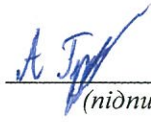
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
Кафедра Мобільних та відеоінформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Методи управління ресурсами в безпроводових IoT-мережах для забезпечення надійності в умовах масштабованості»

на здобуття освітнього ступеня магістра
зі спеціальності172 Електронні комунікації та радіотехніка
освітньо-професійної програмиАпаратура радіозв'язку, радіомовлення і телебачення

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



(підпис) АндрійГРИЦЕНКО *(Ім'я, ПРІЗВИЩЕ)*

Виконав: Здобувачвищої освіти
групи АРДМ-61
Андрій ГРИЦЕНКО

Керівник: Лариса ДАКОВА

Рецензент: Юрій ПЕПА

Київ –2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

Кафедра	Мобільних та відеоінформаційних технологій
Ступінь вищої освіти	Магістр
Спеціальність	172 Електронні комунікації та радіотехніка
Освітньо-професійна програма	Апаратура радіозв'язку, радіомовлення і телебачення

ЗАТВЕРДЖУЮ
Завідувачка кафедрою МВТ
_____ Наталія РУДЕНКО
«__» _____ 2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Гриценко Андрію Анатолійовичу

1. Тема кваліфікаційної роботи: «Методи управління ресурсами в безпроводових IoT-мережах для забезпечення надійності в умовах масштабованості»,
керівник кваліфікаційної роботи Лариса Дакова, к.т.н., доцент,
затверджені наказом Державного університету інформаційно-комунікаційних технологій від 15.10.2024 р. №320.

2. Строк подання кваліфікаційної роботи 25.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи:
   1. Поняття та характеристика IoTмереж;
   2. Управління ресурсами IoT;
   3. Впровадження Інтернету речей;
   4. Науково-технічна література.

4.Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
   1. Огляд мереж IoT.
   2. Ефективне управління частотами.
   3. Виявлення аномалій та реагування на загрози в мережах IoT.

4. Висновки, вступ, реферат.

5. Перелік ілюстративного матеріалу: презентація.

6. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Підбір науково-технічної літератури	27.10.24	Викон.
2.	Огляд мереж IoT	31.10.24	Викон.
3.	Ефективне управління частотами	15.11.24	Викон.
4.	Проблеми масштабованості в мережах IoT	29.11.24	Викон.
5.	Виявлення аномалій та реагування на загрози в мережах IoT	11.12.24	Викон.
6.	Висновки, вступ, реферат	15.12.24	Викон.
7.	Розробка презентації	19.12.24	Викон.

Здобувач вищої освіти _____ Андрій ГРИЦЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Лариса ДАКОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

здобувача вищої освіти Гриценка Андрія Анатолійовича

на тему:«Методи управління ресурсами в безпроводових IoT-мережах для забезпечення надійності в умовах масштабованості»

Актуальність теми зумовлена швидким розвитком Інтернету речей (IoT) та його проникненням у різні сфери життя, включаючи промисловість, медицину, транспорт, "розумний" дім і місто, а також екологічний моніторинг. Кількість підключених пристроїв IoT стрімко зростає, що призводить до значних викликів в управлінні мережами, особливо у масштабуванні, забезпеченні надійності зв'язку та ефективному використанні ресурсів.

Позитивні сторони:

1. Документ має чітку структуру з розділами, які розкривають послідовно ключові аспекти теми роботи. Кожен розділ розглядає певний аспект теми.
2. У роботі детально розглянуто використання нових технологій, таких як когнітивне радіо, блокчейн і 5G. Цедемонструє актуальність дослідження та його прив'язку до сучасних реалій IoT.

Недоліки:

1. Недостатня кількість практичних прикладів застосування технологій та методів розглянутих у роботі.
2. Деякі аспекти тем, такі як безпека та вплив масштабованості на ефективність IoT-мереж, розглянуті достатньо поверхнево. Глибший аналіз та кількісні оцінки зробили б роботу більш ґрунтовною.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: кваліфікаційна робота заслуговує оцінку «добре», а здобувач Гриценко Андрій Анатолійович заслуговує присвоєння кваліфікації: «Магістр з електронних комунікацій та радіотехніки».

Рецензент: к.т.н., доцент _____ Юрій ПЕПА

(науковий ступінь, вчене звання) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

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

Направляється здобувач Гриценко А.А. до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю 172 Електронні комунікації та радіотехніка
освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

на тему:«Методи управління ресурсами в безпроводових IoT-мережах для забезпечення надійності в умовах масштабованості»

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Гриценко Андрій Анатолійович показав гарну теоретичну та інженерну підготовку, уміння володіти технологіями нового покоління, вмілопрацювати з програмно-апаратними засобами мобільного зв'язку, довідковою і науково-технічною літературою. Працюючи над завданнями, які доручались керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу Гриценка Андрія Анатолійовича оцінку «добре» та присвоїти йому кваліфікацію «Магістр з електронних комунікацій та радіотехніки».

Керівник кваліфікаційної роботи _____ Лариса ДАКОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

" " _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута.Здобувач Гриценко А.А.
(прізвище та ініціали)

допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувачка кафедрою
Мобільних та відеоінформаційних технологій _____ Наталія РУДЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

" " _____ 2024 року

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 90 стор., 36 рис., 13 табл., 28 дж.

Мета роботи – дослідження методів планування та оптимізації безпроводових телекомунікаційних мереж.

Об'єкт дослідження – управління ресурсами для забезпечення надійності та масштабованості бездротових мереж IoT.

Предмет дослідження – це бездротові мережі Інтернету речей.

Короткий зміст роботи: в магістерській роботі досягнуто наступних результатів: у першому розділі описано загальні принципи та характеристики структури мережі IoT. Розглянуто управління ттакими ресурсами як: енергія, спектр, обчислювальні потужності та мережі.

У другому розділі аналізуються проблеми масштабованості та надійності мереж IoT. Визначено такі ключові проблеми, як обмеження енергетичних ресурсів, перешкоди між пристроями, проблеми безпеки та збої в роботі мережі.

У розділі 3 детально розглядаються способи оптимізації управління ресурсами, включаючи використання когнітивного радіо для ефективного розподілу частот і штучного інтелекту для прогнозування трафіку і зниження навантаження на мережу, також аналізуються алгоритми і методи енергозбереження для зниження енергоспоживання пристроїв Інтернету речей.

Розділ 4 описує інноваційні технології, що використовуються для управління ресурсами. Розглядаються питання інтеграції зелених технологій та автоматизації управління ресурсами за допомогою штучного інтелекту.

КЛЮЧОВІ СЛОВА:IoT, УПРАВЛІННЯ, МАСШТАБОВАНІСТЬ, РЕСУРСИ, БЕЗПЕКА, МЕРЕЖІ, ПРИКЛАДИ ВПРОВАДЖЕННЯ, ПЕРСПЕКТИВИ РОЗВИТКУ, ДАНІ, ТРАФІК, МАРШРУТИЗАЦІЯ, БЕЗПЕКА

ABSTRACT

Text part of the master's qualification work: 90pages, 36 pictures, 13 table, 28sources.

The purpose of the work – research of methods of planning and optimization of wireless telecommunication networks.

Object of research – there is a process of accessing wireless LTE networks.

Subject of research – methods of optimizing the radio coverage area of the base station for the LTE network during its preliminary planning.

Summary of the work: the master's thesis achieved the following results: the first section describes the general principles and characteristics of the IoT network structure. The management of resources such as: energy, spectrum, computing power and networks is considered. The second section analyzes the scalability and reliability problems of the IoT network. Key problems such as energy resource limitations, interference between devices, security issues and network failures are identified. Section 3 examines in detail ways to optimize resource management, including the use of cognitive radio for effective frequency allocation and artificial intelligence for traffic forecasting and reducing energy consumption in the network, and also analyzes algorithms and saving methods for reducing the consumption of devices in the Internet of Things. Section 4 describes innovative technologies used for resource management. The issues of integrating green technologies and automating resource management using artificial intelligence are considered.

KEYWORDS:IoT, MANAGEMENT, SCALING, RESOURCES, SECURITY, NETWORKS, IMPLEMENTATION EXAMPLES, DEVELOPMENT PERSPECTIVES, DATA, TRAFFIC, ROUTING, SECURITY

ЗМІСТ

ВСТУП 9
1. ОГЛЯД МЕРЕЖ ІОТ 11
1.1 Поняття та характеристика IoT мереж 11
1.2 Бездротові технології зв'язку в IoT 17
1.3 Сучасні методи управління ресурсами в IoT-мережах 20
1.4 Проблеми надійності та масштабованості в мережах IoT 23
1.5 Методи управління ресурсами в безпровідних IoT-мережах 26
2. ЕФЕКТИВНЕ УПРАВЛІННЯ ЧАСТОТАМИ 28
2.1 Основи енергозбереження в мережах IoT 28
2.2 Методи адаптивної маршрутизації 41
2.3 Протоколи управління трафіком в мережах IoT 43
2.4 Оптимізація трафіку в мережах IoT 46
3. УПРАВЛІННЯ НАВАНТАЖЕННЯМ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ 48
3.1 Забезпечення надійності в мережах IoT 48
3.2 Якість обслуговування (QoS) в мережах IoT 53
3.3 Резервування ресурсів і механізми відновлення в мережах IoT 56
3.4 Проблеми масштабованості в мережах IoT 59
3.5 Адаптивні стратегії для розширення мереж Інтернету речей 62
4. ШТУЧНИЙ ІНТЕЛЕКТ (ШІ) ТА МАШИННЕ НАВЧАННЯ (МН) В МЕРЕЖАХ ІОТ 65
4.1 Автоматизація процесів управління в мережах IoT 65
4.2 Прогнозування навантаження в мережах IoT 71
4.3 Виявлення аномалій та реагування на загрози в мережах IoT 75
4.4 Приклади успішного впровадження IoT 77
4.5 Підходи до безпеки та захисту даних в мережах Інтернету речей 81
ВИСНОВКИ 85
ПЕРЕЛІК ПОСИЛАНЬ 86
ДЕМОНСТРАТИВНІ МАТЕРІАЛИ 88

ВСТУП

Розвиток технології Інтернету речей (IoT) докорінно змінює наше життя в сучасному суспільстві. IoT об'єднує фізичні об'єкти, пристрої, датчики та мережі в єдину екосистему та гарантує їх взаємодію в реальному часі. IoT забезпечив автоматизацію, оптимізацію та ефективність процесів у багатьох сферах, від дому до промисловості, промисловості та муніципалітетів. Однією з ключових сфер застосування IoT є створення розумних міст, де системи на основі IoT допомагають керувати міським трафіком, контролювати навколишнє середовище, регулювати споживання енергії та запобігати збоям у водопостачанні. Це робить міську інфраструктуру більш ефективною та екологічною, забезпечує комфорт і безпеку для городян.

У промисловому секторі IoT є невід'ємною частиною концепції Industry 4.0 і дозволяє автоматизувати виробничі процеси, зменшити витрати та підвищити ефективність. Наприклад, системи моніторингу стану обладнання можуть прогнозувати збої та оптимізувати обслуговування. Це не тільки забезпечує надійність обладнання, але й мінімізує непередбачені простої.

Сільське господарство інтегрує IoT для вирішення проблем, пов'язаних зі зміною клімату та зростанням попиту на продукти харчування. Розумні датчики вимірюють вологість ґрунту, температуру та освітлення, що дозволяє фермерам ефективніше управляти такими ресурсами, як вода та добрива. Це зменшує витрати, покращує якість врожаю та зменшує негативний вплив на навколишнє середовище.

У медичному секторі IoT змінює підхід до лікування та діагностики. Сучасні пристрої можуть стежити за станом пацієнта в режимі реального часу, передавати дані лікарям і навіть скорочувати дистанційне спостереження. Це знижує ризик виникнення кризових ситуацій і забезпечує своєчасну медичну допомогу. Розумні будинки є ще одним популярним напрямком для додатків IoT. Автоматизовані системи не можуть використовувати мобільні програми чи голосові команди для

керування освітленням, температурою, безпекою та приладами. Такі технології можуть допомогти зберегти ресурси та підвищити комфорт мешканців будинку. Незважаючи на всі ці переваги, розвиток IoT супроводжується рядом проблем. До них належать обмеження енергетичних і частотних ресурсів, потреба в масштабованості мережі та забезпечення безпеки та конфіденційності даних. Ефективне вирішення цих проблем лежить в основі подальшої інтеграції IoT у повсякденне життя та є ключем до сталого розвитку. Інтернет речей прокладає шлях для багатьох нових систем, які можуть змінити традиційний підхід до процесів управління, покращити взаємодію між людьми та пристроями та закласти основу для цифрової трансформації в усіх сферах життя.

Метою даного дослідження є дослідження сучасних підходів до управління ресурсами для забезпечення надійності та масштабованості бездротових мереж IoT та аналіз ефективності різних методів в реальних мережевих умовах, пошук оптимальних способів управління спектром, енергоефективністю, маршрутизацією та іншими ресурсами для забезпечення надійної роботи мережі навіть в умовах високих навантажень.

Об’єкт досліджень - це бездротові мережі Інтернету речей, що складаються з великої кількості взаємопов'язанихпристроїв, які обмінюються даними в режимі реального часу, ці мережі використовуються в різних сферах, таких як розумні міста, промислові системи, медичні пристрої, системи моніторингу навколишнього середовища та інші галузі, які потребують широкомасштабного підключення пристроїв для збору, передачі та аналізу інформації.

Предмет дослідження - проаналізувати існуючі дослідження з управління ресурсами в бездротових мережах IoT, виявити основні методи, що використовуються для забезпечення надійної та ефективної роботи мереж, визначити основні проблеми, пов'язані зі зростанням кількості підключених пристроїв та збільшенням навантаження на мережу, дослідити вплив розширення мережі на продуктивність, енергоспоживання та якість обслуговування.

1. ОГЛЯД МЕРЕЖ ІОТ

1.1 Поняття та характеристика IoT мереж

Структура, методи управління таключовівиклики Інтернет речей (IoT) - одна з основних технологій сучасного світу, що об'єднує фізичні пристрої в мережу для збору, передачі та аналізу даних.

Приклади мереж IoT, методів управління та ключових викликів.

Основні характеристики мереж IoT Мережі IoT складаються з фізичних пристроїв (датчиків, виконавчих механізмів і пристроїв збору даних), які взаємодіють між собою за допомогою протоколів передачі даних.

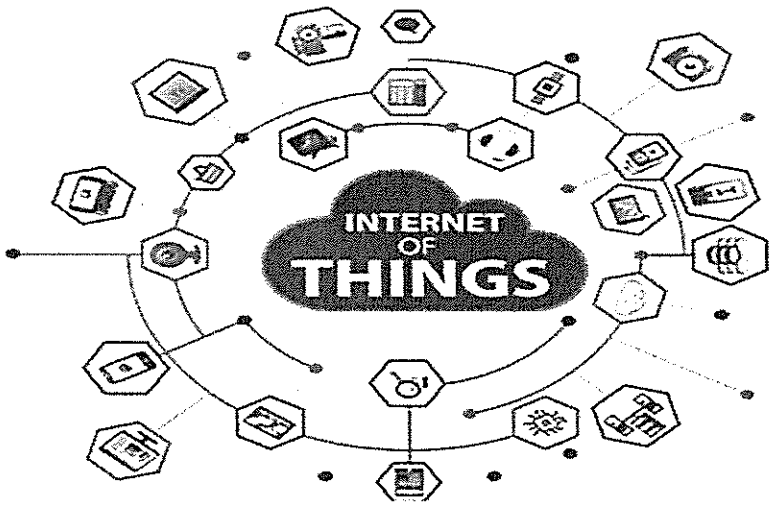


Рис. 1.1 Інтернет речей

Основні характеристики цих мереж:

- Різноманітні пристрої такі як: смартфони, датчики, побутова техніка та промислове обладнання;
- Автономність: пристрої можуть працювати самостійно або з мінімальним втручанням людини;

- Масштабованість: підтримує велику кількість пристроїв у мережі. Гетерогенність: використання різних технологій зв'язку (Wi-Fi, Zigbee, LoRa, LTE, 5G тощо).

Методи управління мережею IoT

Ефективне управління мережею IoT забезпечує стабільну роботу, безпеку та оптимізацію ресурсів включає в себе:

- Управління ресурсами;
- Управління спектром: розподіл частот для зменшення динамічних перешкод (когнітивне радіо);
- Енергозбереження: Оптимізація енергоспоживання за допомогою таких протоколів, як RPL, енергоефективні механізми збору даних;
- Обробка даних: зменшення навантаження на мережу за рахунок використання хмарних і периферійних обчислень.

Методи маршрутизації:

- Ієрархічні протоколи: кластерні мережі для оптимізації передачі даних. Адаптивна маршрутизація(використання AI/ML для вибору оптимальних шляхів передачі) та маршрутизація на основі QoS(задоволення вимог до затримок, пропускної здатності та енергозбереження);
- Безпечна автентифікація(запобігання несанкціонованому доступу до мережі) та шифрування даних(захист інформації за допомогою AES або RSA). Протокол виявлення аномалій - це інтелектуальні алгоритми призначені для розпізнавання зловмисних атак.

Ключові проблемив мережах IoT

IoT має великий потенціал, але також має свої проблеми:

- Безпека пристроїв: більшість пристроїв IoT мають обмежену обчислювальну потужність. Тому складно реалізувати передові методи шифрування;
- Атаки: DoS-атаки, витік даних і можливість перехоплення зв'язку.

Масштабованість

Кількість пристроїв: Мережі IoT повинні підтримувати мільярди підключень, що вимагає ефективного управління ресурсами.

Перешкоди: збільшення кількості пристроїв знижує ризик виникнення перешкод у бездротових мережах.

Інтероперабельність

Існують відмінності в стандартах: використання несумісних протоколів ускладнює взаємодію пристроїв. Також є проблема сумісності: інтеграція нових і старих пристроїв в єдину мережу.

Енергозалежність

Проблема використання батарей: великі IoT-пристрої регулярно працюють від батарей, і споживання енергії потребує заміни або оптимізації. Рішення: впровадження технологій harvesting (збирання енергії з навколишнього середовища). Підтримка передачі даних у режимі реального часу: критичні IoT-додатки (медичні, автомобільні) вимагають мінімальної затримки, але цього складно досягти в гетерогенних мережах.

Останні тенденції та очікування в мережах IoT:

- Інтеграція з 5G і 6G: збільшення пропускної здатності і зменшення затримок;
- AI/ML в IoT: інтелектуальні системи для управління, прогнозування навантаження і оптимізації ресурсів; блокчейн IoT: забезпечення безпеки, прозорості та децентралізації мережі;
- мережеві технології IoT: необхідність забезпечення безпеки, прозорості та децентралізації мережі;
- Зелені технології IoT: впровадження енергоефективних пристроїв і методів передачі даних.

Успішні приклади мережевих додатків IoT:

- Розумні міста: управління трафіком, енергією та безпекою.
- Сільське господарство: моніторинг продуктивності, оптимізація полів. Промисловість: автоматизація виробництва, управління обладнанням;

- Охорона здоров'я: віддалений моніторинг споживачів за допомогою натільних пристроїв. [1]

Мережі Інтернету речей мають великий потенціал у багатьох галузях. У той же час, безпека, масштабованість, інтероперабельність і енергоспоживання залишаються ключовими проблемами, які необхідно вирішувати за допомогою інноваційних підходів, таких як використання штучного інтелекту, блокчейну і «зелених» технологій.

Інтернет речей (IoT) - це концепція, яка об'єднує фізичні пристрої, датчики, програмне забезпечення та інші технології в єдину екосистему для автоматизації взаємодії між об'єктами, а також для збору та обробки даних для прийняття рішень.

Основою цієї концепції є мережі IoT.

Мережа IoT - це інфраструктура підключених до інтернету пристроїв, які взаємодіють і виконують певні функції. Основними елементами мережі є пристрої (об'єкти IoT): датчики, контролеритапристроївводу/виводу. Протоколи зв'язку: гарантують передачу даних між пристроями. Обчислювальні ресурси: хмарні або периферійні обчислення. Інтелектуальні алгоритми: використовуються для аналізу даних і прийняття рішень

Ключові характеристики мережIoT:

- Гетерогенність - мережі IoT містять різноманітні пристрої з різними характеристиками: комунікаційні технології: Wi-Fi, Zigbee, Bluetooth, LoRaWAN, LTE, 5G. Типи пристроїв: розумні датчики, виконавчі механізми, комп'ютери, носимі пристрої;
- Масштабованість - мережі IoT повинні підтримувати мільйони пристроїв одночасно: розумні міста з сотнями тисяч датчиків, що стежать за навколишнім середовищем, дорожнім рухом та інфраструктурою. Розумні міста з сотнями тисяч датчиків, що контролюють навколишнє середовище, дорожній рух та інфраструктуру;
- Енергозалежність - пристрої Інтернету речей часто працюють на обмежених джерелах живлення, таких як батареї, тому оптимізація енергоспоживання має вирішальне значення; Низька підтримка - критично важливі

додатки Інтернету речей (наприклад, автономні транспортні засоби) потребують мінімізації витрат на передачу даних;

- Автономність - пристрої можуть працювати самостійно або з мінімальним втручанням людини;
- Безпека - мережі IoT повинні бути захищені від атак і несанкціонованого доступу та повинні обробляти конфіденційну інформацію.

Архітектура мережі IoT

Мережі IoT складаються з декількох рівнів для ініціювання їх функціонування:

- Фізичний рівень

Включає датчики, пристрої збору даних та інші апаратні компоненти. Він збирає інформацію про навколишнє середовище (температура, вологість, рух тощо);

- Рівень даних

Комунікаційні технології, такі як Wi-Fi, Zigbee, 4G/5G, LoRaWAN. Протоколи: MQTT, CoAP, HTTP;

- Рівень обробки

Обчислення в хмарі, на межі або на самому пристрої. AI/ML використовується для аналізу даних;

- Прикладний рівень

Виконання завдань на основі оброблених даних (управління міською освітою, моніторинг здоров'я).

Переваги мереж IoT:

- Ефективність: автоматизація процесів зменшує витрати на ручне втручання. Дані в режимі реального часу: неможливість швидко реагувати на зміни;
- Зручність: Пристрої Інтернету речей полегшують життя (розумні будинки, носимі пристрої);
- Масштабованість: можливість інтегрувати нові пристрої та функції.

Недоліки та проблеми мереж IoT:

- Безпека - багато пристроїв IoT недостатньо захищені. Існує ризик злому та несанкціонованого доступу;
- Енергоспоживання - залежність від батарей обмежує час роботи пристроїв;
- Сумісність - виробники реалізують несумісні протоколи;
- Інфраструктура - для забезпечення стабільної роботи потрібні високоякісні мережі передачі даних.

Приклади застосування мереж IoT:

- Розумні міста – освіта, транспорт та управління районами, моніторинг навколишнього середовища;
- Промисловий IoT (IIoT) - оптимізація виробничих процесів, віддалений моніторинг обладнання;
- Охорона здоров'я - носимі пристрої дозволяють відстежувати стан здоров'я. Сільське господарство - моніторинг продуктивності та погодних умов для оптимізації врожайності.

Останні тенденції в мережах IoT:

- Інтеграція з 5G і 6G: забезпечення високошвидкісного зв'язку;
- Використання штучного інтелекту для аналізу великих даних;
- Зелені технології Інтернету речей: енергоефективні пристрої, екологічно чисті матеріали. [2]

Мережі Інтернету речей є ключовим елементом цифрової трансформації, забезпечуючи взаємодію між пристроями, автоматизацію процесів та ефективне управління ресурсами. Незважаючи на свій великий потенціал, мережі стикаються з проблемами безпеки, масштабованості та енергозбереження, які вимагають використання інноваційних технологій.

1.2 Бездротові технології зв'язку в IoT

Бездротові технології зв'язку лежать в основі передачі даних в Інтернеті речей (IoT). Вони забезпечують зв'язок між пристроями, обмін даними з хмарними сервісами та інтеграцію в більш масштабні інформаційні системи.

В мережах IoT використовуються різні бездротові технології, в залежності від їх характеристик.

