовах блекауту, дозволяючи ефективно справлятися з викликами та забезпечувати комфортні умови для мешканців.

3.2.3 Сучасні реалії медицини в Україні

Інтернет речей (IoT) відіграє важливу роль у забезпеченні медичних послуг в умовах блекауту, значно підвищуючи надійність, ефективність і доступність медичної допомоги. Завдяки IoT технологіям, багато медичних процесів можуть працювати автономно, забезпечуючи безперервний моніторинг та догляд за пацієнтами навіть за відсутності централізованого електропостачання.

Постійний моніторинг стану здоров'я пацієнтів є одним із ключових аспектів IoT у медицині. Медичні сенсори та пристрої, підключені до мережі IoT, можуть збирати дані про життєво важливі показники, такі як пульс, артеріальний тиск, рівень кисню в крові та інші параметри. Ці дані передаються до медичних центрів у реальному часі, що дозволяє лікарям своєчасно реагувати на будь-які відхилення від норми навіть під час блекауту.

Автономні медичні пристрої, такі як інсулінові помпи, кардіостимулятори та інші життєво важливі пристрої, також грають важливу роль у забезпеченні догляду за пацієнтами. Завдяки IoT, ці пристрої можуть функціонувати незалежно від зовнішніх джерел живлення, забезпечуючи безперервний догляд за пацієнтами навіть у випадках відключення електроенергії. Це особливо важливо для пацієнтів, які потребують постійного медичного спостереження.

Телемедицина та дистанційне консультування є ще однією важливою складовою IoT у медицині. Завдяки IoT, пацієнти можуть отримувати медичну допомогу на відстані через телемедичні платформи, що особливо важливо в умовах блекауту, коли доступ до медичних установ може бути обмеженим. Лікарі можуть дистанційно консультувати пацієнтів, надавати рекомендації щодо

лікування та відстежувати їх стан за допомогою підключених медичних пристроїв.

IoT також забезпечує безпечне збереження та передачу медичних даних навіть під час перебоїв у електропостачанні. Дані можуть зберігатися у хмарних сервісах, забезпечуючи доступ до них у будь-який час і з будь-якого місця. Це дозволяє медичному персоналу ефективно координувати свої дії та забезпечувати безперебійну роботу медичних послуг.

Медичні заклади можуть використовувати резервні джерела живлення та автономні енергетичні системи, такі як акумулятори та генератори, для забезпечення безперервної роботи критичних медичних пристроїв та систем під час блекауту. IoT технології дозволяють ефективно управляти цими джерелами живлення, оптимізуючи їх використання та забезпечуючи надійне електропостачання.

Було проведено аналіз стану технологій передачі даних на великі відстані в мережах Інтернету речей (IoT), зокрема, на основі відомих українських операторів зв'язку та їх рішень із використання технологій LoRaWAN та NB-IoT. Було також розглянуто перспективи розвитку IoT з впровадженням найбільш перспективної технології передачі даних – 5G. У розділі досліджувалися потенційні сфери застосування технології 5G, включаючи медичний сектор, безпілотні автомобілі та розумні будинки.

Отже, розділ 3 надав огляд та порівняння різних технологій передачі даних у мережах IoT, а також висвітлив перспективи технології 5G у різних сферах. Зокрема, було підкреслено важливість цих технологій в умовах блекауту, коли надійний зв'язок та безперебійна передача даних мають критичне значення для підтримання функціонування систем життєзабезпечення та надання послуг.

ВИСНОВКИ

Було висвітлено ключові терміни Інтернету речей (IoT) та представлено архітектуру IoT, що складається з чотирьох рівнів: рівня датчиків, мережевого рівня, рівня обробки даних та прикладного рівня.

Проаналізовано основні технології та протоколи передачі даних на великі відстані у мережах LPWAN, таких як LoRaWAN, SigFox, NB-IoT та Weightless-P.

Розглянуто основні технології та протоколи передачі даних на короткі відстані у мережах WPAN та WLAN, такі як Z-Wave, RFID, Bluetooth Low Energy та Wi-Fi HaLow.

Розглянуто топологію, що використовується для передачі повідомлень в IoT, та проведено порівняльний аналіз протоколів передачі повідомлень з огляду на протокол транспортного рівня, призначення, особливості та операції, які вони виконують у мережі IoT.

Досліджено стан технологій передачі даних на великі відстані в мережах IoT на основі українських операторів зв'язку, зокрема LoRaWAN та NB-IoT. Цей аналіз підкреслив важливість забезпечення надійного зв'язку в умовах блекауту, що дозволяє зберігати функціональність систем навіть у складних умовах.

