ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інженерії програмного забезпечення автоматизованих систем

Пояснювальна записка

до магістерської роботи
на ступінь вищої освіти магістр

на тему: «**ПРОЕКТУВАННЯ ПРОМИСЛОВИХ БЕЗДРОТОВИХ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ З СПРОЩЕНОЮ ПРОЦЕДУРОЮ ІДЕНТИФІКАЦІЇ»**

Виконав: студент 6 курсу, групи ІСДМ-61
спеціальності 126 Інформаційні системи та технології
освітня програма «Інформаційні системи та технології»
(шифр і назва спеціальності)
Назаренко О.М.
(прізвище та ініціали)
Керівник Полоневич О.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтроль Данильченко В.М.
(прізвище та ініціали)

Київ – 2021

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра Інженерії програмного забезпечення автоматизованих систем
Ступінь вищої освіти - «Магістр»
Спеціальність підготовки 126 Інформаційні системи та технології
Освітня програма «Інформаційні системи та технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри ІСТ
_____ К.П.Сторчак
"____" _____2021 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Назаренко Олексій Михайлович
(прізвище, ім'я, по батькові)

1.Тема роботи: «Проектування промислових бездротових систем Інтернету речей з спрощеною процедурою ідентифікації»
Керівник роботи: Полоневич Ольга Володимирівна, к.т.н., доцент, доцент кафедри ІПЗАС.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від _____року №
2. Строк подання студентом роботи _____
3. Вхідні дані до роботи :
1. Науково-технічна література
2. Існуючі методології проектування IIoT

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1. Аналіз основних положень промислового інтернету речей.
2. Дослідження основних архітектур безпротових технологій обміну даних.
3. Розробка моделі архітектури промислового інтернету речей з вибором опорного вузла для находження оптимального рішення.

5. Перелік графічного матеріалу
1. Титульний слайд
2. Постановка завдання
3. Основні технології проектування IIoT
4. Оптимізація мережі для промислового інтернету речей
5. Пропонуємий метод вибору опорного вузла
6. Тестування запропонованого методу

6. Дата видачі завдання

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Приміт ка
1	Підбір науково-технічної літератури		
2	Вивчення матеріалів для подальшої взаємодії з ними		
3	Аналіз основних положень промислового інтернету речей.		
4	Дослідження основних архітектур безпротових технологій обміну даних.		
5	Розробка моделі архітектури промислового інтернету речей з вибором опорного вузла для находження оптимального рішення		
6	Тестування запропонованого методу		
7	Вступ, висновки, реферат		
8	Розробка демонстраційних матеріалів		
9	Попередній захист роботи		

Студент_____ Назаренко О.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Полоневич О.В..
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи 69 с., 21 рис., 16 табл., 13 джерела

ПРОМИСЛОВИЙ ІНТЕРНЕТ РЕЧЕЙ, IIOT, ТИПИ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ, АЛГОРИТМ, LPWAN, СТІЛЬНИКОВИЙ ЗВ'ЯЗОК, NARROWBAND-IOT, LTE-M, ZIGBEE, BLUETOOTH, WIFI, RFID, NFC, ОПТИМІЗАЦІЯ МЕРЕЖІ, ОПОРНИЙ ВУЗОЛ

Об'єкт дослідження: проектування мережі промислового інтернету речей.

Предмет дослідження: бездротова система промислового інтернету речей.

Мета роботи: розробка ефективного методу проектування промислових бездротових систем інтернету речей.

Методи дослідження: методи керованої лавинної розсилки, випадкового вибору еталону, маршрутизації вектору відстані, визначення оптимальної кількості опорних вузлів.

Галузь використання: безпроводові системи промислового інтернету речей.

Проведено дослідження проектування промислових бездротових систем інтернету речей. Визначено, що в системах зв'язку, де особливо жорсткі вимоги до завадостійкості передачі інформації, найефективнішим є використання багатопозиційних сигналів з амплітудно-фазовою модуляцією. Розроблено технологію підбору оптимального вузла та оцінку її продуктивність у промисловому Інтернеті речей; проведено моделювання розробленого алгоритму, застосованого для вибору еталонного вузла. Отримані результати дозволяють побудувати ефективну систему з максимальною швидкістю передачі даних, мінімальним споживанням енергії та найкоротшим шляхом до одержувача.

ЗМІСТ

ВСТУП

Актуальність. Промисловий Інтернет речей (IIoT), також відомий як Промисловий Інтернет, поєднує найважливіші ресурси, передові методи прогнозної та розпорядчої аналітики та сучасних промислових робітників. Це мережа безлічі промислових пристроїв, з'єднаних комунікаційними технологіями, у результаті створюються системи, які можуть відслідковувати, збирати, обмінювати, аналізувати та надавати нові цінні відомості, як ніколи раніше. Ці ідеї можуть потім допомогти промисловим компаніям приймати більш розумні та швидкі бізнес-рішення. У цій магістерській роботі пропонується підхід проектування промислової бездротової системи інтернету речей.

Об'єкт дослідження –проектування мережі промислового інтернету речей.

Предмет дослідження – безпроводова система промислового інтернету речей.

Мета – розробка ефективного методу проектування промислових безпроводових систем інтернету речей.

Завдання дослідження – в процесі дослідження вирішувалися наступні завдання:

1. Аналіз основних положень промислового інтернету речей.
2. Дослідити та здійснити аналіз бездротових технологій обміну даних на теперішній час.
3. Дослідити та здійснити оцінку по основним архітектурам бездротових технологій обміну даних.
4. Розробка моделі архітектури промислового інтернету речей з вибором опорного вузла для находження оптимального рішення.

Методика дослідження – методи керованої лавинної розсилки, випадкового вибору еталону, маршрутизації вектору відстані, визначення оптимальної кількості опорних вузлів.

Наукова новизна – розроблено модель архітектури промислового інтернету речей з находженням оптимальної кількості опорних вузлів.

Практична значущість. Основні результати магістерської роботи можуть бути використані при розробці бездротової системи промислового інтернету речей.

Апробація: Основні результати роботи опубліковано у матеріалах двох науково-практичних конференцій та статті у журналі «Зв’язок»

1 АНАЗІЗ ОСОБЛИВОСТЕЙ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ

1.1.1 Поняття промислового інтернету речей

Промисловий Інтернету Речей — це мережа з Інтернету речей, яка є об'єднанням комп'ютерів і промислових об'єктів, із встановленими на них датчиками та програмним забезпеченням, з можливістю віддаленого контролю та автономним режимом.

Для початку роботи в системі IIoT на промислове обладнання встановлюють сенсори, виконавчі механізми, контролери, людино-машинний інтерфейс та програмний інтерфейс для управління. Через це з'являється можливість отримання інформації, яка дозволяє керівництву отримувати достовірну та точну інформацію про стан виробництва. Дані обробляються у кожному підрозділі. Такий підхід сприяє налагодженню взаємодії з колегами, а також дозволяє їм приймати обґрунтовані рішення у рамках поставлених завдань.

Дані можуть бути використані для запобігання позаплановим простоям або поломкам обладнання, скорочення позапланового техобслуговування, а також зниження ризику виникнення непередбачених ситуацій на виробництві.

Після того, як оброблено величезну кількість неструктурованих даних, що надходять від датчиків, їх фільтрація та адекватна оцінка стають першорядним завданням. Саме тому для того, щоб інформація була зрозумілою та зручною для користувача, необхідно її подати в максимально зрозумілій формі. Дані збираються за допомогою передових аналітичних платформ, призначених для збирання, зберігання або аналізу даних про технологічний процес та подію, що відбуваються в реальному масштабі часу.

За допомогою Промислового Інтернету речей можна створити виробництво, яке буде економнішим, гнучкішим та ефективнішим, ніж існуючі підприємства. В даний час у світі спостерігається зростання використання бездротових пристроїв з підтримкою протоколу IP, таких як смартфони, планшети та датчики, які вже активно використовуються на виробництві. Існуючі бездротові мережі датчиків в

найближчі роки планується розширити і доповнити бездротовими мережами, що дозволить підприємствам значно розширити зони застосування систем моніторингу та управління.

У міру зростання кількості цифрових екосистем виробничих підприємств з ізольованими системами, що самостійно виконують всі необхідні для випуску продукції. Виробничі та бізнес-процеси трансформуються у відкриті системи, що об'єднують різних учасників ринку. У цьому управління виробництвом і збутом цих систем здійснюється не персоналом підприємства, а хмарними сервісами (рис 1). Кінцева мета всіх цих трансформаційних перетворень – не випускати продукцію, а надання послуг споживачам.

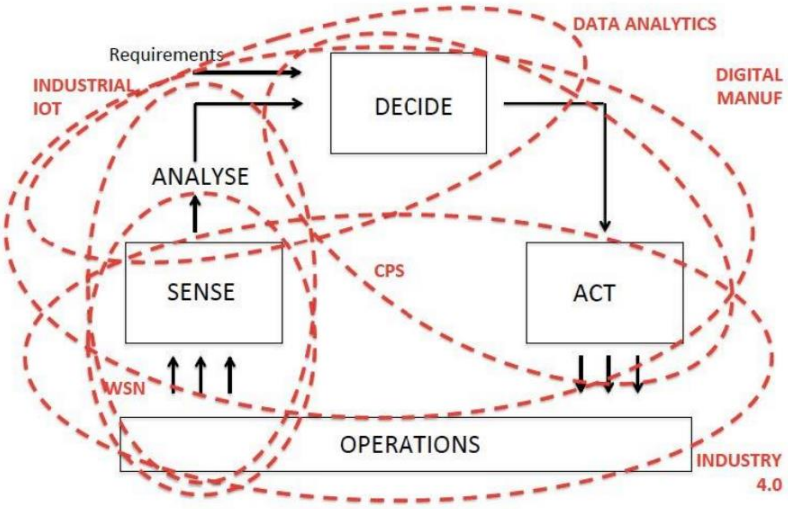

Рисунок 1.1 – Цифрові парадигми у виробництві

У рамках масштабного дослідження «Успіх за допомогою промислового Інтернету Речей» (Winning With the Industrial Internet of Things) у 2015 році компанією Accenture було опитано понад тисячі керівників вищої ланки у всіх країнах світу (з них 736 – глави компаній). На основі даних звіту автори роблять висновок, що промисловий Інтернет речей у світі може досягти рівня у розмірі 14,2 трильйона доларів до 2030 року. А ось це вже загроза майбутньому розвитку цифрової техніки та її розповсюдженню. Адже нині жодна компанія чи держава не

мають необхідних умов для того, щоб розпочати масове поширення нових цифрових технологій.

Згідно зі звітом компанії, вже до 2030 року результати застосування IIoT могли б бути наступними.

- Американський показник сукупного доходу населення міг би збільшитись на $6,1 трлн. Якщо США вкладуть у технологію IIoT не менше 50% своїх інвестицій – до 2030 року вони могли б збільшити ВВП до 7,1 трлн. доларів.
- Німеччині вдалося б збільшити сукупний ВВП на суму 700 мільярдів доларів, або ж на 1,7%.
- Британія, згідно з первинними прогнозами, могла б збільшити сукупний ВВП на $531 мільйонів, тобто в середньому на 1,8%.
- Економічні вигоди від використання IIoT у Китаї будуть більшими за російські, індійські та бразильські. За рахунок можливості проведення заходів щодо підтримки та розвитку промислового Інтернету речей Китай міг би до 2030 року збільшити свій сукупний ВВП на $1 млрд., збільшивши його втричі.

Проте, як зазначає Accenture, у 73% досліджених компаній немає конкретних планів на IIoT. Із них лише 7% мають чітку мету, а також мають необхідні вкладення у проект.

Згідно з дослідженням компанії J'son & Partners Consulting, найбільш поширеними сферами застосування рішень у сфері промислового Інтернету є виробництва, які характеризуються наявністю однієї чи кількох таких важливих умов:

- Використання великої кількості комплектуючих та застосування їх у широкому асортименті.
- Необхідність підвищення якісного рівня виробленої продукції, і навіть зниження ступеня браку.
- Необхідність забезпечення якісного сервісного обслуговування раніше поставленої продукції.
- Необхідність зниження витрат за виробництво і експлуатацію.

- Висока енергоємність.
- Складна робоча обстановка.
- Потреба у впровадженні системи діагностики та ремонту обладнання для зниження незапланованої зупинки виробництва.
- Потреба підвищення продуктивності співробітників.
- Потреба охорони праці.
- Необхідно створити єдину систему, яка б об'єднала всі види діяльності.

1.1.2 Безпека в IIoT як одна з ключових характеристик

Згідно з протоколом TK26, затвердженим у 2019 році, індустріальні системи CRISP будуть використовувати протокол захищеного обміну даними в рамках методичних рекомендацій. Зі зростанням рівня IIOT ймовірність здійснення кібератак збільшується.

Завдяки високому проникненню промислового інтернету речей у критично важливі інфраструктури, а також у виробничі сектори збільшує кількість потенційних атак на критично важливі об'єкти та виробничі сектори зросла. Про це вказують результати роботи аналітиків Frost & Sullivans, проведеної ними в рамках дослідження, опублікованого 13 грудня 2018 року.

Аналітики Frost & Sullivans вважають, що хакерські атаки тільки на енергетичних та комунальних підприємствах обходяться в середньому по $13,2 млн щорічно. Співробітники дослідницького центру компанії Frost & Sullivan провели дослідження з оцінки ризиків для кіберпростору та з'ясували, що підвищення ризиків призводить до створення загальних підходів для забезпечення кібербезпеки. На сьогоднішній день це одна з найактуальніших проблем у сфері ІБ.

До проблем безпеки, пов'язаних з IIoT, можна віднести збільшення площі атак і необхідність віддаленого доступу до неї. З кожним днем все більше пристроїв та датчиків підключаються до мережі, а також створюються нові канали зв'язку,

сховища даних, портів та кінцевих точок. Високий взаємозв'язок між цими двома факторами становить більше вразливостей у разі їх захисту.

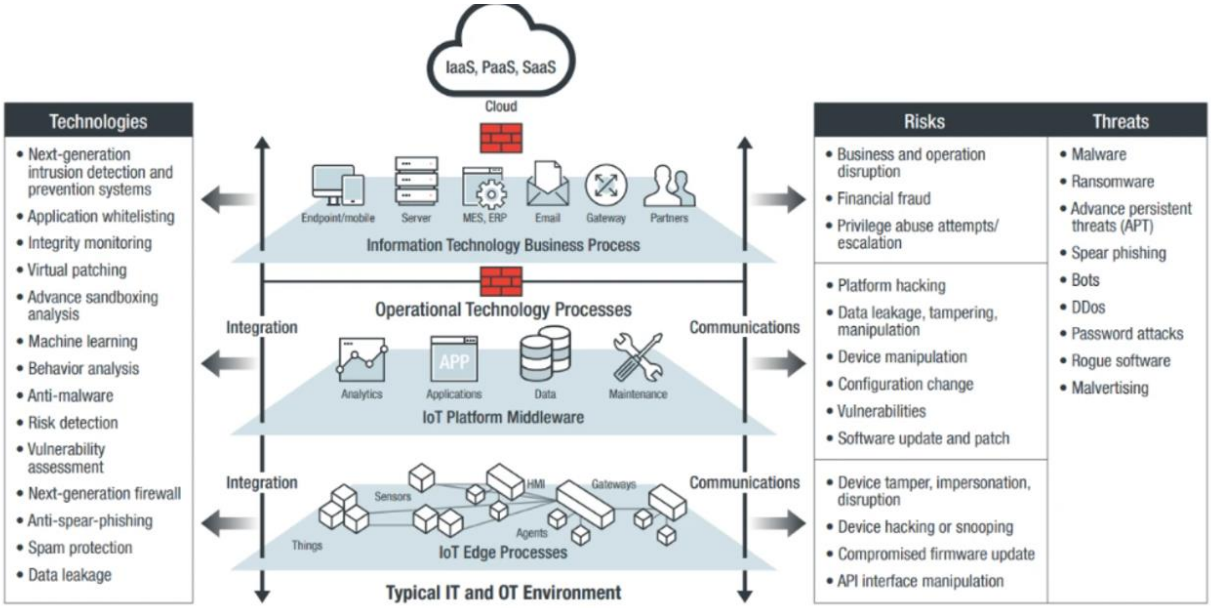

Рисунок 1.2 – Топологія IoT оточення

Не слід забувати, що безпека в Інтернеті речей має бути не лише на рівні локальної мережі, а й на рівні всієї глобальної мережі. Але якщо у малих підприємств є можливість встановити на комп'ютери та сервери лише стандартні заходи безпеки, то об'єкт IIoT вимагатиме від них встановлення додаткових заходів захисту.

На даний момент багато пристроїв IIoT не мають достатнього захисту. Тому для LAN IIoT пріоритетом безпеки є захист усіх пристроїв від несанкціонованого доступу та навіть від злому.

Друга потенційна вразливість заводів-виробників IIoT – це зростання обміну даними між мережами пристрою та об'єктів IIoT. У міру зростання кількості інтелектуального обладнання збільшується кількість захисних споруд, які необхідно побудувати. Несправність обладнання або відмова в обслуговуванні можуть призвести до витоку конфіденційних даних.

Мережеве обладнання може бути атаковане, коли воно не налаштоване належним чином, якщо воно залишене відкритим або використовує неправильні

методи аутенфікації. Саме тому необхідно захищати всі порти та канали передачі даних від хакерів та інших зловмисників.

Незважаючи на те, що деякі аспекти IIoT вказують на збільшення автоматизації в деяких аспектах, все ж таки є технічні фахівці та менеджери, які відповідають за обладнання. Саме вони є основними цілями кібер злочинців.

За відсутності чіткої роздільної здатності кінцевих точок та вбудованої багатофакторної аутенфікації в мережі пристроїв IIoT, ваша мережа пристроїв IIoT може бути ломана. Однак, на відміну від галузі роздрібної торгівлі, яка спеціалізується на безпеці POS та виробництві продукції з високим ступенем захисту, управління кінцевими точками має бути зосереджено на забезпеченні максимальної безпеки продукції.

На даний момент існує проблема з тим, що бездротовий зв'язок недосконалий. Відсутність покриття може призвести до того, що дані будуть неточними або взагалі відсутніми. Якщо у користувача-людини буде поганий зв'язок, то це може призвести до невдоволення клієнтів та негативних відгуків. Якщо надалі додатки стануть все більш поширеними та залежними, ціна та наслідки “помилки” будуть дедалі вищими.

У нашій країні є безліч операторів, які надають послуги стільникового зв'язку та смуги обслуговування. З цієї причини, якщо смуга буде маленька або її зовсім немає, то і бездротові додатки не працюватимуть належним способом або без покриття - зовсім перестануть бути доступними.

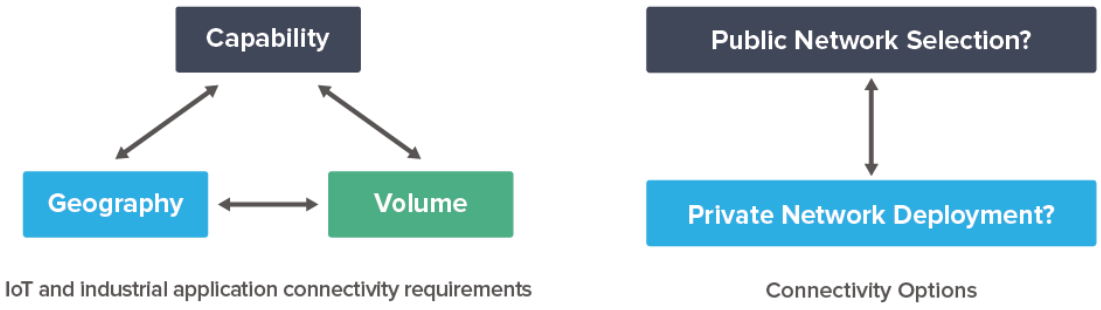

Рисунок 1.3 – Вибір правильного оператора зв'язку

Ще більш незрозумілою є та обставина, що відбувається з тими додатками, які мають можливість використовувати мережу одночасно у всіх місцях. Швидкість обробки даних падає через те, що мережа перевантажується, і продуктивність даних зменшується - нижча пропускна здатність означає нижчу швидкість реакції додатків або, таких додатках як відео, недостатній обсяг даних.