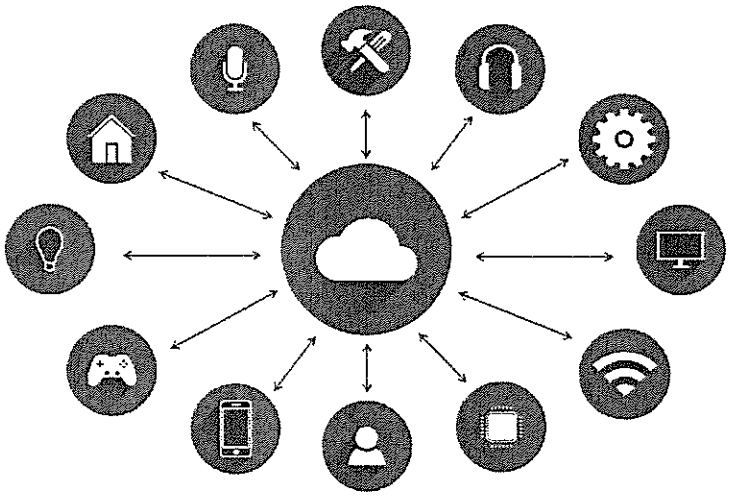


Рис. 1.2 Можливості бездротових технологій

Класифікація бездротових технологій в IoT:

- Wi-Fi малого радіусу дії використовується в розумному будинку та промислових середовищах;
- Bluetooth мережа ідеально підходить для носіння та невеликих мережевих пристроїв IoT;
- Zigbee призначений для розумного будинку та офісних сенсорних мереж;
- NearFieldCommunication (NFC) використовується для безконтактної ідентифікації та оплати;
- Технологія LoRa (LongRange) оптимізована для енергоефективного зв'язку на великі відстані;

- Sigfox - це технологія з низькою пропускною здатністю для передачі невеликих обсягів даних;
- Wi-Fi;
- HaLowє різновидомWi-Fi для енергоефективного зв'язку IoT;
- IoT також є частиною стандартів мобільного зв'язку 4G/5G і забезпечує енергоефективний зв'язок на великі відстані;
- Стандарт 5G: Підтримує високу пропускну здатність і низьку затримку, необхідну для IoT;
- Супутниковий зв'язок: забезпечує глобальний зв'язок у віддалених районах.

Огляд ключових технологій

Wi-Fi має швидкість передачі даних до 10 Гбіт/с (Wi-Fi 6). Високе енергоспоживання обмежує його використання в пристроях на батарейках. Можливості застосування: розумний дім, офісні та промислові IoT-системи. ІснуютьтакірізновидиBluetooth: BluetoothClassictaBluetoothLowEnergy (BLE). BLEпідтримуєнизькеенергоспоживання. Вони застосовуються для таких речей як: носимі пристрої, датчики здоров'я, мітки для відстеження.

Zigbee

Особливості технології: низька швидкість передачі (250 Кбіт/с), ідеально підходить для сенсорних мереж.

Zigbee має низьке енергоспоживання, підтримує великі мережі. Застосовується у таких системах як: розумний дім, промислові сенсорні мережі.

LoRaWAN

LoRaWAN характеризується низькою пропускною здатністю, великим радіусом дії (до 15 км у сільській місцевості).

Його переваги: дуже низьке енергоспоживання. Його можливості використання - це моніторинг навколишнього середовища, сільське господарство, дистанційне керування інфраструктурою.

NB-IoT (вузькосмуговий IoT)

Він працює в ліцензованих частотних діапазонах, низька затримка і висока надійність. Одна базова станція підтримує до 100 000 пристроїв. Може застосовуватись в розумних містах, управлінні освітою, моніторингу води та електроенергії.

Особливості 5G – це низька затримка (<1 мс). Він має висока пропускну здатність (до 20 Гбіт/с), підтримуєmMTC (зв'язок між великими машинами). Застосовується в автономному транспорті, промисловому IoTi, розумних містах.

Супутниковий зв'язок забезпечує зв'язок у віддалених та важкодоступних районах. Застосовується для моніторингу клімату, в сільському господарстві, транспортних системах.

Вибір технології для IoT

Вибір технології залежить від відстані зв'язку: малий радіус дії (Wi-Fi, Bluetooth, Zigbee), великий радіус дії (LoRa, NB-IoT, 5G) та енергоспоживання Енергоефективність мають такі технології якBLE, LoRa, NB-IoT. Технології з великими витратами електроенергії: Wi-Fi, 5G. Технології, що мають високу швидкість передачі даних: Wi-Fi, 5G, а вZigbee, LoRa швидкість доволі низька. Перевагами технологій Zigbee, Bluetooth є низька вартість використання, чого не скажеш про 5G та супутниковий зв'язок.

Проблеми у використанні бездротових технологій зв'язку

Бездротові технології зв'язку також мають деякі проблеми у використанні, серед них:

- Проблема сумісності передбачає, що різні протоколи не можуть використовуватися разом;
- Проблема безпеки являє собоюризик несанкціонованого доступу;
- Проблема енергозбереження – це гостре питання для пристроїв на батарейках;
- Проблема перешкод особливо розповсюджена в неліцензованих зонах.

Тенденції розвитку

Інтеграція зі штучним інтелектом означає автоматичний вибір найбільш підходящого протоколу зв'язку. Wi-Fi 7 використовують для збільшення швидкості

зв'язку та зменшення затримок. Зелені технології IoT підштовхують розробку більш енергоефективних рішень. [3]

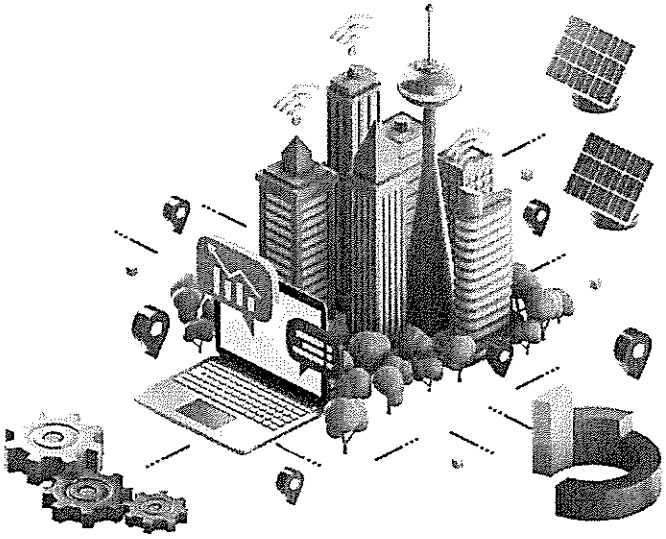


Рис. 1.3 Збір та управління ресурсами

Інтеграція 5G та IoT: створення масштабованих мереж для інтелектуальних систем. Бездротові технології є основою мереж IoT. Різні доступні рішення можуть задовольнити потреби у високошвидкісному та енергоефективному зв'язку. Кожна технологія має свої переваги, недоліки та оптимальну сферу застосування для адаптації Інтернету речей до різних сценаріїв використання.

1.3 Сучасні методи управління ресурсами в IoT-мережах

Інтернет речей (IoT) активно змінює підходи до управління ресурсами в різних галузях. Завдяки динамічному характеру IoT-мереж і великій кількості пристроїв, які до них підключені, ефективне управління ресурсами стало важливим складовою успішної реалізації цієї системи.

Типи ресурсів в IoT

В IoT-мережах ресурси, що потребують управління, включають:

- Обчислювальні ресурси: потужність серверів, хмарних обчислень і периферійних пристроїв;

- Енергетичні ресурси: батареї пристроїв, сонячна енергія;
- Спектральні ресурси: частоти бездротового зв'язку;
- Мережеві ресурси: пропускна здатність каналів зв'язку, доступ до Інтернету.

Сучасні методи управління ресурсами

Хмарні обчислення (CloudComputing) передбачають централізоване зберігання та обробку даних у хмарі. Їхні переваги це масштабованість ресурсів, гнучкі можливості управління потужністю пристроїв, економія на локальній інфраструктурі.

Проблемами є: затримки через віддаленість серверів, залежність від стабільності мережі.

Технологія периферійних обчислень (EdgeComputing) – це обробка даних ближче до джерела їх виникнення. Застосовується для критичних завдань (реакція в реальному часі, наприклад, у розумних автомобілях або виробничих лініях). Має такі переваги: зменшення затримок, економія мережевих ресурсів, підвищення автономності IoT-пристроїв.

Використання штучного інтелекту (AI)

Алгоритм оптимізації використовує:

- машинне навчання для передбачення завантаження в мережу;
- генетичні алгоритми для пошуку оптимального розподілу ресурсів.

Застосовується для інтелектуального керування енерговитратами, розподілу спектральних частот.

Технологія когнітивного радіо має динамічне управління частотами шляхом зондування та аналізу доступного спектра. Має наступні переваги: змінення інтерференції, оптимізація використання спектральних ресурсів. Недоліки: складність реалізації в середовищі з високою динамікою.

Мережеві протоколи

Глобальна мережа малої потужності (LPWAN): LoRaWAN, Sigfox забезпечують низьке енергоспоживання для пристроїв з малим обсягом даних. Протокол NB-IoT (NarrowbandIoT) оптимізований для невеликих даних у

ліцензованих функціях. Динамічне маршрутизація використовує адаптивні протоколи, такі як RPL (RoutingProtocolforLow-PowerandLossyNetworks).

Енергозбереження та управління енергією

Алгоритми оптимізації енергії

Алгоритми оптимізації енергії мають такі складові як:

- Робочий цикл: періодичне увімкнення та вимкнення пристроїв;
- Агрегація даних: зменшення частоти передачі даних через їх об'єднання.

Відновлені джерела енергії являють собою використання сонячної, вітрової енергії для зарядки пристроїв у віддалених місцях, інтелектуальне управління батареями, інструменти для прогнозування залишкового заряду та адаптації завантаження на пристрій.

Методи управління мережею:

- Пріоритизація трафіку QoS (QualityofService)- це розподіл пропускної здатності залежно від типу трафіку, виділення більшої пропускної здатності для критичних даних;
- Балансування навантаження (використання алгоритмів для розподілу даних між швидкісними каналами або вузлами мережі);
- Мобільність пристроїв – це оптимізація управління підключенням до мобільних середовищ (наприклад, динамічне перемикання між Wi-Fi та стільниковими мережами).

Виклики та проблеми:

- Інтерференція: конкуренція між пристроями за спектральні ресурси;
- Безпека: захист даних і мережевих ресурсів від атак;
- Масштабованість: здатність мережі підтримувати мільярди пристроїв. Енергоефективність: забезпечення тривалої роботи пристроїв із обмеженим живленням.

Сучасні тенденції

- Інтеграція IoT із 5G підтримує високі швидкості та низькі затримки;

- Розвиток хмарних і гібридних обчислень забезпечує гнучкість управління;
- IoT-аналітика прогнозує завантаженость мережі та адаптивне управління.

Сучасні методи управління ресурсами в IoT-мережах базуються на технологіях штучного інтелекту, хмарних і периферійних обчисленнях, інноваційних мережевих протоколах і відновлюваних джерелах енергії. Ці підходи спрямовані на забезпечення ефективності, безпеки та адаптації IoT-мереж до швидко змінених умов. [4]

1.4 Проблеми надійності та масштабованості в мережах IoT

Проблеми надійності в мережах IoT:

- Відмова обладнання - низька якість обладнання через бюджетні обмеження;
- Знос обладнання в суворих умовах експлуатації (висока вологість, пил, екстремальні температури). Необхідно обирати більш довговічні матеріали. Резервування критично важливих елементів мережі;
- Затримки та втрата даних через низьку пропускну здатність каналу зв'язку. Перешкоди між пристроями;
- Перевантаження мережі великою кількістю пристроїв. Для вирішення проблеми використовується пріоритезація трафіку з використанням QualityofService (QoS).

Оптимізація маршрутизації та балансування навантаження. Вразливість до атак через недостатній рівень захисту протоколів зв'язку. Використання стандартних паролів та слабких механізмів автентифікації. Необхідне використання захищених протоколів (TLS, DTLS). Інтеграція механізмів автентифікації на основі блокчейну. Енергетична незахищеність: споживання батареї через високий рівень активності та тривале використання.

Допоможе у вирішенні проблеми: Використання алгоритмів енергоефективності (робочий цикл, сплячий режим). Використання відновлюваних джерел енергії. Проблеми синхронізації через відсутність єдиного стандарту для синхронізації годинників пристроїв. Різниця в затримках між вузлами. Необхідне використання часових протоколів, таких як NTP (NetworkTimeProtocol) або PTP (PrecisionTimeProtocol).

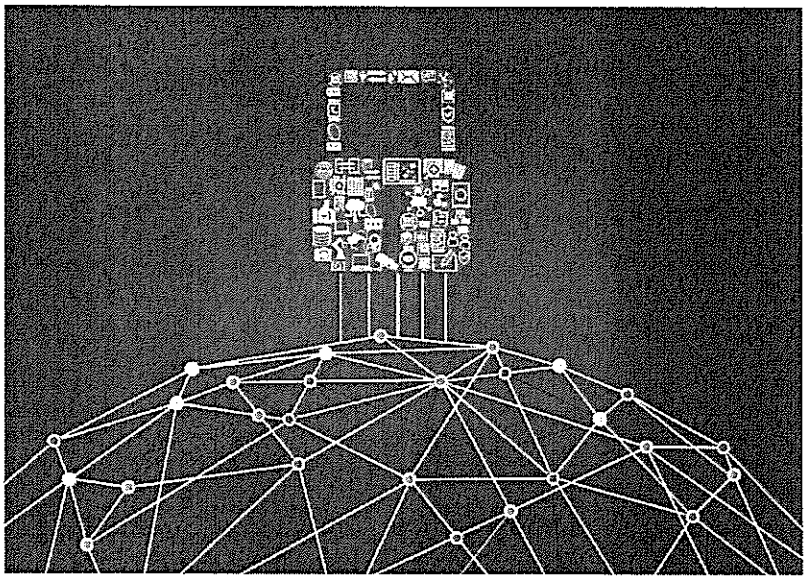


Рис. 1.4 Масштабованість та безпека в мережах IoT

Проблеми масштабованості в мережах IoT

Підтримка мільярдів підключених пристроїв. Використовуйте IPv6 для збільшення адресного простору. Розподілені архітектури, такі як периферійні обчислення. Обмеження пропускної здатності через забезпечення стабільної передачі даних у великих мережах рішення використовуйте технологію LPWAN (LowPowerWideAreaNetwork) для передачі даних з низькою пропускною здатністю. Збільшити пропускну здатність за допомогою інтеграції 5G. Проблема управління даними: Обробка та зберігання великих обсягів даних, що генеруються пристроями IoT необхідне централізоване зберігання даних через хмарні сервіси, використання технологій великих даних та штучного інтелекту для аналізу даних у реальному часі та балансування навантаження. Проблема: Рівномірний розподіл

навантаження між серверами та вузлами мережі. Потрібно використовувати динамічну маршрутизацію та балансування навантаження на основі ШІ. Адаптивні протоколи маршрутизації, наприклад, RPL. Проблема енергоспоживання: Збільшення кількості пристроїв призводить до значного споживання енергії. Вирішенням цієї проблеми є оптимізація роботи датчиків за допомогою енергозберігаючих протоколів та використання енергоефективних чіпів.

Перспективні підходи до вирішення проблеми

Інтеграція з 5G Забезпечує низьку затримку, високу пропускну здатність та підтримує велику кількість пристроїв. Використання штучного інтелекту Прогнозує навантаження на мережу та автоматично керує ресурсами.

Блокчейн для IoT дозволяє використовувати розподілене управління мережею, забезпечує надійність і прозорість транзакцій.

Технологія когнітивного радіо динамічно використовує доступні частоти і мінімізує конкуренцію.

Інтеграція з периферійними обчисленнями

Зменшує навантаження на централізовані сервери, наближаючи дані до пристроїв. [5]

Приклади застосувань розумного міста: використання IoT для масштабованого управління трафіком і моніторингу навколишнього середовища. Приклади застосувань розумного міста: використання Інтернету речей для масштабованого управління дорожнім рухом і моніторингу навколишнього середовища. Промисловий IoT (IIoT): впровадження розподілених рішень для забезпечення надійного зв'язку між роботами та датчиками. Проблеми надійності та масштабованості мереж IoT вимагають інноваційних підходів, таких як інтеграція з 5G та використання штучного інтелекту і когнітивних технологій. Постійне вдосконалення стандартів і протоколів є ключовим для подальшого розвитку IoT.

1.5 Методи управління ресурсами в безпровідних IoT-мережах

Управління ресурсами в безпроводових IoT-мережах є ключовим викликом, остання ці мережі повинні забезпечувати ефективне використання обмежених ресурсів, таких як енергія, спектр частоти, обчислювальна потужність і пропускна здатність. Розглянемо основні методи управління цими ресурсами.

Енергозбереження

- Енергозберігаючі протоколи MAC-протоколи (MediumAccessControl): Використання DutyCycling для мінімізації активного часу пристроїв. Протоколи з низьким енергоспоживанням, як-от B-MAC, X-MAC.
- Режими сну та пробудження: Пристрої перебувають у сплячому режимі й активуються тільки для передачі або прийому даних.
- Збирання енергії (EnergyHarvesting) з навколишнього середовища: Сонячна енергія. Енергія вібрацій чи тепла.
- Радіочастотне збирання енергії (RFEnergyHarvesting).

Управління передачею даних: Змінення кількості переданих пакетів шляхом їх об'єднання. Компресія даних: Використання алгоритмів для зменшення розміру даних перед передачею.

Управління спектральними ресурсами

Когнітивне радіо (CR) Використання вільних частот у реальному часі. Основні функції: Виявлення спектра: аналіз наявності доступних частот. Динамічний вибір частоти: автоматичне перемикання між каналами. Технології розділення спектра FDMA (FrequencyDivisionMultipleAccess): розподіл частотних смуг між пристроями. TDMA (TimeDivisionMultipleAccess): відвідуваннядоступудоспектравчасі. CDMA (множинний доступ з кодовим розділенням): передача даних через унікальні кодові сигнали. Використання LPWAN Низькоенергетичні мережі великого радіуса дії (LoRaWAN, Sigfox, NB-IoT) для мінімізації спектра перевантаження.

Управління обчислювальними ресурсами

Розподілені обчислення Передача частини обчислень на периферійні або хмарні сервери. EdgeComputing: обробка даних на периферії мережі, ближче до пристроїв. FogComputing: обчислення між пристроями та хмарою. Оптимізація обчислень Використання алгоритмів стиснювання й агрегування даних. Застосування машинного навчання для прогнозування навантаження й адаптації обчислень.

Управління трафіком

Адаптивна маршрутизація - динамічний вибір маршрутів залежно від умов мережі (завантаження, затримки, енергоспоживання). Протоколи: RPL (протокол маршрутизації для мереж з низьким енергоспоживанням і втратами), AODV (спеціальний вектор відстані на вимогу), QoS (Якість обслуговування) Пріоритизація трафіку для критичних проявів (розумні міста, медицина). Використання механізмів адаптивного резервування пропускної здатності. Балансування навантаження Розподіл трафіку між усіма вузлами для запобігання перенавантаженню.

Управління пам'яттю та зберіганням даних

Децентралізоване зберігання Зберігання даних на пристроях IoT для зменшення навантаження на центральні сервери. Використання технологій блокчейну для безпечного розподілу даних. Компресія даних Алгоритми для зменшення обсягу даних, що зберігаються, наприклад LZW, HuffmanCoding.

Інтеграція новітніх технологій

Штучний інтелект (AI) Прогнозування використання ресурсів на основі аналізу історичних даних. Автоматизація управління енергоспоживанням та маршрутизацією. Блокчейн - забезпечення безпеки ресурсів та транзакцій між пристроями IoT. Прозорість управління та зберігання даних. Інтеграція з 5G Використання широкосмугових можливостей 5G для підтримки масових IoT-мереж. Підтримка технології NetworkSlicing для виділення окремих ресурсів під різні

2. ЕФЕКТИВНЕ УПРАВЛІННЯ ЧАСТОТАМИ

2.1 Основи енергозбереження в мережах IoT

Ефективне управління частотами має важливе значення для забезпечення надійного зв'язку, мінімізації перешкод і оптимізації використання обмежених ресурсів.

Основи розподілу частот в мережах IoT

Розподіл частот - це процес визначення частотних діапазонів (каналів), які будуть використовуватися різними пристроями та мережами IoT. Тип пристрою: датчики, виконавчі пристрої, шлюзи. Тип трафіку: повільний (сигнали датчиків) або швидкий (відеоспостереження). Тип середовища: міські, сільські, промислові мережі. Основні принципи Мінімізація перешкод: уникайте перешкод між сусідніми пристроями та мережами. Оптимізація смуги пропускання: забезпечення достатнього частотного ресурсу для всіх пристроїв. Справедливий доступ: рівний розподіл частот між учасниками мережі.

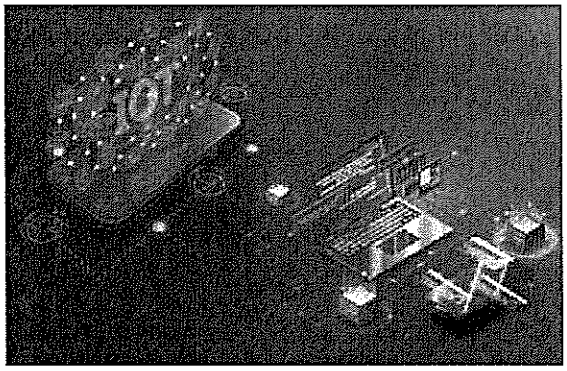


Рис. 2.1 Управління частотами

Фіксований розподіл частот

Частоти заздалегідь призначаються пристроям або підмережам. Переваги Проста реалізація. Не потребує складних алгоритмів керування. Недоліки: Не може адаптуватися до змін у трафіку. Потенційно неефективне використання ресурсів під час низьких навантажень Динамічний розподіл частот Розподіл частот відбувається в реальному часі відповідно до потреб. Методи Спільне використання

спектру: декілька пристроїв спільно використовують тимчасово або просторово розподілену смугу частот. Когнітивний підхід: пристрої аналізують доступність спектру та обирають доступні частоти. Переваги Гнучкість та адаптивність. Зменшення перешкод. Недоліки: складність реалізації. Затримки через необхідність аналізу спектру. Ієрархічний розподіл частот Мережа поділяється на рівні базових станцій, підмереж і кінцевих пристроїв. Частоти розподіляються за рівнями, і вищі рівні мають пріоритет. Приклад: Мережа 5G з ресурсами, зарезервованими для додатків IoT (мережеве розщеплення). Розподіл частот за варіантами використання Частоти розподіляються відповідно до типу варіанту використання: Масштабовані мережі IoT (наприклад, розумні міста) вимагають великої пропускної здатності. Локалізовані мережі (наприклад, промисловий IoT) можуть використовувати вузькі смуги частот.

Алгоритми розподілу частот

- Алгоритми з фіксованими правилами: розподіл каналів відповідно до фіксованого шаблону. Приклад: виділення окремого каналу для кожного пристрою
- Жадібний алгоритм: пристрої займають доступні частоти доти,

доки вони доступні. Переваги: висока швидкість виконання. Недоліки: ризик конкуренції та неефективний розподіл.

- Еволюційні алгоритми: використовують генетичні або ройові алгоритми

для оптимізації розподілу. Переваги: можливість знайти глобальний оптимум. Недоліки: вимагають значних обчислювальних ресурсів.

Алгоритми штучного інтелекту (ШІ)

- Машинне навчання: прогнозування частотних перевантажень.
- Глибоке навчання: визначення оптимальних частотних ресурсів у

складних сценаріях. Наприклад, використання нейронних мереж для прогнозування доступності каналів.

Децентралізований алгоритм - це залежне визначення частот, які будуть використовуватися кожним пристроєм. Приклад: протокол ALOHA для випадкового вибору частоти.

Проблеми та виклики

Перешкоди Сусідні пристрої можуть використовувати однакові частоти. Рішення: розділення каналів за часом (TDMA), площею (SDMA) і кодом (CDMA).Енергоспоживання Пошук частоти вимагає значного споживання енергії, що важливо для пристроїв IoT. Рішення: використання енергоефективних алгоритмів. Загрози безпеці: атаки на когнітивне радіо, частотні завади. Рішення: шифрування каналу, виявлення зловмисників. Масштабованість Розподіл частот ускладнений через велику кількість пристроїв. Рішення: використання багаторівневих моделей управління. [7]

Сучасні тенденції

Інтеграція з 5G Використання технологій міліметрового діапазону хвиль та мережевого зрізу для розподілу частот між пристроями IoT. Використання неліцензованих частот Розвиток технологій Wi-Fi 6, Wi-Fi 7 та LoRa в діапазоні 6 ГГц. Штучний інтелект для управління частотним діапазоном.

Адаптивні механізми в мережах IoTрозглядає методи і алгоритми, які динамічно налаштовують параметри мережі для оптимальної продуктивності, знижуючи споживання енергії і підвищуючи стійкість до змін навколишнього середовища. Завдяки адаптивності мережі IoT можуть ефективно працювати в умовах високої динамічності та мінливості.

Поняття адаптивних механізмів

Адаптивність - це здатність системи автоматично змінювати свої параметри у відповідь на зміни навколишнього середовища, вимог користувача або умов експлуатації Основні цілі адаптивних механізмів Оптимізація використання ресурсів (спектру, енергії, обчислювальних потужностей). Зменшення завад та покращення якості зв'язку Масштабованість для підтримки зростаючої кількості пристроїв. Реакція на зовнішні впливи (наприклад, зміна смуги пропускання, втрата зв'язку).