Проаналізовано перспективи розвитку IoT на основі технології передачі даних 5G, яка вважається найбільш перспективною. Розглянуто можливі сфери застосування технології 5G, включаючи медичний сектор, безпілотні автомобілі, квадрокоптери та розумні будинки. В умовах блекауту впровадження 5G є критично важливим для підтримання надійного зв'язку та забезпечення безперебійної роботи різних систем.

ПЕРЕЛІК ПОСИЛАНЬ

1. Contributors to Wikimedia projects. Internet of things - Wikipedia. *Wikipedia, the free encyclopedia*. URL: https://en.wikipedia.org/wiki/Internet_of_things.
2. Sethi P., Sarangi S. R. Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*. 2017. Т. 2017. С. 1–25. URL: <https://doi.org/10.1155/2017/9324035>.
3. The Convergence of Edge Computing and IoT: Driving Smarter Decision-Making: A Comprehensive Study. *IEEE Xplore*. URL: <https://ieeexplore.ieee.org/document/10687465>.

4. Internet of Things: A Hands-On Approach. Vijay Madisetti, 2014. 446 c.
URL: <https://jcer.in/jcer-docs/E-Learning/Digital%20Library%20/E-Books/Internet-of-things-a-hands-on-approach-%20Arshadeep.pdf>
5. Rayes A., Salam S. Internet of Things From Hype to Reality. Cham : Springer International Publishing, 2019. URL: <https://core.ac.uk/download/pdf/326762892.pdf>.
6. Y.2060 : Overview of the Internet of things. ITU: *Committed to connecting the world*. URL: <https://www.itu.int/rec/t-rec-y.2060-201206-i>.
7. Інтернет-речей: що це і як він працює. *GigaTrans – Інтернет для вашого офісу*. URL: https://gigatrans.ua/ua/news/internet-vesh-ey-chto-eto-takoe-i-kak-on-rabotaet?utm_source=chatgpt.com.
8. Contributors to Wikimedia projects. LoRa - Wikipedia. *Wikipedia, the free encyclopedia*. URL: <https://en.wikipedia.org/wiki/LoRa#LoRaWAN>.
9. Технологія LoRaWAN: особливості та переваги | Romsat.ua. *Romsat*. URL: <https://romsat.ua/news/company/lorawan-technology/>.
10. Contributors to Wikimedia projects. Sigfox - Wikipedia. *Wikipedia, the free encyclopedia*. URL: <https://en.wikipedia.org/wiki/Sigfox>.
11. ТЕХНОЛОГІЯ SIGFOX – Sigfox. *Sigfox – The Global Communications Service Provider for the Internet of Things (IoT)*. URL: <https://sigfox.ua/technology/>.
12. NB-IoT (Narrow Band IoT) operation in the 5G System. *5G HUB TECHNOLOGIES, INC*. URL: <https://5ghub.us/nb-iot-narrow-band-iot-operation-in-the-5g-system/>.
13. Weightless-P - IoT Global Network. *IoT Global Network*. URL: <https://www.iotglobalnetwork.com/products/single/id/914/weightless-p>.
14. Contributors to Wikimedia projects. MQTT - Wikipedia. *Wikipedia, the free encyclopedia*. URL: <https://en.wikipedia.org/wiki/MQTT>.
15. Contributors to Wikimedia projects. Z-Wave – Википедия. *Википедия – свободная энциклопедия*. URL: <https://ru.wikipedia.org/wiki/Z-Wave>.
16. Z-Wave vs Zigbee vs WiFi | Which Is Best For Your Home? - HomeSeer Smart Home Systems. *HomeSeer Smart Home Systems*. URL: https://homeseer.com/zwave-vs-zigbee-vs-wifi/?utm_source=chatgpt.com.

17. *mouser.com*. URL: <https://eu.mouser.com/pdfdocs/STMicroelectronicsIntroductiontoNFC.pdf>.
18. Contributors to Wikimedia projects. NFC – Википедія. *Википедія – свободная энциклопедия*. URL: <https://ru.wikipedia.org/wiki/NFC>.
19. Radio Frequency Identification RFID. *U.S. Food and Drug Administration*. URL: <https://www.fda.gov/radiation-emitting-products/electromagnetic-compatibility-emc/radio-frequency-identification-rfid>.
20. Учасники проєктів Вікімедіа. Bluetooth з низьким енергоспоживанням – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Bluetooth_з_низьким_енергоспоживанням.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ



НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ



Кафедра інформаційних систем та технологій

Магістерська робота

**СИСТЕМА ПЕРЕДАЧІ ДАНИХ ДЛЯ ІОТ-МЕРЕЖ З
ОБМЕЖЕНИМИ РЕСУРСАМИ**

Виконав: студент групи ІСДМ-63, Рейнгольд Олександр Юрійович

Керівник: Поперешняк С.В.

Київ - 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут інформаційних технологій

бакалаврська робота на тему:

**Система передачі даних для IoT-мереж з обмеженими
ресурсами**



**Виконав студент групи ІСД-63
Рейнгольд Олександр**

Керівник: Поперешняк С.В.