Автоматизація промислового Інтернету речей і роботизована промисловість включає широкий спектр додатків та сценарних варіантів застосування - від масового розгортання датчиків або лічильників з періодичними потребами у підключенні до автоматизації, що потребує безперервного високопродуктивного з'єднання.

Отже, різні галузі мають різні проблеми, вирішення яких потребує нових підходів. Також необхідно враховувати специфіку роботи в даній сфері та особливості продукту, який ви маєте намір продавати. Наявність бездротового зв'язку є важливим внеском, який вносить розуміння, як працює технологія бездротового зв'язку в промисловому IOT.

1.2 Типи бездротових технологій промислового Інтернету речей

IoT – це багаторівнева система, в якій є багато різних варіантів підключення до інтернету. Кожна з них має свої сильні сторони і може бути використана у різних сценаріях використання Інтернету речей.

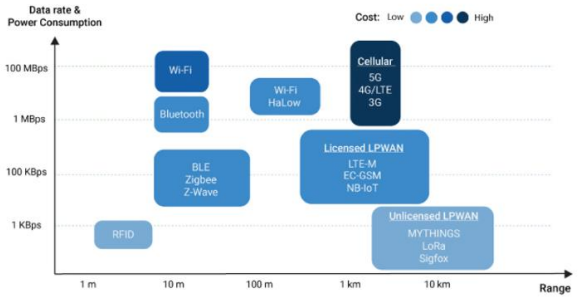

Рисунок 1.4 – Швидкість передачі даних і енергоспоживання

1.2.1 LPWAN

На сьогоднішній день існує безліч LPWAN мереж, які мають низькі енергоспоживання та є новим явищем у IoT. Завдяки використанню сучасних технологій, що забезпечують зв'язок на відстані від невеликих недорогих батарей, термін служби яких становить роки, ця група технологій спеціально створена для того, щоб підтримувати великі мережі IoT, що охоплюють великі промислові та комерційні міста.

Для виконання багатьох завдань, таких як моніторинг довкілля та управління об'єктами, використовують LPWAN, тому що він дозволяє підключати всі типи датчиків IOT. З іншого боку, це може бути пов'язане з тим, що LPWAN може надсилати лише маленькі блоки даних з низькою швидкістю і тому він краще підходять для випадків, де потрібна висока пропускна здатність і не залежить від часу.

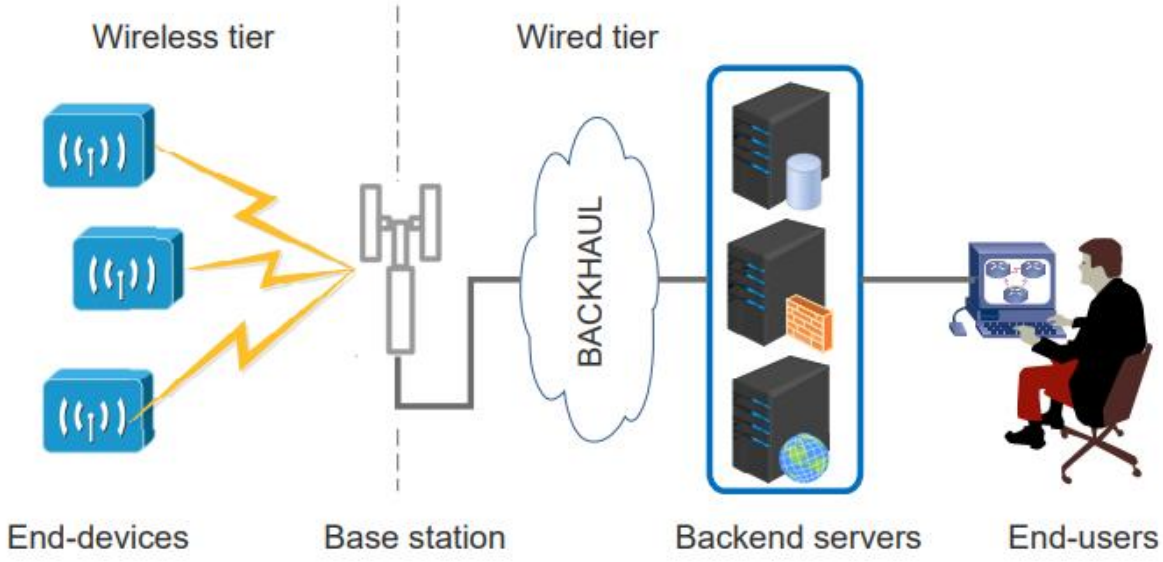

Рисунок 1.5 – Загальна архітектура мережі LPWAN.

Неліцензійний Sigfax є однією з найпопулярніших мереж LPWAN. При роботі з мережею Інтернет у діапазонах 868 та 902 МГц, оператор може бути лише один. Він здатний передавати повідомлення на відстань 30-50 км у сільських чи міських умовах, а також до 1500 повідомлень на день по 12 байт на годину.

Зменшення кількості пакетів вихідних каналів відбувається за рахунок обмеження чотирьох повідомлень по 8 байт на день. За допомогою цієї технології можна передавати дані на кінцеві точки, але при цьому вони можуть бути піддані впливу перешкод та збоїв.

Не всі LPWAN однаково гарні. Наприклад, сьогодні є такі технології, які працюють як на ліцензованому (NB-IOT, LTE-M), так і в неліцензійному (наприклад, MYTHINE, LoRa, SigFox і т.д.) спектрі з різним ступенем ефективності за ключовими факторами мережі. Наприклад, тоді як енергоживлення стає серйозним викликом для ліцензованих мереж LPWA на базі стільникового зв'язку. Одним з основних факторів, що впливають на вибір компанії-постачальника ліцензійного програмного забезпечення, є якість обслуговування та масштабованість. Ще один важливий фактор, який необхідно врахувати при виборі системи безпеки – це стандартизація.

Можливість доступу довільної фази або RPMA — це пропрієтарний протокол, розроблений компанією Ingenu Inc. У порівнянні з Sigfox, він має меншу дальність дії (50 кілометрів у прямому напрямку та 5-10 кілометрів поза прямою видимістю) і забезпечує кращий двонаправлений зв'язок.

У LoRa Alliance є ліцензія на використання LoRa, яка дозволяє передавати дані на субгігагерцових частотах, що робить його менш схильним до перешкод. Завдяки CSS (модуляція з розширеним спектром частот) LoRa може визначити розміри пакетів, які були отримані. Базовий чіп, використаний для реалізації LoRa, доступний лише Semtech Corporation, компанії-розробнику технології. У протоколі рівня керування доступом до середовища (MAC) LoRaWAN, що управляє з'єднанням пристроїв LPWAN та шлюзів, є можливість передавати дані з одного пристрою на інший.

В рамках проекту Weightless SIG було створено три стандарти LPWAN: Weightless-N, Weightless-P та Weightless-W. Вони теж є двонаправленим і працює у не використовуваному ТВ-спектрі. Weightless-N та Weightless-P найчастіше використовуються для роботи протягом дня, вони мають більш короткий термін автономної роботи. У режимі роботи з діапазоном, що не ліцензується, Weightless-

N і Weightless-P мають можливість працювати на частоті до 1 ГГц, але також можуть підтримувати роботу в ліцензованому діапазоні з використанням широкосмугової технології 12,5 кГц.

Стандарти Партнерського проекту 3GPP, що працює у ліцензованому спектрі, були розроблені компанією Narrowband-IoT (NB-IoT). Вони мають продуктивність, порівнянну з іншими стандартами, що дозволяє постачальникам послуг швидко підключати їх до стільникового Інтернету речей у своїх портфелях послуг.

Також відомо, що NB-IoT, розроблений компанією CAT-NB1, може працювати на існуючій інфраструктурі LTE та світової мережі мобільного зв'язку (GSM). У його розпорядженні є швидкість висхідного каналу близько 200 кбіт/с, а також використовується лише 200 кГц доступної смуги пропускної спроможності.

У LTE-M, також відомому як CAT-M1, швидкість передачі даних вище, ніж у NB-IoT, а також найвища швидкість передачі даних з усієї LPWAN. Деякі компанії-постачальники (наприклад, Orange або SK Telecom) проводять роботи з розгортання як ліцензійних, так і неліцензованих технологій для захоплення обох ринків.

LPWAN включає й інші технології:

- WAVIoT
- ThingPark Wireless від Actility
- Symphony Link від Link Labs Inc.
- DASH7 від компанії Haystack Technologies Inc.
- GreenOFDM від GreenWaves Technologies
- Ultra Narrow Band від компаній Telensa, Nwave та Sigfox

Через менші вимоги до живлення та менший радіус дії LPWAN дозволяє використовувати ряд програм M2M та IoT, деякі з яких раніше були обмежені бюджетом або проблемами з харчуванням.

Вибір LPWAN залежить від конкретної програми, яка має бути максимально швидкою, об'ємною та з максимальною площею покриття. Якщо ви хочете отримати компактніші повідомлення по вихідній лінії зв'язку, то LPWAN - це ваш

варіант. Завдяки цим можливостям багато технологій LPWAN також мають можливість низхідного каналу. LPWAN використовуються для додатків, пов'язаних з інтелектуальною діяльністю (наприклад, таких як інтелектуальне освітлення, моніторинг та відстеження активів, інтелектуальні міста, точне сільське господарство, контроль енергоспоживання, виробництво та промислові розгортання IoT).

1.2.2 Стільниковий зв'язок (3G/4G/5G)

Якісний мобільний зв'язок з підтримкою різних програм для голосових дзвінків та потокового відео – це стільникові мережі, які добре зарекомендували свою роботу на споживчому ринку мобільного зв'язку. Вони також пред'являють високі експлуатаційні витрати та вимоги до потужних характеристик.

Крім того, стільникові мережі не підходять для більшості програм IoT, що працюють від сенсорного живлення, але вони добре справляються з завданнями, пов'язаними з керуванням парком транспортних засобів та логістики. Також можна відзначити, що в даний час автомобілісти мають можливість користуватися послугами мобільної інформаційно-розважальної системи, маршрутизації трафіку, розширених систем допомоги водієві (ADAS).

Завдяки новій технології бездротового зв'язку, яка була представлена компанією МТС у рамках презентації «5G», стільниковий зв'язок нового покоління 5G з високою швидкістю передачі даних та наднизьким рівнем затримки позиціонується як майбутнє автономних транспортних засобів та доповненої реальності. Вже відомо про те, що 5G забезпечуватиме спостереження за суспільною безпекою в режимі реального часу для підключення медичного обслуговування, а також низку інших корисних функцій, які будуть доступні в майбутньому.

Завдяки тому, що стільниковий Інтернет – найпоширеніший тип підключення до Інтернету речей, він і є найпопулярнішим, тому що:

- Чудова якість покриття.

- Спрощення глобального розгортання.
- Працює без попереднього налаштування, відразу з коробки
- У разі встановлення з'єднання з іншими мережами воно буде безпечніше, порівняно з іншими
- Має хорошу роботу в мобільному, внутрішньому та зовнішньому застосуванні
- Забезпечує низьку та високу швидкість

Також як телефони та інші мобільники, стільниковий Інтернет речей як передачу та прийом даних використовує технологію 2G, 3G, 4G, 5G, LPWAN, LTE-M - технологій. За допомогою таких бездротових технологій можна підключити будь-який пристрій до мобільного Інтернету. Завдяки LPWAN виробники можуть збільшити покриття, підтримувати стабільні з'єднання на місці та оптимізувати час автономної роботи своїх систем IoT.

Одним з найнадійніших і доступних способів підключення до Інтернету для виробників, що створюють пристрої Інтернету речей, є стільниковий Інтернет речей. Крім цього, вам необхідно буде ще щось розпакувати в процесі використання стільникового Інтернету речей, а також вам потрібно знати безліч скорочень.

Компанія-постачальник комунальних послуг встановлює на своїй території інтелектуальні лічильники та слідкує за споживанням ресурсів у режимі реального часу. За допомогою стільникового Інтернету речей можна вирішувати безліч завдань, пов'язаних з використанням його як засіб зв'язку. Використовується він скрізь – починаючи з безпілотників і закінчуючи інтелектуальними парковками, автономним сільськогосподарським обладнанням та споживчими пристроями, такими як розумний годинник. Насправді, стільниковий Інтернет речей настільки широко поширений і його використання не залежить від наявності надійного з'єднання, що, швидше за все, він покладається на стільниковий зв'язок.

Однак у вужчому сенсі стільниковий Інтернет речей ідеально підходить як інструмент для логістики (виробництва), так і для відстеження активів (управління ланцюжками постачання, служби екстреної допомоги, охорони здоров'я та

безпеки). На сьогоднішній день стільникові пристрої IoT можуть передавати або приймати сигнали з будь-якої точки світу в будь-яке інше місце. Завдяки тому, що оператори мобільних мереж (MNO) вже побудували великі мережі, призначені для максимального охоплення, стільниковим зв'язком можна буде скористатися практично в будь-якому місці. Мережеве обладнання 5G дозволяє здійснювати передачу даних бездротового зв'язку в реальному часі, на високій швидкості.

Найбільшим обмеженням мобільного зв'язку завжди був час автономної роботи, енергоспоживання та автономність у роботі. Тому стільникові пристрої Інтернету речей економлять електроенергію під час використання їх як бездротових пристроїв передачі невеликих пакетів даних без споживання великої енергії.

Technology	Frequency	Data rates	Range	Power consumption	Use cases
Bluetooth	< 1 GHz	.1 – 1 MBps	tbc		Industrial IoT
Wi-Fi				Medium	Smart home uses
ZigBee					Smart home uses
2G	Cellular bands	±10 MBps	Several km	High	Logistics, supply chain
3G	Cellular bands		Several km	High	Smart grids, connected consumer devices, logistics
4G	Cellular bands		Several km	High	Healthcare, security
5G	Cellular bands		Several km	High	Emergency services, connected cars
NB-IoT	Cellular bands	250 KBps	Several km	Low	Smart meters, Asset tracking
LTE-M	Cellular bands	1 MBps	Several km	Low	Asset tracking

Рисунок 1.6 – Технології та їх характеристики

Основу становлять кілька ключових компонентів: це оператор мобільного зв'язку, який надає послуги мобільного зв'язку, та обладнання, яке забезпечує

зв'язок. Для того щоб детальніше вивчити можливості сучасних стільникових IoT, вам необхідно ознайомитися з такими базовими поняттями, такими як сім-карти, модеми, діапазон частот та класифікації мобільних мереж (2G, 3G, 4G, 5G, NB-IoT, LoRaWAN).

IoT SIM-карти

Смартфони та інші мобільні пристрої потребують SIM-карти для підключення до мережі. Однак на відміну від вашого смартфону ви не бажаєте, щоб ваш IoT-пристрій був обмежений в будь-якій стільникової компанії. Якщо Ваша SIM-картка працює тільки від мережі Vodafone або Київстару, то радіус дії Вашого пристрою не перевищує зони покриття цих провайдерів.

Як наслідок, це одна з причин, через яку надмірність така важлива для стільникових IoT. Незалежно від того, який стільниковий оператор використовуватиметься для підключення до інтернету речей (SIM-картки), виробники повинні передбачати можливість використання SIM-карток, що працюють у будь-якій стільниковій мережі. З цієї причини такі пристрої можуть бути підключені до будь-якої мережі, що має кращу якість покриття в даній області, і гарантувати, що якщо одна з мереж вийде їх ладу або раптово зникне зона покриття, пристрій буде продовжувати працювати через іншу мережу.

Модеми, модулі та чіпсети

Якщо ви вибираєте SIM-карту, визначальну до якої мережі можна отримати доступ з вашого пристрою, то вибраний вами модем впливає не тільки на типи мереж та діапазони частот для підключення вашого пристрою, але й на типи та діапазони частот, до яких можуть підключатися ваші пристрої. І хоча використання модему спрощує процес розробки та сертифікації IoT, він обходиться значно дорожче за покупку вихідних компонентів, необхідних для побудови індивідуальнх рішень.

Смуги частот

Діапазон частот - це радіочастотна (RF) смуга, яка становить від 30 герц (Гц), і до 300 гігагерц (ГГц). При використанні частини діапазону від 800 МГц до 5 ГГц для з'єднань 2G, 3G та 4G стільниковий зв'язок використовує частину спектра від

800 до 5 ГГц. До 35 ГГц можуть бути використані діапазони частот, які використовуються у стандарті стільникового зв'язку п'ятого покоління (5G).

У кожній мережі є кілька діапазонів частот, які використовуються для різних операторів і країн. Тільки в рамках 4G є 27 різних частот.

Пристрій може працювати тільки в діапазонах частот, на підтримку яких він сертифікований. Дуже важливим є питання, який саме оператор стільникового зв'язку буде обраний вами для розгортання мережі, тому необхідно врахувати всі можливі варіанти.

Не слід забувати і про умови експлуатації пристрою. Низькі частоти мають більш широке охоплення, що підвищує діапазон роботи вашого пристрою. Також у меншій кількості випадків будівлі та тунелі заважатимуть передачі сигналів на низьких частотах. Це з тим, що у містах, де низькі частоти використовуються більше пристроїв передачі і вони мають велику пропускну спроможність.

І тут можна буде користуватися кількома діапазонами. Багато сучасних пристроїв мають можливість працювати з різними мобільними мережами – наприклад, з такими як NB-IoT та LTE-M, в яких є модем, що працює глобально у всьому діапазоні частот.

Глобальне покриття

На сьогоднішній день стільниковий зв'язок M2M є найнадійнішим і найвигіднішим способом для організації масштабних міжнародних мереж. У вас немає необхідності в створенні нової інфраструктури, яка була створена для кожного нового розгортання - вам достатньо підключити існуючу мережу. Зі збільшенням кількості нових країн, які будуть охоплені мережею стільникового зв'язку, ваш оператор стільникового зв'язку може укласти угоду про роумінг з іншим мобільним оператором, який обслуговує цей регіон. У разі відсутності, ви можете скористатися послугами місцевого оператора, але потім вам доведеться скоригувати транспортний процес, щоб переконатися, що необхідна SIM-картка потрапляє до потрібного міста.

Ймовірно, стільниковий зв'язок – це WAN (глобальна бездротова мережа) з можливістю підключення на великі дистанції по всьому світу за допомогою радіо

сплесків, які надсилаються і приймаються через вежі стільникової мережі. Щоб підключити Wi-Fi, вам необхідно буде знаходитися в безпосередній близькості до точки доступу або маршрутизатора, що дозволить уникнути мобільності на великі відстані. Як і у випадку з WiFi, Bluetooth-з'єднання також розташоване на невеликій відстані від точки доступу, що вимагає, щоб ваш пристрій знаходився в межах десяти – ста метрів від точки доступу, залежно від класу потужності.

Вбудована аутентифікація та безпечне підключення

Для аутентифікації в стільникових мережах SIM-картка використовується для з'єднання пристрою із законним абонентом та забезпечення безпечного зв'язку. Якщо хакер зможе підробити IP-адресу, то він не зможе підробити і особистість абонента, який знаходиться на SIM-карті.

Під час роботи з пристроєм, підключеним до Wi-Fi клієнта, він використовує підключення до всіх інших мереж Wi-Fi. Небезпеку представляють не тільки самі ці пристрої (наприклад, якщо вони мають проблему з безпекою), але й їхні власники (наприклад, якщо вони мають проблеми з безпекою). Всі пристрої знаходяться в ізольованому приміщенні і не пов'язані з іншими пристроями, які підключені до Інтернету. Вам надається ряд переваг у сфері безпеки під час використання стільникового зв'язку. Це мережа Інтернет та можливість підключення до неї ваших пристроїв, які мають вихід до Інтернету.