Класифікація адаптивних механізмів

Механізми адаптивного управління спектром:

- Динамічне підстроювання частоти для уникнення перешкод;

- Когнітивне радіо: пристрій аналізує спектр в режимі реального часу і вибирає найбільш підходящі частоти;
- Динамічний розподіл частот: частоти розподіляються відповідно до потреб трафіку;
- Механізми адаптивного енергоспоживання використовуються для подовження терміну служби пристроїв IoT з обмеженим ресурсом батареї;
- Адаптивне керування потужністю передачі: зменшує потужність при наближенні до вузлів. Перемикання між активним і сплячим режимами: зменшує енергоспоживання, коли пристрій неактивний;
- Агрегація даних: зменшує кількість переданих пакетів шляхом об'єднання переданих пакетів. Адаптивні протоколи зв'язку покликані забезпечити ефективну передачу даних у мінливому середовищі;
- Адаптивний MAC (контроль доступу до середовища) змінює параметри доступу до середовища відповідно до навантаження.Наприклад протокол IEEE 802.15.4, який динамічно змінює частоту передачі;
- Адаптивні маршрутизатори: змінюють шляхи передачі даних у відповідь на перевантаження або збої в мережі;
- Адаптивні механізми управління трафіком покликані зменшити затримку, втрату пакетів і перевантаження мережі. Пріоритезація даних: надання пріоритету важливому трафіку (наприклад, екстреним сповіщенням). Динамічне стиснення даних: зменшує обсяг даних, що передаються під час перевантаження. Адаптивні механізми безпеки забезпечують безпеку мережі від мінливих загроз;
- Адаптивне шифрування: зміна алгоритму шифрування відповідно до рівня загрози;
- Виявлення аномалій: використання машинного навчання для виявлення несанкціонованої поведінки.

Адаптивні технології

Машинне навчання та штучний інтелект (ШІ) Використання алгоритмів для аналізу трафіку, прогнозування змін у середовищі та автоматичного налаштування параметрів. Приклади: Нейронні мережі для оптимізації енергоспоживання.

Когнітивне радіо забезпечує адаптивний доступ до частотних діапазонів шляхом виявлення доступних частотних діапазонів. Мережеві протоколи наступного покоління такі протоколи, як MQTT, CoAP і LoRaWAN, мають вбудовані механізми адаптації до мінливих умов. Хмарні та туманні обчислення обробляють великі масиви даних для визначення оптимальної конфігурації мережі. Туманні обчислення дозволяють локальну адаптацію та зменшують затримки.

Проблеми та виклики адаптивності

Обчислювальні ресурси - досягнення високого рівня адаптивності вимагає значних обчислювальних потужностей. Затримки Адаптивні алгоритми повинні аналізувати дані в режимі реального часу, що може викликати затримки Конфлікти інтересів Адаптивність одного параметра (наприклад, енергоспоживання) може погіршити інші параметри (наприклад, якість зв'язку) Безпека Збільшення складності систем робить їх більш вразливими до атак.

Сучасні тенденції та перспективи

Інтеграція з 5G та 6G Використання методів мережевого розщеплення для адаптивного виділення ресурсів для конкретних додатків IoT. Штучний інтелект та технології великих даних Аналітика великих даних Використання адаптивних моделей для вдосконалення адаптивних моделей. Розвиток автономних систем Повністю автономні мережі IoT, які визначають та керують власними параметрами.Розвиток енергоефективних пристроїв Нові акумулятори та протоколи передачі даних, орієнтовані на мінімізацію енергоспоживання.

Реальні приклади

Розумний дім: енергозбереження завдяки динамічному налаштуванню Wi-Fi та Zigbee. Сільське господарство: Адаптація LoRaWAN до змін погоди та щільності датчиків. Транспортні системи: адаптивне управління світлофорами на основі інтенсивності руху. Адаптивні механізми в мережах Інтернету речей є ключовими для забезпечення стабільності, енергоефективності та масштабованості в умовах стрімкого зростання кількості підключених пристроїв та обсягів даних.

Управління енергоспоживанням в мережах IoT є одним з найважливіших питань для розробки енергоефективних систем: Оскільки пристрої IoT часто

живляться від батареї або мають обмежений доступ доживлення, ефективне управління енергоспоживанням має важливе значення для продовження терміну служби мережі, зниження експлуатаційних витрат і забезпечення стабільної роботи.

Характеристики управління енергоспоживанням в IoT

Обмежене енергопостачання: Більшість пристроїв IoT живляться від батареї. Довготривала робота: у багатьох сценаріях (наприклад, сільське господарство, дистанційні датчики) заміна батареї може бути складною або неможливою. Високі витрати на електроенергію: неефективне управління енергоспоживанням призводить до збільшення операційних витрат. Зростання кількості пристроїв: з мільярдами пристроїв Інтернету речей навіть невелика оптимізація енергоспоживання має значний вплив у глобальному масштабі. Основні цілі Продовження терміну служби батарей. Мінімізація споживання енергії без втрати якості роботи. Збалансування енергоспоживання в масштабах мережі. Інтеграція відновлюваних джерел енергії (сонячна, вітрова).

Компоненти управління енергоспоживанням

Датчики: мають обмежену потужність і часто працюють циклічно (активність/сон). Актуатори: споживають більше енергії, оскільки виконують фізичні дії (наприклад, відкривання клапанів). Шлюзи: відповідають за обробку і передачу даних; енергоспоживання залежить від навантаження. Протоколи зв'язку Низькоенергетичні протоколи, такі як Zigbee, Bluetooth Low Energy (BLE), LoRaWAN, NB-IoT. Мережеві функції Маршрутизація даних: вибір оптимальних маршрутів,зменшення кількості передач та перезавантажень. Агрегація даних: уникнення непотрібного дублювання інформації.

Технології управління енергоспоживанням являють собою:

- Енергоефективний дизайн пристроїв;
- Використання енергоефективних компонентів (мікроконтролерів, комунікаційних модулів);

- Інтеграція технологій енергозбереження (отримання енергії з навколишнього середовища): сонячна енергія, кінетична енергія, радіочастотна енергія.

Адаптивне керування режимами роботи:

- Режим сну: пристрій більшу частину часу перебуває в режимі сну і прокидається лише тоді, коли йому потрібно виконати завдання;
- Активація за подією: пристрій активується лише в разі виявлення події;
- Робочий цикл: пристрій перемикається між активним і сплячим режимами за потреби.

Оптимізація протоколів зв'язку

- Мінімізація передачі даних: агрегація даних: кілька вимірювань об'єднуються в один пакет;
- Фільтрація даних: передаються лише важливі дані.

Вибір найбільш підходящого протоколу

Великий радіус дії, низьке енергоспоживання LoRaWAN; NB-IoT: стабільний зв'язок навіть у невеликих зонах зв'язку. Динамічний контроль потужності передачі: пристрої використовують мінімально необхідну потужність. Енергоефективна маршрутизація Вибір шляхів передачі даних на основі залишкової енергії вузлів, наприклад, LEACH (Low Energy Adaptive Clustering Hierarchy). Використовуються алгоритми. Аналіз та прогнозування енергоспоживання Машинне навчання використовується для прогнозування навантаження на мережу та коригування поведінки обладнання. Балансування енергоспоживання Завдання перерозподіляються між вузлами для забезпечення рівномірного використання енергоресурсів.

Алгоритми управління енергоспоживанням

Жадібний алгоритм Простий підхід для вибору дії з найменшим споживанням енергії в будь-який момент часу; Еволюційний алгоритм Оптимізація поведінки мережі за допомогою генетичних алгоритмів, роїв частинок тощо; Алгоритм машинного навчання Використовується для адаптації параметрів мережі до мінливих умов.

Виклики в управлінні енергоспоживанням

Зростання складності мереж IoT Зростання кількості пристроїв вимагає більш складних та ефективних механізмів. Балансування енергоспоживання та продуктивності Економія енергії може знизити якість передачі даних, що може знизити якість передачі даних. Використання відновлюваних джерел енергії Нестабільність таких джерел енергії може вплинути на роботу мережі.

Сучасні тенденції та перспективи

Розвиток технологій збору енергії Інтеграція пристроїв, які використовують енергію з навколишнього середовища. Інтелектуальні системи управління Використання штучного інтелекту для прогнозування попиту на енергію та управління ресурсами; Використання мережевого зрізу для виділення енергооптимізованих сегментів мережі;

Розумні міста: адаптація вуличного освітлення до руху пішоходів;

Сільське господарство Сільське господарство: Використання сонячної енергії для живлення датчиків вологості IoT.

Промислові IoT-системи: оптимізація роботи двигунів і датчиків для зниження енергоспоживання. [8]

Стратегії енергозбереження в мережах IoT стосуються методів, підходів і технологій, спрямованих на мінімізацію споживання енергії пристроями IoT. Оскільки більшість пристроїв IoT живляться від батарей або мають обмежений доступ до живлення, енергозбереження є важливим для забезпечення довговічності та ефективності мережі.

Тривалий час автономної роботи: більшість пристроїв IoT мають обмежені енергетичні ресурси (батареї, накопичувачі). Витрати на заміну батарей: заміна джерел живлення у великих мережах може бути дорогою або технічно складною. Зменшення впливу на навколишнє середовище: зниження споживання енергії допомагає зменшити викиди вуглецю. Підвищення ефективності мережі: оптимальне використання енергії знижує ризик виходу пристрою з ладу. Основні проблеми енергозбереження Різні пристрої з різними вимогами до

енергоспоживання. Високі вимоги до пропускної здатності та швидкості обробки даних. Баланс між якістю обслуговування (QoS) та енергозбереженням.

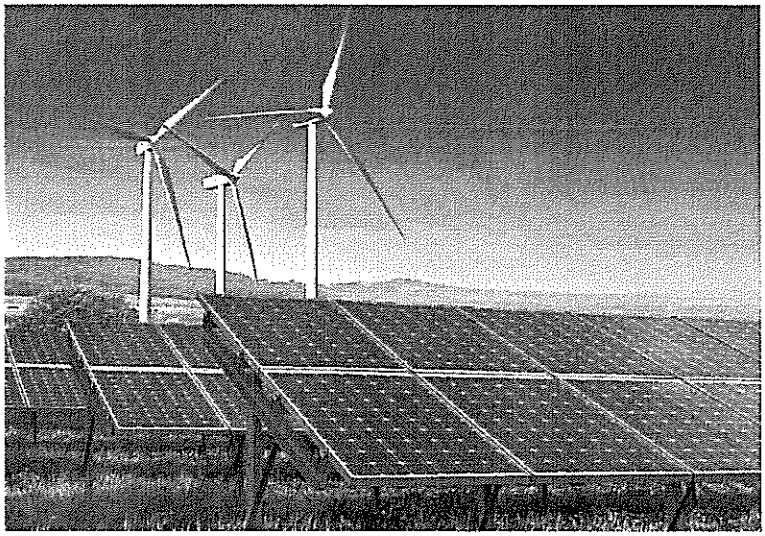


Рис. 2.2 Технології та можливості енергозбереження

Класифікація стратегій енергозбереження

Рівень пристроїв Мета: оптимізація продуктивності окремих пристроїв та мінімізація енергоспоживання. Методи: використання енергоефективних компонентів. Перехід у сплячий режим або зменшення активності. Рівень мережі Мета Знизити загальне споживання енергії шляхом оптимізації роботи всієї мережі. Методи Інтелектуальна маршрутизація. Балансування навантаження. Рівень додатків Мета Зниження енергоспоживання за рахунок зменшення обсягу інформації, що передається. Методи Стиснення даних. Інтелектуальне керування частотою передачі.

Основні стратегії енергозбереження

Режими енергозбереження Сплячий режим: пристрій більшу частину часу перебуває в сплячому режимі і працює лише під час передачі або обробки даних. Гібридний режим: наприклад, робочий цикл: пристрій перемикається між активним та сплячим режимами за визначеним графіком Енергозбереження через управління живленням Динамічне регулювання потужності передачі: пристрій регулює потужність сигналу відповідно до відстані до приймача. Зниження частоти

процесора: тактова частота мікроконтролера знижується в періоди низького навантаження.

Енергоефективні протоколи зв'язку

Протоколи з низьким енергоспоживанням: Zigbee. Bluetooth Low Energy (BLE). LoRaWAN. адаптивна стрибкоподібна зміна частоти: Зменшує частоту передачі при незначних змінах навколишнього середовища. Стиснення та агрегація даних Стискає дані перед передачею для зменшення енергоспоживання. Агрегація: об'єднання даних з декількох пристроїв в один пакет перед передачею; Енергоефективна маршрутизація Вибір шляхів передачі для мінімізації споживання енергії, наприклад, LEACH (Low Energy Adaptive Clustering Hierarchy). Енергоефективне управління кластерами Об'єднання вузлів у кластери з головним вузлом кластера, відповідальним за передачу даних

Технології, що підтримують енергозбереження

Використання енергії з навколишнього середовища: сонячна енергія: від сонячних панелей. Електрична енергія. Кінетична енергія: використання руху. Термоелектрична енергія: виробництво енергії з різниці температур. Машинне навчання та штучний інтелект Оптимізація режиму роботи пристрою. Хмарні обчислення та туманні обчислення Перенесення обчислень з пристрою на більш енергоефективні сервери в хмарних або туманних мережах.

Алгоритми енергозбереження.

Адаптивні алгоритми - налаштування робочих параметрів відповідно до рівня енергії, що залишилася в пристрої. Адаптивні алгоритми Регулювання робочих параметрів відповідно до залишку енергії в пристрої. Прогностичні алгоритми Використання історичних даних для прогнозування майбутнього попиту на енергію. Алгоритми розподілу енергії Розподіл енергоресурсів між вузлами відповідно до їх ролі в мережі.

Виклики при впровадженні стратегій енергозбереження:

- Баланс між якістю послуг та енергозбереженням;

- Надмірне скорочення споживання енергії може вплинути на якість послуг; Складність мережі Велика кількість пристроїв з різними вимогами ускладнює оптимізацію;
- Обмеження технологій збору енергії Енергетичні ресурси є нестабільними.

Сучасні тенденції та перспективи

Інтеграція з 5G та 6G Створення енергоефективних сегментів мережі з використанням технологій розгалуження мережі. Розробка автономних пристроїв Розробка автономних пристроїв, що повністю живляться від відновлюваних джерел енергії. Інтелектуальне управління Максимізація енергоефективності за допомогою алгоритмів машинного навчання. Регулювання освітлення та роботи кондиціонерів залежно від присутності людини. Сільське господарство: вимірювання вологості ґрунту за допомогою датчиків Інтернету речей, що збирають енергію. Промисловість: енергоефективні системи моніторингу обладнання на великих підприємствах.

Оптимізація живлення пристроїв

«Пристрої Інтернету речей часто працюють на обмежених енергетичних ресурсах, тому оптимізація енергоспоживання має вирішальне значення для мінімізації витрат і збільшення часу безвідмовної роботи».

Характеристики та важливість оптимізації енергоспоживання

Енергетичні ресурси обмежені: більшість пристроїв Інтернету речей живляться від батареї або використовують зібрану енергію. Тривалий життєвий цикл: багато пристроїв встановлюються у важкодоступних місцях, де регулярна заміна батарей ускладнена. Масштабованість мереж IoT: за рахунок оптимізації енергоспоживання мережі можна розширювати без значного збільшення витрат на електроенергію. Основні цілі оптимізації – мінімізувати енергоспоживання при збереженні функціональності. Подовжити термін служби батареї. Підвищити ефективність використання енергії в масштабі мережі.

Методи оптимізації енергоспоживання

- Апаратна оптимізація Використання малопотужних та енергоефективних мікроконтролерів (наприклад, ARM Cortex-M). Використання комунікаційнихмодулів,щопідтримуютьенергоефективніпротоколи(BLE, Zigbee, LoRaWAN).
- Використання датчиків з низьким енергоспоживанням та здатнихпрацюватив сплячому режимі.
- Інтеграція технологій збору енергії, таких як сонячні панелі, термоелектричні генератори та кінетичні перетворювачі.
- Оптимізація програмного забезпечення Адаптивне управління енергоспоживанням: динамічне налаштування режиму роботи пристрою: сплячий режим: пристрій переходить у сплячий режим за відсутності активності. Активний режим: пристрій активується лише для передачі або обробки даних. Робочий цикл: регулюйте час активності та сну відповідно до поточних потреб. Зменшити активність під час низьких навантажень.
- Зменшення обсягу даних, агрегація даних: об'єднання декількох вимірювань в один пакет. Стиснення даних: зменшуйте розмір пакета перед передачею. Використовуйте алгоритми фільтрації, щоб забезпечити передачу лише важливих даних.
- Адаптивна потужність передачі: динамічно регулюйте потужність передачі залежно від відстані до приймача та умов навколишнього середовища.
- Оптимізація протоколів зв'язку. Краще використовувати протоколи з низьким енергоспоживанням: Zigbee і BLE (для коротких відстаней). LoRaWAN та NB-IoT для великих відстаней та адаптивні частоти передачі: пристрої передають дані тільки тоді, коли це необхідно;
- Енергоефективна маршрутизація Вибір шляхів передачі даних на основі енергетичного стану вузлів. Використання кластеризації для зменшення навантаження на окремі вузли (наприклад, LEACH - Low Energy Adaptive Clustering Hierarchy).

Алгоритми оптимізації енергоспоживання:

- Адаптивні алгоритми;

- Встановлення режиму роботи пристрою в залежності від умов експлуатації та залишку енергії;
- Еволюційні алгоритми Пошук оптимальних параметрів мережі за допомогою генетичних алгоритмів та методів рою частинок;
- Алгоритми машинного навчання;
- Оцінка енергоспоживання;
- Оптимізація графіків передачі даних.
- Децентралізовані алгоритми
- Пристрої самостійно визначають режими своєї роботи без центрального контролера.

Технології, що підтримують оптимізацію

- Збір енергії Сонячна енергія: використовується для пристроїв, встановлених на відкритому повітрі. Термоелектрична енергія: підходить для промислового середовища. Кінетична енергія: використовує рух для заряджання пристроїв;
- Інтелектуальне керування: використовує штучний інтелект для автоматичного регулювання режиму роботи пристроїв;
- Граничні та туманні обчислення: переміщують обчислення з пристроїв IoT на проміжні вузли для зменшення споживання енергії.

Проблеми оптимізації енергоспоживання

Різноманітність пристроїв Велика кількість різних пристроїв ускладнює стандартизацію оптимізації. Баланс між енергоефективністю та QoS Переоптимізація може вплинути на якість передачі даних Обмеження технологій збору енергії Природні умови роблять енергетичні ресурси нестабільними. [9]

Сучасні тенденції та перспективи

Інтеграція з мережами 5G та 6G Виділення енергоефективних сегментів мережі за допомогою мережевої нарізки; Розробка автономних пристроїв Інтеграція пристроїв, що живляться лише від відновлюванихджереленергії; ПрогнозуванняенергоспоживанняВикористовуйтемашинненавчаннядляаналізупопиту на енергію;

Приклади з життя

Сільське господарство: датчики Інтернету речей, що працюють на сонячній енергії. IoT-датчики, що використовують сонячну енергію. Розумні міста: вуличне освітлення, що активується датчиками руху. Промисловість: енергоефективні системи моніторингу обладнання.

Оптимізація енергоспоживання в мережах Інтернету речей є важливим аспектом забезпечення сталої роботи пристроїв, особливо у великих і складних мережах, що працюють у динамічному середовищі. Інноваційні технологіїтаалгоритмидозволяютьзначнознизити енергоспоживання, забезпечуючи при цьому високу якість роботи мережі.

2.2 Методи адаптивної маршрутизації

Методи адаптивної маршрутизаціїв мережахIoT- цетехнології тапідходи,які забезпечують оптимальне пересилання даних міжвузлами з урахуванням динамічнихзміну мережі. Методи адаптивної маршрутизації гарантують високу ефективність роботи мережі в умовах обмеженихресурсів, мобільності вузлівтазмін топології.

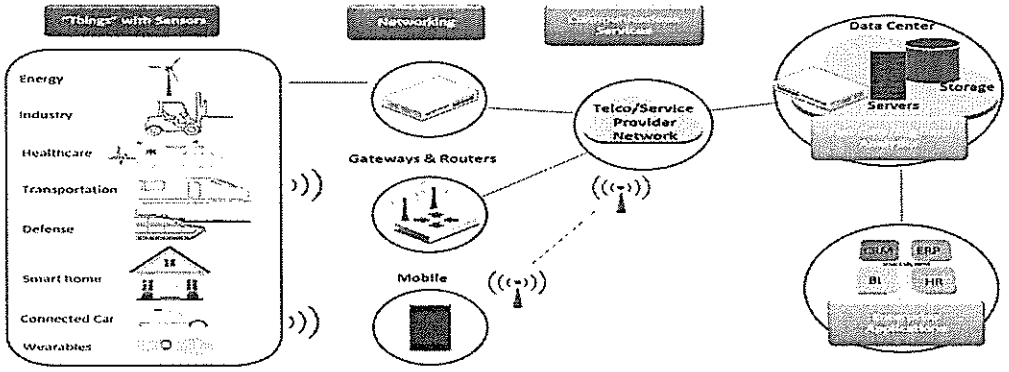


Рис. 2.3 Маршрутизація в IoT

Характеристика методів адаптивної маршрутизації

Адаптивна маршрутизація змінюєшляхипередачі даних відповідно допоточногостанумережі,такого як залишкова енергія вузлів, пропускна здатність і затримка, динаміка мережі (зникнення або поява вузлів)тощо.Адаптивність важлива в IoT тому що:мережі IoT часто є динамічними, вузли можуть додаватися, виходити з ладу або змінювати місце розташування. Обмежені ресурси: Пристрої Інтернету речей мають обмежені ресурси енергії, пам'яті та обчислювальної потужності.

Різноманітність додатків: різні додатки IoT мають різні вимоги до швидкості передачі, затримкита енергоефективності

В принципах адаптивної маршрутизації враховується енергетичний баланстауникаються вузли з низьким зарядом батареї.

Адаптація пропускної здатності

Перевантажені вузли та канали Мобільна адаптація Використовуються алгоритми, що враховують динамічні зміни в топології мережі

Адаптація до типу трафіку

Маршрути оптимізуються відповідно до пріоритетутаважливості трафіку (наприклад,важливідані передаються найшвидшим маршрутом).

Адаптивні алгоритми маршрутизації

Адаптивні алгоритми на основі кластеризації Об'єднують вузли в кластери для зменшення кількості міжкластерних передач. Приклад LEACH, PEGASIS (Power-Efficient GAthering in Sensor Information Systems). Алгоритми машинного навчання Використовують історичні дані для прогнозування змін у мережі та вибору оптимальних маршрутів. Адаптивне навчання для оптимізації переадресації трафіку. Гібридні алгоритми Поєднання елементів централізованої та розподіленої маршрутизації для підвищення ефективності.

Переваги методів адаптивної маршрутизації:

- Гнучкість: здатність працювати при зміні параметрів мережі. Енергоефективність: продовження терміну служби вузлів і мереж;
- Підвищення надійності: адаптація до змін навколишнього середовища та відмов вузлів;

- оптимізація QoS: забезпечення необхідних характеристик передачі даних.[10]

Методи адаптивної маршрутизації в IoT є основою для створення ефективних, енергоефективних і надійних мереж, які можуть адаптуватися до динамічних умов роботи. Такі методи дозволяють значно підвищити продуктивність мереж IoT, знизити витрати і збільшити час безвідмовної роботи.

2.3 Протоколи управління трафіком в мережах IoT

Протоколи управління трафіком в мережах IoT - це набір правил і механізмів,які контролюють передачу даних в мережі, оптимізують використання ресурсів і гарантують якість обслуговування (QoS) для різних додатків Інтернету речей (IoT). Ці протоколи допомагають ефективно управляти обмеженими ресурсами (енергією, пропускною здатністю і обчислювальною потужністю) пристроїв IoT і підтримувати надійність зв'язку в високо динамічних мережах.

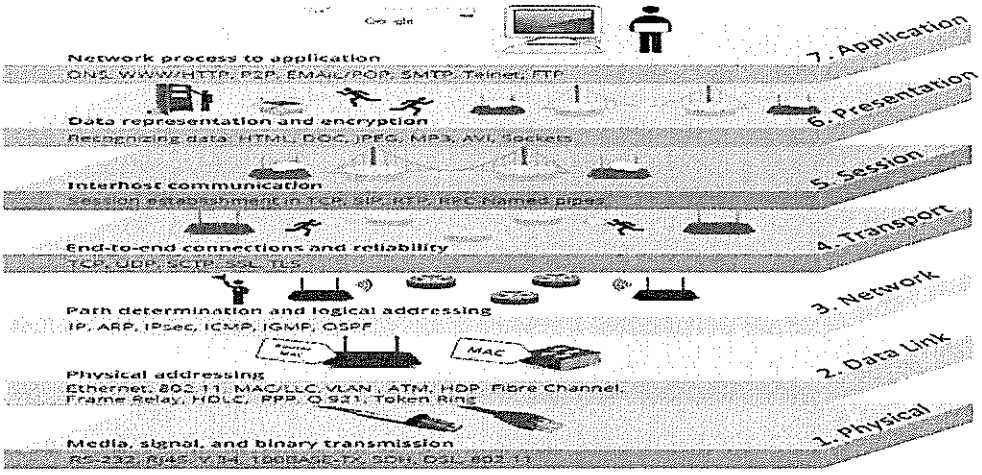


Рис. 2.4 Рівні мережі та стандарти

Характеристики управління трафіком в IoT

Неоднорідність пристроїв: Пристрої Інтернету речей мають різну пропускну здатність, енергетичні обмеження та типи з'єднання. Динамічна топологія: пристрої

можуть динамічно підключатися і відключатися. Різноманітність трафіку: масовий трафік датчиків: невеликі обсяги повідомлень, що періодично надсилаються. Критичний трафік: дані в режимі реального часу (наприклад, медичні програми).