Київ 2024

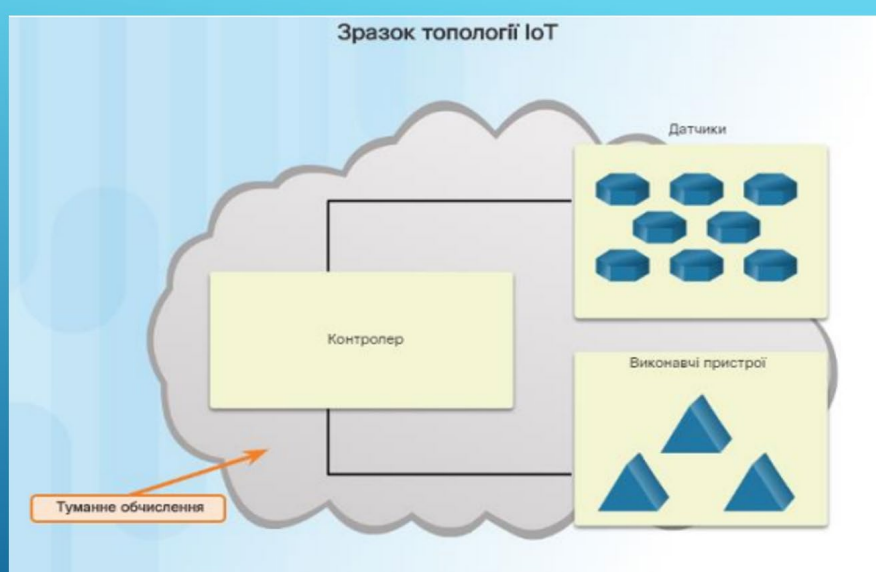
ІНТЕРНЕТ РЕЧЕЙ(IOT)

Інтернет речей (IoT) - це ідея поєднання мільйонів розумних пристроїв і датчиків, які підключені до Інтернету. Ці пристрої та датчики збирають і обмінюються даними з метою їх подальшого використання та аналізу різними організаціями, такими як міста, урядові органи, лікарні і приватні особи.

У центрі концепції IoT лежить здатність пристроїв підключатися один до одного та до Інтернету, створюючи мережу, яка дозволяє обмінюватися даними та взаємодіяти безпосередньо. Це створює безліч можливостей для збору інформації та контролю різних процесів.

ЯК ЦЕ ПРАЦЮЄ?

У роботі Інтернету речей (IoT) датчики збирають дані і підключаються до мережі за допомогою дротового Ethernet або бездротового зв'язку. Контролери відповідають за збір даних з датчиків і забезпечення мережевого з'єднання. Контролери можуть приймати рішення на місці або надсилати дані на більш потужний комп'ютер для подальшої обробки.



АВТОМАТИЗАЦІЯ РОЗУМНОГО БУДИНКУ

- ▶ Звичайні будинки можуть бути перетворені в розумні будинки завдяки автоматизації з використанням Інтернету речей (IoT). Ось деякі ключові аспекти автоматизації розумного будинку:

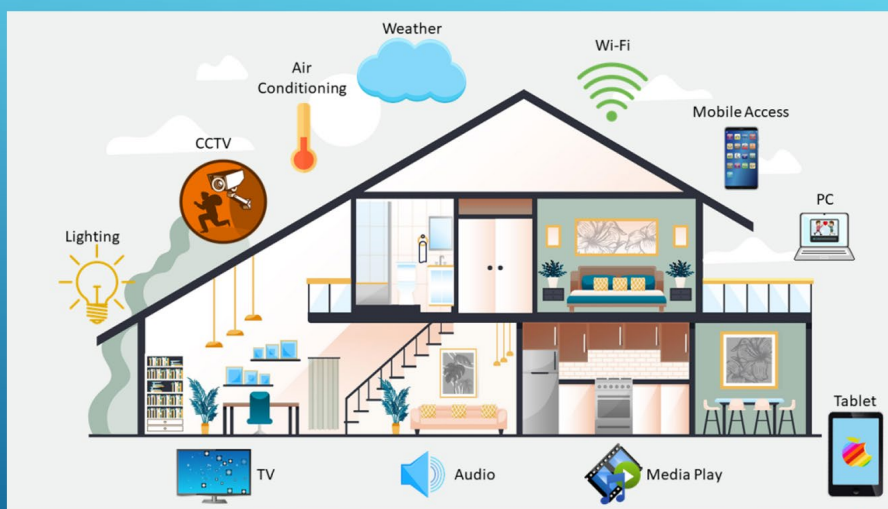
Зручне управління: Інтерфейси управління, такі як смартфони або голосові асистенти, дозволяють власникам контролювати освітлення, опалення, охолодження, безпеку та інші системи в будинку з будь-якого місця.