Типи мобільних мереж, які використовує стільниковий IoT

З часом, мобільні оператори стали більш швидкими та потужними. Як правило, виробники обладнання для Інтернету речей мають можливість вибирати між потужністю та швидкістю, але це не є головним фактором, який необхідно враховувати. Пізніші моделі стільникових мереж можуть означати більше енергоспоживання, але менше покриття. Мережа карта, яка використовуватиметься для підключення до комп'ютера, вплине на радіус дії пристрою, зону покриття, частоту використання, а також ціну та термін служби.

Але навіть ті з вас, хто чув термін мережі 2G, 3G або 4G, не знають відмінності між ними. В даний час для задоволення потреб більшості стільникових пристроїв IoT існують інші типи мереж, які не так добре знайомі, як NB-IoT та

LoRaWAN. Звичайно ж, це не так. Чим вище розвинена мережа і що більше вона споживає енергії від підключених пристроїв, тим менше енергії споживатимуть на завантаження чи розвантаження великих обсягів даних. Для того щоб зробити мережу складнішою, в ній можуть використовуватися більш дорогі модеми.

Мережі 2G

Близько трьох десятків років тому з'явилися мобільні мережі другого покоління (2G). Саме на цьому фундаменті і був побудований весь наш мобільний зв'язок. За допомогою стандарту стільникового зв'язку 2G дав можливість людям передавати текстові повідомлення, графічні повідомлення, а також мультимедійні повідомлення.

На сьогоднішній день у стільниковому зв'язку 2G відмінно себе зарекомендували як для передачі даних логістики, телеметри, управління ланцюжками поставок, так і для передачі базових оповіщень, оновлень статусу та даних про місцезнаходження за дуже низької енерговитрати.

Мережі 2G незабаром зникнуть. Для того щоб звільнити пропускну спроможність для мереж 3G та 4G оператори стільникового зв'язку почали відключати мережі 2G, щоб звільнити пропускну спроможність для мережевих операторів 4G та 5G. Багато компаній стільникового зв'язку вже припинили свою роботу, а деякі навіть закрили свої мережі. Незважаючи на те, що оператори відмовляються від своїх мереж 2G, пристрої інтернету речей, які від них залежать, будуть застарілими, якщо вони не будуть сумісними з іншими мережами.

Мережі 3G

Нові стільникові оператори 3G, які використовують технологію 2G для передачі даних, надають швидше передачу даних і дозволяють смартфонам безпосередньо з'єднуватися з інтернетом. Однак у цьому випадку мережа 3G споживає на 50 відсотків більше електроенергії, ніж мережа 2G.

Як і 2G, 3G використовувався для таких речей, як логістична діяльність, тематика та управління ланцюжків постачання. Завдяки технології UMTS, 3G може спростити складніші процеси, такі як спільне використання файлів, потокова передача, аналітику та віддалене керування пристроями. У цьому він був ідеальним

для споживачів, які мають можливість користуватися Інтернетом речей та інтелектуальними мережами.

Незабаром буде перехід на 3G, але це може статися вже найближчими роками. На даний момент існують програми IoT, створені у всіх мережах 3G, але багато компаній-виробників обладнання для мереж 3G задумалися про те, щоб їх обладнання використовувало 4G або глобальні мережі з низьким енергоспоживанням (LPWAN).

Мережі 4G LTE

Дальність зв'язку за допомогою 4G LTE (довго рядкова еволюція) становить більш ніж у 10 разів більше, ніж 3G, і це найшвидша у світі технологія мобільних мереж. Завдяки технології 4G LTE можна передавати голосові виклики з низькою пропускною здатністю (це називається «голосовий зв'язок на перспективу») та забезпечувати систему замкнутого телебачення (CCTV).

Крім цього, завдяки можливості вивантаження та завантаження даних у кілька разів швидше за 4G LTE вони відмінно працюють для передачі відео, таких як камери безпеки. Завдяки цьому його використовують у багатьох галузях медицини, а також автоспорту. За допомогою підключення до мережі 4G інженери можуть передавати величезні обсяги інформації від автомобілів на комп'ютери.

На даний момент у більшості випадків для підключення 4G LTE використовується потужніша енергія від мережі, ніж потрібна більшість процесів IoT (на 50 відсотків більше, ніж при підключенні 3G). Однак ряд функцій енергозбереження може зробити його придатним для життя.

Мережі 5G

Вже сьогодні, 5G – це майбутнє Інтернету технологій та інтернету речей. Проте зараз інтернет-технології розвиваються не так активно, як це було раніше, тому мережа 5G ще не має широкого поширення на території України. З урахуванням того, що у 2025 році вони становитимуть лише близько 15 відсотків від загальної кількості мобільних телефонів у всьому світі.

Завдяки цьому ця технологія може бути використана як основа для створення мереж Інтернет речей, які будуть використовуватися для мобільного додатка з

інтенсивним використанням даних, таких як безпілотні автомобілі та служба екстреної допомоги. На сьогоднішній день мережа 5G може запропонувати можливість передачі даних практично в реальному часі та підтримує стабільне з'єднання з пристроями, що рухаються на дуже високих швидкостях. Однак у мережах 5G можна використовувати менше енергії, ніж у мережах 3G.

Як правило це пов'язано з тим, що в даний час існують дуже мало моделей, які могли б зробити можливим підключення до 5G. Однак у зв'язку з тим, що оператори поступово відмовляються від своїх мереж двох і трьох G і переходять на економніші мережі, це не означає, що виробники інтернету речей повинні вибирати між надто великим енергоспоживанням і надто малим покриттям. Нові рішення для задоволення потреб користувачів Інтернету речей з'явилися у стільниковому зв'язку.

Narrowband-IoT (NB-IoT)

За допомогою широкосмугового Інтернету технологій, який використовують прогалини в радіочастотному спектрі, для того, щоб зробити більш ефективним зв'язок і запобігти перешкодам. Такі незаповнені ділянки, відомі як «захисні смуги», використовуються передачі сигналів. За допомогою широкосмугових з'єднань, таких як 4G LTE, ізолюють пристрої до менш вузьких діапазонів.

Вузько смуговий Інтернет речей пропонує дві основні функції енергозбереження: режим енергозбереження, який полягає в тому, що він дозволяє заощаджувати електроенергію, та переривчастий прийом (DRX), який дозволяє заощаджувати електроенергію. Загалом це означає, що DRX дозволяє продовжити час, протягом якого пристрій не «працює», і тим самим продовжити період часу, протягом якого воно не «активно слухає» сигнал. За допомогою таких пристроїв, які використовують NB-IoT, можна працювати від батареї до року. Але оскільки в ньому використовується технологія NB-IoT, його можна використовувати і для Інтернету. Немає потреби в різних модемах для різних областей. Тому глобальне підключення – це недорого.

NB-IoT ідеально підходить для використання всередині приміщень або на теренах, де велика кількість підключених пристроїв. Також часто його

використовують при створенні систем контролю за активами (наприклад, таких як розумні лічильники), програм розумного міста (наприклад, розумних світлофорах) та систем сигналізації, де передача даних відбувається переривчаста і не вимагає високих швидкостей завантаження/вивантаження.

Long term evolution (LTE-M)

Технологія LTE-M (скорочена від довгострокової еволюції машинного зв'язку) була розроблена спеціально для Інтернету речей. Пристрої з підтримкою технології 4G можуть бути використані для підключення пристроїв IoT до мереж 4G, що надають їм більшу пропускну спроможність та мобільності, ніж NB-IoT, а також доступ до голосового зв'язку в довгостроковій перспективі (VoLATE) – більш просунутій голосовій службі. Для цього використовуються дорожчі модеми, які споживають більше енергії, ніж звичайні модеми, а також енергоспоживання в режимі очікування.

Завдяки більш високому споживанню енергії, LTE-M, як і раніше, може використовувати PSM і DRX, щоб значно продовжити термін служби батареї смартфона, дозволяючи йому добре працювати в багатьох додатках, які використовуються для роботи з LTE-M.

Чим більше інформації потрібно передати або отримати в більшому обсязі, LTE-M споживає менше енергії, ніж NB-IOT, тому що більш висока пропускна здатність дозволяє йому завантажити та вивантажити інформацію набагато швидше. Це сприяє тому, що пристрої з підтримкою IoT будуть "орієнтовані на майбутнє", оскільки оновлення мікропрограм може вводити нові функції, які потребують більшого споживання даних.

1.2.3 Zigbee та інші протоколи Mesh

«Zigbee» — це малопотужний стандарт бездротового зв'язку малого радіусу дії (IEEE 802.15.4), що використовується в топології сітки для розширення зони покриття шляхом ретрансляції даних датчиків по кількох вузлах, розташованих на одному кінці датчика. Однак Zigbee має вищі швидкості передачі даних, ніж

LPWAN, але при цьому значно меншу енергоефективність через конструкцію комірчастої мережі.

За Zigbee відповідає стандартна функціональність бездротової сенсорної мережі, яка потребує високої надійності, низької вартості, споживання, а також низької швидкості передачі даних. На початку 1990-х років у рамках проекту «ZigBee» створювалися спеціальні цифрові радіомережі, які мали бути створені в стилі ZigBee та відповідати вимогам стандарту IEEE 802.15 для спеціальних цифрових радіомереж. З цього моменту протягом півроку ZigBee Alliance публікує Специфікацію 1.0 (13 червня 2005 року).

До складу WSN входить недорогий бездротовий датчик, здатний збирати, зберігати, обробляти інформацію про навколишній світ та обмінюватися даними із сусідніми пристроями. Наприклад, будинок в якому знаходиться WSN може бути використаний для управління освітленням, опалення, вентилювання та кондиціювання повітря (HVAC), спостереження за безпекою та виявлення надзвичайних ситуацій. Як приклад можна навести промисловий контроль, який можна використовувати для поліпшення існуючої системи управління виробництвом, виявлення нестабільних ситуацій, управління виробничими процесами тощо.

Завдяки адаптивному робочому процесу, низької швидкості передачі та радіозв'язку зі слабким покриттям, ZigBee забезпечує наднизьку споживану та ефективну роботу (завдяки адаптованому до робочого процесу, низькому швидкісному каналу та радіозв'язку з низьким покриттям)

Standard	ZigBee/IEEE 802.15.4	Bluetooth	UWB	IEEE 802.11 b/g
Working frequency	868/915 MHz, 2.4GHz	2.4 GHz	3.1 - 10.6 GHz	2.4 GHz
Range (m)	30 – 75+	10 – 30	~10	30 – 100 +
Data rate	20/40/250 kbps	1 Mbps	100+ Mbps	2 – 54 Mbps
Devices	255 – 65k	8		50 – 200
Power consumption	~1 mW	~40 – 100 mW	~80 – 300 mW	~160 mW – 600W
Cost ($US)	~2 – 5	~4 – 5	~5 – 10	~20 – 50

Рисунок 1.7 – Характеристики технологій

Одним із основних напрямків діяльності альянсу ZigBee є розробка проблем взаємодії стеку протоколів IEEE 802.15.4/ZigBee. Є три рівні членства: "Приймач", "Учасник" або "Промоутер".

Приймач надає можливість користуватися остаточними специфікаціями, використовувати логотип Zigbee Member, брати участь у заходах щодо сумісності, семінару та конференції розробників.

Учасник надає повну свободу у роботі комітетів та робочих груп, а також у робочих нарадах за участю представників Альянсу. На даний момент учасники мають право голосу в робочих групах і можуть отримати ранній доступ до всіх стандартів та нормативних актів компанії Zigbee Alliance, що розробляються.

Промоутер дає можливість усім членам робочої групи, а також право остаточного затвердження всіх стандартів та місце серед членів Ради директорів Альянсу.

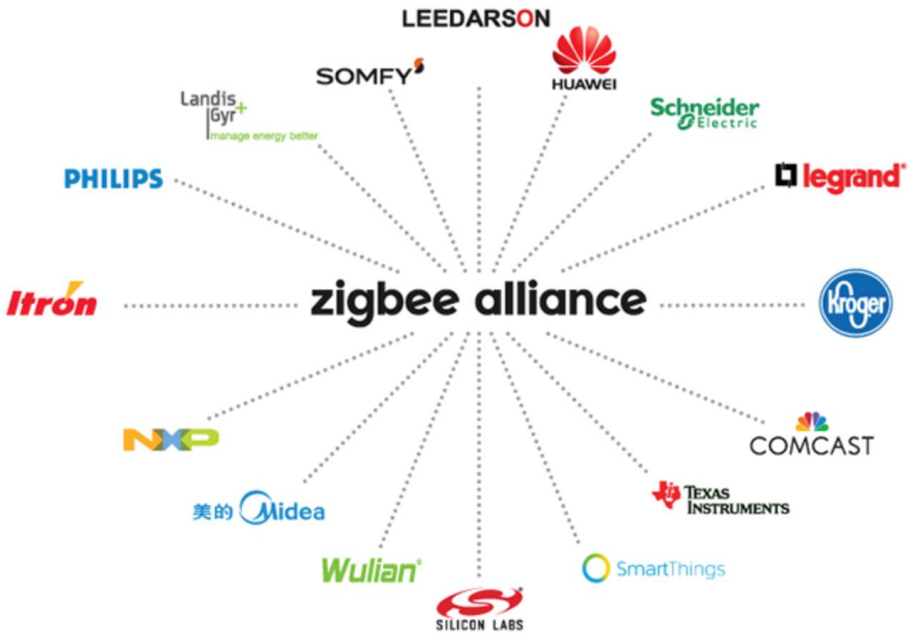

Рисунок 1.8 – Альянс ZigBee

Перед тим, як перейти до більш детального розгляду ZigrBee, ми повинні ознайомитися зі стандартом IEEE 802.15.4. Він визначає протоколи фізичного та канального рівнів для низько швидкісної бездротової персональної мережі (LR-WPAN), він був затверджений у 2003 році.

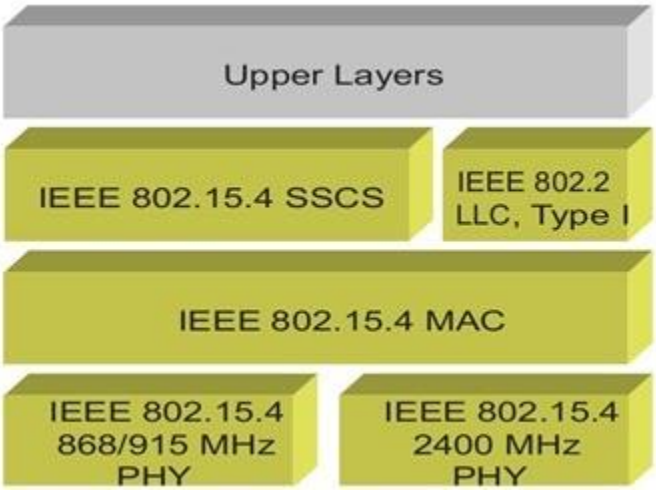

Рисунок 1.9 – Шари ZigBee

Ці пристрої можна класифікувати як повнофункціональні та обмежені функції (FFD) та пристрої, які мають обмеження за функціональністю (RFD). Щоб керувати мережею, координатор PAN, який відповідає за обслуговування мережі та керування іншими пристроями, повинен бути призначений координатором PAN, який відповідає за обслуговування мережі та керування іншими пристроями. Також він вказує на два типи мережевої топології: зоряну топологію і однорангову топологію.

У структурі «зірка» є центральний вузол, який координує мережу. Одна з особливостей такої мережі полягає в тому, що вона може утворювати довільні схеми підключення та розширюватись до будь-яких меж, які існують на сьогодні. Вона може передавати інформацію по каналу 868 МГц у Європі, 916 МГц в Америці з Австралією та 2400 МГц у всьому світі.

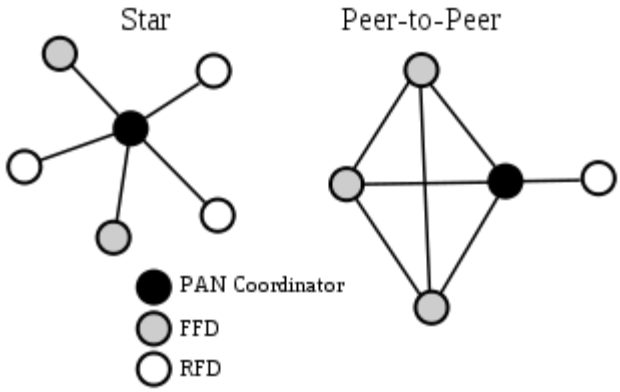

Рисунок 1.10 – Структура «зірка» та «один до одного»

У пристроях встановлені три різні режими: передача, прийом та сон. Цей спосіб економить електроенергію щодо робочих циклів і пристрої в сплячому режимі. Як і у випадку з іншими моделями, він характеризується якістю/потужністю отриманого сигналу каналу - Link Quality Indication (LQI)

Рівень передачі між вузлами мережі встановлює, що MAC-рівні містять структуру супер кадру. Координатор мережі визначає час між двома маяками, встановленими в момент запуску. По активності супер кадр ділиться на активний (робочій) і пасивний (сон). Це допомагає заощаджувати енергію у неактивні періоди. Крім того, на них встановлюються маяки інших пристроїв, які можуть бути синхронізовані з іншими пристроями, також повідомляється про очікування даних в координаторах.

Стандарт IEEE 802.15 дозволяє використовувати протокол ZigBee для перших двох рівнів та додає поверх протоколу структуру. Яка є надійною та безпечною для передачі між пристроями, яка забезпечується мережевим рівнем.

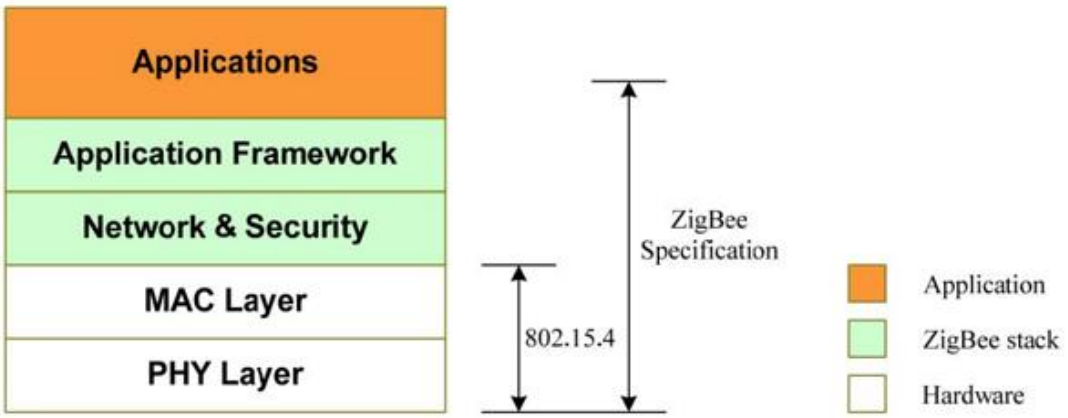

Рисунок 1.11 – Структура рівнів протоколу ZigBee

Залежно від того, які пристрої використовуватимуться, формуються три типи пристроїв:

- ZigBee Coordinator: Містить у собі всі функції обслуговування мереж, а також контролю їх роботи. І лише в одній мережі

- ZigBee Router: Підключається до координатора або інших маршрутизаторів. Його можна зробити нульовим, а також утримувати в ньому один або кілька дочірніх вузлів. Бере участь у якісній маршрутизації
- ZigBee End Devices: Не входить до складу маршрутної мережі

Є три типи топології мережі: зірка, дерево та мережа. У ZigBee немає зіркової топології, тому він не може бути використаний як маршрутизатор. Крім того, у ZigBee є лише один оператор – це координатор ZigBee.

У випадку топологічної структури дерева або кластерного дерева координатором ZigBee, а також маршрутизатор ZigBee може бути оголошений маяк. Маршрутизатор ZigBee визначає динамічний робочий цикл кожного кластера, що дозволяє пристроям переходити в сплячий режим без участі координатора. За допомогою пристрою буде вибрано лот, який передає свій маячок, щоб уникнути колізії. У цьому випадку забезпечується гарантована пропускна здатність (GTS).