Вимоги до якості обслуговування: низька затримка, мінімальна втрата пакетів, оптимальне використання ресурсів.

Цілі протоколів управління трафіком Гарантія QoS: стабільна пропускна здатність, збереження затримок і надійності. Мінімізація енергоспоживання: оптимізація передачі даних і продовження терміну служби пристрою. Зменшення перевантажень: уникнення вузьких місць у мережі, спричинених надмірним трафіком. Адаптація до мінливих умов: пристосування до динамічних змін топології та пропускної здатності.

Класифікація протоколів управління трафіком.

За мережевим рівнем:

Канальний рівень: протоколи, що контролюють доступ до середовища передачі (наприклад, CSMA/CA);

Мережевий рівень: протоколи, які визначають шлях передачі даних (наприклад, RPL).

За транспортним рівнем:

Протоколи, що керують потоком та підтвердженням передачі даних (наприклад,CoAP, MQTT).

За призначенням:

Протоколи для зменшення споживання енергії (наприклад, IEEE 802.15.4); протоколи для забезпечення QoS (наприклад,6LoWPAN,RPL).

Протоколи управління навантаженням (наприклад,протоколи балансування навантаження).

Загальні протоколи управління трафіком:

- IEEE 802.15.4: стандарт для низькошвидкісних бездротових персональних мереж (LR-WPAN). Як це працює: забезпечує енергоефективний обмін даними. Використовує механізми контролю доступу до медіа (CSMA/CA).

Застосування ZigBee, базового стандарту для потокових протоколів. Особливості Низьке енергоспоживання Підтримує швидкість до 250 кбіт/с;

- 6LoWPAN (IPv6 через малопотужні бездротові персональні мережі): Протокол для транспортування пакетів IPv6 в мережах з низькою пропускною здатністю. Принцип роботи: стискає заголовки IPv6 для зменшення обсягу даних. Підтримує фрагментацію та повторне збирання пакетів. Переваги Забезпечує прямий доступ до Інтернету для пристроїв IoT. Забезпечує масштабованістьісумісність з існуючими мережами;
- RPL (Routing Protocol for Low Power and Lossy Networks): протокол маршрутизації для мереж з низькою пропускною здатністю. Принцип роботи: створення спрямованого ациклічного графа (Directed Acyclic Graph, DAG) для маршрутизації. Метрики вибору маршруту: затримка, енергія, якість каналу. Застосування Підходить для великомасштабних сенсорних мереж і додатків IoT. Особливості Гнучкість та адаптивність до змін у мережі. Визначення протоколу обмеженого застосування (CoAP): Полегшений протокол для передачі даних між вузлами IoT. Як це працює: метод «запит-відповідь». Підтримуєпідтвердження доставкитаретрансляцію. Переваги Низька затримка. Ефективне управління енергоспоживанням;
- MQTT(MessageQueuing Telemetry Transport): Протокол обміну повідомленнями для пристроїв IoT. Як це працює: використовує модель «опублікувати-підписатись». Центральний брокер керує обміном повідомленнями. Переваги Простий у впровадженні. Підходить для пристроїв з низькою пропускною здатністю.

Сучасні тенденції

Інтеграція зі штучним інтелектом та машинним навчанням: машинне навчання для прогнозування трафіку та адаптивного управління. Децентралізовані методи: децентралізовані підходи, такі як блокчейн, для зменшення навантаження на централізовані вузли. [11]

Граничні обчислення: обробка даних на рівні пристроїв для зменшення обсягу переданого трафіку; в IoT протоколи управління трафіком є ключовим

елементом ефективної роботи мережі, забезпечуючи високу надійність, енергозбереження та адаптивність до різних сценаріїв використання IoT.

2.4 Оптимізація трафіку в мережах IoT

Оптимізація трафіку в мережах IoT (Internet of Things) є критично важливою для забезпечення ефективності роботи, мінімізації затримок, економії енергії та забезпечення стабільності. Нижче детально розглядаються основні аспекти, підходи та методи оптимізації.

Особливості мережі IoT Мережі IoT мають декілька ключових характеристик, які впливають на потребу оптимізації трафіку: Велика кількість пристроїв: датчики, камери, розумні побутові пристрої тощо. Обмежені ресурси: низька енергоємність, невелика обчислювальна потужність. Різнотипний трафік: дані можуть бути критичними до затримки (наприклад, у системах безпеки) або низькопріоритетними. Динамічність мережі: топологія мережі змінюється через переміщення пристроїв.

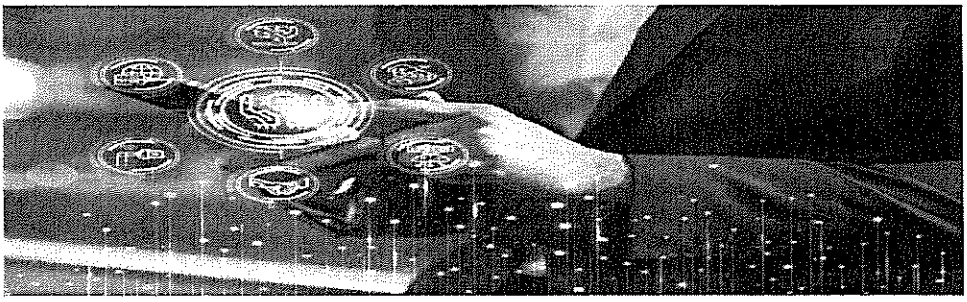


Рис. 2.5 Оптимізація трафіку

Протоколи маршрутизації. Енергозберігаючі протоколи LEACH (Low Energy Adaptive Clustering Hierarchy): кластеризує вузли для мінімізації передачі даних до центрального вузла. Кластеризація RPL (Routing Protocol for Low Power and Lossy Networks): створює ієрархічну структуру маршрутизації на основі показників енергоспоживання та затримок. Адаптивні протоколи Протоколи, які автоматично

обирають найкращий маршрут на основі навантаження на мережу, енергетичних ресурсів вузла та якості зв'язку. Зменшення обсягу переданих даних Агрегація даних: об'єднує схожі пакети в один пакет для зменшення частоти передачі. Фільтрація даних: усуває дублікати даних або відкидає нерелевантні дані. Стиснення даних Використовуйте методи стиснення, такі як RLE (Run-Length Encoding) та LZ (Lempel-Ziv) для зменшення розміру повідомлень.

Проблеми оптимізації

Безпека: зменшення затримок не повинно ставити під загрозу безпеку. вона не повинна бути порушена. Масштабованість: методи оптимізації повинні залишатися ефективними у великих мережах. Сумісність: пристрої різних виробників повинні взаємодіяти без складнощів.

Перспективи

Розвиток 5G/6G сприятиме скороченню затримок і підвищенню ефективності. Інтеграція технології блокчейн для забезпечення безпеки та оптимізації передачі даних. Впровадження цифрових двійників для моделювання мережі та оптимізації в режимі реального часу. [12]

Оптимізаціятрафіку в мережах IoTє багатогранним завданням і вимагає використання новітніх технологій та інноваційних підходів. Ефективна маршрутизація, зменшення обсягу даних, адаптивне управління та інтелектуальний аналіз можуть бути об'єднані для забезпечення стабільності мережі навіть у складних умовах.

3. УПРАВЛІННЯ НАВАНТАЖЕННЯМ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ

3.1 Забезпечення надійності в мережах IoT

Управління навантаженням в мережах Інтернету речей є важливим завданням для гарантування ефективності, стабільності та продуктивності мережі. Це завдання включає в себе різні аспекти, такі як балансування трафіку, уникнення заторів, ефективний розподіл ресурсів і підтримка якості обслуговування (QoS). Основні аспекти і методи управління навантаженням в мережах IoT підсумовані нижче.

Особливості управління навантаженням в мережах IoT

Особливості включають в себе: неоднорідність пристроїв: різні типи пристроїв мають різні вимоги до трафіку, енергоспоживання і продуктивності. Динамічна топологія: пристрої з'являються і зникають, умови мережі змінюються. Обмежені ресурси: вузли часто мають обмежені енергетичні, обчислювальні потужності та пам'ять.

Масштабованість: велика кількість пристроїв генерує великі обсяги трафіку, створюючи ризик перевантаження. Завдання управління навантаженням Балансування трафіку: рівномірний розподіл даних між пристроями, вузлами та серверами. Ефективне використання ресурсів: мінімізує споживання енергії та пропускної здатності.

Уникнення перевантажень: запобігає перевантаженню окремих вузлів і каналів зв'язку QoS: забезпечує стабільне з'єднання з мінімальною підтримкою критично важливих даних Методи управління навантаженням

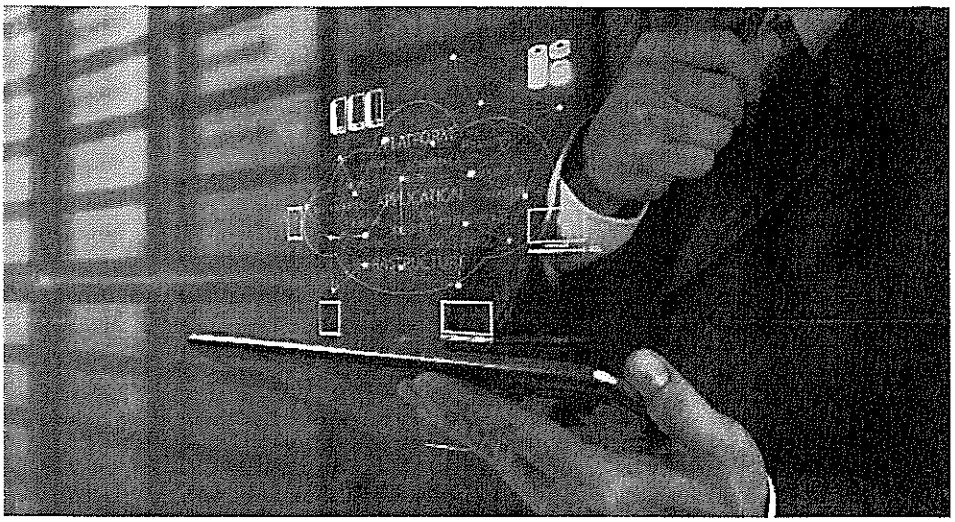


Рис. 2.6 Управління навантаженням

Балансування навантаження

Адаптивне балансування

Розподіляє трафік у реальному часі відповідно до поточного стану мережі. Для забезпечення рівномірного розподілу використовуються такі алгоритми, як round-robin, найменш зв'язний та динамічно зважений round-robin.

Розподілене балансування

Кожен вузол приймає рішення на основі локальної інформації, таким чином зменшуючи навантаження на центральний сервер. Такі протоколи, як RPL, використовують такі метрики, як підтримка та кількість переходів для оптимізації маршрутів.

Штучний інтелект і машинне навчання

Прогнозування навантаження на мережу на основі історичних даних. Оптимізація розподілу ресурсів за допомогою алгоритмів нейронних мереж або навчання з підкріпленням. Використання ресурсів частотного спектру Динамічне управління спектром Адаптивне використання доступних каналів залежно від навантаження. Когнітивні бездротові пристрої IoT аналізують частотний спектр і вибирають найменш перевантажені канали. Реалізація програмно-визначених мереж (SDN) Централізоване управління: Контролер SDN може динамічно вносити зміни в маршрут і політику на основі поточного стану мережі. Гнучкість: мережа може бути швидко переналаштована при зміні навантаження.

Проблеми управління навантаженням

Обмеження потужності: необхідно враховувати низьке енергоспоживання вузлів. Безпека: управління трафіком не повинно створювати вразливості в системі безпеки. Масштабованість: воно повинно ефективно працювати навіть у дуже великих мережах. Сумісність: IoT-пристрої від різних виробників повинні підтримувати загальні протоколи управління. Інструменти та методи управління навантаженням Моделі трафіку: використання симуляції для тестування нових підходів. Протоколи (MQTT, CoAP): оптимізовані для IoT для зменшення затримок. Механізми оптимізації: децентралізовані платформи, такі як туманні обчислення;

Очікування від 5G і 6G: забезпечення кращої пропускної здатності і зменшення затримок. Інтеграція з блокчейном: децентралізоване управління даними та підвищення надійності; специфічні для IoT протоколи: розробка нових методів маршрутизації та управління. [13]

Ефективне управління навантаженням - ключ до стабільної роботи мереж IoT. Це включає в себе цілий ряд методів від балансування трафіку до використання штучного інтелекту, периферійних обчислень і динамічної маршрутизації. У міру зростання розмірів мереж Інтернету речей ці підходи стануть ще більш важливими, і необхідно буде заохочувати розробку нових інноваційних рішень.

Забезпечення надійності в мережах IoT є важливим аспектом забезпечення стабільної, безпечної та ефективної роботи пристроїв, інфраструктури та додатків. Через специфічні характеристики мереж IoT, такі як масштаб, гетерогенність і обмеженість ресурсів,для забезпечення надійності потрібні спеціалізовані підходи і методи.

Визначення надійності в мережах IoT

Надійність в мережах IoT означає: Стабільність - здатність мережі продовжувати працювати. Доступність - безперервний доступ до сервісів і даних з пристроїв IoT. Безпека - захист даних і пристроїв від несанкціонованого доступу та атак. Цілісність - забезпечення точності та цілісності даних.

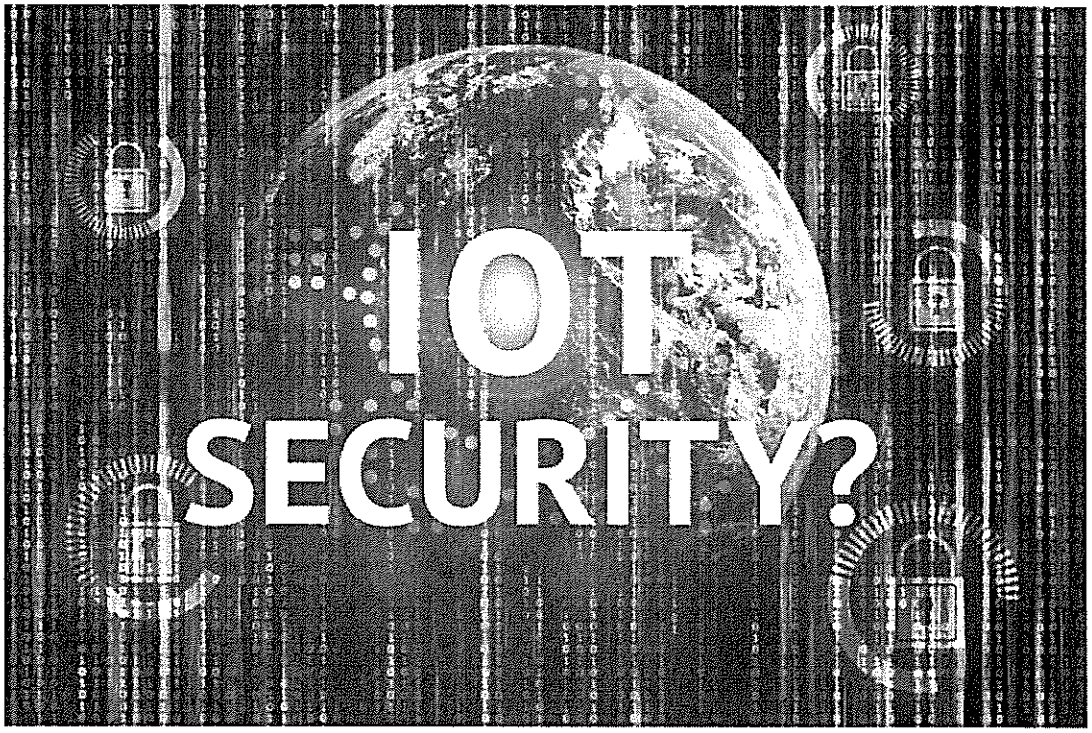


Рис. 3.1 Надійність мереж

Ключові аспекти надійності.

Фізична надійність – це надійність апаратного забезпечення пристроїв IoT (датчиків, шлюзів, контролерів). Захист пристроїв від впливу навколишнього середовища (вологість, температура, механічні пошкодження). Надійність передачі даних Гарантія доставки повідомлень без втрат, дублювання або значних затримок. Використання протоколів для перевірки та повторної передачі в разі втрати пакетів (наприклад, MQTT з QoS). Надійність програмного забезпечення Захист від багів та збоїв у прошивці. Усунення вразливостей безпеки за допомогою регулярних оновлень прошивки. Надійність інфраструктури Стійкість мережевої інфраструктури до збоїв вузлів, каналів зв'язку та серверів.

Резервне копіювання

Резервне копіювання: зберігання критично важливих даних на декількох пристроях або в хмарі. Резервний шлях: забезпечення альтернативного шляху передачі даних у разі виходу з ладу основного шляху передачі даних. Реплікація даних: зберігання копій даних на різних вузлах. Резервний вузол: використання додаткового пристрою для заміни вузла, що вийшов з ладу.

Контроль помилок

Протоколи передачі MQTT (Message Queuing Telemetry Transport): забезпечує різні рівні надійності (QoS 0, 1, 2); CoAP (Constrained Application Protocol): підтримує перевірку доставки даних; TCP/IP: для критично важливих додатків, що вимагають високої надійності; Управління мережею Протоколи динамічної маршрутизації, такі як RPL (Routing Protocol for Low Power and Lossy Networks) Протоколи динамічної маршрутизації адаптують маршрути для обходу несправних вузлів.

Автоматичне відновлення

Використовуйте механізми для автоматичної реконфігурації мережі після збою. Кластеризація Розподіліть пристрої в кластери з кластерними головами, які виконують функції обробки та передачі даних. У разі збою відбувається заміна головного вузла.

Безпечна автентифікація

Використання захищених протоколів обміну ключами (наприклад, DTLS). Шифрування Захист переданих даних за допомогою таких протоколів, як Advanced Encryption Standard (AES). Захист від атак Використання IDS/IPS (системи виявлення та запобігання вторгнень) для виявлення аномалій.

Моніторинг та діагностика

Моніторинг у реальному часі: виявлення виявлених несправностей до того, як вони стануть фатальними. Прогнозування відмов: аналіз даних для прогнозування відмов (предиктивне обслуговування). Використання технології штучного інтелекту Саморегулювання мережі: Штучний інтелект може автоматично модифікувати мережі у відповідь на зміни. Аналіз трафіку: аномалії потоку даних та оптимізація.

Проблеми надійності

Енергетичні обмеження: Низька ємність акумуляторів пристроїв IoT. Масштабованість: збільшення кількості пристроїв ускладнює управління. Гетерогенність: різноманітність пристроїв і протоколів ускладнює інтеграцію.

Інструменти надійності платформи IoT AWS IoT, Microsoft Azure IoT і Google Cloud IoT надають інструменти моніторингу та управління. Програмно-визначені

мережі (SDN): гнучке управління трафіком та відмовостійкість; Розвиток інтеграції Blockchain для забезпечення прозорості та безпеки. Розвиток технології 6G для підвищення надійності зв'язку. Впровадження цифрового двійника для моделювання та оптимізації мережі. [14]

Забезпечення надійності мереж Інтернету речей є складним завданням, яке охоплює всі аспекти роботи, від апаратного забезпечення до протоколів і програмного забезпечення. Резервування, кластеризація, безпека, динамічна маршрутизація і моніторинг можуть бути об'єднані для створення стабільних і безпечних систем IoT, які ефективно працюють навіть у складних умовах.

3.2 Якість обслуговування (QoS) в мережах IoT

Якість обслуговування (QoS) в мережах IoT – це набір технологій, протоколів і інструментів, які гарантують надійність, стабільність і ефективність пристроїв і додатків IoT навіть в умовах обмежених ресурсів і високих навантажень. QoS особливо важливий для промислової автоматизації, охорони здоров'я, розумних міст, транспорту та інших сценаріїв, де потрібна висока продуктивність.

Визначення QoS в IoT

- Під QoS в IoT мається на увазі забезпечення наступних характеристик мережі:
- Пропускна здатність: гарантується рівень пропускної здатності, необхідний длякритичноважливихзастосувань;
- Затримка: мінімізація затримки при передачі даних;
- Джиттер: стабільність часу доставки пакетів;
- Втрата пакетів: мінімізація втрати даних під час передачі.
- Пріоритезація: обробка трафіку відповідно до його важливості.

Проблеми забезпечення QoS в IoT - це гетерогенність (пристрої мають різні вимоги до QoS), обмеженість ресурсів (пристрої IoT мають обмежені ресурси енергії, пам'яті та обчислювальної потужності), висока масштабованість (необхідно

підтримувати мільйони пристроїв), динаміка трафіку (збільшення обсягу даних і зміна мережевих умов), надійність (здатність забезпечити QoS у разі збою).

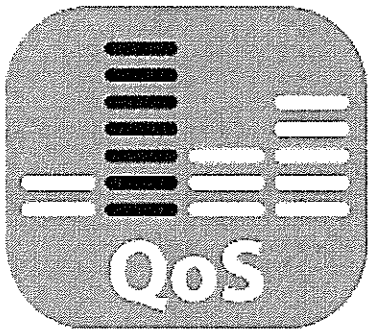


Рис. 3.2 Якість обслуговування в IoT

Як забезпечити QoS в IoT

Класифікуйте трафік відповідно до його важливості:

Критичний трафік: моніторинг здоров'я, управління енергією;

Некритичний трафік: передача даних про навколишнє середовище. Використовуйте мітки, такі як Differentiated Services Code Point (DSCP) для визначення класу обслуговування.

Пріоритезація трафіку

Пріоритетна обробка: критичні пакети обробляються швидше. Протокол IEEE 802.11e: забезпечує QoS для бездротових мереж Wi-Fi.6LoWPAN: Оптимізовано для малопотужних пристроївIoT. Планування черги

Алгоритми керування чергою не можуть забезпечити пріоритезацію або контроль для FIFO (First In First Out): Основний метод, який не враховує QoS; WFQ (Weighted Fair Queuing): розподіляє ресурси пропорційно вагам; RED (Random Early Detection): дозволяє уникнути перевантажень, відкидаючи пакети на ранній стадії; RED (Random Early Detection): дозволяє відкидати пакети на ранній стадії. Пріоритетна черга: визначає пріоритетність обробки високопріоритетних пакетів. Керування смугою пропускання Певна смуга пропускання обмежується або

виділяється для критично важливих додатків. За допомогою багатопротокольної комутації міток (MPLS): На основі QoS.

Управління затримками

Використовуйте спеціальні протоколи передачі: CoAP (Constrained Application Protocol): забезпечує мінімальні накладні витрати для малопотужних пристроїв; MQTT: підтримує рівні QoS (0,1,2) для встановлення гарантій доставки. Підтримка. Розподіл ресурсів Динамічний розподіл ресурсів у режимі реального часу для вузлів IoT. Алгоритми машинного навчання використовуються для прогнозування та оптимізації розподілу.

Маршрутизація з урахуванням QoS

Динамічна маршрутизація: маршрути змінюються відповідно до навантаження та умов мережі. Протоколи маршрутизації: RPL(RoutingProtocolfor Low Energy and Lossy Networks): оптимізує маршрути з урахуванням енергії та якості зв'язку; AODV (Ad hoc On-Demand Distance Vector): мінімізує затримки. Використання периферійних обчислень Обробка даних поблизу джерела для зменшення затримок і розвантаження централізованих серверів (периферійні обчислення). Технологія: fog computing: розподілені обчислення на межі мережі;

Моніторинг QoS

Системи моніторингу: оцінюють пропускну здатність, перехоплення і втрату пакетів. Платформи IoT (AWS IoT, Azure IoT): створення вбудованих інструментів моніторингу. Використання штучного інтелекту Прогнозування пікових навантажень та адаптація мережевих ресурсів. Алгоритми машинного навчання для оптимізації маршрутів і трафіку.

Інструменти і технології QoS

Протоколи QoS: MQTT, CoAP: підтримка різних рівнів надійності; IPv6: покращена адресація та підтримка IoT; IPv6: підтримка IoT та мереж з підтримкою IoT. Мережеві технології SDN (Software Defined Network): централізоване управління для динамічного забезпечення QoS. Хмарні сервіси: інструменти для моніторингу та обробки великих обсягів даних. Виклики QoS Інтероперабельність: інтеграція різних протоколів та платформ. Обмеження ресурсів: Вузли IoT часто

мають низьку потужність і пам'ять. Динамічність: часті зміни трафіку та умов роботи мережі.