- ▶ **Сенсори і датчики:** Встановлення сенсорів і датчиків по всьому будинку дозволяє виявляти рух, присутність, температуру, вологість та інші параметри. Ці дані можуть використовуватися для автоматичного управління різними пристроями і системами.

Енергоефективність: Розумний будинок може зменшити споживання енергії шляхом автоматичного вимкнення світла або оптимізації температури відповідно до присутності людей і часу доби.

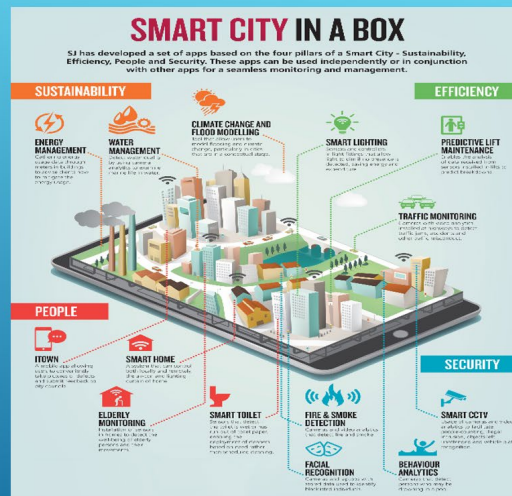
- ▶ **Безпека:** Системи безпеки в розумному будинку включають в себе відеоспостереження, датчики проникнення, детектори витоку газу або пожежі, які можуть негайно сповіщати власників про потенційну небезпеку.

Розумна електроніка: Розумні пристрої, такі як телевізори, аудіосистеми, кухонна техніка та інші, можуть бути інтегровані в розумну систему будинку, що дозволяє зручно керувати ними через один інтерфейс.



SMART MICTO

- Інтернет речей (IoT) в розумних містах відкриває безліч можливостей для покращення життя мешканців та ефективного управління міською інфраструктурою. Завдяки IoT можна допомогти вдосконалити системи громадського транспорту, розумне паркування, моніторинг трафіку і оптимізацію світлофорів. Це дозволяє зменшити затори, покращити безпеку дорожнього руху та знизити викиди шкідливих речовин. Також IoT може використовуватися для моніторингу та оптимізації споживання енергії в місті. Розумні лічильники, системи освітлення та опалення можуть адаптуватися до реальних потреб і забезпечувати ефективне використання енергії. Ця технологія допомагає оптимізувати процеси управління відходами, включаючи моніторинг рівня наповнення сміттєвих контейнерів, оптимізацію маршрутів збору сміття та реагування на надзвичайні ситуації, такі як пожежі або витoki. За допомогою сенсорів IoT можна постійно контролювати рівень забруднення повітря в місті і негайно реагувати на проблеми. Це сприяє поліпшенню якості життя мешканців та збереженню здоров'я.



ІОТ У МЕДИЦИНІ ТА ХІРУРГІЇ

- Медична діагностика та хірургія, поєднані з Інтернетом речей (IoT), відкривають нові можливості для точнішої діагностики, ефективного лікування та поліпшення якості медичної допомоги. За допомогою носимих пристроїв, сенсорів та медичних пристроїв, IoT дозволяє збирати реальні дані про стан пацієнтів. Ці дані можуть включати серцевий ритм, кров'яний тиск, рівень цукру в крові та інші показники здоров'я.
- Це допомагає лікарям моніторити пацієнтів в реальному часі та здійснювати більш точну діагностику. IoT дозволяє встановлювати зв'язок між лікарем і пацієнтом на віддаленій відстані. Це забезпечує можливість проводити консультації, моніторити стан пацієнтів та надавати необхідну медичну допомогу без присутності фізично в одному місці. Також може використовуватися для покращення точності та ефективності хірургічних процедур. Наприклад, розумні хірургічні інструменти та роботизовані системи можуть допомагати хірургам виконувати операції з більшою прецизією та меншим втручанням. Ця технологія дозволяє автоматизувати та моніторити медичну апаратуру, таку як медичні пристрої, лікарняні ліжка та інше обладнання. Це допомагає забезпечити безперебійну роботу, уникнути випадкових помилок та забезпечити оптимальні умови для пацієнтів.



МАГАЗИНИ ТА ПОСЛУГИ

- Технології все більше використовуються для автоматизації завдань, які раніше виконували люди. Ресторани швидкого харчування використовують термінали самообслуговування для прийому замовлень, банки надають доступ до автоматизованих банкоматів та мобільних додатків, а супермаркети та універмаги мають системи самообслуговування.

Крім цього, розроблені системи контролюють рівень запасів та автоматично розміщують замовлення, щоб точно відповідати попиту та уникнути надлишкових запасів.