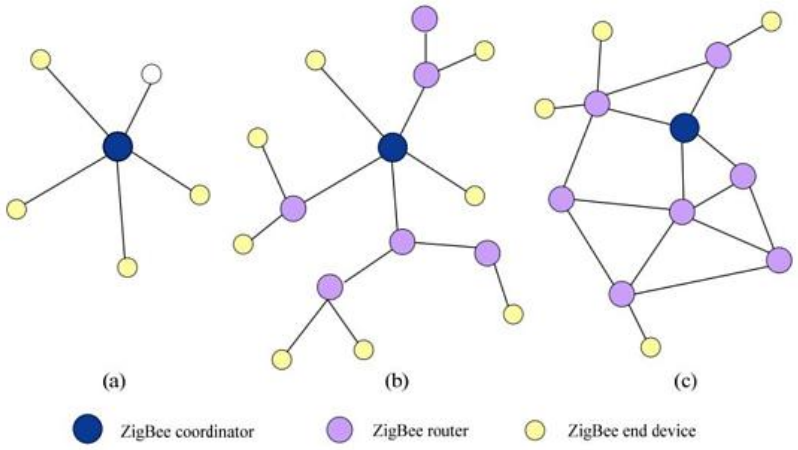

Рисунок 1.12 – Типи пристроїв та їх структура

І нарешті, у комірчастій топологічній структурі немає синхронізації, отже, немає режиму включення маяка, який означає, що маршрутизатори ZigBee повинні бути завжди включеними. Через те, що мережа перевантажена, не завжди можна гарантувати пропускну здатність.

	Pros	Cons
Star	1. Easy to synchronize 2. Support low power operation 3. Low latency	1. Small scale
Tree	1. Low routing cost 2. Can form superframes to support sleep mode 3. Allow multihop communication	1. Route reconstruction is costly 2. Latency may be quite long
Mesh	1. Robust multihop communication 2. Network is more flexible 3. Lower latency	1. Cannot form superframes (and thus cannot support sleep mode) 2. Route discovery is costly 3. Needs storage for routing table

Рисунок 1.13 – Переваги та недоліки структур Star, Tree, Mesh

Програма Zigbee 3.0 розроблена для передачі даних через гучну радіочастоту, яку можна зустріти на більшості сучасних підприємств. Нова версія версії 3.0 була створена на основі існуючого стандарту Zigbee, але уніфікувала профілі додатків для конкретних ринків, які можуть бути використані для підключення до бездротової мережі, незалежно від їхнього ринкового призначення та функцій.

Окрім того, схема сертифікації ZigBee 3.0 гарантує сумісність продукції від різних виробників. Забезпечується доступ до всіх пристроїв через мережу Zigbee 3.0. Це дає можливість здійснювати моніторинг та керування таких пристроїв як: смартфони та планшети, у локальній або глобальній мережі інтернет.

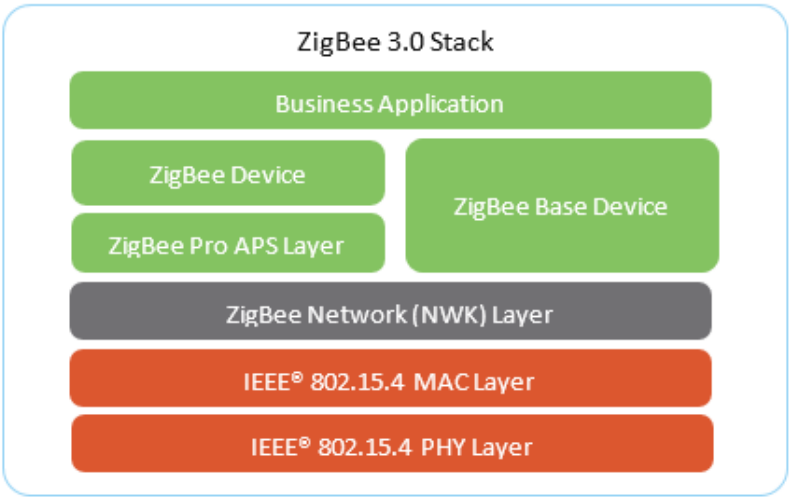

Рисунок 1.14 – Стек технологій ZigBee 3.0

Функції протоколу Zigbee включають:

- Підтримка багатьох мереж, таких як точка-точка та інші.
- багато точкові та комірчасті мережі
- Низький робочий цикл – тривалий термін служби батареї
- Відсутність затримок
- Спектр поширеності DSSS до 65000 вузлів у мережі
- Для безпечних підключень до даних використовується 128-бітове шифрування AES
- Запобігання зіткненням, повторним спробам та підтвердженням

ZigBee має ряд переваг перед іншими протоколами для WSN. До основних переваг можна віднести той факт, що ZigBee це стандарт, який уніфікований на всіх рівнях, що гарантує можливість використання продуктів різних виробників один з одним.

Однак це ще один плюс – можливість підключення кожного пристрою до будь-якого іншого, дозволяє розширити мережу географічно та забезпечити самовідновлення, якщо вибраний шлях до вузла не працює. До вузла може бути кілька шляхів, але вони не завжди бувають прямими. З кожним додатковим пристроєм збільшується ймовірність того, що ваша мережа буде надійною.

При цьому вони не споживають багато енергії і працюють в мережі без батареї (Green Power). Пристрої, які призначені для збору енергії, не мають батарею, вони отримують її за рахунок вилучення необхідної енергії за допомогою пересування та використання руху, світла, п'єзоелектричного ефекту або ефекту Пельтьє. Саме завдяки цьому ця технологія може бути використана для пристроїв з малою кількістю підключень до мережі (наприклад, коли на них немає живлення), а також може бути відключена більшу частину часу і не споживати енергію.

Висока мобільність мережі ZigBee забезпечує її високу масштабованість - вона може бути підключена до тисяч пристроїв, і вони зможуть зв'язуватися один з одним по найбільш оптимальному доступному шляху.

Wireless mesh network (WMN) – це бездротова мережа, що складається з радіовузлів і радіоканалів, розташованих у комірковій топології. В цьому випадку, можливо, використовуватиметься бездротова однорангова мережа.

Ця сітка є багатою, вона складається з безлічі з'єднань між пристроями або вузлами. У бездротових мережах часто використовуються пористі клієнти, маршрутизатори та шлюзи. Якщо вузли постійно або часто переміщуються і мережа не встигає оновлювати маршрути, сітка витрачає більше часу на оновлення маршрутів, ніж на доставку даних. Однак у бездротовій мережі топологій спостерігається тенденція до статичної структури. Це означає те, що розрахунки маршрутів можуть проводитися та здійснюватися у їх пунктах призначення. У цьому випадку це автономна система бездротової однорангової мережі з малою кількістю користувачів. Крім цього, якщо він часто покладається на шлюзи, то це не бездротова однорангова мережа.

Найчастіше клієнтами Mesh-сервісу є ноутбуки, мобільні телефони, а також інші бездротові пристрої. Якщо у вас є мережні маршрутизатори, вони перенаправляють трафік на шлюз і від нього. Так само зону обслуговування радіовузла часто називають ніздрюватою хмарою. Під час роботи радіовузлів, які створюють радіомережу, доступ до цієї пористої хмаринки залежить від спільної роботи радіовузлів та радіохвиль. Незважаючи на те, що мережа має надмірність у вигляді безлічі дрібних отворів, вона є надійною і надає достатню свободу пересування. Коли один вузол більше не може працювати і інші вузли також не можуть його обслуговувати, вузли, що залишилися, з'єднуються один з одним безпосередньо або через один проміжний вузол. Не виключено, що в майбутньому бездротові мережі будуть створюватися і відновлюватися. При цьому вони не повинні обмежуватися певною технологією або протоколом, а повинні бути універсальними для всіх бездротових технологій.

Якщо інфраструктура не матиме центрального сервера, то вона буде децентралізована (без центру) або централізовано керована (зі своїм центром). Перший є досить дешевим (досить сказати, що він не вимагає від користувача будь-яких додаткових витрат), а другий досить надійним. Всі ці вузли є частиною мережі

і служать маршрутизаторами передачі даних від найближчих вузлів до однорангових вузлві, які розташовані занадто далеко, щоб досягти їх за одну операцію, внаслідок чого мережа може охоплюватися великими відстанями. Ізольована комірка з високою рухливістю та малою мобільністю має бути досить стабільною. У разі виникнення неполадок у роботі системи маршрутизації, її сусід може швидко знайти новий маршрут за допомогою протоколу маршрутизації.

Модулі, які входять до складу Mesh-мереж можуть бути як фіксованими, так і мобільними. Також існують рішення, які можуть бути використані для зв'язку в різних умовах, наприклад в тунелях, нафтових вишках, спостереженні за полем бою, високошвидкісних мобільних відео-додатках на борту громадського транспорту, телеметрична гонка в реальному часі або самообслуговування. Не менш важливим варіантом використання WiFi для бездротових сіток є протокол VoIP, який може бути використаний для передачі голосу і відео за допомогою мобільного телефону. У схемі якості обслуговування бездротової мережі використовується схема з маршрутизацією локальних телефонних дзвінків через мережу та підтримкою маршрутизації місцевих телефонних дзвінків. Багато програм, які використовуються в бездротових мережах, мають аналоги з програмами в однорангових бездротових мережах.

Цей принцип аналогічний тому, як пакети переміщують по дротовому Інтернету. Дані передаються від одного комп'ютера до іншого доти, доки зрештою не досягнуть місця призначення. Кожен пристрій має свої алгоритми динамічної маршрутизації, які дозволяють їм цього досягти. Такі протоколи повинні реалізовуватись за допомогою пристроїв динамічної маршрутизації, які передають інформацію від інших пристроїв у мережі. Надалі пристрої визначають собі, що робити з даними, які вони отримують – або відправити їх наступним пристроям, або скопіювати, залежно від протоколу. При використанні алгоритму маршрутизації необхідно забезпечити, щоб дані йшли найбільш оптимальним (найшвидшим) маршрутом до місця призначення.

1.2.4 Bluetooth/BLE та WiFi

Хоча це і не звичайний спосіб передачі даних через Bluetooth, він став загальним у спільноті Інтернету речей. Ця технологія використовується для створення систем, які можуть бути використані в Інтернеті. З цієї причини технологія Bluetooth є найпоширенішою серед усіх існуючих технологій. У зв'язку з цим передбачається, що з'єднання між пристроями буде швидкісним та безшовним для Інтернету речей.

По суті, Bluetooth mesh IoT це система, яка є комп'ютерною мережевою системою, заснованою на Bluetooth Low Energy (BLE), яка забезпечує зв'язок пристроїв «багатьох до багатьох» через радіомодуль Bluetooth. Через Bluetooth, в мережі Інтернету речей можна передавати повідомлення за призначенням, тобто від одного пристрою до іншого.

Bluetooth IoT змінює умови гри бездротового пристрою. З цієї причини не дивно, що саме цей фактор визначає нову хвилю можливостей як для нових підключень (від мереж усередині самої будівлі до інтелектуальних сервісів на території міста), так і для підключення до мереж, включаючи промислову автоматизацію.

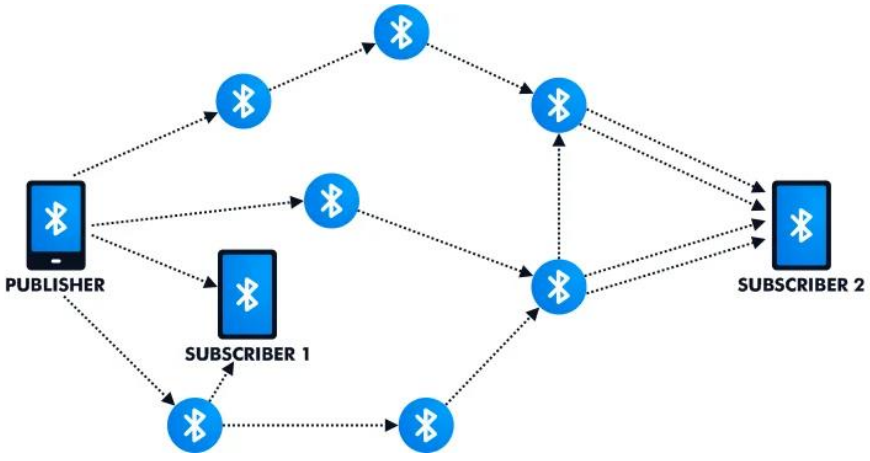

Рисунок 1.15 – Структура підключення Bluetooth

За допомогою бездротової технології Bluetooth Low Energy користувачі можуть заощаджувати енергію, утримуючи пристрої у стані сну, коли вони не

використовуються. Завдяки Bluetooth Low Energy можна легко підключитись до будь-якого пристрою, який має вбудований адаптер бездротового зв'язку.

IoT BLE, пристрій може працювати у трьох режимах: рекламний, скан та підключення. За сценарієм інтеграції двох пристроїв BLE один з одним необхідно використовувати один з них. На відміну від інших, він повинен спочатку провести сканування реклами, а потім ініціювати з'єднання. Здебільшого реклама складається з широкоформатних рекламних оголошень, які можна знайти іншими скануючими пристроями.

В даний час Wi-Fi є технологією бездротової мережі, яка використовує різні частоти радіохвиль для з'єднання та обміну даними та інформацією між пристроями. Цю технологію використовують у сучасних смартфонах та комп'ютерах, вона широко поширена. Мікрочіпи для бездротового зв'язку в IoT, необхідні для зв'язку між пристроями, і керування ними здійснюється за допомогою надійної прошивки, так як Wi-Fi дуже вразливий для зловмисників.

IoT пристрої з підтримкою WiFi – це величезні нерухомі центри, проте є і невеликі, які однаково підтримують WiFi. При використанні Wi-Fi пристрій має бути досить близьким до точки доступу Wi-Fi, щоб користуватися бездротовою мережею.

Незважаючи на те, що процес передачі даних між пристроями Bluetooth і Wi-Fi схожий за функціональністю, є деякі відмінності в тому, як ці технології складаються з точки зору функцій.

Швидкість: на даний момент Wi-Fi має максимальну швидкість, яка перевищує швидкість доступну в Bluetooth IoT. Вона може передавати дані зі швидкістю до 54 Мбіт/с, а його аналоги Bluetooth – лише на 3 Мбіт/с. З цим пов'язана та обставина, що Bluetooth зазвичай передає маленькі фрагменти даних, як числові значення з розумного годинника IoT з підтримкою Bluetooth, а Wi-Fi – найкращий варіант для передачі великих файлів даних, HD-фото та відео.

Визначення розташування: за допомогою бездротових технологій можна визначити розташування за допомогою пристроїв Bluetooth IoT та Wi-Fi IoT, до яких вони були підключені. Але, на відміну від Wi-Fi, Bluetooth дещо надійніший.

У цьому випадку найкращим варіантом є точність та якість використовуваних пристроїв.

Безпека та конфіденційність: незважаючи на те, що здебільшого Bluetooth не використовується з протоколом безпеки, отримана безпека цілком достатня для багатьох цілей. При роботі з конфіденційними даними WiFi надає більш безпечний варіант, ніж Bluetooth. Є рівні захисту Wi-Fi IoT, які дозволяють додати безпеку за рахунок безпеки за допомогою протоколів WEP, WPA, WPA2 та WPA3.

Виявлення близькості: Дані про близькість, надані BLE для IoT, набагато точніші, ніж дані, отримані від аналога Wi-Fi. Якщо ви хочете бути впевненими на 100% точно, то вам варто придбати Bluetooth-гарнітуру.

Споживання енергії: спочатку BLE розроблявся як пристрій роботи з малим енергоспоживанням, ніж WiFi. Необхідність додаткового джерела живлення для підключення вашого пристрою виникає, якщо ви працюєте по Wi-Fi, яке можна підключити до вашого пристрою.

Найчастіше Bluetooth має обмежений діапазон у порівнянні з Wi-Fi. Багато бюджетних пристроїв бездротового зв'язку оснащені діапазоном 100 метрів, який можна побачити в пристроях Bluetooth IoT дальньої дії. Тим самим, багато дешевих бездротових пристроїв мають радіус дії близько 10 метрів. Тому дальність дії Bluetooth, як і раніше, залежить від інших зовнішніх факторів – товщини стін та відстані між ними. Залежно від потужності передавача, типу антени, частоти, зовнішніх факторів, що впливають на дальність передачі даних, діапазон Wi-Fi та Bluetooth IoT може бути різним. Саме тому багато маршрутизаторів Wi-Fi, які розташовані на відкритому повітрі, можуть охопити більший діапазон частот, ніж звичайні маршрутизатори.

В даному випадку очевидно, що ні Bluetooth, ні Wi-Fi IoT не можуть здобути перемогу в цьому протистоянні. Немає можливості мати пристрій IoT, що працює через Bluetooth тільки тому, що йому потрібний проміжний пристрій, який дозволить йому транслювати дані, отримані пристроєм від пристрою Bluetooth IoT, за допомогою Wi-Fi. У більшості випадків Bluetooth найкраще підходить для

мобільних пристроїв з обмеженим живленням. Однак, Wi-Fi більше підходить для великих пристроїв, які мають прямий доступ до Інтернету.

Для того щоб зробити правильний вибір на користь тієї чи іншої технології, необхідно врахувати всі її переваги та недоліки, а також особливості роботи з ними.

Сучасний світ технологій пропонує нам безліч варіантів використання технології бездротового зв'язку Bluetooth і WiFi. Завдяки використанню технології Bluetooth з низьким енергопотенціалом всі пристрої IoT можуть підключатися до мережі без будь-яких додаткових витрат на обладнання. При цьому вартість використання додатків та рівень їхнього енергобалансу був суттєво обмежений застосуванням технології BLE в Інтернет речей. Такі можливості дозволяють зробити Bluetooth більш відповідним майданчиком для використання в роботі пристроїв Інтернету речей.

Мережна технологія Mesh – це одна з найцікавіших революцій, яка краще пов'язується з програмами IoT у порівнянні з іншими доступними варіантами підключення. Зокрема, це стосується архітектури та будівництва, де Bluetooth Mesh IoT дозволяє підключити до будь-якої будівлі чи великої території. Також пристрої будуть здатні працювати з мережею Bluetooth, що гарантує їм велику гнучкість у роботі та дозволить збільшити кількість розумних підприємств у найближчому майбутньому.

1.2.6 RFID и NFC

Радіочастотний ідентифікатор (RFID) являє собою мініатюрний пристрій з мікро чіпом, який зберігає інформацію. За допомогою спеціального пристрою, який називається «пам'ять транспондера», в мітку записується унікальний номер (ідентифікатор) та додаткова інформація. Мітка потрапляє в зону реєстрації RFID зчитувача та передається на комп'ютер за допомогою спеціального програмного забезпечення для подальшої обробки даних та зберігання.

За типом джерела живлення RFID-мітка поділяється на три типи.

Пасивні - Дані транспондери мають вбудоване джерело енергії, яке дозволяє передавати сигнал за допомогою модуляції відбитого сигналу частоти. Відбитий від мітки модульований сигнал передається на антену зчитувача, яка приймає його та передає на приймач. Діапазон застосування високочастотних міток становить від 1см до 2м, а надвисокочастотних (860-960 МГц) і надвискочастотних (2,4-2,5 ГГц) - від 1 до 10 метрів. Ці мітки можуть служити роками, вони не втрачають своїх властивостей і не псуються з часом.

Активні – збільшені розміри транспондерів із власним джерелом живлення. Вони можуть використовуватися для читання інформації на відстані до 300 метрів. Крім того, вони можуть бути оснащені додатковою електронікою, наприклад, датчиками для моніторингу температури, вологості та інших зовнішніх факторів. Вони мають найбільший обсяг інформації для передачі приймачем, вони найнадійніші та високоточні. При цьому активні мітки можуть генерувати вихід високого рівня. Вони можуть використовуватися не тільки на відкритій місцевості, а й у більш агресивних умовах: воді, тілах людей або звірів, металах (корабельні контейнери, автомобілі). Однак, незважаючи на всі ці переваги, активні мітки мають ряд недоліків, які обмежують їхній повсюдний доступ: вони досить дорогі, а їх батареї обмежені терміном служби (до 10 років).

Напівпасивні - Невеликі чіпи, які мають власне джерело енергії, можуть бути використані для живлення від батареї. Їхня дальність залежить тільки від чутливості приймача зчитувача.