Перспективи QoS Розвиток технологій 5G та 6G, які забезпечують високу пропускну здатність та низьку затримку. Інтеграція блокчейну для надійного і прозорого управління QoS. Автономні системи на основі ШІ для адаптивного управління ресурсами. [15]

Забезпечення QoS в мережах IoT є складним завданням, яке вимагає адаптивного управління ресурсами, пріоритизації трафіку, надійних протоколів і моніторингу технологій. Поєднання сучасних протоколів, периферійних обчислень і штучного інтелекту дозволяє забезпечити високу якість обслуговування в умовах зростаючих вимог до мереж IoT.

3.3 Резервування ресурсів і механізми відновлення в мережах IoT

Резервування ресурсів і механізми відновлення в мережах IoTє важливим аспектом забезпечення відмовостійкості, надійності та безперервності систем IoT. Методи резервування та ефективні механізми відновлення можуть гарантувати, що мережа продовжить працювати навіть при виході з ладу одного компонента.

Значення резервування та відновлення вIoT

Мережі IoT містять мільйони пристроїв, часто працюють в різних середовищах, ресурси яких обмежені. Механізми резервування та відновлення необхідні для Забезпечення безперервності обслуговування Пом'якшення впливу збоїв вузлів і мереж. Підвищення стійкості до атак і стихійних лих. Оптимізація продуктивності мережі.

Типи резервування

Апаратне резервування: використання додаткових пристроїв (запасних датчиків, шлюзів або вузлів) для заміни компонентів, що вийшли з ладу. Приклад: резервні шлюзи в розумних будинках для забезпечення безперервності даних. Резервування шляхів передачі: використання декількох шляхів або технологій для передачі даних (Wi-Fi, Zigbee, 4G/5G). Динамічне перемикання між мережами в

разі виходу з ладу основного каналу зв'язку. Резервне копіювання даних: зберігання копій даних у хмарних сховищах або на локальних серверах. Технології: Amazon S3, Google Cloud IoT. Резервування програмного забезпечення: використання резервних копій програмного забезпечення та прошивки для швидкого відновлення системи після збою.

Алгоритми та протоколи резервування

Кластеризація: вузли IoT організовані в кластери, кожен кластер має головний вузол, який може бути замінений у разі збою; Протокол маршрутизації для мереж з низьким енергоспоживанням і втратами (RPL): забезпечує резервний шлях для передачі даних; Резервування E2E: схема резервування «джерело-одержувач» для передачі даних; Резервування на основі хмарних та периферійних обчислень

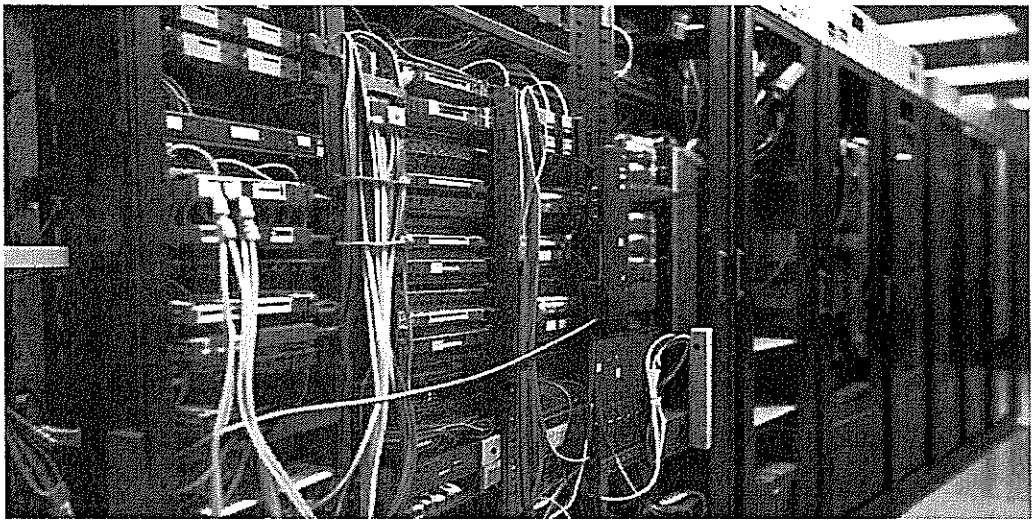


Рис. 3.3 Зберігання та відновлення даних в IoT

Хмарні обчислення: дані та процеси створюють резервні копії на хмарній платформі, такій, як AWS IoT або Azure IoT Hub. Захист даних гарантується у разі виходу з ладу локального вузла. Граничні та туманні обчислення: надлишкові обчислювальні ресурси розташовані близько до кінцевого пристрою. Це зменшує затримки передачі та підвищує надійність в режимі реального часу.

Механізми відновлення в IoT. Класифікація механізмів відновлення.

Превентивне відновлення: використовує системи моніторингу для прогнозування та запобігання шкідливим збоям. Алгоритми машинного навчання для аналізу стану вузла. Реактивне відновлення: автоматичне перемикання на резервні ресурси після виявлення збою.

Самовідновлення: системи, які автоматично переналаштовують маршрути, оновлюють прошивку та замінюють несправності.

Етапи відновлення

Виявлення несправностей: виявлення несправностей за допомогою датчиків та систем моніторингу. Технологія: система управління мережею (NMS). Діагностика: використання журналів та аналізу для визначення причини несправності.

Перехід на резервування: активація резервного обладнання, з'єднань або обчислювальних ресурсів. Відновлення первинних ресурсів: ремонт або заміна вузла, що вийшов з ладу.

Методи та способи відновлення

Маршрутизація обхідного шляху: FCR: увімкнення відновлення маршрутів при відмові вузла; Ad hoc On-Demand Distance Vector (AODV): під час зміни топології.

Відновлення маршрутів.

Динамічне балансування навантаження: розподіляє навантаження між вузлами, щоб уникнути перевантажень. Протокол: Алгоритм балансування навантаження IoT (LBIA). Планування передачі: протоколи, які враховують затримку, втрату пакетів і пріоритет: MQTT: рівні QoS гарантують передачу повідомлень; технологія Software Defined Networking (SDN): гнучке управління ресурсами для швидкого відновлення після збоїв;

Відновлення даних

Хмарне відновлення: автоматичне відновлення даних з резервних копій. Розподілене сховище: використовує блокчейн для зберігання та захисту даних. Інструменти резервного копіювання та відновлення для платформ IoT: AWS IoT, Microsoft Azure IoT та Google Cloud IoT пропонують вбудовані рішення для

резервного копіювання та відновлення. Програмно-визначені мережі (SDN): керуйте мережами для забезпечення відмовостійкості. Системи моніторингу: PRTG Network Monitor, Zabbix для моніторингу стану вузлів;

Виклики та обмеження Масштабованість: зі збільшенням кількості пристроїв стає складніше реалізувати резервування. Енергоефективність: резервування вимагає додаткових ресурсів. Вартість: впровадження резервних пристроїв є дорогим.

Перспективи розвитку Штучний інтелект: прогнозує збої та оптимізує ресурси. 6G мережа: підвищує відмовостійкість та надмірність зв'язку. Блокчейн: забезпечує децентралізоване та безпечне резервне копіювання даних. [16]

Резервування ресурсів та механізми відновлення в мережах IoT є ключовими елементами побудови відмовостійких та надійних систем. Різноманітні методи резервного копіювання, профілактики та пост-відновлення в поєднанні з новітніми технологіями, такими як периферійні обчислення та штучний інтелект, забезпечують високу якість обслуговування та безперервність роботи навіть уразі серйозних збоїв інавантажень.

3.4 Проблеми масштабованості в мережах IoT

Масштабованість мереж IoT (Інтернет речей) є однією з основних проблем, пов'язаних зі збільшенням кількості підключених пристроїв, оскільки IoT стає все більш поширеним в різних секторах (розумні міста, промисловість, охорона здоров'я, сільське господарство і т.д.), також зростають проблеми з продуктивністю, інфраструктурою та управлінням. В IoT масштабованість означає здатність мережі підтримувати зростаючу кількість пристроїв (вузлів) без істотного погіршення продуктивності. Забезпечити ефективну обробку, передачу та зберігання даних при збільшенні обсягів трафіку. Підтримувати функціональність і надійність навіть при динамічній зміні структури мережі.

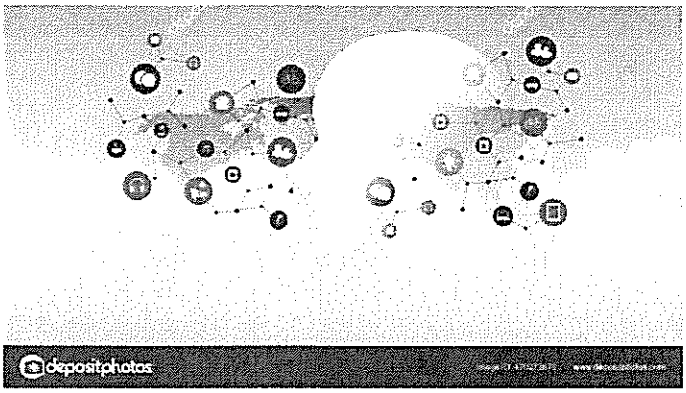


Рис. 3.4 Розповсюдженість IoT

Ключові проблеми масштабованості

Обмеження інфраструктури

Пропускна здатність мережі: особливо в бездротовому IoT, кількість пристроїв збільшується за рахунок перевантаження мережі; застарілі протоколи, такі як IPv4, мають унікальну обмежену кількість адрес. Обчислювальні ресурси: Обчислювальна потужність і пам'ять пристроїв IoT часто обмежені. Централізовані системи обробки даних (хмара) можуть стати вузьким місцем.

Енергетичні обмеження: багато пристроїв IoT працюють від батарей з обмеженим терміном служби, що ускладнює їх підтримку у великих мережах Проблеми передачі даних Збільшення обсягу трафіку: великі обсяги даних надсилаються з багатьох пристроїв, що призводить до перевантаження мережі. Підвищене навантаження призводить до збільшення затримок і втрати пакетів. Кілька протоколів: використання різних протоколів (MQTT, CoAP, Zigbee, LoRaWAN) ускладнює інтеграцію та уніфікацію передачі даних.

Управління та конфігурація

Моніторинг та управління великими мережами: моніторинг, діагностика та усунення несправностей ускладнюються зі збільшенням кількості пристроїв. Керування пристроями: пакетна конфігурація, оновлення програмного забезпечення (FOTA) та контроль доступу стають дедалі складнішими. Безпека: ризик атак (ботнетів, таких як Mirai) зростає зі збільшенням розміру мережі. Проблеми надійності Відмова пристрою: у великих мережах реакція одного вузла

може вплинути на стабільність системи. Балансування навантаження: можливість розподіляти трафік між пристроями та вузлами;

Підходи до вирішення проблем масштабованості

Використання сучасних протоколів IPv6: доступно більше адрес, що важливо для великих мереж IoT.

Протоколи з низьким енергоспоживанням:

- CoAP: оптимізований для невеликих обсягів даних;
- LoRaWAN;
- NB-IoT: передача даних на великі відстані з мінімальним енергоспоживанням.

Розподілені обчислення

Туманні обчислення: переміщення частини обчислень з хмари в мережу Переміщення до кінцевої точки. Зменшує затримки та обсяг даних, що передаються на централізовані сервери.

Граничні обчислення: одночасна обробка даних на пристрої або локальному шлюзі. Приклад: обробка відео з камери на пристрої замість того, щоб надсилати його в хмару.

Оптимізація передачі даних

Стиснення даних: зменшення обсягу переданих даних за допомогою алгоритмів стиснення.

Використання буферизації: дані тимчасово зберігаються на пристрої для зменшення пікових навантажень.

Пріоритезація трафіку: Пріоритизація трафіку відповідно до важливості для забезпечення QoS (якості обслуговування).

Автоматизація управління Платформи IoT для централізованого управління: AWS IoT, Azure IoT Hub та Google Cloud IoT дозволяють централізовано керувати пристроями.

Штучний інтелект (ШІ): використовується для моніторингу, прогнозування несправностей та оптимізації мережевих ресурсів.

Енергоефективність

Енергозберігаючі алгоритми: оптимізують роботу пристрою та подовжують термін служби батареї. Енергоефективні протоколи: BLE (Bluetooth Low Energy), Zigbee, LoRa. Використання SDN та NFV SDN (програмно-визначена мережа): гнучке управління трафіком та балансування навантаження. NFV (Network Function Virtualisation): віртуалізація мережевих функцій для швидкого реагування на зміни;

3.5 Адаптивні стратегії для розширення мереж Інтернету речей

Адаптивні стратегії є ключем до успішного розширення мереж Інтернету речей і дозволяють їм реагувати на мінливі умови та виклики, такі як збільшення кількості пристроїв, обсягів даних, вимог до обробки та безпеки.

Це підхід, якийпоєднує собігнучкість, автономність іоптимізацію,щоб забезпечити стабільну роботу мережі навіть під час швидкого розширення.

Адаптивні стратегії масштабування мереж IoT включають методи і прийоми, які дозволяють системі автоматично адаптуватися до мінливих умов: збільшення кількості вузлів і збільшення кількості датчиків.

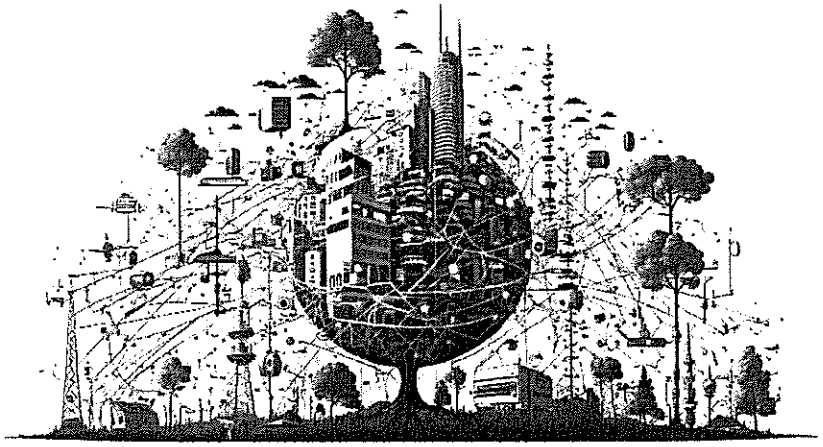


Рис. 3.5 Стратегії розвитку цифрових систем

Динамічний розподіл ресурсів являє собою зменшення затримок при передачі даних, підвищення стійкості до збоїв, автоматичне управління мережею.

Ключові аспекти стратегій адаптації

Розподілені обчислення

Туманні обчислення: перенесення частини обчислень з хмари на периферійні пристрої або локальні шлюзи. Це зменшує затримки та централізоване навантаження на сервер.

Граничні обчислення: обробка даних виконується на пристрої або поблизу нього. Особливо кориснодлячутливих до затримок додатків, таких як автономні транспортні засоби та розумні будинки.

Гібридні обчислення: поєднання хмарних, туманних і периферійних обчислень для оптимізації використання ресурсів.

Динамічне балансування навантаження

Адаптивне балансування трафіку: трафік перенаправляється в режимі реального часу за допомогою програмно-визначених мереж (SDN). Знижує ризик перевантаження окремих вузлів. Віртуалізація мережевих функцій (NFV): віртуалізація ресурсів дозволяє динамічно реконфігурувати мережу відповідно до потреб.

Кешування даних: часткове використання даних на локальних вузлах для зменшення необхідності передачі даних через центральний сервер.

Адаптивні мережеві протоколи

Протоколи з низьким енергоспоживанням: протоколи, такі як MQTT, CoAP і Zigbee, які автоматично збільшують частоту передачі даних залежно від навантаження на мережу. Протоколи, які автоматично збільшують частоту передачі даних в залежності від навантаження на мережу, наприклад, MQTT, CoAP, Zigbee та ін.

Динамічний вибір маршруту: протоколи, які адаптуються до умов мережі (наприклад, RPL, протоколи маршрутизації для мереж з низьким енергоспоживанням і втратами). Механізми пріоритизації трафіку: розподіл каналів для критичних і некритичних даних відповідно до їх важливості. Збільшення обчислювальних потужностей.

Хмарні обчислення: хмара надає додаткові обчислювальні ресурси при збільшенні трафіку. Використання моделей «Інфраструктура як послуга» (IaaS) та

«Платформа як послуга» (PaaS). Контейнери та оркестрування: швидке масштабування обчислювальних ресурсів завдяки використанню технологій контейнеризації (Docker, Kubernetes).

Автоматизація управління

Машинне навчання та штучний інтелект: для прогнозування навантаження, виявлення помилок та автоматичної оптимізації ресурсів. Автоматичне оновлення пристроїв: прошивка по повітрю (FOTA) забезпечує оновлення програмногозабезпеченнядлямільйонів пристроїв без втручання людини. Системи моніторингу в режимі реального часу: інструменти для виявлення перевантажень, збоїв і проблем безпеки.

Попередній розподіл ресурсів: резервування каналів і обчислювальних потужностей, щоб впоратися з піковими навантаженнями. Гнучкі SLA (Угоди про рівень обслуговування): умови обслуговування, що змінюються залежно від навантаження. Сегментація мережі Кластеризація вузлів: організація пристроїв Інтернету речей у кластери для зменшення перешкод і підвищення ефективності передачі даних. Гібридна архітектура: поєднання централізованого та розподіленого підходів для оптимізації розподілу навантаження.

4. ШТУЧНИЙ ІНТЕЛЕКТ (ШІ) ТА МАШИННЕ НАВЧАННЯ (МН) В МЕРЕЖАХ ІОТ

4.1 Автоматизація процесів управління в мережах IoT

Штучний інтелект (ШІ) та машинне навчання (МН) є невід'ємною частиною сучасного Інтернету речей (IoT). Він став невід'ємною частиною системи; разом з IoT, ШІ/МН сприяє створенню інтелектуальної екосистеми, яка може адаптуватися до змін і вирішувати складні проблеми в режимі реального часу.

Основні завдання AI/ML в IoT:

- Обробка великих обсягів даних: IoT генерує великі обсяги даних, AI/ML може допомогти проаналізувати ці дані для отримання цінної інформації;
- Прогнозування: алгоритми машинного навчання можуть передбачати майбутні події, такі як збої в роботі обладнання, зміни трафіку та потреби в ресурсах;
- Автоматизація: інтелектуальне управління пристроями, оптимізація процесів і мінімізація втручання людини;
- Адаптація: AI/ML може допомогти системам IoT адаптуватися до змін навколишнього середовища, наприклад, регулювати параметри мережі в залежності від навантаження. Підвищення безпеки: усунення кіберзагроз і ненормальної поведінки пристроїв.

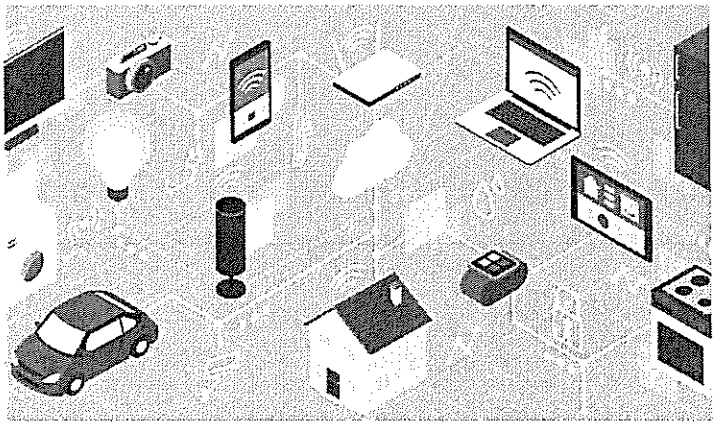


Рис. 4.1Можливості ШІ в IoT

Ключові методи AI/ML в IoT

Методи машинного навчання: використовуються для класифікації та прогнозування. Наприклад, виявлення несправностей в пристроях IoT. Неконтрольоване навчання: використовується для виявлення закономірностей у даних. Наприклад, для групування поведінки пристроїв. Навчання з підкріпленням: алгоритми навчаються, взаємодіючи з навколишнім середовищем. Використовується для оптимізації шляхів передачі даних.

Методи ШНМ

Нейронні мережі: використовуються для складного аналізу даних, таких як розпізнавання зображень і обробка мовлення. Глибоке навчання: використовує багатошарові нейронні мережі для аналізу великих обсягів даних. Використовується для обробки відеопотоків та аналізу датчиків Інтернету речей. Обчислювальний інтелект: алгоритми, такі як генетичні алгоритми і ройовий інтелект для вирішення складних завдань оптимізації.

Застосування ШІ/ММ в різних аспектах IoT

Обробка потокових даних: ШІ/ММ повинен обробляти дані в режимі реального часу (наприклад, від датчиків).

Предиктивна аналітика: Алгоритми машинного навчання допомагають прогнозувати поведінку пристроїв, наприклад, споживання енергії

Управління мережею

Оптимізація трафіку: Штучний інтелект збалансовує навантаження на мережу та уникає заторів.

Автоматизоване керування: інтелектуальне налаштування параметрів мережі відповідно до змін уреальному часі.

Підтримка якості обслуговування (QoS)

Пріоритезація трафіку: розподіляє мережеві ресурси між критично важливими додатками.

Зменшення затримок: інтелектуальна оцінка затримок і перенаправлення трафіку. Виявлення загроз безпеці: використання AI/ML для виявлення аномалій у поведінці пристроїв і запобігання атакам.

Шифрування даних: використання адаптивних алгоритмів шифрування на основі ризиків. Розумні пристрої Розумний дім: автоматизація систем енергоменеджменту, освітлення та безпеки. Промисловий IoT (IIoT): оптимізація виробничих процесів, скорочення простоїв за допомогою предиктивної діагностики.

Застосування AI/ML в конкретних сценаріях IoT

Розумні міста Транспорт: аналіз даних з датчиків для оптимізації дорожнього руху та зменшення заторів. Енергетика: прогнозування споживання енергії та оптимізація розподілу ресурсів. Охорона здоров'я Віддалений моніторинг безпеки: аналіз даних з медичних пристроїв в режимі реального часу. Прогнозування: прогнозує спалахи захворювань на основі історичних даних. Сільське господарство Моніторинг причин: AI/ML аналізує дані з датчиків для оптимізації росту. Прогнозування погоди: прогностичні моделі застосовуються для підвищення врожайності.

Переваги використання AI/ML в IoT Ефективність: зниження витрат на обслуговування та оптимізація використання ресурсів. Швидкість прийняття рішень: реагування на події в режимі реального часу Масштабованість: здатність підтримувати велику кількість пристроїв. Безпека Своєчасне виявлення загроз і кібератак.

Проблеми впровадження AI/ML в IoT Обмеженість ресурсів: деякі пристрої IoT мають низьку обчислювальну потужність. Затримка: складні алгоритми AI/ML потребують часу для виконання. Безпека даних: передача та зберігання даних повинні бути безпечними. Вартість: Технологія AI/ML є дорогою у впровадженні.

Перспективи розвитку AI/ML в IoT Інтеграція з 5G: використання високошвидкісних мереж для оптимізації даних. Децентралізація: роль периферійних обчислень, коли дані обробляються на периферії, зростатиме. Автономні системи: повністю автоматизовані рішення IoT без втручання людини. Нові алгоритми: розробка більш енергоефективних і швидких моделей AI/ML.

Інтеграція AI і машинного навчання в мережі IoT є етапом розвитку технології. Це дозволить створити інтелектуальні екосистеми, які не тільки

підвищать ефективність і знизять витрати, але й відкриють нові горизонти автоматизації, безпеки та адаптивності систем. Можливо, у відповідь на виклики, роль AI/ML в IoT продовжує розширюватися, і ці технології стають основою для створення розумних рішень у багатьох секторах, включаючи міський, медичний, сільськогосподарський і промисловий. Інші розробки в області AI/ML в мережах IoT включають вдосконалені алгоритми, розвиток апаратної підтримки і збільшення обчислювальної потужності пристроїв будуть супроводжувати його.

Автоматизація процесів управління в мережах IoT є ключовим елементом для ефективної роботи Інтернету речей. Технологія дозволяє централізовано або децентралізовано керувати великою кількістю пристроїв і виконувати складні операції з мінімальним втручанням людини.