Залежно від типу пам'яті RFID-мітки, що використовується, діляться на три типи.

RO (Read Only) – це спеціальні пристрої, призначені для запису інформації на магнітну стрічку. Їх практично неможливо підробити, оскільки такі мітки мають дуже чітку ідентифікацію.

WORM (Write Once Read Many) – крім унікального ідентифікатора, такі транспондери мають блок одноразово записування пам'яті з можливістю багаторазового читання;

RW (Read and Write) – транспондери з ідентифікацією та блоком пам'яті, в який можна багаторазово писати та читати.

Залежно від частоти, RFID-мітки поділяються на чотири групи.

Низькочастотні LF (125-134 кГц, стандарт ISO/IEC 18000-2:2009) - Вони найдешевші і часто використовуються для створення безконтактних чіпів для тварин і людей. Добре справляються з роботою, але при цьому мають невеликий радіус дії. Транспондери даного спектра мають колізії – помилки одномоментної передачі у середовищі колективного користування.

Високочастотні HF (13,56 МГц, ISO/IEC 18000-3:2010) – Низька ціна, відсутність екологічних проблем, підтримка стандарту ISO 14443, широкий спектр рішень. Цей тип використовують для ідентифікації особи та оплати послуг. При використанні цих систем для передачі інформації між ними виникають колізії та проблеми зі здатністю зчитування на великі відстані, в умовах високої вологості та наявності металу.

Ультрависокочастотні UHF (860-960 МГц, стандарт ISO/IEC 18000-63(C)) - Забезпечені анти колізійними механізмами, що дозволяють працювати на великих дистанціях. Використовуються у складській та виробничій логістиці.

Радіочастотні UHF-мітки ближнього поля - Для роботи з ними використовуються спеціальні пристрої, які дозволяють їм працювати в магнітному полі антени у воді, а також у присутності металу. Такі прилади використовують під час продажу товарів в аптеках або на складах з метою контролю якості продукції з металу та води.

Матеріал, з якого виготовлений об'єкт, за матеріалом маркування поділяють на три типи.

- для металу
- для об'єктів, що не містять метал
- універсальні

По виконанню RFID-мітки вона може виглядати як:

- наклейки;

- інтегрований в об'єкт (бирка, етикетка);
- корпусована – для використання в екстремальних умовах (екстремальні температури, захист від промокання тощо)

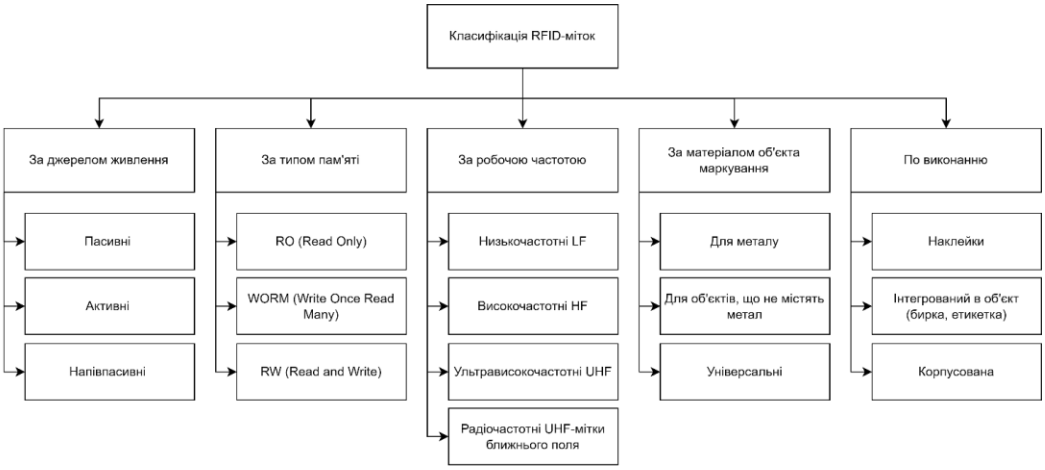

Рисунок 1.16 – Класифікація RFID-міток

Бездротовий режим передачі за допомогою RFID-чіпа дозволяє передавати інформацію про об'єкт на персональний комп'ютер у реальному часі. У цій технології використовується стек IoT. Сучасний ринок програмного забезпечення пропонує велику кількість RFID-рішень для різних платформ та пристроїв: BizTalk RFID, 123RFID, RapidRead, SessionOne та ін.

Застосування технології RFID у тих місцях, які вимагають автоматизації контролю переміщення об'єкта з урахуванням великої номенклатури продукції, а також швидкості та надійності роботи протягом тривалого часу.

- Забезпечення контролю над дотриманням технологічного процесу з виробництва.
- У складській логістиці відбувається контролю над переміщенням товарів. Це допомагає прискорити процес прийняття та відвантаження, підвищити надійність та прозорість операцій.
- Захист продукцію від крадіжки, а також крадіжок із зломом.
- Радіочастотні системи відстежують шлях товару з магазину до прилавка, щоб вчасно виставити товар на полиці у тому магазині, де на нього є великий попит.

- Маркування товару контрольними знаками із вбудованою RFID – міткою.

Переваги радіочастотної технології:

- наявність можливості запису інформації;
- Незалежність транспондер від орієнтації зчитувача.
- Робота у відсутності у прямій видимості.
- Можливість зчитування з відривом до 300 метрів.
- Вищий обсяг зберігання даних.
- Зчитувачі можуть одночасно зчитувати більше 1000 міток за секунду, уникаючи зіткнень з колізіями.
- Висока стійкість до вологи, а також забруднення.
- Тривалий термін служби.
- Багатофункціональне використання.
- Високий рівень захисту завдяки унікальному ідентифікатору та алгоритмам шифрування даних.

Недоліки радіочастотної технології:

- Висока стійкість до механічних пошкоджень.
- Дуже висока вартість.
- Виготовлення такого виробу потребує певних навичок та умінь.
- Виникає перешкоди внаслідок електромагнітного впливу.
- Мінімальний набір технологічних та організаційних рішень.
- Відсутність чіткого визначення, що таке «стандарт» та «норма».

NFC (Near-Field Communication) - ця серія протоколів зв'язку, для електронних пристроїв, щоб вони могли обмінюватися даними на відстані. Після того, як був випущений NFC, він став використовуватися у всіх додатках, які мають у своєму складі безпеку, зручність і транзакції.

В основі NFC лежить технологія радіочастотної ідентифікації (RFID), яка дозволяє сумісному обладнанню використовувати радіохвилі як для керування, так і для зв'язку з іншими активними електронними мітками, що не мають живлення!

NFC передає інформацію за допомогою магнітної індукції та електричної передачі, яка також може індукувати електричні струми в активних компонентах. Це означає, що пасивні пристрої можуть живитися від електромагнітного поля, створюваного активним компонентом NFC, і потребують власного джерела живлення.

NFC передає дані з частотою 13,56 мегагерц. Ви можете передавати дані зі швидкістю 106, 212 та 424 кбіт на секунду. Це дозволяє передавати різні дані в обох напрямках – від контактної інформації до обміну музичними файлами та фотографіями.

Для того, щоб створити RFID як удосконалення друкованих штрих-кодів, були використані нові технології, які дозволяють зберігати та передавати прості ідентифікатори. Це можливо завдяки тому, що RFID зчитується партіями (менше 1 мс), а також за допомогою швидкості зчитування в діапазоні від 1 до 100 метрів.

Завдяки використанню NFC як поліпшення QR-кодів, можна зберігати кілька типів даних. NFC може бути прочитаний протягом однієї мілі секунди, але з більш коротким діапазоном 0-10 см.

Різниця між NFC і RFID полягає в тому, що систему NFC можливо використовувати як зчитувач (як у випадку з RFID), так і в якості мітки. Також можна зберігати і передавати кілька типів даних, як простих, і складних. RFID застосовується в основному для більш простих завдань, таких як визначення місцезнаходження продукту або відстеження запасів. На відміну від NFC полягає в тому, що вони використовуються для більшої кількості програм, що вимагають невеликої передачі даних – реєстрації продукту, або навіть як каталізуючий процес для безконтактних платежів.

Даний тип бездротового зв'язку має ряд переваг перед іншими типами бездротового зв'язку, тому що в ньому використовуються мікросхеми, що працюють із дуже низьким енергоспоживанням. І ця перевага полягає в тому, що NFC може бути застосована до технології IoT.

З системою автономного збору та передачі даних, швидше за все, виникнуть певні проблеми. Завдяки NFC можна вирішувати деякі проблеми, з якими стикаються люди. Декілька прикладів:

- За допомогою NFC можна налаштувати підключення для двох пристроїв IoT, це спрощує процес синхронізації. Не потрібно жодних дротів.
- Завдяки NFC дані можна безпечно передавати на різні рівні. Використовуючи можливості відкритих мережевих ресурсів, хакери можуть зламати систему, використовуючи переваги відкритих мереж. Дані пристрої мають вбудовані функції, що обмежують можливості підслуховування, а також прості в установці налаштування додаткового забезпечення безпеки.
- NFC є переконливою ознакою того факту, що споживач бажає здійснити певну операцію, тому що чіп NFC має бути розташований поряд із чіпом, який ініціює транзакцію. Цей спосіб захисту дозволяє уникнути злому та проникнення в систему.
- У разі відсутності живлення, теги NFC пасивно обмінюватимуться даними, навіть якщо у них немає зв'язку. Користувач може торкнутися комп'ютера за допомогою NFC та отримати інформацію про нього.

Масштабованість означає здатність системи пристосовуватися під запити споживачів, що змінюються, при збереженні всіх функцій.

Як уже говорилося раніше, ці функції NFC в IoT є лише вершиною айсберга! Завдяки переваги NFC у сфері безпеки, простоті використання та впровадження технології Інтернету речей буде підняте на новий рівень. За словами розробників, у майбутньому NFC стане простим IoT-пристроєм.

2 ОСОБЛИВОСТІ ПРОЕКТУВАННЯ БЕЗПРОВОДОВИХ МЕРЕЖ ІІОТ

2.1 Аспекти, які потрібно враховувати про проектуванні мереж ІІоТ

Існує багато місця для промислового Інтернету речей (IoT), який пов'язаний з необхідністю в бездротовому підключенні промислових датчиків. Однак у сучасних умовах для промислового обладнання та додатків потрібні додаткові заходи щодо забезпечення безпеки та надійності.

З’явлення процесорів з низьким енергоспоживанням, розумних бездротових мереж, датчиків низького споживання та «аналітики великих даних» привели до бурхливого інтересу у виробників промислового Інтернету речей. Така технологія дозволяє розмістити безліч датчиків, де б вони не були: будь-де в інфраструктурі зв'язку та енергопостачальної мережі, а також скрізь, де є цінна інформація. І це не дивно. Адже саме на сьогоднішній день у світі існує безліч різноманітних транспортних засобів, які мають сенсори різного типу. На сьогоднішній день спеціальні датчики та мережі вже поширені у промисловому виробництві, включаючи нафтопереробні заводи та виробничі лінії. Операційні технології (ОТ) були створені як окремі мережі, що підтримують високий рівень надійності та безпеки мережі, яка неможлива без використання традиційних мереж зв'язку. Високі стандарти відбору технологій та їх застосування в найкритичніших для бізнесу програмах промислового Інтернету речей дають можливість відфільтрувати доступні технології до таких, які найкраще підходять для критично значимих для бізнесу програм промислового Інтернету речей. При цьому способи з'єднання даних датчиків з мережею визначають їхню безпеку та надійність при роботі в суворих умовах промислового застосування.

Як правило, системна складова для промислових додатків найчастіше виступає як надійність і безпека. У глобальному огляді промислових користувачів

WSN, надійність та безпека займають одне з перших місць. При цьому варто відзначити ту обставину, що прибутковість компанії залежить від якості та ефективності її роботи, а також безпека працівників значною мірою залежить від цих мереж. І саме тому, насамперед важлива надійність та безпека промислових бездротових сенсорних мереж.

Принциповим в проектуванні мережі для забезпечення надійності є система аварійного перемикання, коли механізми аварійного перемикача при можливих проблемах дозволяють системам відновлюватися без втрат даних. На даний момент у бездротовій сенсорній мережі є дві основні можливості використовувати цю надмірність. Крім того, у цій концепції є ідея просторової надмірності. Кожен бездротовий елемент містить як мінімум два інших, з якими може взаємодіяти (або не взаємодіяти), і схема маршрутизації, яка дозволяє передавати дані на будь-який з вузлів, але досягати наміченого кінцевого пункту призначення. А правильно сформована мережа з кількох вузлів, які можуть з'єднуватися один з одним через один або кілька сусідніх вузлів, має більш високу надійність і стійкість, ніж мережа точка-точка, завдяки автоматичному відправленню даних альтернативним шляхом, якщо другий шлях недоступний. По-друге, можна використовувати кілька каналів, які доступні в радіочастотному діапазоні. Як правило, такі перемикання здійснюються за принципом «перемикача каналів», тобто пари вузлів можуть перемикатися між каналами при кожній передачі, тим самим запобігати тимчасовим проблемам з будь-яким з каналів в мінливій і суворій радіосистемі, типовій для промислових додатків. Стандарт IEEE 802.15 має у своєму складі 15 каналів із розширеним спектром, які дозволяють системам перемикання каналів значно більшу стійкість, ніж системи без покупок (одноканальні). Існують стандарти бездротових систем, які включають подвійне просторове або канальне резервування, відоме під назвою перемикання каналів з тимчасовим інтервалом (TSCH), зокрема IEC60590 (WirelessHART) та майбутній стандарт 6TiSCH. За допомогою цих стандартів радіосигнали поширюються по всьому світу і використовуються у радіозв'язку, доступному у всьому світі. Компанія SmartMesh розробила новий спектр 2,4 ГГц в рамках проекту створення нового покоління

пристроїв з низьким енергоспоживанням і обмеженим ресурсом, який був запущений компанією Analog Devices в 2002 році.

Але саме TSCH є важливим будівельним матеріалом для забезпечення надійності даних у суворих радіосистемах, а також створення та обслуговування стільникової мережі. Не секрет, що промисловий бездротовий зв'язок необхідно обслуговувати протягом багатьох років, і на протязі його терміну служби залежатимуть від різних радіочастотних проблем і вимог до передачі даних. Саме тому останній інгредієнт, необхідний для створення надійної та стійкої бездротової мережі – це програмне забезпечення для інтелектуального управління мережами, яке в динаміці оптимізує топографію мережі з урахуванням якості зв'язку, постійно відстежуючи якість зв'язку, щоб максимізувати пропускну спроможність, незважаючи на перешкоди чи зміни у радіочастотній середовище.

Ще один важливий елемент промислової бездротової сенсорної мережі – безпека. З метою забезпечення безпеки у WSN, основними цілями є:

- **Конфіденційність**: При передачі даних через мережу ніхто не може їх прочитати, окрім передбачуваного одержувача.
- **Цілісність**: Підтверджується факт того, що будь-яке отримане повідомлення є не чим іншим, як тією інформацією про те саме повідомлення, яка була отримана від відправника і без будь-яких додаткових змін у змісті.
- **Справжність**: У повідомленні йдеться про те, що воно надійшло з відомого джерела. У разі використання часу як частини схеми аутентифікації також забезпечує захист повідомлення від запису та відтворення.

Для досягнення цих цілей необхідно включити у WSN надійні технології безпеки, такі як шифрування (наприклад, AES-128) з надійними та керованими ключами, генератори випадкових чисел криптографічної якості для запобігання нападникам повторного відтворення, перевірки цілісності повідомлення (MIC). Такі нові технологічні рішення безпеки бездротового зв'язку можуть бути легко увімкнені в багато пристроїв, що використовують Wi-Fi, але не всі продукти і протоколи WSN включають всі заходи. Це ще один момент, який необхідно

враховувати при підключенні безпечного WSN до небезпечного шлюзу. Не варто забувати про те, що в процесі проектування системи потрібно враховувати вразливість та наскрізну безпеку.

Як правило, сфери, що розвиваються, додають до своїх застарілих продуктів нові продукти та послуги промислового Інтернету речей, а їх клієнти розміщують їх у своїх старих середовищах, де використовується як старе, так і нове обладнання. Промислові WSN повинні забезпечувати простоту використання продуктів Industrial IoT, які дають змогу плавно переходити для існуючого польового персоналу. Мережі повинні швидко само формуватися для того, щоб на ній можна було швидко встановити обладнання, не створюючи проблем із обслуговуванням. Деякі з них можуть бути встановлені на мобільні пристрої, які мають можливість розгортання у важкодоступній або небезпечній місцевості, тому пристрої IoT повинні функціонувати від акумуляторів щонайменше п'ять років.

Системи мають бути доступні для глобального розгортання. Це необхідно для того, щоб вони були доступні всім користувачам, які мають доступ до Інтернету речей. За допомогою цих стандартів можна виконати вимоги міжнародних галузевих стандартів радіозв'язку, зокрема IEEE 802.15.4e TSCH.

Не менш важливим є правильне розташування датчика або контрольної точки у програмі промислового Інтернету речей. Відсутність провідного зв'язку не означає, що його не буде. Однак якщо вам необхідно підключити бездротовий вузол, який може бути підключений до мережі, або заряджати його, то вартість і непрактичність розгортання стають непідйомними. З цієї причини, наприклад, за допомогою проводів неможливо додати датчиків до обладнання для моніторингу обстановки на місці його експлуатації. Але знання, отримане під час проведення моніторингу в процесі експлуатації, може дозволити клієнтам здійснювати профілактичне обслуговування цього обладнання, тим самим уникаючи небажаного та дорогого простою.

Забезпечення максимальної гнучкості при розгортанні кожного вузла в промисловій WSN має бути можливим завдяки використанню акумуляторів, які здатні працювати від них не менше п'яти років, що дає користувачам максимальну

гнучкість покрити для промислових додатків інтернету речей. Однак для того, щоб отримати промисловий WSN на основі TSCH продукти SmartMesh від Analog Devices зазвичай використовуються при струмі нижче 50 мкА, що дозволяє їм працювати 5 років від двох батарейок AA. Там де є хороші джерела енергії в середовищі, можна постійно запускати вузли збору.

Щоб бути конкурентоспроможним на ринку, компанії необхідно мати розвинені промислові мережі моніторингу та управління. В основі цих систем лежать системи, що впливають на базову вартість виробництва товарів, а також своєчасність даних має велике значення. Як правило, за останні десятиліття детерміновані системи WSN на основі TSCH пройшли перевірку на практиці у широкому спектрі прикладних завдань. Це тимчасові системи передачі даних, такі як WirelessHART, які дозволяють передавати дані із зазначенням часу та обмеження терміну. Ці мережі мають можливість надавати вузлам, які потребують більшої кількості можливостей передачі даних, додаткові часові інтервали, а також передавати по мережі з невеликою затримкою. Такий розподіл інформації також сприяє поліпшенню можливості розгортання мережі з великою кількістю даних, що передаються. Якщо бездротовий інтернет в TSCH буде відсутній за розкладом або його не буде зовсім, то мережа впаде через неорганізований потік радіо трафіку.

З цієї причини пакети, які були відправлені в мережу TSCH з точністю до хвилини або години, можна знайти на кожному вузлі для координації сигналів керуючої системи в мережі вузлів WSN, при необхідності. Наявність інформації про час дозволяє програмі грамотно структурувати отримані відомості так щоб їх можна було правильно впорядкувати. Це допоможе уникнути плутанини у разі виникнення ситуації, коли інформацію отримано не по порядку.

Виробничі мережі повинні функціонувати постійно, але якщо вони будуть ненадійними, проблеми виникнуть завжди. Не варто забувати і про те, що якість мережі залежить не тільки від якості самої установки, але і від умов експлуатації. Невід'ємною умовою успішної роботи будь-якого підприємства є своєчасне попередження про можливі проблеми. Однак у більшості випадків бездротові сенсорні мережі не рівні за рівнем з іншими бездротовими мережами, які

забезпечують видимість метрик керування мережею. Не виключено і те, що в системі управління промисловою бездротовою мережею повинні бути такі елементи як індикація стану мережі, а також можливість передачі даних по радіоканалу:

- Якісний бездротовий зв'язок, що вимірюється силою сигналу (RSSI).
- Коефіцієнт успішних наскрізних пакетів.
- Якість та кількість сіток; наявність альтернативних маршрутів підтримки надійної мережі; якість та кількість вузлів, які не мають достатньої кількості альтернативних маршрутів для підтримки надійної мережі.
- Наявність та стан вузла та часу автономної роботи.