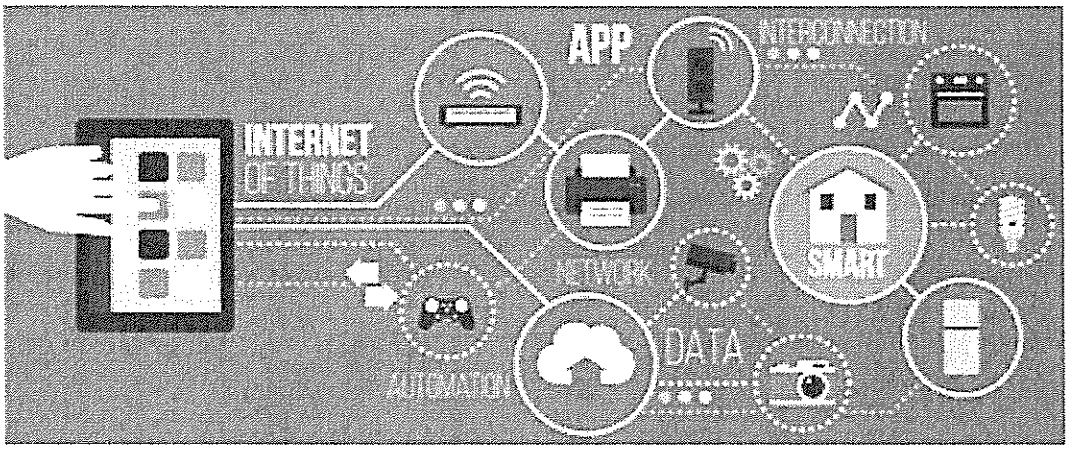


Рис. 4.2 Управління в мережах Інтернету речей

Основні цілі автоматизації процесів управління в IoT

Підвищення ефективності: мінімізація ресурсів і скорочення часу, що витрачається на обробку даних, виконання завдань і управління пристроями. Масштабованість: автоматизація дозволяє ефективно управляти мережами з тисячами або мільйонами IoT-пристроїв. Безперервність бізнесу: автоматизоване виявлення та відновлення несправностей. Оптимізація використання ресурсів: автоматизовані процеси покращують розподіл мережевих ресурсів, таких як енергія, пропускна здатність і обчислювальна потужність. Забезпечення безпеки Автоматичне виявлення загроз та їх відключення в режимі реального часу.

Ключові аспекти автоматизації процесів управління

Безперервний моніторинг: система автоматично збирає дані з усіх IoT-пристроїв. Виявлення аномалій: система автоматично виявляє аномалії в роботі пристроїв за допомогою алгоритмів штучного інтелекту.

Дистанційна діагностика: система автоматичного аналізу даних для визначення причини збоїв.

Управління конфігурацією

Автоматична конфігурація: Пристрої IoT підтримують свої налаштування відповідно до своєї ролі в мережі. Динамічна адаптація: конфігурації пристроїв змінюються в режимі реального часу у відповідь на зміни в навколишньому середовищі та робочому навантаженні.

Управління трафіком

Балансування навантаження: трафік розподіляється між великою кількістю вузлів, щоб уникнути заторів.

Пріоритезація трафіку: автоматично визначає критичні додатки та забезпечує якість обслуговування (QoS).

Енергозбереження

Моніторинг енергоспоживання: автоматичний контроль енергоспоживання кожного пристрою. Режим енергозбереження: автоматичний перехід у сплячий режим, коли пристрій неактивний. Виявлення загроз безпеці: автоматична система аналізує дані на предмет атак, таких як DDoS і несанкціонований доступ. Оновлення безпеки: виправлення та оновлення автоматично встановлюються для підтримки безпеки пристрою.

Технології, що використовуються для автоматизації

Штучний інтелект (ШІ) та машинне навчання (ML) ШІ для моніторингу: аналізує дані та прогнозує збої. ML для адаптації: алгоритми дозволяють системам вчитися на історичних даних і адаптувати свою поведінку Програмно-визначені мережі (SDN) Централізоване управління: керування всією мережею з одного контролера. Гнучка маршрутизація: автоматично перенаправляє трафік на основі поточного стану мережі.

Граничний IoT

Локальні обчислення: використовує IoT для обробки даних і зменшення затримок. Адаптація в режимі реального часу: швидко реагує на локальні зміни. Хмарні обчислення Централізоване зберігання даних: автоматизовані процеси хмарної агрегації для аналізу та зберігання великих обсягів даних. Розподілені системи: використання хмари для синхронізації та управління глобальними мережами IoT.

Використання автоматизації в різних галузях IoT

Промисловий IoT (IIoT) Моніторинг обладнання: системи автоматизації відстежують стан машин і прогнозують збої. Оптимізація процесів: автоматизація покращує виробничі лінії та мінімізує втрати

Розумні міста

Управління дорожнім рухом: автоматичні світлофори зменшують затори Енергетичні системи: автоматичне управління освітленням будівель та енергоспоживанням.

Охорона здоров'я

Дистанційний моніторинг безпеки: пристрої Інтернету речей автоматично збирають і передають дані лікарям. Управління обладнанням: автоматизація обслуговування медичного обладнання.

Сільськогосподарські зрошувальні системи: автоматичне регулювання поля на основі даних датчиків Моніторинг врожаю: аналіз даних для визначення оптимального часу збору врожаю;

Проблеми автоматизації в IoT

Сумісність пристроїв: різні протоколи та стандарти уможливлюють автоматизацію;

Проблеми автоматизації в IoT

Затримки в обробці даних: великі обсяги інформації спричиняють затримки.

Безпека: автоматизовані системи вразливі до кібератак;

Вартість використання: потенційні інвестиції в розробку та впровадження автоматизованих систем;

Інтеграція ШІ та машинного навчання: додаткова розробка алгоритмів для глибшого аналізу даних; Розвиток стандартів: уніфікація протоколів для спрощення впровадження автоматизації;

Розширення ролі периферійних обчислень: використання периферійних обчислень для більш ефективного управління;

5G IoT: поява мереж 5G значно збільшить можливості автоматизації. [18]

Автоматизація процесів управління в мережах IoT - важливий крок для повного використання потенціалу Інтернету речей. Це важливий крок для повного використання потенціалу Інтернету речей. Автоматизація робить системи IoT більш ефективними, адаптивними і безпечними. Впровадження автоматизованих процесів для подолання викликів значно спрощує управління складними мережами, знижує витрати і створює нові можливості для інновацій в різних галузях.

4.2 Прогнозування навантаження в мережах IoT

Прогнозування навантаження в мережах IoT є важливим завданням для забезпечення ефективної роботи таких систем. Враховуючи постійне зростання кількості пристроїв Інтернету речей та обсягів даних, які вони генерують, правильне прогнозування навантаження допомагає оптимізувати використання ресурсів, забезпечити якість обслуговування (QoS)тауникнути перевантаження мережі.

Основні цілі прогнозування навантаження

Оптимізація ресурсів: передбачення періодів пікового навантаження шляхом проактивного попереднього розподілу ресурсів. Підтримка якості обслуговування (QoS): забезпечення стабільності мережевих послуг навіть у періоди високого навантаження. Запобігання перевантажень: зменшіть ризик втрати даних або відключення системи через перевищення доступних ресурсів. Енергозбереження: Вимикайте неактивні пристрої або зменшуйте обчислювальне навантаженнявперіодинизької активності. Планування масштабування:

проактивне розширення мережевої інфраструктури, коли очікується збільшення трафіку.

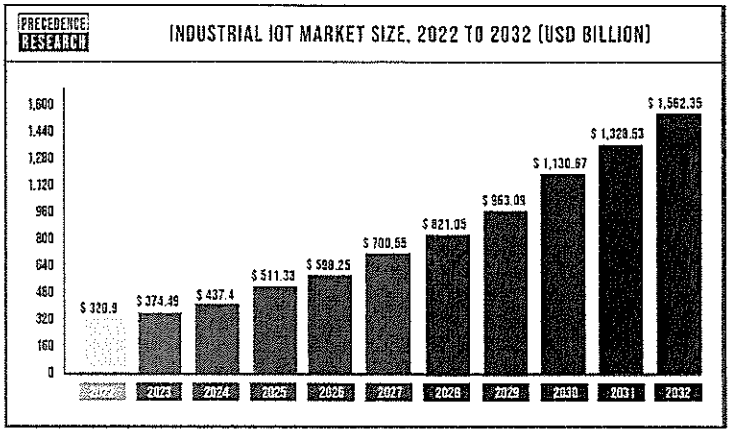


Рис. 4.3Тенденція до збільшення використання IoT

Фактори, що впливають на навантаження на мережу IoT

Тип пристрою: різні пристрої IoT (датчики, камери, медичні прилади) генерують різні обсяги даних. Частота обміну даними: датчики можуть передавати дані безперервно або через певні проміжки часу. Географічне розташування: концентрація пристроїв на певній території може спричинити локальні затори. Моделі поведінки користувачів: використання пристроїв може змінюватися залежно від часу доби, сезону або події. Методи прогнозування навантаження.

Методи прогнозування навантаження

Математичні методи

Статистичний аналіз: використання історичних даних для визначення середніх значень, тенденцій та сезонності.

Аналіз часових рядів: Такі методи, як авторегресійне інтегроване ковзне середнє (ARIMA), можуть прогнозувати навантаження на основі історичних даних.

Аналіз Фур'є: аналіз частотної складової періодичних змін.

Методи машинного навчання (ML)

Лінійна регресія: моделі, які прогнозують взаємозв'язки між змінними (наприклад, час та інтенсивність руху).

Дерево рішень та ансамблеві методи: алгоритми, такі як випадкові ліси та градієнтне підсилення, забезпечують високоточні прогнози.

Глибокі нейронні мережі (глибоке навчання): використовуйте рекурентні нейронні мережі (RNN) або довгу короткочасну пам'ять (LSTM) для аналізу часових рядів.

Кластеризація: наприклад, методи K-середніх для групування пристроїв зі схожими навантаженнями. Навчання з підкріпленням: алгоритми взаємодіють з навколишнім середовищем для адаптації до змін у поведінці мережі.

Методи штучного інтелекту (ШІ)

Експертні системи: використовують правила і логічні схеми для прогнозування піків трафіку у поєднанні з аналітикою Інтернету речей, що автоматично аналізують потоки даних і навантаження.

Інтеграція ШІ для прогнозування. Гібридні підходи – це поєднання статистичних методів і машинного навчання: наприклад, використання ARIMA для аналізу тенденцій і нейронних мереж для прогнозування відхилень. Використання периферійних і хмарних обчислень: обробка даних ближче до пристрою і одночасний аналіз у хмарі для довгострокового прогнозування;

Інструменти прогнозування навантаження

Платформи аналітики Інтернету речей: наприклад, AWS IoT Analytics, Azure IoT Hub, Google Cloud IoT Core та ін. Бібліотеки машинного навчання: наприклад, TensorFlow, PyTorch, Scikit-learn; системи візуалізації даних: наприклад, Tableau, Power BI для аналізу і моніторингу прогнозів; програмно-визначені мережі (SDN): використовуються для динамічного управління трафіком і оптимізації мережі.

Промисловий IoT (IIoT)

Планування технічного обслуговування: простоїв обладнання можна уникнути, передбачаючи перевантаження. Оптимізація виробничих процесів: окремі параметри системи попередньо встановлюються відповідно до очікуваного навантаження

Розумні міста

Управління транспортом: оптимізація роботи світлофорів шляхом прогнозування заторів Енергетика: визначення часу пікового споживання енергії.

Охорона здоров'я

Моніторинг охорони здоров'я: прогнозування збільшення навантаження на обладнання Інтернету речей у лікарнях. Планування використання ресурсів охорони здоров'я: оцінка потреб в обладнанні та персоналі.

Сільське господарство

Іригаційні системи: оцінка споживання води на основі кліматичних умов. Аналіз пропускної здатності: оцінка навантаження на датчики Інтернету речей під час збору даних.

Проблеми прогнозування навантаження

Неточні дані: відсутність або неправильні дані ускладнюють точні прогнози.

Динамічність мережі: Постійно мінлива природа систем IoT ускладнює прогнозування. Обмеженість ресурсів: Пристрої IoT часто мають обмежену обчислювальну потужність.

Кіберзагрози: можливі атаки на системи прогнозування, які можуть вплинути на їхню точність. Складність інтеграції: можливість координувати алгоритми прогнозування з іншими компонентами IoT.

Прогнозування навантаження в мережах IoT - інструмент для забезпечення їх стабільної роботи. Завдяки сучасним технологіям, таким як машинне навчання, штучний інтелект і математичне моделювання, можна точно передбачити майбутні потреби в ресурсах і вчасно адаптувати системи. Однак для того, щоб такі рішення були успішними, необхідно вирішити низку проблем, таких як динамічність мереж Інтернету речей, обмеженість ресурсів і необхідність інтеграції з іншими компонентами системи.

Подальший розвиток прогнозування навантаження надасть мережам IoT нові можливості, такі як підвищення ефективності, енергозбереження, масштабованість і здатність адаптуватися до змін в режимі реального часу. Тому прогнозування навантаження є важливим напрямком для досліджень і розробок IoT.

4.3 Виявлення аномалій та реагування на загрози в мережах IoT

Інтернет речей (IoT) є ключовим компонентом сучасних технологій, що об'єднує мільярди пристроїв у глобальну мережу. Однак розподілена природа IoT, обмеженість ресурсів пристроїв та їхня висока вразливість створюють серйозні виклики для кібербезпеки. Виявлення аномалій та реагування на загрози є ключовими завданнями для забезпечення стабільності та захисту мереж IoT.



Рис. 4.4 Кіберзлочинність та можливості протидії

Основні типи аномалій

Мережеві аномалії: аномальний трафік, наприклад, пікселі даних або великі затримки. Аномалії в поведінці пристроїв: зміна частоти обміну даними, передача даних у неробочий час.

Аномальний доступ: несподівані спроби підключення або невідомі пристрої.

Аномалії в даних: раптові стрибки або падіння значень, що генеруються датчиками, або нелогічні дані.

Основні DDoS-загрози: Масові завантаження, спрямовані на виведення з ладу пристроїв і серверів IoT.

Шкідливе програмне забезпечення та ботнети: Використання пристроїв IoT як частини шкідливих мереж, таких як ботнет Mirai.

Перехоплення даних: атаки типу «людина посередині» (MitM), які перехоплюють конфіденційну інформацію. Атаки на прошивку: Використання вразливостей у програмному забезпеченні пристроїв IoT. Фізичні атаки: несанкціонований доступ до пристроїв через апаратне забезпечення.

Методи виявлення аномалій в мережах IoT

Традиційні методи Порогові методи: встановлення порогових значень для параметрів трафіку, таких як швидкість передачі даних та рівень енергії.

Технології реагування на загрози

Автоматизація реагування

Системи виявлення вторгнень (IDS): Snort, Suricata для моніторингу трафіку.

Системи запобігання вторгненням (IPS): інтегровані рішення для блокування виявлених загроз; SIEM-системи (SIEM): інтегровані рішення для блокування виявлених загроз.

SIEM-системи (Security Information and Event Management): збір та аналіз подій безпеки в режимі реального часу. Реагування на основі машинного навчання Системи автоматичного блокування: використовують машинне навчання для створення правил автоматичного блокування. Машинне навчання для створення правил автоматичного блокування. Динамічні політики оновлення: безперервне навчання моделей і реагування на нові загрози. [19]

Проблеми виявлення аномалій в мережахIoT

Обмежені ресурси пристроїв: недостатня обчислювальна потужність для запуску складних алгоритмів. Великі обсяги даних: IoT генерує величезні обсяги даних, що ускладнює їх аналіз в реальному часі. Різноманітність пристроїв: безліч моделей і протоколів дозволяють реалізовувати різноманітні рішення. Затримка і захоплення: реакція на загрозу повинна бути миттєвою, але це складно у великих мережах;

4.4 Приклади успішного впровадження IoT

Успішні рішення IoT

Розвиток технології Інтернету речей (IoT) уможливив низку інноваційних рішень, які трансформують інші сектори – від виробництва до охорони здоров'я. Успішні проекти демонструють, як IoT може підвищити продуктивність, оптимізувати витрати та створити нові можливості для бізнесу та суспільства.

Промисловість (Industrial IoT - IIoT)

Платформа Predix IoT від General Electric (GE) - це промислова платформа IoT. Обладнання, що використовується для моніторингу та оптимізації продуктивності. Збір даних в режимі реального часу за допомогою датчиків. Застосування аналітики великих даних та машинного навчання. Як наслідок підвищення ефективності обладнання на 20%, зниження витрат на технічне обслуговування.

Хмарна IoT-платформа MindSphere від Siemens використовується для підключення та аналізу промислових даних. Застосовується для моніторингу виробничих процесів, оптимізації енергоспоживання. В результаті до 15% скорочення витрат на електроенергію, скорочення простоїв виробництва на 10-15%.

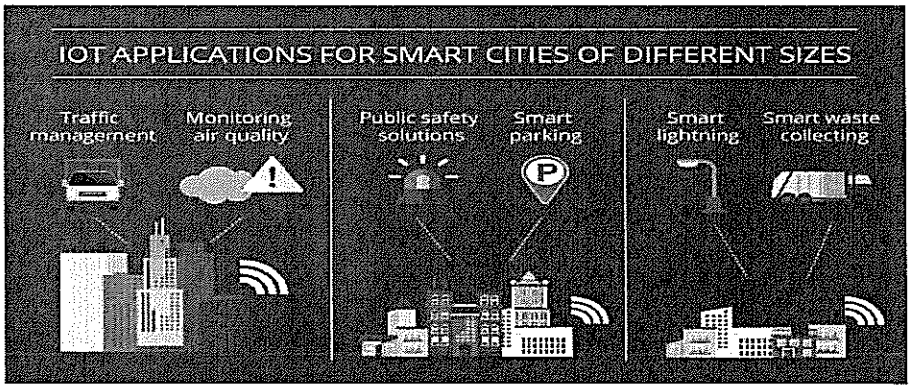


Рис. 4.5 Використання Інтернету речей в різних сферах

Компанія John Deere використовує функції розумного сільського господарства такі як: датчики для моніторингу продуктивності, вологості та

температурного режиму, автоматизація сільськогосподарської техніки. Як наслідок збільшення врожайності на 20-25%, економія води та добрив до 30%.

Розумні міста

Барселона (Іспанія) - один з піонерів у застосуванні IoT для створення розумних міст:

- Розумне освітлення, яке автоматично підлаштовується до часу прибуття

та від'їзду;

- Управління паркуванням за допомогою датчиків, які повідомляють про порожні місця;
- Система моніторингу якості повітря та води в результаті

30-відсоткове скорочення споживання енергії;

- Покращення якості повітря на 20%.

Сінгапур - один з найпрогресивніших прикладів розумних міст:

- Рішення IoT-системи для управління дорожнім рухом:

адаптивні світлофори та моніторинг заторів, в результаті 15% зменшення заторів на дорогах;

- Розумні сміттєві баки з датчиками, в результаті збільшення ефективності збору відходів на 20%;
- Додатки для охорони здоров'я, що аналізують дані з натільних пристроїв.

Приклади використання IoT в Україні на державному рівні

Український бізнес і державні організації вже активно користуються перевагами технології Інтернету речей.

Ось кілька прикладів з впровадження IoT: Вже після початку війни Рівненський водоканал запустив разом з Київстар проєкт на базі технології NB-IoT, який дозволив вести автоматизований збір, облік і обробку даних з лічильників води в багатоквартирних будинках Квасилова. Таких технологій як «Розумний облік» по всій Україні має ставати все більше, адже «розумні» технології

допомагають заощаджувати, швидко реагувати на аварії, не допускаючи великих втрат ресурсів, а також завжди мати точний облік в режимі реального часу.

У вересні 2023 Київстар запустив сигнал точного позиціонування RTK. Ця технологія має великий потенціал для сільського господарства, геодезії, будівництва, логістики - де є потреба отримувати точні дані про місцеположення обладнання, а також потенційно для проєктів, направлених на гуманітарне розмінування території». Вже кілька років київська влада реалізує проєкт із будівництва міської опорної мережі та інфраструктури для впровадження Інтернету речей. У майбутньому це дозволить моніторити стан довкілля, контролювати мікроклімат у школах чи лікарнях та підвищити ефективність роботи комунальних служб.

«Розумні міста» в Україні: як технологія допоможе у відбудові

IoT може стати корисним інструментом для підтримки громадського середовища — технологія може посісти важливе місце у відновленні країни після перемоги. Інтернет речей знадобиться для автоматизації та підвищення безпеки під час відбудови зруйнованих міст чи створення їхньої нової інфраструктури. Для реалізації технології є всі передумови: так, скажімо, один з постачальників IoT-рішень, якими зараз є мобільні оператори в Україні, компанія Київстар, має велику експертизу щодо впровадження таких рішень.

Зокрема, IoT для відбудови дозволяє модернізувати комунальні та транспортні системи, створюючи розумне місто — Smart City. «Розумні» лічильники, які самі передають дані для обліку, сміттєві контейнери з датчиками наповнення, GPS-трекери для муніципального транспорту, освітлення та відеоспостереження, які реагують на рух, — все це допоможе місцевій владі та комунальним компаніям робити міста більш комфортними сучасними та безпечними для українців.

Охорона здоров'я

Розумні пристрої для діабету від Medtronic такі як: інсулінова помпа, підключена до датчика глюкози, автоматична доставка інсуліну на основі значень глюкози та моніторинг через мобільний додаток для покращення якості життя.

HealthSuite від Philips – це хмарна платформа для збору та аналізу даних про стан здоров'я. Використовується для домашнього моніторингу здоров'я, виявлення відхилень у стані здоров'я за допомогою штучного інтелекту: зменшення кількості госпіталізацій на 20% і як наслідок зниження витрат на охорону здоров'я.

Fitbit та Apple Health: пристрої для моніторингу здоров'я, що носяться з собою. Продукти компанії можуть відстежувати пульс, фізичну активність та сон, надавати персоналізовані рекомендації. В результаті підвищується обізнаність людей про своє здоров'я, покращується профілактика захворювань.

Енергетика

Розумні нафтові свердловини від BP: використовують датчики Інтернету речей для моніторингу нафтових і газових свердловин. Вони мають змогу здійснювати: аналіз тиску, температури та потоку газу, прогнозувати події за допомогою штучного інтелекту. Внаслідок використання нових технологій зниження операційних витрат на 10-15% та покращена безпека працівників.

Розумні лічильники від компанії Enel

Завдяки використанню електролічильників від компанії Enel користувачі отримали зниження споживання енергії на 8% та підвищення точності лічильників споживання.

Транспорт і логістика

IoT в логістиці Amazon: використання Інтернету речей для управління складськими запасами і доставкою. Використання IoT в роботах на складі для автоматизації комплектації замовлень та відстеженні посилок в режимі реального часу дало змогу скоротити час обробки замовлень та підвищити точність доставки.

Оріон від ДБЖ. Це система Інтернету речей для оптимізації маршрутів доставки. В результаті використання системи: заощаджено 10 млн галонів палива на рік, час доставки скоротився на 8%.

Сільське господарство

Монсанто застосовує моніторинг місцезнаходження за допомогою Інтернету речей: датчики аналізують стан ґрунту, потреби у волозі та добривах. Завдяки

цьому вдалося досягти наступних результатів: збільшення врожайності на 20% та 30%-ої економії ресурсів, особливо води.

Роздрібна торгівля

«Розумна» політика від Wal-Mart: спрацьовують датчики на полицях, коли товари закінчуються. Завдяки їх використанню на 30% скоротилося використання товару та збільшились продажі.

Amazon Go використовує магазини без касирів з IoT-камерами та датчиками для автоматизованого оформлення замовлення. Завдяки цьому в магазинах зменшились черги.

Успішні приклади рішень Інтернету речей демонструють, як ці технології сприяють підвищенню ефективності, інноваціям та економії в галузі. Ці приклади демонструють потенціал Інтернету речей для вирішення складних проблем і підвищення якості життя, а також стимулюють розвиток нових бізнес-моделей і ринків.

Інтернет речей(IoT) стрімко трансформує сучасний світ, дозволяючи пристроям взаємодіяти один з одним і користувачами, автоматизуючи процеси і підвищуючи ефективність. Але з розвитком IoT мережі стикаються з низкою проблем, які потребують вирішення.

4.5 Підходи до безпеки та захисту даних в мережах Інтернету речей

Захист даних та безпека в мережах Інтернету речей є значним викликом через збільшення кількості пристроїв, їх неоднорідність та взаємодію з конфіденційною інформацією. Вразливі пристрої Інтернету речей можуть бути використані для атак, які ставлятьпід загрозу конфіденційність, цілісністьі доступність даних.

Основними загрозами є:

- Кібератаки: злом пристроїв, шкідливе програмне забезпечення і атаки на відмову в обслуговуванні (DoS);
- Порушення конфіденційності: перехоплення даних і несанкціонований доступ. Фізичні атаки: крадіжка або маніпуляції з пристроями;

- Масштабованість: Зі збільшенням кількості IoT-пристроїв збільшується і поверхня атаки;
- Низька обчислювальна потужність пристрою: обмежує застосування традиційних заходів безпеки.