Для вирішення таких проблем у кращих промислових реаліях інтелектуальні мережі використовують автоматичну переадресацію даних альтернативними шляхами, при якій безперервно оновлюють топологію мережі для максимального збільшення можливостей підключитися.

І тут варто відзначити той факт, що багато компаній прагнуть того, щоб їх товари були більш інтелектуальними. Але це далеко не єдине місце, де розумним додаткам має належати промислове IoT. Корпоративні мережі Інтернету речей повинні бути оснащені інтелектуальною системою безпеки, яка відображала б найкраще, що можуть запропонувати корпоративні IT та ОП. Щоб адаптувати мережу до потреб користувачів, мережі повинні мати широкі можливості налаштування. Враховувати при цьому всі вимоги до низького енергоспоживання для того, щоб забезпечити максимально тривалий термін служби батареї, необхідно знати про доступність мережного живлення та інтелектуальну маршрутизацію. Крім цього, необхідно буде автоматично адаптувати мережу під зміни радіо поглинаючого середовища, яке може вплинути на динамічну зміну топології.

Компанія Analog Device розробила SmartMesh Network Manager, який надає користувачеві можливість перепрограмувати вузли в повітрі у разі потреби, а також забезпечує можливість оновлення майбутніх функцій у міру розвитку потреб клієнтів.

З погляду бізнесу, інтернет речей – це багато в чому промислове явище з чітко сформульованими бізнес-драйверами та досить переконливою рентабельністю інвестицій. Однак у цих критично важливих для бізнесу додатках промислова бездротова сенсорно-оптична мережа має бути повністю задоволена високими вимогами щодо інтелекту, безпеки та надійного зв'язку протягом багатьох років. Для того, щоб виконати ці вимоги, необхідно використовувати існуючі та нові стандарти бездротових мереж для промислових клієнтів, які будуть відігравати ключову роль у процесі перетворення свого бізнесу та послуг в епоху індустріального Інтернету речей.

2.2 Використання LORA для проектування безпроводових мереж IIoT

За допомогою радіо технології LoRa компанія Semtech представила (і запатентувала) технологію створення бездротових пристроїв. Для кодування за допомогою однієї частотної модуляції SF, використовується модуляція з розширеним спектром частот (CSS), що дозволяє кодувати за допомогою однієї частотної траєкторії SF (коефіцієнта розширення). Відповідно до цього виходить, кожен переданий символ має довжину в межах SF біт. Цей фактор був обумовлений тим, що в якості основи для побудови віртуальних каналів були використані властивості кореляції зв'язування, які демонструються, словом, chirp; таким чином, віртуальні канали та стратегія адаптивного швидкісного потоку передачі можуть бути легко реалізовані за допомогою передачі повідомлень з різними значеннями SF. Однак, ширина смуги частот сигналу становить фіксовану частоту (BW = 125, 250 або 500 кГц), у тому числі тривалість може бути розрахована як $T_C = 2^{SF}/BW$. Однак у даному випадку більш високий SF означає нижчу швидкісну передачу даних, але кращу перешкодостійкість (завдяки додатковому виграшу у оброботці). Відповідно до теорії, механізм прямого виправлення помилок підвищує стійкість до шумів та перешкод на слух, але ціна, яку доведеться заплатити за цю послугу – це зниження пропускної спроможності; однак, деякі швидкості кодування (CR) можуть вказуватися в діапазоні від CR = 4/5 до CR = 4/8.

На основі фізичного рівня LoRa, який відомий як LoRaWAN, був розроблений повний комунікаційний комплекс. Крім того, у характеристиках LoRaWAN додаються додаткові обмеження, які залежать від регіональних параметрів. Наприклад, під час роботи на європейському континенті, дозволена смуга пропускання становить BW ∈ [125,250] кГц та SF ∈ [7..12]. Один фізичний канал може містити до шести квадрантних віртуальних каналів (по одному значенню SF). У зв'язку з різною тривалістю символу фактична швидкість передачі даних варіюється від 11 до 300 кілобайт/с. Корисне навантаження повідомлення складає від 51 байт (при SF = 12) до 242 байт (при SF = 7).

На відміну від багатьох існуючих мереж, що використовують mesh-архітектуру, де вузли мережі передають від одного до іншого, LoRa – мережа використовує топологію «зіркоутворення». За допомогою цього можна знизити енергоспоживання пристроїв (за рахунок відсутності необхідності пересилати пакети від інших пристроїв) та спростити структуру мереж.

Безпосередньо в мережі LoRaWAN вузол з'єднується не з вузлом зв'язку, а передає дані на кілька шлюзів. При цьому кожен шлюз передає отриманий пакет даних від кінцевого вузла у хмару через транспортну систему (стільникова мережа, Wi-FI, Ethernet або інше). Керування здійснюється за допомогою сервера керування мережею. Він відкидає зайві пакети, здійснює перевірку безпеки та керує швидкістю передачі даних. З цієї причини така архітектура позбавляє необхідності проведення операції хендовера при пересуванні мобільних датчиків в межах дії мережі. Асинхронний режим роботи вузлів у мережі дозволяє передавати дані в міру їх накопичення або переривання. Як спосіб доступу до ресурсів мережі використовується метод ALOHA. З цієї причини відмова від постійної синхронізації пристроїв (як на звичайних мобільних мережах) дозволить заощадити заряд батареї. На даний момент у мережі з «зірковою» топологією складно організувати велику ємність мережі одночасно з великою кількістю користувачів. Для реалізації такої можливості LoRaWAN використовується адаптивна швидкість передачі інформації та використання багатоканальних

мультикодемних трансіверів в шлюзах, щоб повідомлення могли бути передані одночасно по декількох каналах.

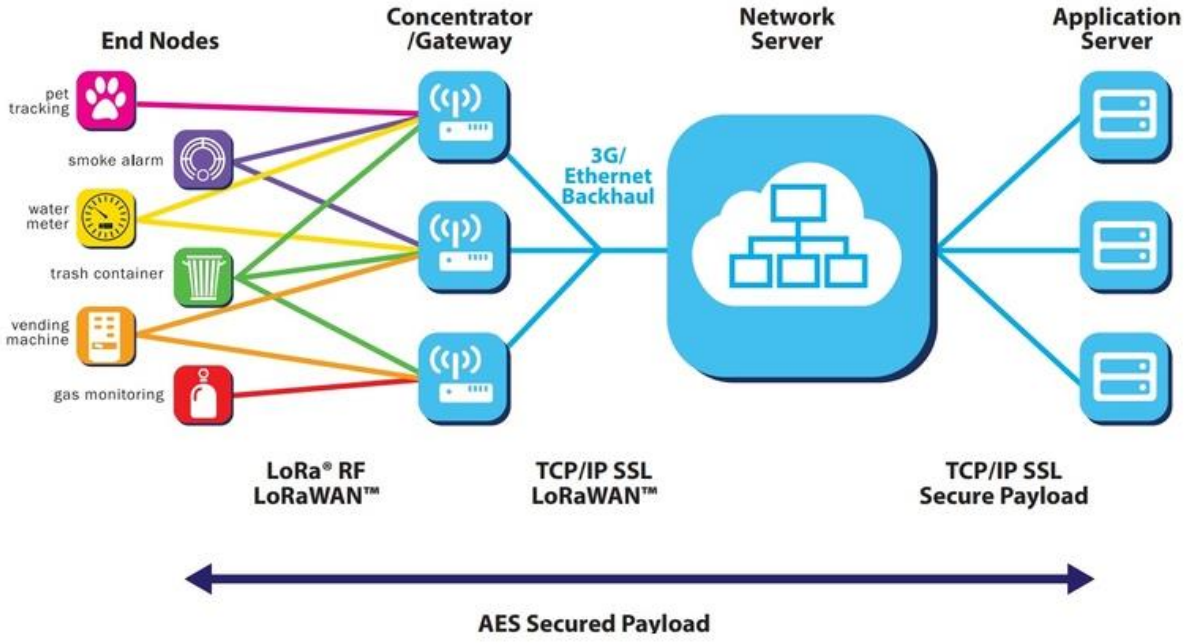

Рисунок 2.1 – Захищене корисне навантаження AES

Найбільш критичні фактори для пропуску - це число каналів, що одночасно транслюються, швидкість передачі даних (час на каналі), довжина корисного навантаження і частота вузлів. Оскільки в Lora використовується модуляція на основі розширення спектру, сигнал майже повністю ортогональний один до одного, коли використовуються різні коефіцієнти розширень.

Коефіцієнт розширення також змінюється за зміни ефективної швидкості передачі. Використання цієї властивості дозволяє отримати різні швидкості передачі на одному каналі одночасно. Найкращим способом з'єднання вузла є його розташування поблизу шлюзу. Це дозволить йому збільшити час перебування в ефірі та зменшити час передачі інформації. Можна збільшити потужність у системі за допомогою установки більшої кількості камер спостереження або збільшення кількості шлюзів. Але знизити кількість камер спостереження та збільшити пропускну здатність каналу у шість-вісім разів.

На даний момент проблема можливих колізій при одночасної передачі даних декількома пунктами вирішується центральним серверами LoRaWAN мережі, які адресно відправляють дані до вузлів (end-node), а також виділяють тайм-слоти для передачі та прийняття індивідуально для кожної кінцевої точки (end-node). За 32-бітним DevAddr, унікальним для кожного вузла (end-node), здійснюється адресна доставка.

На центральному сервері LoRaWAN мережі приймають рішення про необхідність зміни швидкості передачі даних точкою (end-node), потужності передачі, вибору каналу передачі, її початку та тривалості за часом, контролює заряд батареї кінцевого вузла (end-node), тобто повністю контролює всю мережу та керує всіма абонентськими вузлами. LoRaWAN пакети передаються кінцевому вузлу (end-node) з унікальним ідентифікатором AppEUI, що належить додатку на сервері сервіс-провайдера, для якого він призначений і цей ідентифікатор використовується центральним сервером LoRaWAN. На практиці найчастіше послугами сервісу користуються виробники кінцевих пристроїв (end-node) і вони підтримують сервіси обробки даних, куди передаються пакети з сервера LoRaWAN мережі для роботи з цими даними кінцевому користувачеві.

Протокол передачі даних між LoRa та компанією-виробником пристрою був розроблений альянсом LoRa, до складу якого входять виробники пристроїв, кінцеві користувачі (дослідники) та дослідницькі установи. Наприклад, LoRaWAN забезпечує верхній рівень каналів зв'язку між радіотелевізійною передачею та радіостанцією, визначаючи рівень сигналу, який використовується для чистого середовища ALOHA. Мережева топологія представлена гібридною бездротовою та провідною зірковою топологією з декількома BS (шлюзами), що тунелюють провідні прямі або магістральні канали висхідних та східних ліній зв'язку. Основним результатом роботи проекту є зниження складності впровадження в систему та обслуговування бездротової мережі. Так як низхідна лінія зв'язку не може бути обмежена для підвищення ефективності використання смуг пропускання, то і цільові програми повинні ґрунтуватися лише на висхідній лінії зв'язку.

Щодо шлюзів слід зазначити таке: кожен із них має програмний код (так званий «перенаправник» пакетів) для передачі повідомлень з використанням протоколу, залежного від реалізацій. Наприклад, шлюз тунелює тільки ті зображення, які отримані в результаті обробки даних LoRa, тобто, вони непрозорі. У цьому описі говориться, що LoRaWAN складається з 2-х рівнів; перший включає бездротове підключення до кінцевих систем; другий – серверна частина.

Мережеве управління здійснюється централізовано. Для того щоб отримати еталонну модель мережі, описану в специфікаціях LoRaWAN, необхідно використовувати два або три різні типи серверів (залежно від версії стандарту): мережного сервера (NS), серверів додатків (AS) та серверів приєднання (JS). Також зверніть увагу на те, що деталі реалізації виходять за рамки тих специфікацій, де описуються лише операції, які мають бути виконані.

NS є абстрактною логічною сутністю, що реалізує центр зіркоподібної топології. Задає формат пакету, автентифікацію та надає необхідні підтвердження. Він також керує функцією протоколу каналу передачі даних LoRaWAN, наприклад, стратегією адаптації швидкісної передачі даних. Коли користувач проходить автентифікацію, NS перенаправляє його вхідний висхідний канал до відповідного AS і ставить у чергу в низхідний канал з будь-якого AS, щоб доставити корисне навантаження відповідного кінцевого пристрою. Для того щоб JS був присутній, повідомлення Join-requests та Join-accept (через які виконується процедура зв'язування) передаються кінцевим пристроям та JS NS відповідно. У новій версії LoRaWAN 1.1 представлений JS реалізований шифрований спосіб управління об'єднанням кінцевих пристроїв безпечним шляхом.

Також є підтримка трьох ролей - обслуговування (sNS), домашній (hNS) і NS, що пересилає (fNS). Як правило, NS - керує рівнем каналів зв'язку для кожного з пристроїв і тільки sNS управляє поведінкою каналу передачі даних кінцевого пристрою. Активний роумінг здійснюється за умови, що sNS не змінюється та виконується пасивний. Але якщо увімкнути передачу обслуговування, то кінцевий пристрій буде керуватися відвіданою мережею, але дані користувача, як і раніше, будуть передаватися у вихідну hNS. На даний момент у специфікації немає нічого

про протоколи для реалізації інтерфейсів з fNS та шлюзом, а також між hNS та AS. Позначаються лише зв'язки між NS та інтерфейсом JS-NS. У разі використання протоколу HTTP, кодуючи корисні дані за допомогою об'єктів JSON, необхідно використовувати об'єкт JSON. Є кілька варіантів реалізації. З цієї причини архітектура Suchan дозволяє легко відокремитися від власників інфраструктури та власників даних, що дозволяє створювати нові бізнеси.

3 ОПТИМІЗАЦІЯ МЕРЕЖІ ДЛЯ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ

Розглядаємо промислові мережі Інтернету речей, які складаються з N вузлів, як показано на рисунку 3.1. До складу вузла входять набори вершин $N = \{n_1, ..., n_N\}$ та відповідний набору ребер $E \subset N \times N$. Тоді матриця зв'язності C у такій топології є симетричною матрицею N × N, де край між будь-якими двома вузлами i та j представлений якраз навпроти будь-якого іншого вузла i або j. Якщо один із вузлів пов'язаний з іншим, то $c_{i,j} = 1$, інакше $c_{i,j} = 0$. Ми також припускаємо, що мережа підключена і що завжди є шлях між будь-якою парою вузлів. В цьому випадку E-простір всіх можливих матриць зв'язності C з таким графом. Оскільки $c_{(i,j)} = c_{(j,i)}$ та $c_{(i,i)} = 0$, ясно, що $E \subset \{0,\ 1\}^{\frac{N(N-1)}{2}}$.

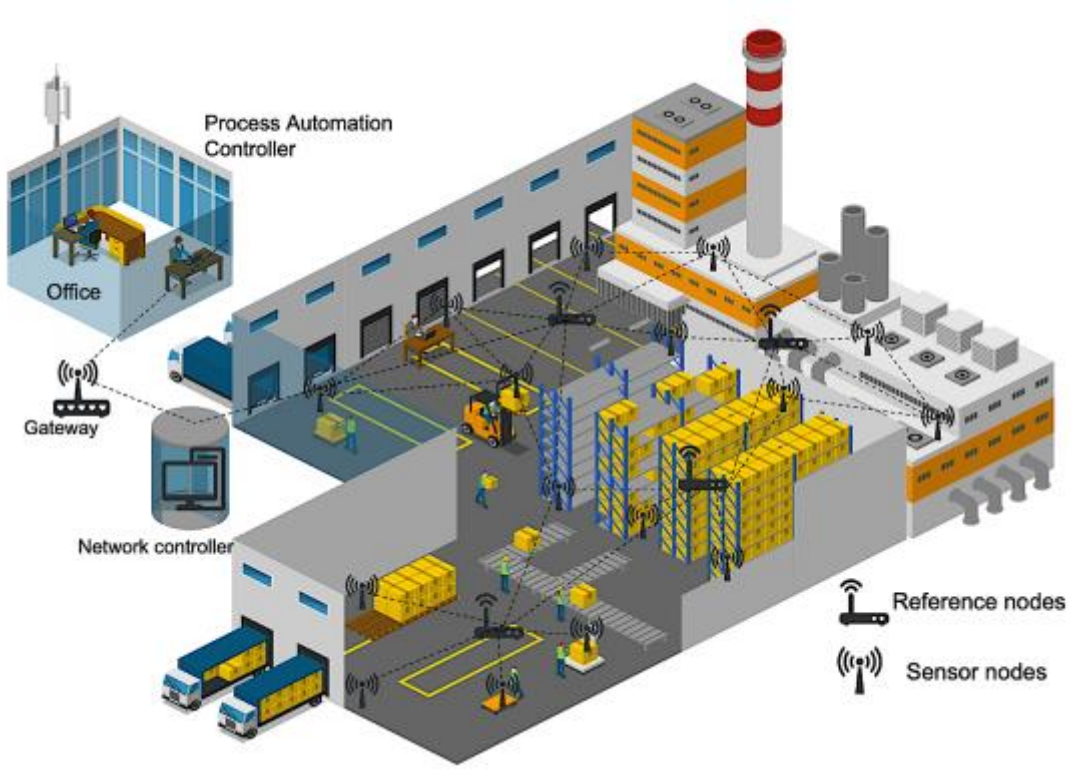

Рисунок 3.1 - Промислова архітектура для Інтернету речей.

На основі еталонних вузлів M <N зі структурою зв'язності $R = \{R_1, \ldots, R_M\} \subset N$. Ці еталонні вузли використовуються для складання вимірів стрибків від

звичайних вузлів за допомогою керованого мережевого лавинного трафіку. Даний етап проходить після того, як опорні вузли передають зондові пакети вузлам, що залишаються в мережі. Кожен із вузлів, своєю чергою, розраховує кількість переходів до опорних вузлів, і спрямовує найкоротший шлях (мінімальна кількість надій на опорні вузли) від опорних вузлів до опорних вузлів. Після того, як процес лавинного розсилання завершується - опорні вузли збирають всі вимірювання відстані перехід від звичайних вузлів і створюють матрицю просторів **H**(R). Тут варто звернути увагу на ту обставину, що запис (i, j) з **H**(R) є найкоротшою відстанню стрибка між звичайним вузлом n_i і опорним вузол R_j. Оскільки звичайне вузлове з'єднання n_i створює вектор h_i (вектор руху), що складається з відстаней стрибків до M точок опори, ми можемо записати матрицю вимірювань відстані між опорними вузлами у вигляді суми квадратів відстаней стрибків як

$$\boldsymbol{H}(R) = [\boldsymbol{h}_1^T, \dots, \boldsymbol{h}_N^T] \tag{3.1}$$

де h_i є віртуальний вектор координат, який використовується для визначення положення вузла ni. За допомогою цієї віртуальної системи координат (VCS) ми визначаємо логічну відстань d_R щодо набору опорних вузлів R:

$$d_R(n_i, n_j) = \|h_i - h_j\|_2 \tag{3.2}$$

На наступному етапі формується спільне завдання вибору опорних вузлів та оптимізації мережі. Припустимо, що $P(e_k|R)$ це ймовірність того, що $e_k \in E$ є рішенням матриці змішаності для даного H(R). У свою чергу $\hat{e}_k$ – це оцінна матриця суміжності, яка визначає ймовірність помилки у матриці суміжності наступним чином:

$$P_e(R) = \sum_{e_k \in E} \sum_{j \neq k} P(e_k|R)\, P(\hat{e}_k \equiv e_j | e_k; R) \tag{3.3}$$

Завдання вибору оптимального набору опорних вузлів для R^* може бути сформульовано як

$$\begin{aligned} &\min_{R} \quad P_e(R) \\ &s.t. \ |R| \leq M \end{aligned} \tag{3.4}$$

У наступному розділі буде розглянуто напрямок оптимізації, а також запропоновано ітераційний підхід для пошуку рішення, близького до оптимального.

3.1 Пропонуємий метод вибору опорного вузла

На даному етапі нами розробляється схема підбору оптимального вузла для забезпечення максимальної продуктивності підключення, яка забезпечує максимальну ефективність і надійність VCS. Якщо всі вузли відомі, то завдання, поставлене в (3.4), є NP – складним і, отже, вимагає експонентного часу виконання. Теоретично можна використовувати лише набір вимірювань для опори основних елементів конструкції, але насправді обчислювальна потужність обмежена, і доступом до неї мають лише одиниці. У результаті виходить, що в даному випадку ми послаблюємо обидва ці припущення і вирішуємо проблему ітеративним шляхом, де на кожній ітерації відбувається оновлення матриці зв'язності разом з вибором опорних вузлів. $R^{(i)}$ - набір опорно-стовпових елементів на і-й ітерації, а також їх кількість. Таким чином нам не відомо про жодну заздалегідь встановлену топологію мережі; тому у разі випадковим чином вибирається $R^{(1)}$. Щоб зменшити ймовірність помилки $P_e(\cdot)$, ми збільшуємо кількість опорних вузлів на і-й стадії так, щоб ймовірність помилки $P_e(\cdot)$ була мінімальною.

$$n^{(i)} = \underset{n \in N \mid R^{(i-1)}}{\arg min} \quad P_e\left(R^{(i-1)} \cup n\right) \tag{3.5}$$

де n(i) - оптимальний набір вузлів

На жаль, оцінити $P_e(\cdot)$ неможливо через відсутність практичного обмеження за кількістю вимірювань стрибків. З цієї причини нам доводиться послаблювати обмеження у верхній межі кожної ітерації, використовуючи вимірювання стрибків. Для того, щоб зробити це, ми використовуємо підхід мережевої оптимізації, пов'язуючи **H**(R) і **C**. Ця ідея полягає в наступному:

- Насамперед ми створюємо вузли в рівні, де зв'язок між будь-якими двома довільними вузлами n_i або n_j визначається як підключеною, відключеною та неоднозначною на основі наступних критеріїв:
  - Вузли n_i і n_j пов'язані між собою за умови, що їх відстані переходу дорівнюють одній надії щодо одного і того ж опорного вузлика.
  - Вузли n_i і n_j вимикаються, якщо їх відстані переходу більше одного переходу по відношенню до одного і того ж основного опорного вузла.
  - Неоднозначність зв'язку між вузлами n_i та n_j очевидна за відсутності можливості визначити інформацію про зв'язок. Це проблема з перевертанням на VCS.
- Ця класифікація призводить до часткової заповненої матриці зв'язності з деякою двозначністю. В α(R) ми бачимо невизначеність у матриці зв'язності.
- Далі, за допомогою того факту, що шанс помилки обмежений зверху величиною $P_e(R) < \alpha(R)$. При використанні даного кордону проблема вибору опорного вузла пом'якшується таким чином:
-

$$n^{(i)} = \underset{n \in N \mid R^{(i-1)}}{\arg min} \; a\left(R^{(i-1)} \cup n\right) \tag{3.6}$$

Цей запропонований ітераційний метод узагальнюється в Алгоритм-1 для вибору випадкових наборів опорних вузлів. І тільки після цього, використовуючи опорні вузли (3.6), ми вибираємо опорні вузли на їх функцію неоднозначності зв'язності. І все-таки рішення (3.6), як і раніше, важке.

АЛГОРИТМ-1 (Ітераційний вибір еталонного вузла)

$\boldsymbol{Data}$: N,

$\boldsymbol{Result}$: $\boldsymbol{R^{(M)}}$,

$\boldsymbol{R^{(1)}} \leftarrow$ случайный узел из множества $\boldsymbol{N}$;

$\boldsymbol{for\ i \leftarrow 2\ to\ M\ do}$

$$\boldsymbol{n^{(i)} = \underset{n \in N \mid R^{(i-1)}}{\arg min}\ a\left(R^{(i-1)} \cup n\right);}$$

$$\boldsymbol{R^{(i)} \leftarrow R^{(i-1)} \cup n^{(i)};}$$

$\boldsymbol{end}$

Йому необхідна інформація про зв'язність щодо вузлів $N|R^{(i-1)}$, яку він не може отримати за допомогою і-ї ітерації. Для вирішення цієї проблеми ми застосовуємо жадібний підхід до оцінки $\alpha(R^{(i)})$, використовуючи лише доступні дані про зв'язність із набору опорних вузлів $R^{(i-1)}$. На і-ї ітерації стратегія вибору опорного вузла включає наступні кроки:

- З погляду логічної відстані $d_R^{(i-1)}(\cdot)$ даного набору опорних вузлів $R^{(i-1)}$ ми вибираємо найдальший вузол з урахуванням логічної відстані $d_R^{(i-1)}$ поточного набору. Саме тому цей параметр вибирає той самий опорний пункт, який знаходиться на відстані не менше ніж від поточного набору опорних вузлів, щоб досліджувати глибину мережі.

$$n^{(i)} = \underset{n \in N \mid R^{(i-1)}}{\arg min} \left(\underset{m \in R^{(i-1)}}{min}\ d_{R^{(i-1)}}(n, m) \right) \tag{3.7}$$

- Далі нам необхідно вибрати вузловий вузол, у якого найбільше неоднорідних ребер на основі матриці зв'язків по відношенню до набора опорних елементів $R^{(i-1)}$. З цим критерієм можна мінімізувати локальну невизначеність, тобто

$$n^{(i)} = \underset{n \in N \mid R^{(i-1)}}{\arg min} \left(a^{(i-1)}(n) \right) \tag{3.8}$$

де $\alpha^{(i-1)}(n)$ - локальна неоднозначність вузла n на (i - 1) -ї ітерації.

- Таким чином, цей критерій говорить про те, що у випадку, коли ми маємо кілька записів за другим критерієм, нам необхідно ухвалити рішення на основі першого критерію. Тут йдеться про те, що якщо є можливість появи кількох кандидатів з однаковою функцією неоднозначною, то нам необхідно прийняти рішення на основі перших критеріїв, тобто на основі логічної відстані.

Тестування запропонованого методу.

Тут проводиться тестування запропонованого нами методу визначення опори для встановлення у вибраному місці за допомогою MATLAB щодо помилок підключення, швидкості доставки пакетів та загального споживання енергії. Щоб отримати дані про параметри моделі, використовуються таблиця 1 з параметрами моделювання. Надалі ми створюємо випадковий промисловий трафік IoT з числом вузлів датчика N у двовимірній області. Після цього ми випадково вибираємо ребра між парами вузлів датчиків і мережевого графа, таким чином, мережевий граф є зв'язковим. Зауважте, що $\beta = |E| \frac{N\,(N-1)}{2}$ є відсотком ненульових елементів з матриці зв'язності **C**. Надалі нам необхідно вибрати з безлічі посилальних вузлів на основі різних критеріїв, які обговорювалися раніше. І нарешті, як приклад, ми використали метод керованої лавинної розсилки, щоб зібрати виміри стрибків від опорних вузлів. Ми також оцінили ефективність запропонованого методу щодо загального енергоспоживання, оскільки це важливий показник для вузлів IoT з живленням від батареї. Порівнюємо загальне енергоспоживання запропонованого способу та методу випадкового вибору еталону. Облік результатів усереднений за п'ятьма моделями Монте-Карло. Однак, крім цього, у нашому випадку ми можемо варіювати кількість опорних вузлів, фіксуючи N = 100 та β = 15% (мінімальний поріг для підключення до мережі).

Таблиця 1: Параметри моделювання

ПАРАМЕТР	ЗНАЧЕННЯ
Область моделювання	100m × 100m
Дальність зв'язку	50m
Кількість опорних вузлів R	0 - 30
Кількість сенсорних вузлів N	100
Моделювання запускається	500
Відсоток ненульових записів β	15%
Поріг чутливості	−120dB

Невизначеність підключення

Рисунок 3.2a говорить про продуктивність різних методів вибору опорних вузлів у порівнянні з неоднозначністю мережевих підключень та кількості опорного вузла. Також ми досліджуємо результати з оптимально вирішуваним (3.5) та повним перебором (3.4). З цього ми можемо показати, що запропонований нами метод майже повністю відповідає оптимальному рішенню. У цьому випадку пошук буде більш продуктивним, якщо кількість посилань невелика через відсутність інформації про підключення. В алгоритм-1 сказано, що перший опорний вузол $R^{(1)}$, який був обраний випадковим чином, повинен бути вибраний з безлічі можливих.

Швидкість доставки пакетів

Потім ми проводимо дослідження продуктивності маршрутизації пропонованої нами схеми за допомогою випадкового вибору вузла джерела та призначення (якщо це можливо). Крім того, ми порівнюємо результати маршрутизації з результатами випадкової вибірки на основі логічної відстані (LDR) або стратегії вибору опорного вузла. LDR частково побудований на класичній методиці маршрутизації вектору відстані та базується на вимірах числа стрибків між двома опорними вузлами. У цьому випадку він просто передає пакети даних до сусідніх вузлів відповідно до логічної відстані. У LDR є кілька недоліків, серед яких ризик нескінченного зациклювання, що виникає через неоднозначність віртуальних координат. У той же час метод, заснований на зв'язності, визначає

найкоротший шлях між вихідною та кінцевою точкою, і якщо немає однозначності в зв'язності, цей метод може буди точно розрахований за допомогою добре відомого алгоритму Дейкстри. Якщо в поточному сценарії невизначеність можливості підключення може викликати втрату доставки пакета через відсутність у матриці, що базується на з'єднанні, помилки в її побудові. Зі збільшенням кількості опорних вузлів в обох випадках збільшується швидкість доставки пакетів. Щоб прискорити доставку пакетів, ми врахували відсоток успішно доставлених пакетів до пункту відправлення. Рисунок 3.2b показує швидкість доставки для підходу, заснованого на підключенні, та підходу LDR. Вибір еталонних вузлів покращує швидкість доставки пакетів на 20%. Завдяки цьому методу можна вибрати найвигідніший опорний вузол для кожного конкретного випадку.

Загальне споживання енергії

Ми також демонструємо продуктивність запропонованої схеми загального енергоспоживання зі збільшенням кількості опорних вузлів. Енергія E_T складається з основної роботи електроніки та енергії передачі. Енергія всіх вузлів (M+N) у мережі IoT розраховується як:

$$E_T = \sum_{i=1}^{M+N} E_{e_i} + (M+N)\left(\sum_{i=1}^{M+N} E_{t_i} + \sum_{i=1}^{M+N} E_{r_i}\right) \tag{3.9}$$

де E_{e_i} - енергія, яка необхідна для роботи базової електроніки.

E_{t_i} - енергія передачі,

E_{r_i} - залишкова енергія і-го вузла

Рисунок 3.2c показує збільшення загального споживання мережі внаслідок збільшення кількості опорних вузлів. Крім того, ми порівнюємо результати з маршрутизаціями на основі зв'язності з випадковими параметрами вибору опорних вузлів. Рисунок 3.2c демонструє, що запропонована схема використовує менше електроенергії, тому що вона використовує локальну інформацію лише від сусідів по ланцюжку і не координується з опорними пунктами за межами їхнього

надійного діапазону; у такий спосіб ми зменшуємо загальне споживання енергії за одиницю.

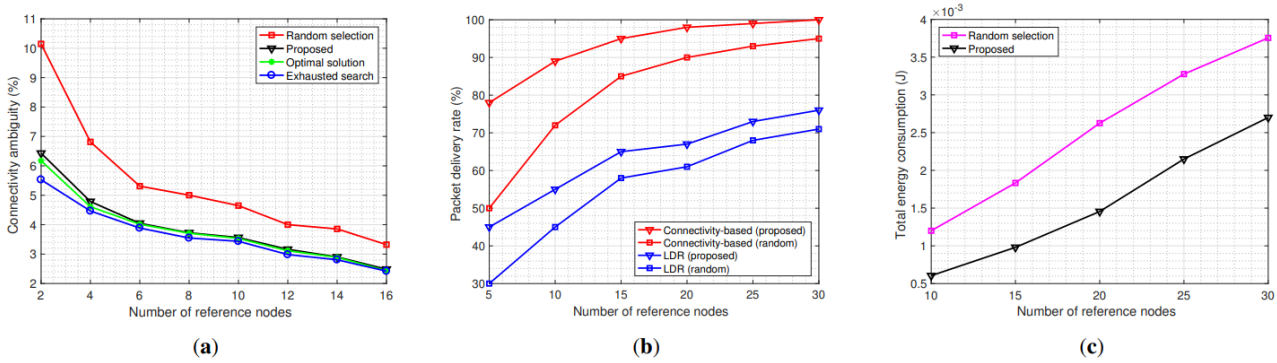

Рисунок 3.2 – (a) Число опорних вузлів порівняно з неоднозначністю підключення; (b) Кількість опорних вузлів. Швидкість доставки пакетів; (c) Кількість посилальних вузлів. Загальне споживання енергії.

3.2 Методологія проектування промислових бездротових систем інтернету речей

Термін «Бездротові Системи IIoT» (IIoT-WS) використовується в цьому документі в усіх аспектах і охоплює всі бездротові системи, які в якійсь мірі стикаються з компромісом PLR, такі як промислові WSN (IWSN), ультра-висока швидкість зв'язку (TSN). Різні варіанти компромісу були розглянуті в ході дослідження останніх робіт. Нова система стандартів була представлена у вигляді нових або модифікованих стандартів, наприклад, IEEE 803.1, MTC на основі LTE-стандарту, WirelessHART і 6TiSCH. Безпосередньо програмна частина була створена за допомогою розробки бездротових технологій, заснованих на базових станціях з безліччю антен, пріоритету доступу на рівні MAC Wi-Fi, конструкторського лавиноподібного поширення і так далі. Але в першу чергу, з точки зору апаратного забезпечення вчені звернулися до IIoT-WS зі своїми модельними уявленнями про зв'язок, моделями помилок пакетів, схемами

кодування, інноваційним дизайном апаратури і багатообіцяючим підходом проектування знизу вгору.

У порівнянні з попередніми роботами ця робота відрізняється тим, що вона включає в себе новий підхід до проектування - методологію проектування, що об'єднує широкий спектр рівнів проектування (наприклад, системних, архітектурних, програмних і апаратних) для забезпечення найкращого орієнтованого не тільки на додатки і ресурсозберігаючий компроміс PLR. На цьому етапі використовується системний підхід Meet-In-The-Middle (MITM), який дозволяє вирішувати проблему PLR в два етапи. Спочатку застосовується системний підхід Meet-in-The-Middle (MITM) для проектування глобальної бездротової системи і потім проводиться багато кратерній аналіз проектів (MCDA), щоб допомогти підібрати оптимальні значення для проектних. У методології пропонується широкий погляд на концепцію "система - реалізація", приводячи до вирішення, що одночасно найкращим чином відповідає вимогам конкретного додатка (і найближче до теоретично оптимальної кордоні) і найбільш наближає до теоретично оптимальної кордоні.

Навчальний приклад

При розгляді системи, яка була створена для того щоб їздити на звичайному автомобілі, ми побачимо, що вона має дуже високий рівень абстракції. Тут мова йде про те, що дана система обмежує горизонтальне рух автомобіля шляхом зниження його вертикальної швидкості. Пасивно-активна система має тільки м'яку або жорстку настройку. Це дозволяє водієві відчувати себе комфортно при їзді на будь-якій швидкості. Завдяки цьому компромісного варіанту, активна підвіска може бути замінена легко монтованої автономної напівактивної системою підвісок (ASAS). На думку розробників ASAS, це автономна система підвіски, яка складається з безлічі вузлових систем, що збирають енергію з навколишнього середовища і використовують її для прийняття рішень, обміну інформацією або забезпечення найкращого коефіцієнта демпферірованія відповідно до профілю дороги. Саме тому ASAS повинна не тільки справлятися з жорсткими умовами

експлуатації будь-якої автомобільної системи (наприклад, забезпечувати швидку реакцію), але і мати справу з обмеженим джерел енергії.

Необхідність дотримання жорстких вимог ASAS до конструкції системи бездротового зв'язку (умова для можливості "plug-and-play") вплинуло на конструкцію системи бездротового зв'язку. Це може бути пов'язано з тим, що вимоги до надійності виражаються в низькій частоті бітових помилок; швидкий відгук - в обмеженій за потужності схемах; обмежена доступна енергія - в обмежених по потужності схемах. З одного боку, це вимога компромісу PLR, з іншого - це протиріччя між вимогами до бездротової системі і її проектуванням. Фактично, цей компроміс можна знайти в багатьох інших подібних промислових бездротових додатках і високопродуктивних WSN.

Системні вимоги

За допомогою цього методу можна оцінити вплив вимог, пов'язаних з часом (або частотою) на зв'язок в системі PLR.

1) Ширина смуги когерентності (розкид затримки):

Багато хто з сучасних бездротових ліній зв'язку представляють собою середовище з відсутністю прямої видимості, де передається сигнал можна досягти лише за допомогою багатопроменевої (наприклад, мобільний зв'язок в щільної міської середовищі). При використанні в якості точки-точки бездротового зв'язку, наприклад, при супутникового зв'язку, приймач буде отримувати кілька разів один і той же сигнал від атмосферних явищ. Однак, якщо у вас є багато вченість, то ви створюєте тимчасову дисперсію в прийнятої вами інформації, що може привести до меж символічної інтерференції (ISI). Розбіжність (T_M) - це статистична міра затримки між першим, другим і третім компонентами багато вченого сигналу. При поширенні затримку можна пояснити шириною смуги когерентності (B_C), виміром площинності частотних каналів, які визначаються рівнянням 1. Така залежність демонструє ту обставину, що в системі без ISI можна досягти або смуги пропускання сигналу (B_S) менше B_C, або при тривалості символу більш, ніж розкид затримки.

$$B_c = \frac{1}{T_m} \tag{3.10}$$

На основі даних, отриманих при проектуванні IIoT-WS, ці два параметри використовуються для характеристики профіль завмирання каналу і, отже, характеризують мінімальну НЕ корелювати дистанційне відстань між каналами і розподіл каналів Wi-Fi.

2) Час когерентності (допплерівській розкид):

Даний феномен полягає в тому що ефект Допплера - це зсув частоти, який відбувається внаслідок ненульовий відносної швидкості двох об'єктів. Однак його використання актуально тільки в тих випадках, коли ми говоримо про швидкі об'єктах, таких як супутники, або ж в тих випадках, коли мова йде про високошвидкісних транспортних системах. Для того щоб передати сигнал від автомобіля на швидкості 120 км / год (v = 33 м / с), необхідно використовувати рівняння 2, де говориться, що сигнал, який передається від автомобіля, що рухається з відносною швидкістю 120 км / год (v = 33 м / с) має зсув частоти (також відомий як допплерівський розкид – B_d) всього 0,1 ppm. Крім того, деякі з сучасних систем працюють з кришталево-чистим кристалічним генератором зі зрушенням частоти ± 40 ppm.

$$B_d(ppm) = \frac{v}{c} 10^6 \tag{3.11a}$$

$$B_d(Hz) = \frac{v}{c \cdot f_c} \tag{3.11b}$$

де f_c - центральна частота сигналу, а c - швидкість світла.

Крім того, для тих додатків, де доппель-тест має значення (наприклад, у випадку з каналом), допплерографія може вказувати на міру частотної дисперсності. Слідуючи цьому визначенню, рівняння 3 показує зв'язок між

тимчасовим розподілом в допплерівському поширенні і часом когерентності (T_C), яке можна розглядати як статистичне дослідження кореляції загасання під час синхронізації за допомогою допплерівського поширення.

$$T_c = \frac{1}{B_d} \tag{3.12}$$

За цими параметрами можна оцінити тривалість ефектів завмирання в каналі, які були використані при проектуванні IIoT-WS. Таким чином, їх можна використовувати як засіб для визначення мінімального некартельованих тимчасового інтервалу, протягом якого така система може мати дві некорреліpованних передачі.