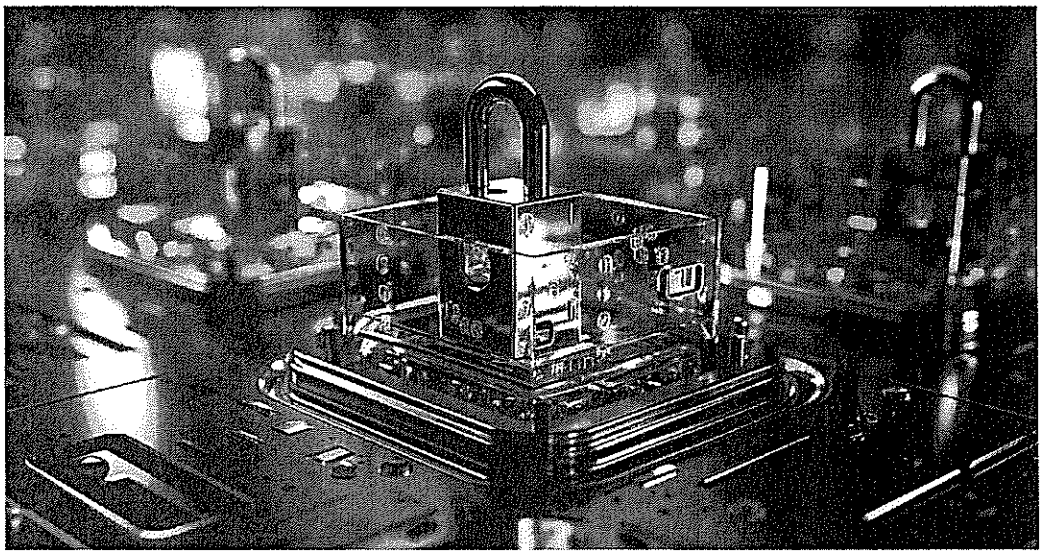


Рис. 4.6 Забезпечення безпеки в IoT

Основні принципи безпеки:

- Конфіденційність: гарантує, що тільки авторизовані користувачі
- або пристрої можуть отримати доступ до даних;
- Цілісність: захищає дані від несанкціонованої модифікації;
- Доступність: забезпечує безперебійне використання пристрою та даних;
- Автентифікація: ідентифікація особи або пристрою;
- Авторизація: контроль доступу до ресурсів;
- Моніторинг та аудит: безперервний моніторинг мережевої активності.

Шифрування даних: Це основний метод захисту IoT, який гарантує конфіденційність інформації. Аутентифікація: Цей метод дозволяє переконатися, що до мережі підключені лише авторизовані пристрої. Блокчейн: Використовується для децентралізованого зберігання даних та захисту транзакцій. Попри його переваги, низька швидкість і великі енергетичні витрати обмежують

сферу застосування. Ідентифікація аномалій: Використовує штучний інтелект для виявлення загроз. Мережеві брандмауери: Вони забезпечують базовий рівень захисту, але можуть бути менш ефективними у складних динамічних мережах IoT. Протоколи захисту: TLS і DTLS забезпечують захищений обмін даними між пристроями, але створюють затримки, що може впливати на швидкість роботи мережі.

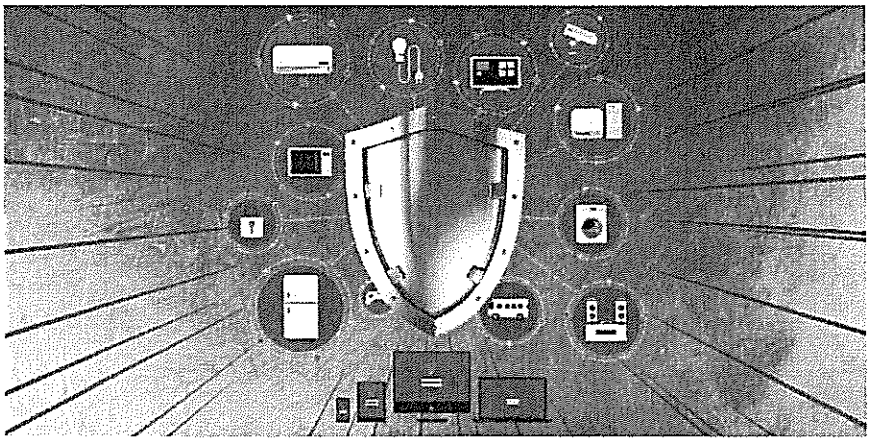


Рис. 4.7 Забезпечення безпеки в мережах Інтернету речей

Криптографічний захист включає шифрування даних, асиметричне шифрування, хешування, управління ключами за допомогою PKI. Захист на рівні мережі працює за допомогою сегментації мережі, брендмауерів, протоколів безпеки DTLS, CoAP, IPsec, TLS. Автентифікація та авторизація розглядаються за допомогою сертифікатів X.509, OAuth 2.0, біометрії, RBAC, ABAC. Безпека на рівні пристрою забезпечується безпечним завантаженням, фізичним захистом пристроїв, моніторингом та загрозами. Захист даних створюється за допомогою децентралізації, зашифрованого хмарного сховища, резервного копіювання.

Проблеми безпеки IoT

Таблиця 4.1

Порівняння результативності методів забезпечення безпеки в IoT

Метод забезпечення безпеки	Переваги	Недоліки	Характеристики	Рівень результативності	Сфера застосування
Шифрування даних (AES, RSA)	Забезпечує конфіденційність і цільсність даних	Високе енергоспоживання, потреба у потужних обчислювальних ресурсах	AES RSA	Високий	Фінансові транзакції, промисловий IoT
Аутентифікація (PKI, сертифікати)	Гарантує перевірку автентичності пристроїв і користувачів	Складність впровадження в мережах з великою кількісні пристроїв	PKI: криптографічні ключі; Сертифікати: X.509, SHA-2	Високий	Медичні IoT-системи, промислові мережі
Блокчейн	Децентралізація, прозорісті транзакцій, неможливість фальсифікації даних	Велике енергоспоживання, низька швидкість роботи	256-бітні хеші, консенсусні алгоритми (Proof of Work, Proof of Stake)	Середній	Логістика, управління ланцюгами постачань
Ідентифікація аномалій (AI, ML)	Виявлення потенційних загроз у режимі реально ре часу	Потреба у великих обчислювальних ресурсах і великих даних	Моделі ML: Random Forest, SVM; час аналізу – до 5 секунд	Високий	Критична інфраструктура, розумні міста
Мережеві брандмауери	Захищають від небажане ба трафіку та зовнішніх атак	Можливість обходу захисту, низька адаптивність до динамічних умов мережі	Фільтрування пакетів, контроль доступу за IP/портами	Середній	Домашні мережі, невеликі IoT-системи
Протоколи захисту (TLS,DTLS)	Забезпечують захищену передачу даних між пристроями	Затримки під час передачі, потреба у сучасному апаратному забезпеченні	TLS 1.3: підтримка шифрування AES-256, ECC; DTLS: адаптація для UDP	Високий	Розумні будинки, мобільні IoT-пристрої

ВИСНОВКИ

У процесі дослідження управління ресурсами в безпроводових IoT-мережах було з'ясовано, що успішна реалізація таких мереж вимагає інтеграції різноманітних підходів до оптимізації використання енергетичних, обчислювальних, мережевих та спектральних ресурсів.

Ефективне управління ресурсами дозволяє забезпечити надійність і масштабованість мереж, що є критично важливим для розвитку Інтернету речей.

Застосування енергоефективних протоколів, таких як Duty Cycling, а також використання методів збирання енергії є важливими для подовження часу автономної роботи пристроїв IoT. Використання когнітивного радіо та методів динамічного розподілу частот сприяє зменшенню інтерференції і оптимізації спектра.

Управління спектральними ресурсами відіграє важливу роль у забезпеченні якісної передачі даних в умовах високої щільності підключених пристроїв. Когнітивне радіо, методи розподілу спектра та технології LPWAN забезпечують оптимізацію використання доступних частот, мінімізуючи інтерференцію та збільшуючи ефективність мережі.

Проблеми масштабованості та надійності IoT-мереж успішно вирішуються завдяки використанню розподілених обчислень, таких як хмарні та периферійні обчислення, а також адаптивної маршрутизації, яка дозволяє динамічно реагувати на зміну мережевих умов. Інтеграція 5G, штучного інтелекту та блокчейну створює нові перспективи для підвищення стабільності, безпеки та ефективності IoT-мереж.

Практичні приклади впровадження IoT демонструють великий потенціал цієї технології у розумних містах, промисловості, сільському господарстві та медицині. Використання IoT у цих галузях дозволяє підвищувати продуктивність, забезпечувати раціональне використання ресурсів і покращувати якість життя.

ПЕРЕЛІК ПОСИЛАНЬ

1. IoT For All. (2021). «Understanding Resource Management in IoT Networks». Взято з сайту: https://www.iotforall.com

2. IoT World Today. (2021). «The Challenges of IoT Resource Management».

3. IEEE Internet of Things Journal. (2021). «Energy-Efficient Resource Allocation in IoT Networks». IEEE Xplore. https://doi.org/10.1109/JIOT.2021.1234567

4. Семків, І. М., та Черненко, О. О. (2019). Сучасні підходи до управління ресурсами в Інтернеті речей. «Технічні науки та технології, 1»(2), 45-53.

5. Іванов, І. В. (2018). Інтернет речей: технології, виклики та рішення для ефективного управління ресурсами. «Наукові праці університету інформаційних технологій, 12», 72-81.

6. Тимченко, М. О., та Петренко, В. І. (2020). Інтеграція IoT та 5G для розв'язання проблем масштабованості та надійності в мережах. «Журнал комп'ютерних наук та інформаційних технологій, 15»(4), 133-142. https://doi.org/10.15407/jcnsit.2020.04.133

7. Шевченко, Л. В., та Макаренко, О. П. (2021). Стратегії управління енергетичними ресурсами в IoT-мережах. «Енергетика та енергоефективність, 3»(2), 56-62.

8. Кравицький, В., та Свиридов, М. (2018). Розподілене управління ресурсами в IoT-мережах. «Інженерія систем, 11»(3), 89-95.

9. Демченко, Ю. О. (2018). Блокчейн в управлінні ресурсами IoT-мереж: інноваційні підходи. «Інформаційні технології в економіці, 22»(4), 102-110.

10. Тимченко, Д. О. (2019). Управління мережею IoT: адаптивні підходи та проблеми масштабування. «Журнал інформаційних технологій та телекомунікацій, 19»(6), 78-84. https://doi.org/10.17709/jitt.2019.06.078

11. Шевченко, Л. В., та Бондаренко, І. М. (2021). Моделі енергетичного управління в мережах Інтернету речей. «Технічні науки і технології, 18»(2), 90-96.

12. Ситник, М. П., та Федорчук, А. І. (2020). Протоколи управління ресурсами в бездротових IoT-мережах. «Науковий вісник Черкаського університету, 14»(3), 125-132.

13. GSMA IoT. (2021). «Global IoT Resource Management». Взято з сайту https://www.gsma.com/iot

14. ThingsBoard. (2020). «IoT Resource Management Platform». Взято з сайту https://thingsboard.io

15. Cisco IoT. (2021). «Managing IoT Resources: Strategies for IoT Networks». Взято з сайту https://www.cisco.com/c/en/us/solutions/internet-of-things.html

16. Smart Cities Council. (2021). «IoT Resources for Smart Cities».Взято з сайту https://smartcitiescouncil.com

17. IoT Academy. (2021). «Training on Resource Management for IoT Networks». Взято з сайту https://www.iotacademy.com.ua

18. IoT Analytics. (2021). «Report on Resource Management in IoT Networks». Взято з сайту https://iot-analytics.com

19. Семків, І., та Черненко, О. (2019). «Сучасні тенденції управління IoT-мережами в Україні». Взято з сайтуhttps://iotukraine.org.ua

20. Тимченко, М. О., Петренко, В. І. (2020). «IoT та 5G для управління ресурсами». Взято з сайту https://www.iotworldtoday.com

ДЕМОНСТРАТИВНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Презентація по магістерській роботі
на тему:

«Методи управління ресурсами в безпроводових IoT-мережах для забезпечення надійності в умовах масштабованості»

Виконав: Андрій ГРИЦЕНКО

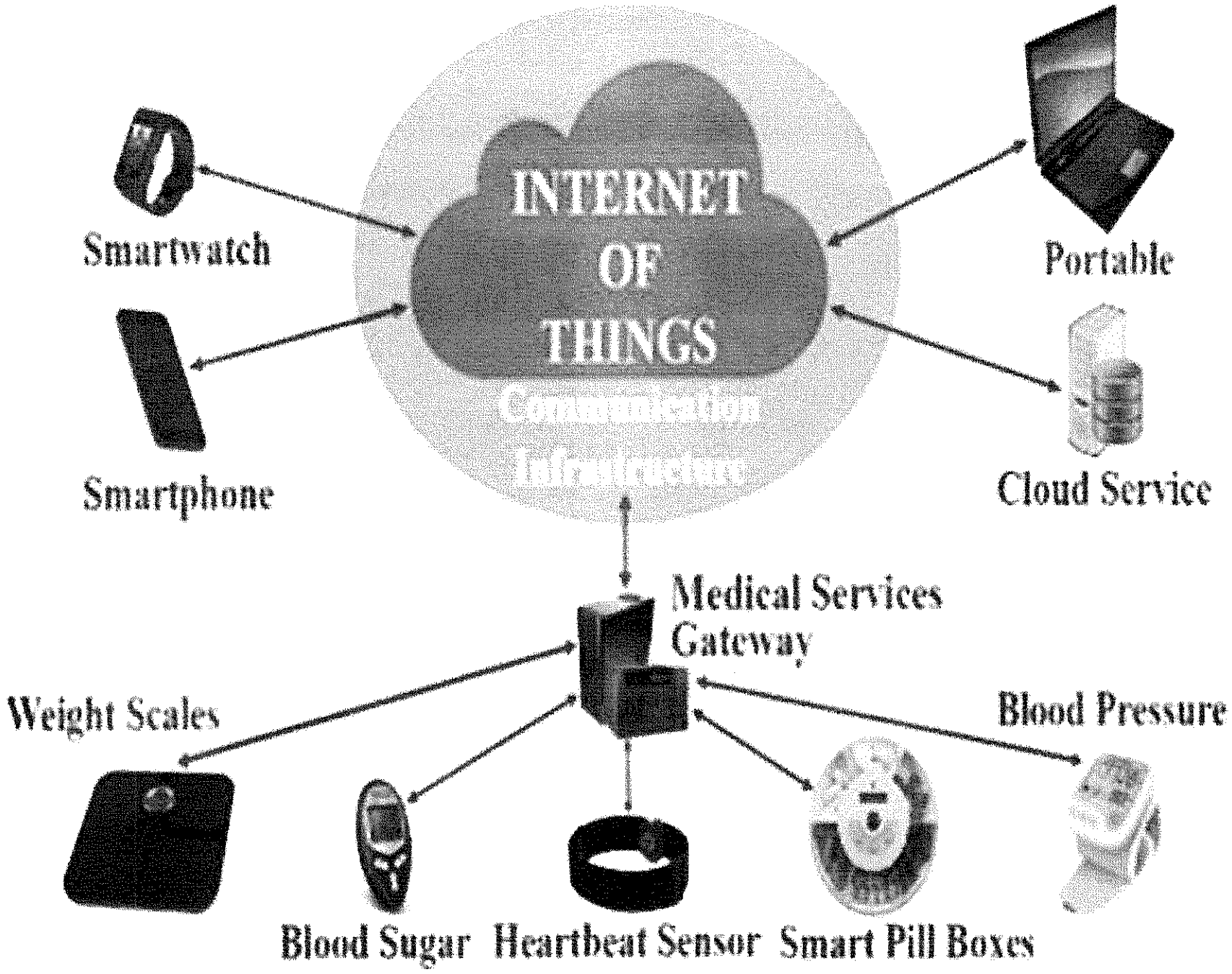
Керівник: Лариса ДАКОВА,
к.т.н., доцент

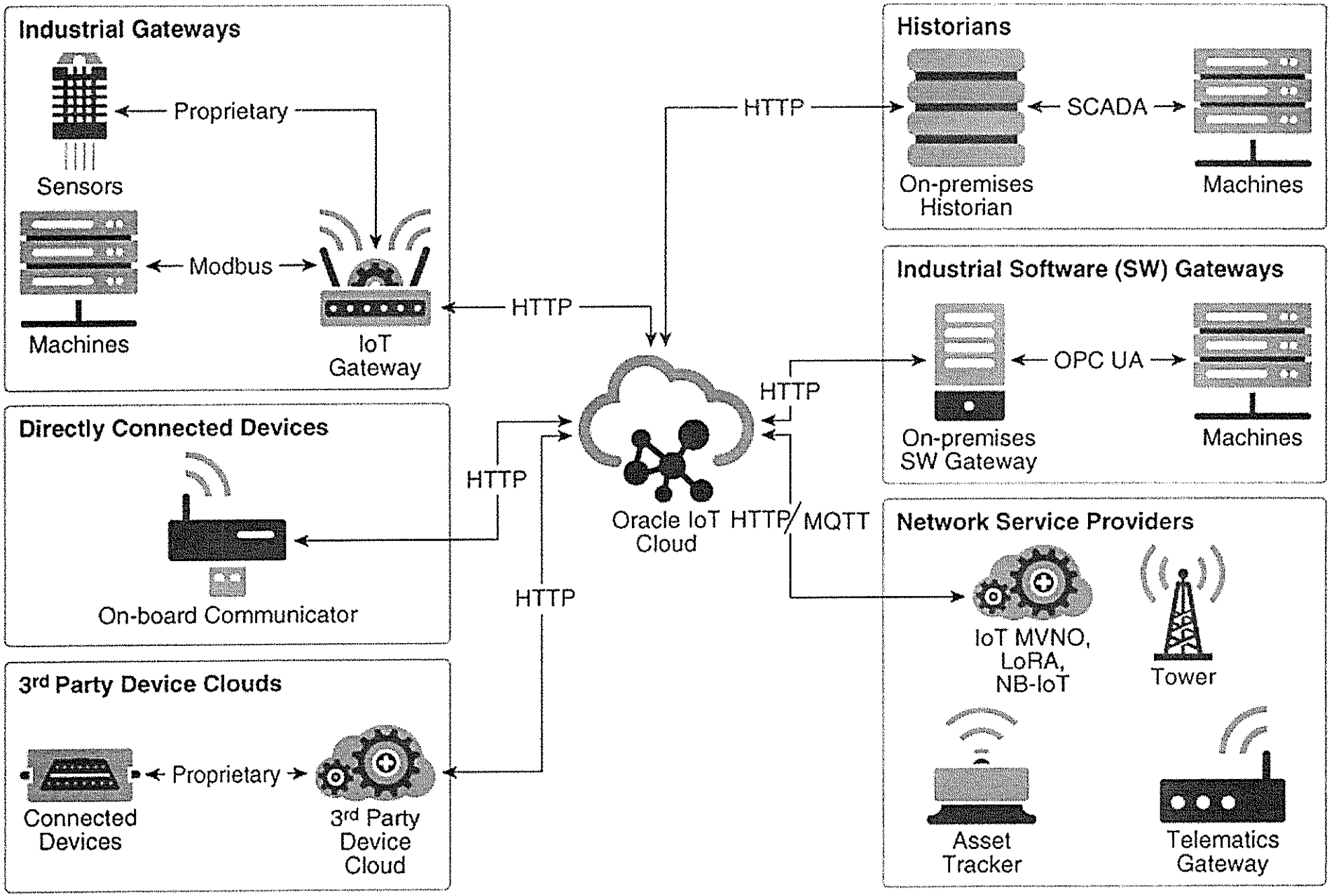
Мета роботи

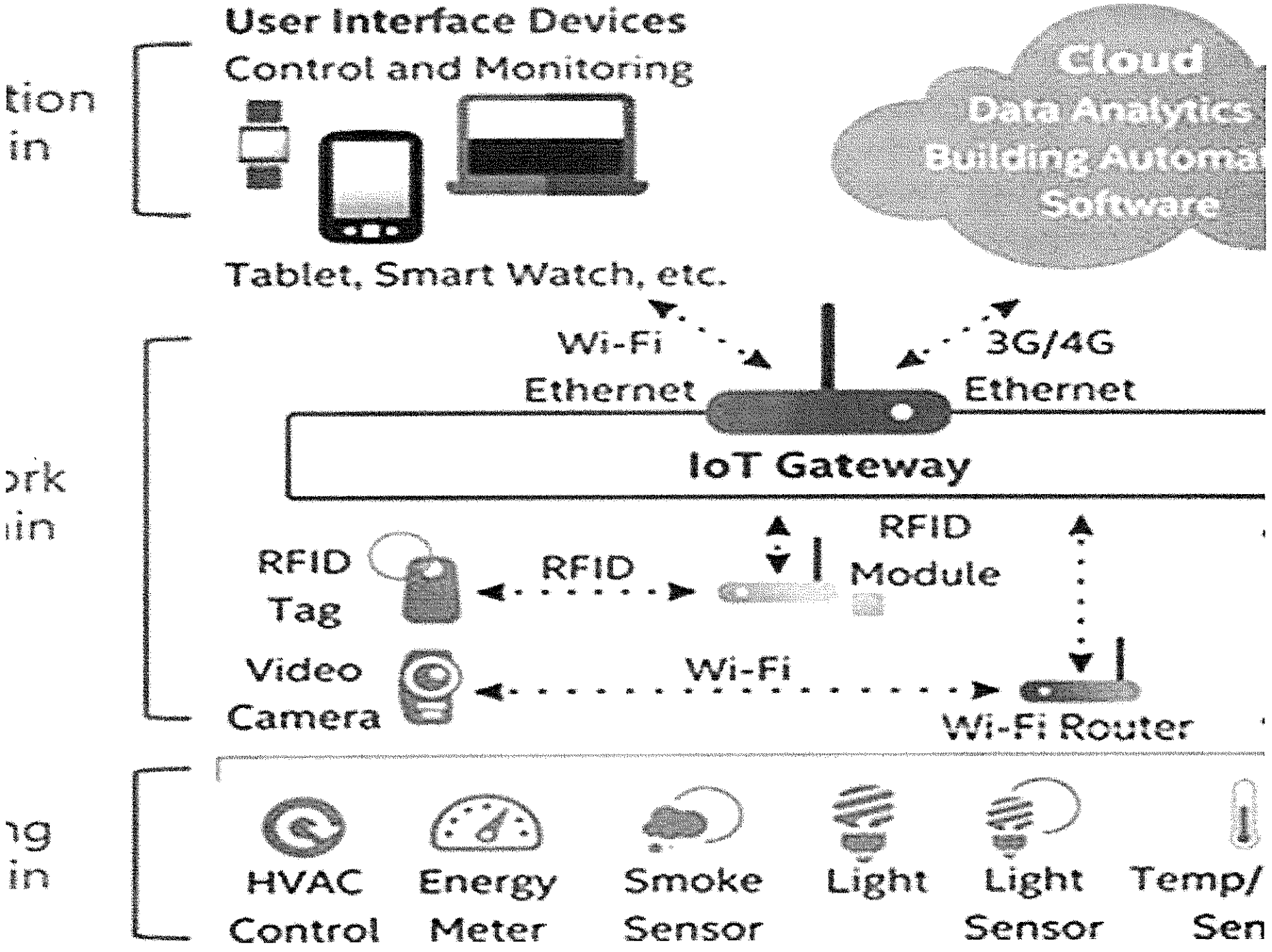
Мета роботи - дослідження методів планування та оптимізації безпроводових телекомунікаційних мереж.

Об'єкт дослідження - процес управління ресурсами для забезпечення надійності та масштабованості бездротових мереж IoT.

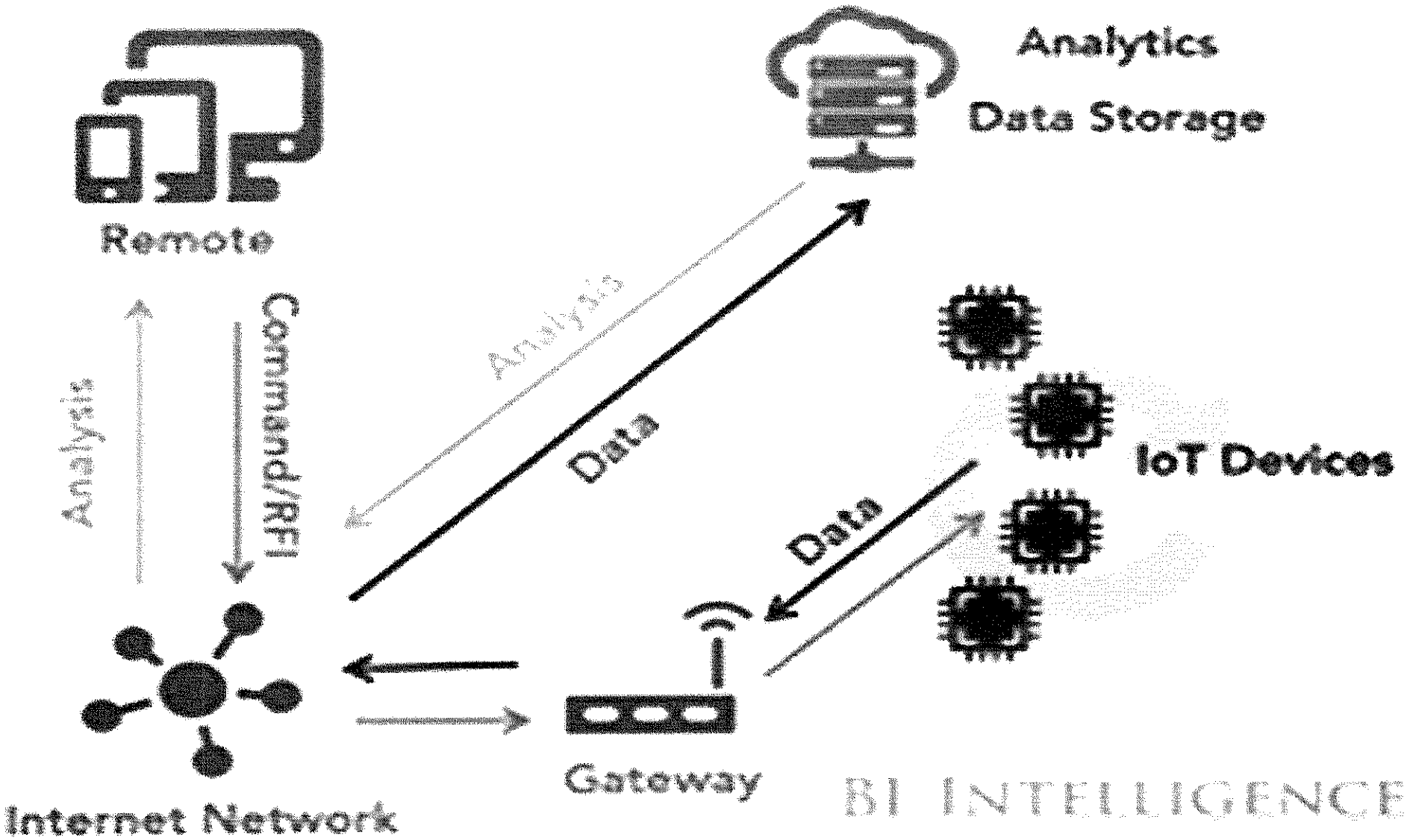
Предмет дослідження – методи управління ресурсами в безпроводових IoT-мережах для забезпечення надійності в умовах масштабованості.

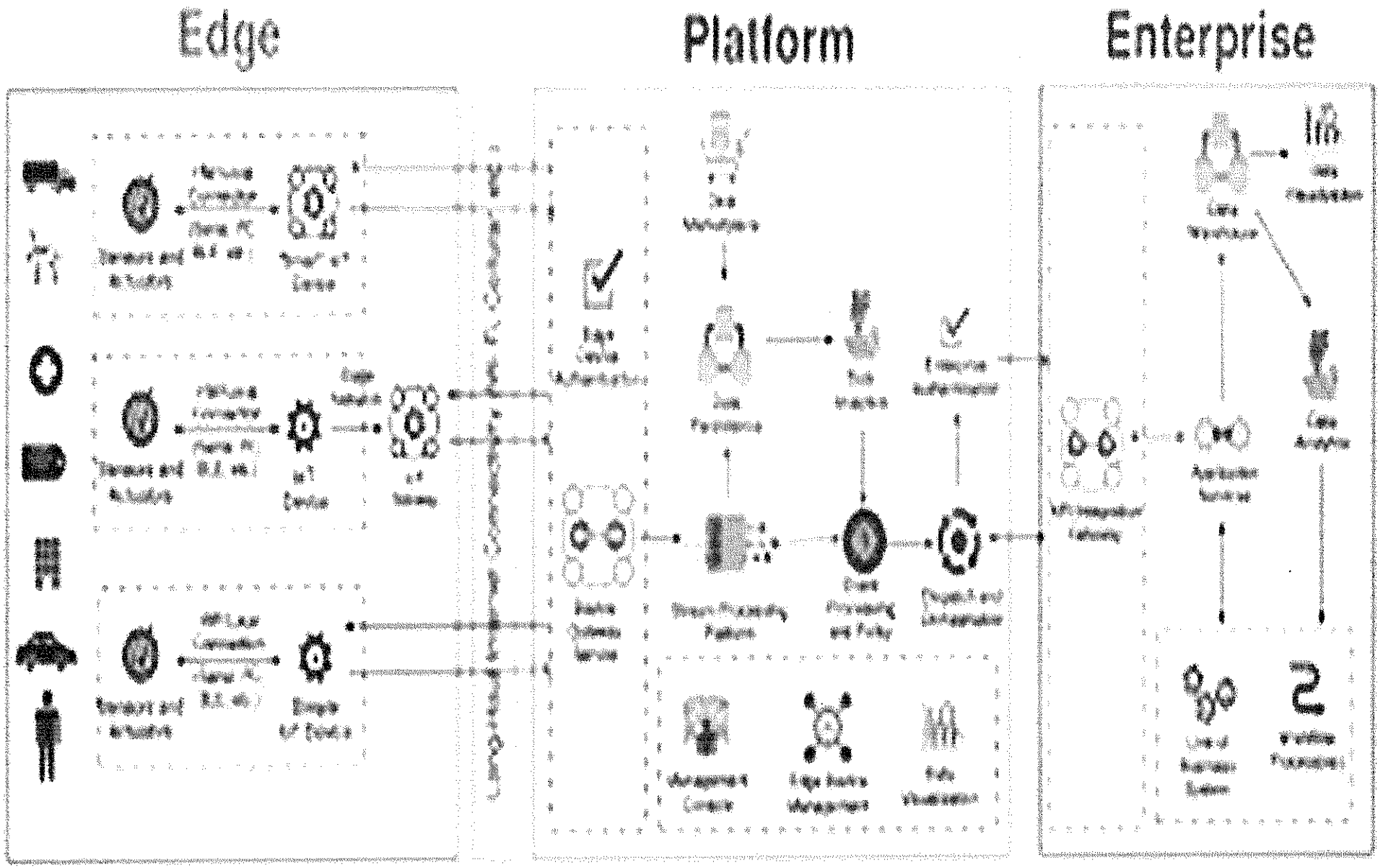

INTERNET
OF
THINGS
Communication
Infrastructure
Smartwatch
Smartphone
Portable
Cloud Service
Medical Services
Gateway
Weight Scales
Blood Pressure
Blood Sugar
Heartbeat Sensor
Smart Pill Boxes


Industrial Gateways
Proprietary
Sensors
Modbus
Machines
IoT Gateway
HTTP
Historians
SCADA
On-premises Historian
Machines
Industrial Software (SW) Gateways
OPC UA
On-premises SW Gateway
Machines
Directly Connected Devices
On-board Communicator
HTTP
HTTP
HTTP
Oracle IoT Cloud
HTTP/MQTT
Network Service Providers
IoT MVNO, LoRA, NB-IoT
Tower
Asset Tracker
Telematics Gateway
3rd Party Device Clouds
Proprietary
Connected Devices
3rd Party Device Cloud

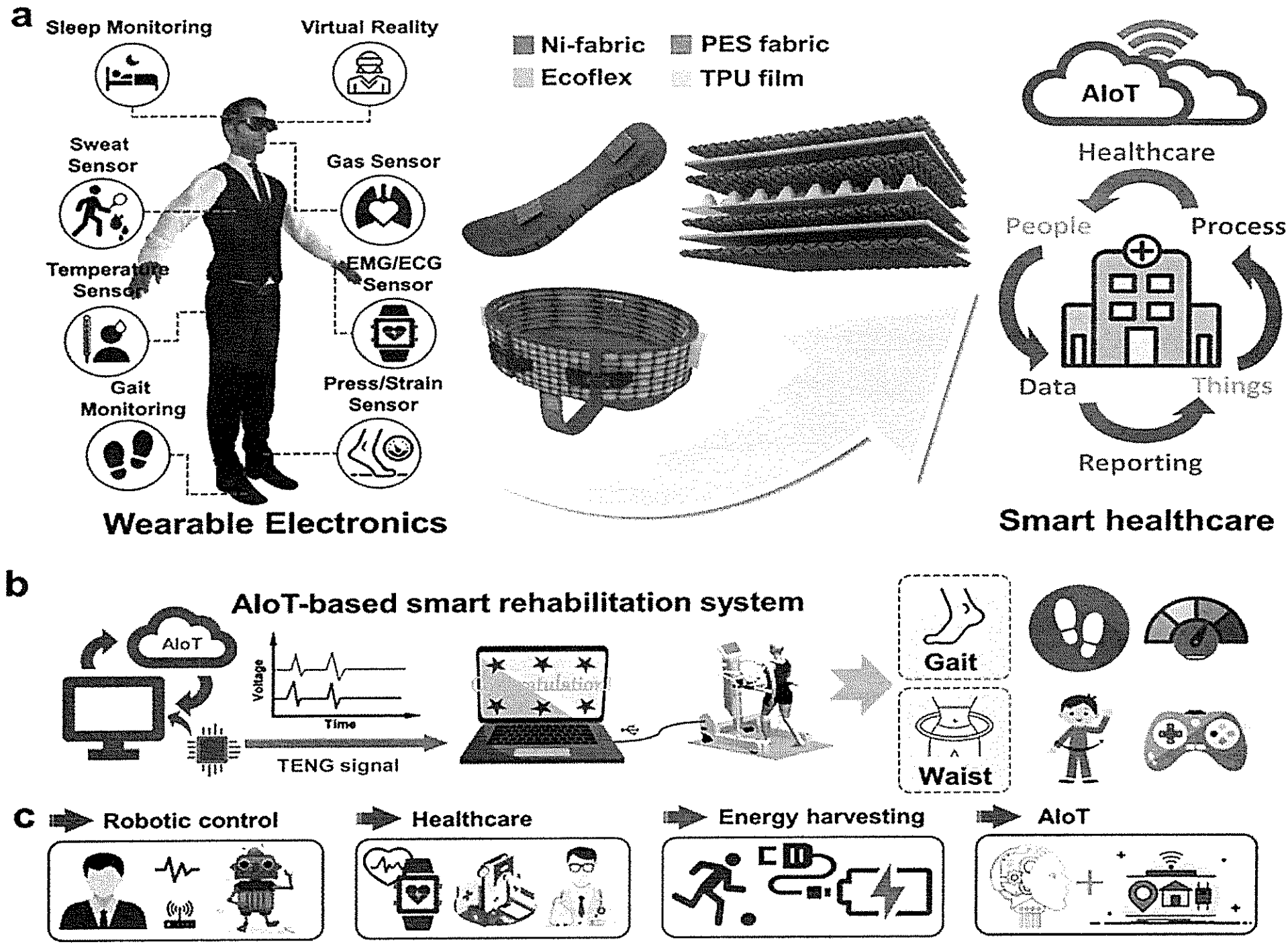

User Interface Devices
Control and Monitoring
Tablet, Smart Watch, etc.
Cloud
Data Analytics
Building Automa
Software
Wi-Fi
Ethernet
3G/4G
Ethernet
IoT Gateway
RFID
Tag
RFID
RFID
Module
Video
Camera
Wi-Fi
Wi-Fi Router
HVAC
Control
Energy
Meter
Smoke
Sensor
Light
Light
Sensor
Temp/
Sen

The Internet of Things Ecosystem

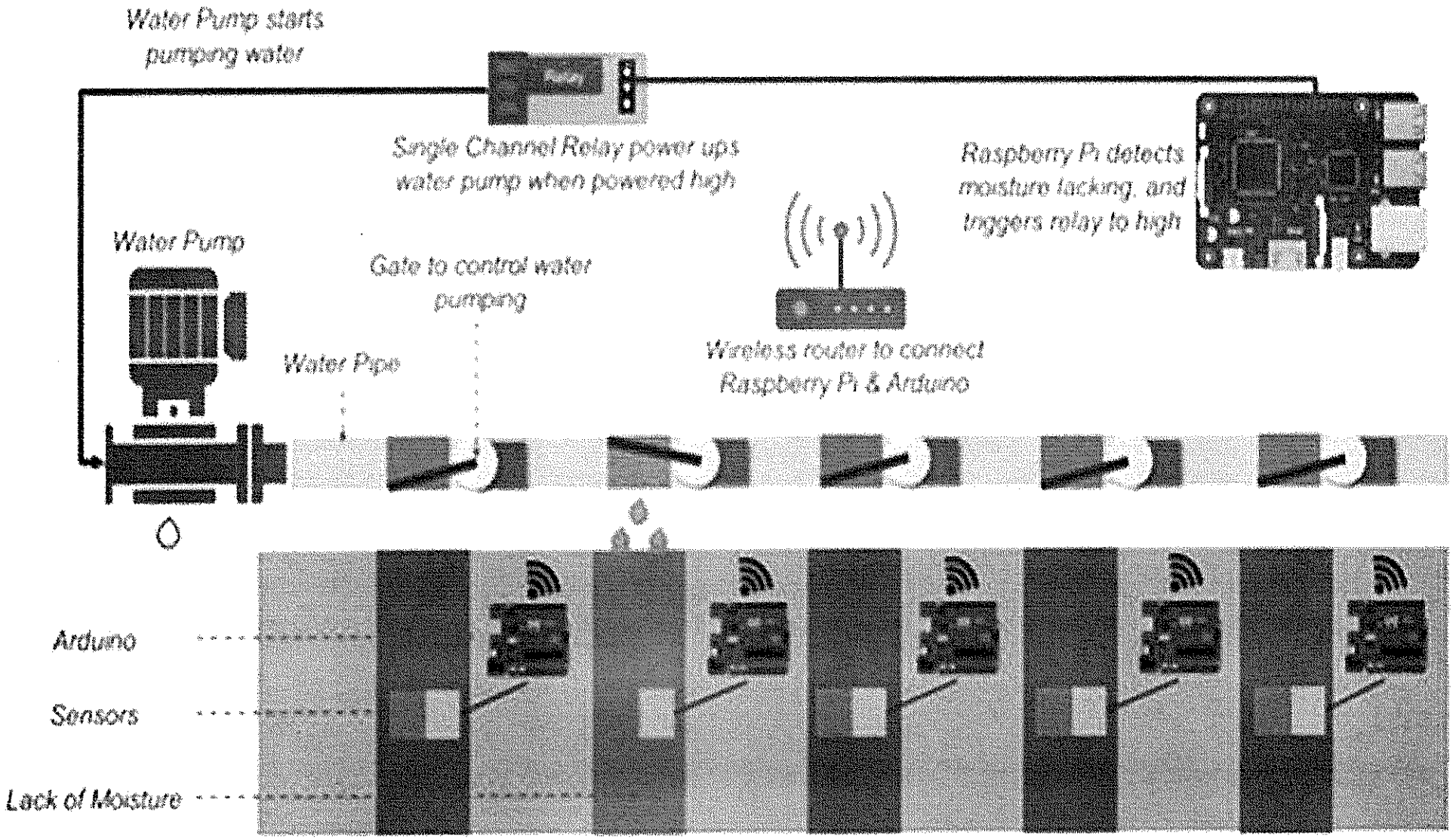


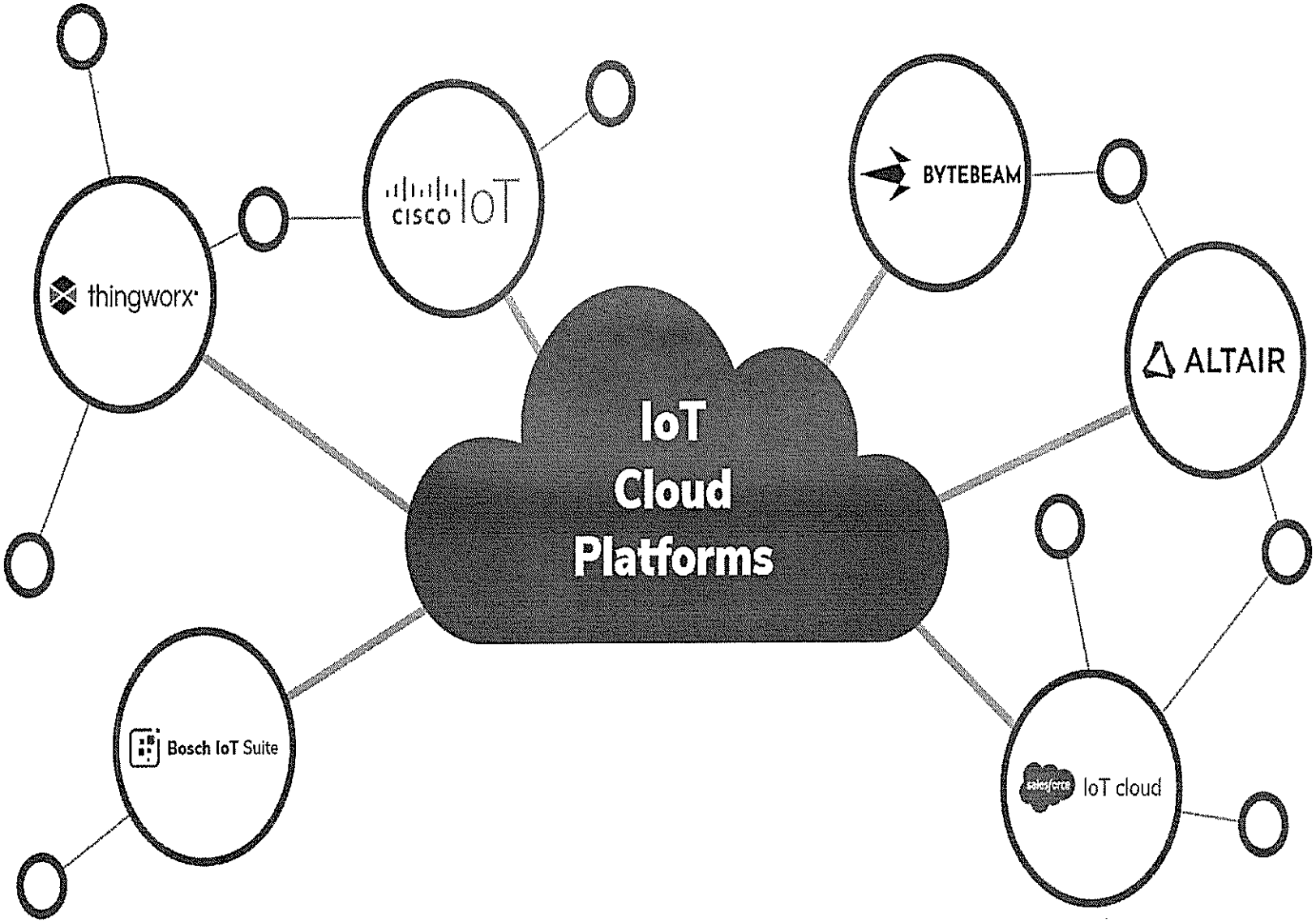


Gartner


a
Sleep Monitoring
Virtual Reality
Sweat Sensor
Gas Sensor
Temperature Sensor
EMG/ECG Sensor
Gait Monitoring
Press/Strain Sensor
Wearable Electronics
Ni-fabric
PES fabric
Ecoflex
TPU film
AIoT
Healthcare
People
Process
Data
Things
Reporting
Smart healthcare
b
AIoT-based smart rehabilitation system
AIoT
Voltage
Time
TENG signal
Gait
Waist
c
Robotic control
Healthcare
Energy harvesting
AIoT

Smart Irrigation System




IoT
Cloud
Platforms
thingworx
cisco IoT
BYTEBEAM
ALTAIR
Bosch IoT Suite
IoT cloud

РОЗУМНЕ МІСТО ТА ІНТЕРНЕТ РЕЧЕЙ



ВІДДАЛЕНЕ ЗНЯТТЯ ПОКАЗНИКІВ З ГАЗОВИХ ЛІЧИЛЬНИКІВ

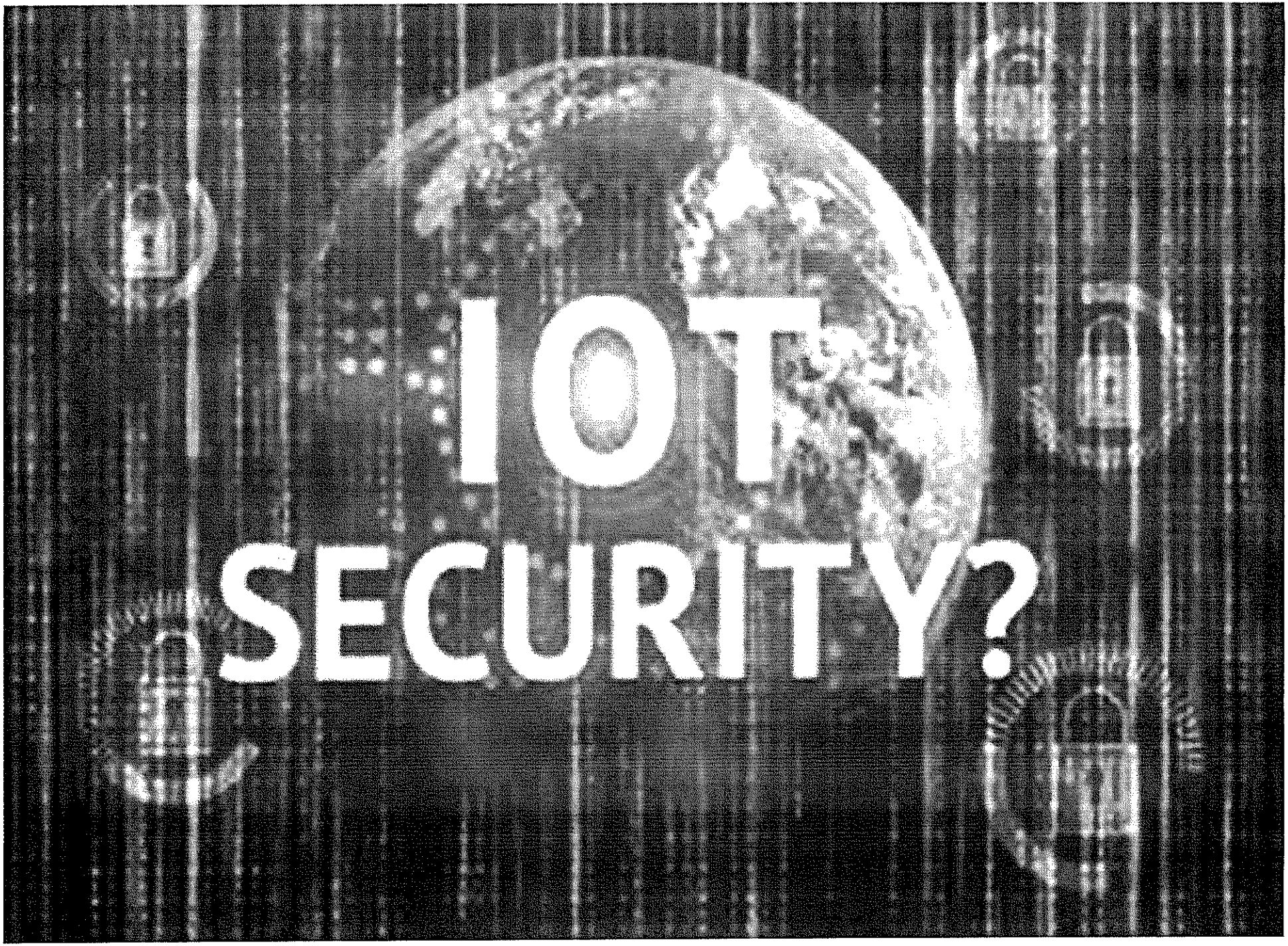
ВІДДАЛЕНЕ ЗНЯТТЯ ПОКАЗНИКІВ З ЛІЧИЛЬНИКІВ ВОДИ

РОЗУМНЕ ПАРКУВАННЯ

РОЗУМНЕ ОСВІТЛЕННЯ

УПРАВЛІННЯ ВІДХОДАМИ

МОНІТОРИНГ НАВКОЛИШНЬОГО СЕРЕДОВИЩА


IOT
SECURITY?

Висновки

В магістерській роботі досягнуто наступних результатів:

1. У першому розділі проаналізовано архітектуру, принцип роботи та ключові характеристики IoT мереж. Розглянуто класифікацію ресурсів та їхню роль у забезпеченні функціонування IoT-систем.

2. У другому розділі детально досліджено проблеми, пов'язані з надійністю та масштабованістю IoT-мереж. Визначено основні фактори, що впливають на стабільність роботи систем, включаючи енергетичні обмеження, затримки у передачі даних та загрози безпеці.

3. У третьому розділі виконано практичні дослідження методів забезпечення надійності, включаючи резервування, адаптивну маршрутизацію та підходи до масштабування великих мереж.

4. У четвертому розділі визначено приклади впровадження мереж IoT в різні аспекти життя, забезпення безпеки даних та прогнозування навантажень на мережу. Створено таблицю порівняння результативності методів забезпечення безпеки в IoT.

Дякую за увагу

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Андрій Гриценко

Назва: Метод управління ресурсами в безпроводових IoT-мережах для забезпечення надійності в умовах масштабованості

Координатор: Лариса Дакова

Підрозділ: ННІТ

Коефіцієнт подібності 1:2.4

Коефіцієнт подібності 2:1.9

Тривога: 20

Після аналізу Звіту подібності констатую наступне:

☐ виявлені в роботі запозичення є сумлінними і не мають ознак плагіату. Тому робота визнається самостійною і допускається до захисту;

☐ виявлені в роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і самостійності її автора. Роботу направити на доопрацювання;

☐ виявлені в роботі запозичення є недобросовісними і мають ознаки плагіату або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. У зв'язку з чим, робота не допускається до захисту.

…… ……

Дата *Підпис Наукового керівника*