3) Швидкість передачі даних:

Швидкісний канал (R) є визначальним фактором при проектуванні бездротової системи передачі даних і визначає її якість в цілому. Як правило, вона буває досить складною в процесі її вибору.

На думку авторів дослідження, це може бути пов'язано з тим, що велика швидкість передачі даних не завжди призводить до зниження енергоспоживання. Не виключено, що це відбувається тільки в радіосистеми з 100-відсотковим циклом роботи. А це значить що, якщо ви хочете заощадити на електроенергії то вам необхідно вибрати варіант R і робочий цикл (DC), який забезпечить мінімальне енергоспоживання приймача. Як і у випадку з іншими системами, для заданого R в трансивері постійного струму загальне енергоспоживання залежить від його конструкції (RX) і передавача (TX). З іншого боку, якщо велике R призведе до скорочення часу передачі і зниження швидкості передачі, то це також вимагатиме від приймача сполучення з великим міжполосним шумом, що підвищить енергоспоживання передавача для підтримки підвищеного SNR в приймальному пристрої. І так само за іншим принципом, інші підходять до даного процесу з боку коефіцієнта шуму (NF), забезпечуючи максимально можливий коефіцієнт шуму (NF), який мінімізує споживання енергії в трансивері, як показано на рисунку 3.3.

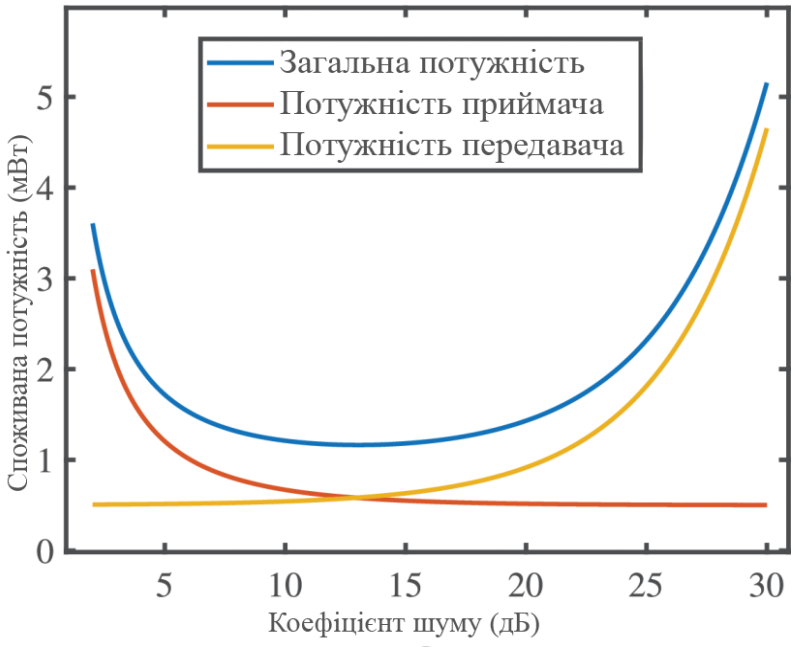

Рисунок 3.3 – Мінімізація споживання енергії в трансивері

Апаратний компонент

Є багаторівневі інтеграції Системи можуть бути розроблені з нуля, починаючи з протоколу і закінчуючи інтегрованим приймачем і мікро контролером, вони можуть бути реалізовані на базі існуючих платформ, наприклад, ZigBee, або з комбінацією обох варіантів. Ця стаття присвячена тим варіантам реалізації системи IIoT-WS, які існують на сьогоднішній день.

З системного вимоги до систем бездротового зв'язку слід зробити висновок, що вона повинна бути реалізована або за допомогою спеціалізованого інтегрального пристрою (ASIC), або за допомогою готового модуля (COTS). За результатами дослідження на рисунок 3.4, можна зробити висновок про те, що кожен з підходів має свої достоїнства і недоліки. Це може бути пов'язано з високою продуктивністю і низькою потужністю, а також повним контролем над параметрами проектування. Також COTS дешевше, швидше виходять в ринок, але не забезпечують достатню надійність, а також контроль.

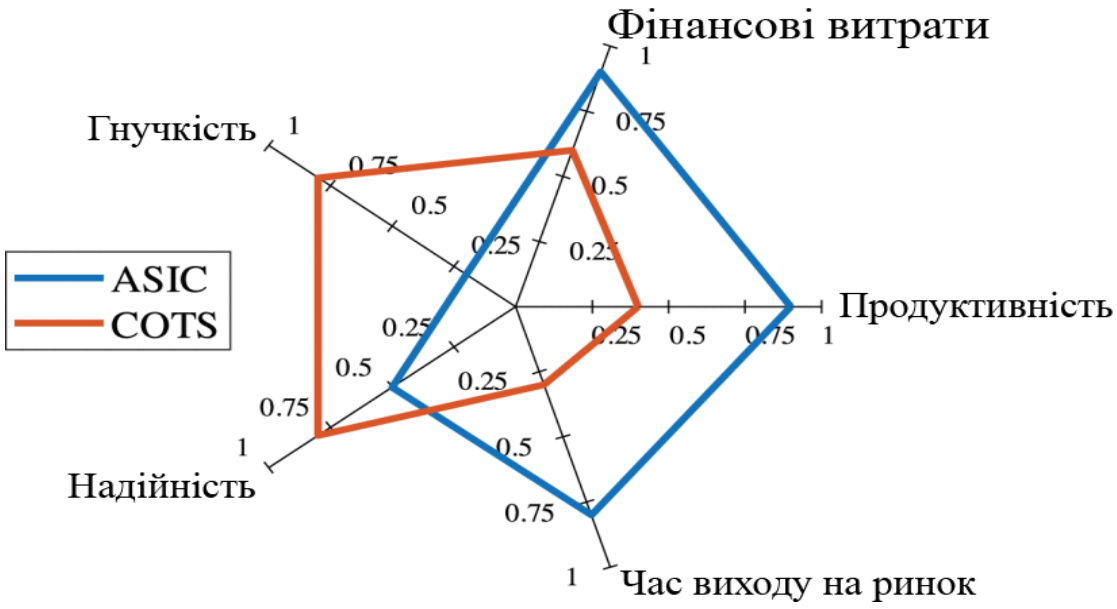

Рисунок 3.4 – Порівняння ASIC та COTS

На основі ASIC можна буде створити найбільш оптимальні умови для повторного застосування в обмежених умовах, що потребують від користувача додаткових витрат часу і фінансових ресурсів. На основі цієї інформації можна зробити висновок про те, що багато доступні COTS мають більш загальні платформи, які зосереджені на дальності і малому енергоспоживанні з широкою ступенем вторинного використання. Виходячи з цього, нами була розроблена загальна методика проектування, яка забезпечує найкращу конфігурація COTS для самого широкого спектра IIoT-WS.

ВИСНОВКИ

Маючи уявлення по особливості IIoT, про технології передачі даних за допомогою різних протоколів та особливості проектування мереж IoT ми розробили нову технологію підбору оптимального вузла та оцінили її продуктивність у промисловому Інтернеті речей (IIoT). Як основу для побудови системи IIoT було взято теоретичний граф, який є модель базисної структури. Далі нам потрібно було оцінити можливість мережевої помилки за допомогою функції неоднозначності, яка була застосована до інформації про підключення. Однак, ми використовували ітераційний метод для визначення оптимальної кількості опорних вузлів на основі конкретних критеріїв їх вибору. Це дає можливість показати, що пропонований нами метод точно створює віртуальну систему координат для мережі IoT. І це ще один важливий момент – ми показали, що метод практично оптимальний, енергоефективний та перевищує метод випадкового вибору щодо швидкості транспортування пакетів та можливості підключення до мережі.

СПИСОК ЛІТЕРАТУРИ

1. Мар'ян М. В. Алгоритми ідентифікації об'єктів Інтернет речей на основі технології блокчейн / Algorithms for Internet things objects identifying based on blockchain technology [Електронний ресурс] / МУРИН Васильович Мар'ян // dspace.wunu.edu.ua. – 2018. – Режим доступу до ресурсу: http://dspace.wunu.edu.ua/jspui/bitstream/316497/32438/1/%D0%9A%D1%96%D0%BC21_%D0%9C%D1%83%D1%80%D0%B8%D0%BD_%D0%9C.pdf.
2. Brooks T. The key to understanding wireless connectivity in the industrial IoT [Електронний ресурс] / Tim Brooks // Infovista. – 2020. – Режим доступу до ресурсу: https://www.infovista.com/blog/understanding-wireless-connectivity-in-the-industrial-iot.
3. Heiney S. Industrial Internet of Things (IIoT) Security: Everything You Need to Know [Електронний ресурс] / Sam Heiney // ImperoSoftware. – 2021. – Режим доступу до ресурсу: https://www.imperosoftware.com/industrial-internet-of-things-complete-guide/.
4. Shea S. LPWAN (low-power wide area network) [Електронний ресурс] / Sharon Shea // IoT Agenda. – 2017. – Режим доступу до ресурсу: https://internetofthingsagenda.techtarget.com/definition/LPWAN-low-power-wide-area-network.
5. EMnify. Cellular IoT: What Business Leaders Should Know [Електронний ресурс] / EMnify // EMnify. – 2020. – Режим доступу до ресурсу: https://www.emnify.com/blog/cellular-iot.
6. Acosta G. The ZigBee Protocol [Електронний ресурс] / Gonzalo Acosta // netguru. – 2018. – Режим доступу до ресурсу: https://www.netguru.com/blog/the-zigbee-protocol.
7. Digi I. Understanding the Zigbee 3.0 Protocol [Електронний ресурс] / International Digi // digi. – 2018. – Режим доступу до ресурсу: https://www.digi.com/blog/post/understanding-the-zigbee-3-0-protocol.
8. Wireless mesh network [Електронний ресурс] // Wikipedia – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Wireless_mesh_network.
9. Почему Bluetooth IoT? [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.mokoblue.com/ru/why-bluetooth-iot/.
10. Вичугова А. RFID [Електронний ресурс] / Анна Вичугова // bigdataschool. – 2019. – Режим доступу до ресурсу: https://www.bigdataschool.ru/wiki/rfid.
11. Weiss J. Wireless Sensor Networking for the Industrial Internet of Things [Електронний ресурс] / J. Weiss, Y. Ross // analog – Режим доступу до ресурсу: https://www.analog.com/ru/technical-articles/wireless-sensor-networking-for-ind-iot.html.
12. Sisinni E. Wireless Communications for Industrial Internet of Things: The LPWAN Solutions [Електронний ресурс] / E. Sisinni, A. Mahmood // ResearchGate. – 2021. – Режим доступу до ресурсу: https://www.researchgate.net/publication/347587880_Wireless_Communications_for_Industrial_Internet_of_Things_The_LPWAN_Solutions.

13. Network Optimization for Industrial Internet of Things (IIoT) [Електронний ресурс] / Khalil, Ruhul, Saeed, Nas // repository.kaust.edu.sa. – 2020. – Режим доступу до ресурсу: https://repository.kaust.edu.sa/bitstream/handle/10754/664172/Final_Manuscript.pdf?sequence=1.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

Мета, завдання магістерської роботи

Актуальність. Промисловий Інтернет речей (IIoT), також відомий як Промисловий Інтернет, поєднує найважливіші ресурси, передові методи прогнозної та розпорядчої аналітики та сучасних промислових робітників. Це мережа безлічі промислових пристроїв, з'єднаних комунікаційними технологіями, у результаті створюються системи, які можуть відслідковувати, збирати, обмінювати, аналізувати та надавати нові цінні відомості, як ніколи раніше. Ці ідеї можуть потім допомогти промисловим компаніям приймати більш розумні та швидкі бізнес-рішення.

У цій магістерській роботі пропонується проектування промислової бездротової системи інтернету речей.

Об'єкт дослідження – Промисловий інтернету речей.

Предмет дослідження – Бездротова система промислового інтернету речей.

Завдання дослідження – в процесі дослідження вирішувалися наступні завдання:

- Аналіз основних положень промислового інтернету речей.
- Дослідити та здійснити аналіз бездротових технологій обміну даних на теперішній час.
- Дослідити та здійснити оцінку по основним архітектурам бездротових технологій обміну даних.
- Розробка моделі архітектури промислового інтернету речей з вибором опорного вузла для находження оптимального рішення

Поняття промислового інтернету речей

Промисловий Інтернету Речей — це мережа з Інтернету речей, яка є об'єднанням комп'ютерів і промислових об'єктів, із встановленими на них датчиками та програмним забезпеченням, з можливістю віддаленого контролю та автономним режимом.

У міру зростання кількості цифрових екосистем виробничих підприємств з ізольованими системами, що самостійно виконують все необхідне для випуску продукції. Виробничі та бізнес-процеси трансформуються у відкриті системи, що об'єднують різних учасників ринку.

Кінцева мета всіх цих трансформаційних перетворень – не випускати продукцію, а надання послуг споживачам

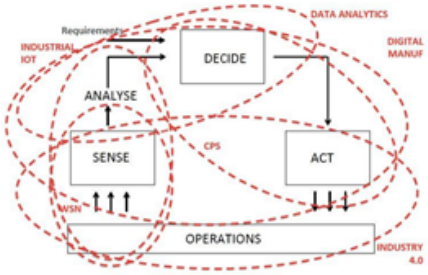

Рисунок 1 – Цифрові парадигми у виробництві

Безпека в IIoT як одна з ключових характеристик

Згідно з протоколом TK26, затвердженим у 2019 році, індустріальні системи будуть використовувати протокол захищеного обміну даними в рамках методичних рекомендацій.

Завдяки високому проникненню промислового інтернету речей у критично важливі інфраструктури, а також у виробничі сектори збільшує кількість потенційних атак на критично важливі об'єкти та виробничі сектори зросла

З кожним днем все більше пристроїв та датчиків підключаються до мережі, а також створюються нові канали зв'язку, сховища даних, портів та кінцевих точок. Високий взаємозв'язок між цими двома факторами становить більше вразливостей у разі їх захисту.

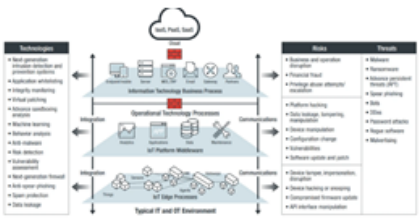

Рисунок 2 – Топологія IoT точення

Сфери використання різних типів бездротових технологій

ТЕХНОЛОГІЯ	СФЕРА ВИКОРИСТАННЯ
LPWAN	Моніторинг, Збір даних
СТІЛЬНИКОВИЙ ЗВ'ЯЗОК (3G/4G/5G)	Моніторинг, Трекінг, Логістика, Збір даних
ZIGBEE ТА ІНШІ ПРОТОКОЛИ MESH	Розумний будинок, Моніторинг
BLUETOOTH/BLE	Розумний будинок, Додатки, Трекінг
WIFI	Розумний будинок, Додатки
RFID И NFC	Ідентифікація, Система пропуску, Логістика
LORAWAN	Трекінг, Моніторинг, Збір даних

Оптимізація мережі для промислового інтернету речей

Розглянемо промислову мережу Інтернету речей, яка складаються з N вузлів, як показано на рисунку 3.1.

Основні еталонні вузли використовуються для складання вимірів стрибків від звичайних вузлів за допомогою керованого мережевого лавинного трафіку. Кожен із вузлів, своєю чергою, розраховує кількість переходів до опорних вузлів, і спрямовує найкоротший шлях (мінімальна кількість надій на опорні вузли) від опорних вузлів до опорних вузлів

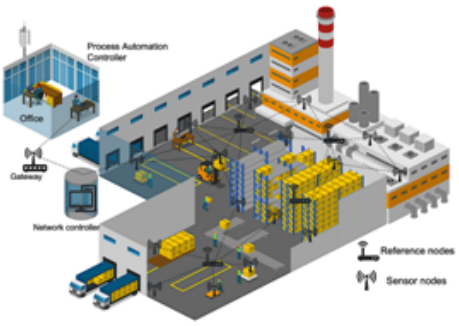

Рисунок 3 – Промислова архітектура для Інтернету речей

Пропонуємий метод вибору опорного вузла

На даному етапі нами розробляється схема підбору оптимального вузла для забезпечення максимальної продуктивності підключення, яка забезпечує максимальну ефективність і надійність VCS.

$$n^{(i)} = \underset{n \in N \setminus R^{(i-1)}}{\arg min} \; a\left(R^{(i-1)} \cup n\right) \quad (1)$$

Цей запропонований ітераційний метод узагальнюється в Алгоритм-1 для вибору випадкових наборів опорних вузлів. І тільки після цього, використовуючи опорні вузли (1), ми вибираємо опорні вузли на їх функцію неоднозначності зв'язності.

Data: N,
Result: $R^{(M)}$,
$R^{(1)} \leftarrow$ случайный узел из множества N;
for $i \leftarrow 2$ ***to*** M ***do***
$n^{(i)} = \underset{n \in N \setminus R^{(i-1)}}{\arg min} \; a\left(R^{(i-1)} \cup n\right)$;
$R^{(i)} \leftarrow R^{(i-1)} \cup n^{(i)}$;
end

Алгоритм – 1 (ітераційний вибір еталонного вузла)

Тестування запропонованого методу

Тут проводиться тестування запропонованого нами методу визначення опори для встановлення у вибраному місці за допомогою MATLAB щодо помилок підключення, швидкості доставки пакетів та загального споживання енергії. Щоб отримати дані про параметри моделі, використовуються таблиця 1 з параметрами моделювання.

Рисунок 4a говорить про продуктивність різних методів вибору опорних вузлів у порівнянні з неоднозначністю мережевих підключень та кількості опорного вузла.
Рисунок 4b показує швидкість доставки для підходу, заснованого на підключенні, та підходу LDR.
Рисунок 4c показує збільшення загального споживання мережі внаслідок збільшення кількості опорних вузлів.

ПАРАМЕТР	ЗНАЧЕННЯ
Область моделювання	100m × 100m
Дальність зв'язку	50m
Кількість опорних вузлів R	0 - 30
Кількість сенсорних вузлів N	100
Моделювання запускається	500
Відсоток ненульових записів β	15%
Поріг чутливості	−120dB

Таблиця 1 – Параметри моделювання

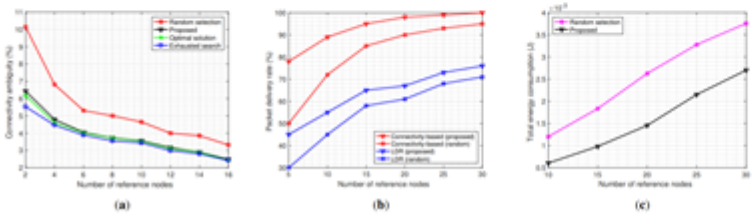

Рисунок 4 – (a) Число опорних вузлів порівняно з неоднозначністю підключення; (b) Кількість опорних вузлів. Швидкість доставки пакетів; (c) Кількість посилальних вузлів. Загальне споживання енергії.

Висновки

Маючи уявлення по особливості IIoT, про технології передачі даних за допомогою різних протоколів та особливості проектування мереж IoT ми розробили нову технологію підбору оптимального вузла та оцінили її продуктивність у промисловому Інтернеті речей (IIoT). Як основу для побудови системи IIoT було взято теоретичний граф, який є модель базисної структури. Далі нам потрібно було оцінити можливість мережевої помилки за допомогою функції неоднозначності, яка була застосована до інформації про підключення. Однак, ми використовували ітераційний метод для визначення оптимальної кількості опорних вузлів на основі конкретних критеріїв їх вибору. Це дає можливість показати, що пропонований нами метод точно створює віртуальну систему координат для мережі IoT. І це ще один важливий момент – ми показали, що метод практично оптимальний, енергоефективний та перевищує метод випадкового вибору щодо швидкості транспортування пакетів та можливості підключення до мережі.