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

Кафедра Інформаційно-телекомунікаційних мереж

«На правах рукопису»
УДК 004.021

«До захисту допущено»
В.о. завідувача кафедри
_____ Лариса ГЛОБА
«___»_____2021р.

Магістерська дисертація

на здобуття ступеня магістра
за освітньо-науковою програмою «Інформаційно-комунікаційні технології»
зі спеціальності 172 «Телекомунікації та радіотехніка»
на тему: «Модифікований метод передачі даних в мережі Інтернету Речей»

Виконав:
студент VI курсу, групи ТІ-91мн
Міхненко Ярослав Олександрович

Керівник:
Професор кафедри ІТМ
д.т.н., с.н.с. Скулиш Марія Анатоліївна

Рецензент:
Професор кафедри ТК
д.т.н., проф. Лисенко Олександр Іванович

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

Київ – 2021 рік

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Інформаційно-телекомунікаційних мереж

Рівень вищої освіти – другий (магістерський)

Спеціальність – 172 Телекомунікації та радіотехніка

Освітньо-професійна програма «Інформаційно-комунікаційні технології»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Лариса ГЛОБА
«___»_____2021 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Міхненку Ярославу Олександровичу

1. Тема роботи «Модифікований метод передачі даних в мережі Інтернету Речей», науковий керівник дисертації професор кафедри інформаційно-телекомунікаційних мереж ІТС Скулиш Марія Анатоліївна, д.т.н., затверджені наказом по університету від «15» березня 2021 р. №817-с.
2. Термін подання студентом роботи 11.05.2021 р.
3. Вихідні дані до роботи: проблема енергозбереження в Інтернеті речей, асинхронний метод енергозбереження при передачі пакетів інформації між вузлами сенсорної мережі Інтернету речей.
4. Зміст роботи:
    1. Проаналізувати проблеми архітектури мережі Інтернету речей.
    2. Проаналізувати методи підвищення енергоефективності мережі Інтернету речей.
    3. Модифікувати метод передачі інформації для підвищення енергоефективності мережі Інтернету речей.
    4. Модифікувати архітектуру мережі Інтернету речей для застосування запропонованого методу.
    5. Провести оцінку запропонованого рішення.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо):
    1. Тема, актуальність, мета, задачі.
    2. Аналіз проблем архітектури мережі в IoT.

3. Аналіз існуючих методів підвищення енергоефективності мережі Інтернету речей.

4. Модифікація методу передачі інформації для підвищення енергоефективності мережі Інтернету речей.

5. Модифікація архітектури мережі Інтернету речей для застосування запропонованого методу.

6. Оцінка запропонованого рішення. Результат роботи.

7. Загальні висновки.

6. Дата видачі завдання 10 жовтня 2019 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Проаналізувати проблеми архітектури мережі Інтернету речей.	10.09.2019 – 10.12.2019	виконано
2	Провести аналіз існуючих технологічних рішень з питанньподовження часу життя мережі Інтернету речей	10.12.20.19 – 15.03.2020	виконано
3	Проаналізувати методи підвищення енергоефективності мережі Інтернету речей.	15.03.2020 – 13.08.2020	виконано
4	Запропонувати модифікацію методу передачі інформації для підвищення енергоефективності мережі Інтернету речей.	13.08.2020 – 22.01.2021	виконано
5	Висвітити місце використання модифікованого методу в сучасній архітектурі Інтернету речей.	22.01.2021 – 07.02.2021	виконано
6	Провести оцінку запропонованого рішення.	07.02.2021 – 25.04.2021	виконано

Студент Ярослав МІХНЕНКО

Науковий керівник Марія СУЛИШ

РЕФЕРАТ

Робота містить 70 сторінок, 15 рисунків, та 10 таблиць. Було використано 35 джерел.

Мета роботи: підвищити енергоефективність сенсорної мережі IoT за рахунок модифікації методу передачі інформації, що дозволить збільшити час роботи вузлів збору та передачі інформації сенсорної мережі IoT.

Проведено детальний аналіз проблем Інтернету речей, особливу увагу було звернено на питання модернізації архітектури мережі задля підвищення енергоефективності та збільшення терміну служби мережі. Детально розібрано метод випадкового циклу Sleep/Wake. Поставлено та виконано завдання модифікації архітектури бездротової сенсорної мережі Інтернету речей. Запропоновано координований метод циклу Sleep/Wake для передачі пакетів інформації в межах сенсорної мережі Інтернету речей. Після проведення оцінки нового методу та його імітаційного моделювання, було зроблено висновок, що такий модифікований метод може бути корисним для впровадження, оскільки:

1. Життєвий цикл мережі за допомогою запропонованого координованого методу обчислення робочого циклу та визначення черг збільшився від 3,8% до 11,25%.

2. Збільшився термін служби сенсорної мережі в порівнянні з асинхронним циклом черг в сенсорних мережах Інтернету речей від 8,4% до 14,8%.

Ключові слова: IoT, Інтернет речей, координований метод, енергозбереження, бездротова сенсорна мережа, архітектура, термін служби мережі, цикл випадкового режиму.

ABSTRACT

The thesis contains 70 pages, 15 figures, and 10 tables. 35 sources have been used.

The purpose of the work is to increase the energy efficiency of the IoT sensor network by modifying the method of information transmission, which will increase the operating time of the nodes of collection and transmission of information of the IoT sensor network.

The detailed analysis of the problems of the Internet of Things has been made. Special attention has been paid to modernizing the architecture of the network for improving its energy efficiency and extending its lifetime. The method of random Sleep/Wake cycle has been analyzed in detail. The task to modify the architecture of the wireless sensory network of the Internet of Things has been fulfilled. The co-ordinated Sleep/Wake cycle method is proposed for transmitting information packets within the sensory network of the Internet of Things. After evaluating the new method and its simulation model, it was concluded that this modified method might be useful for implementation, since:

1. The life cycle of the network with the proposed coordinated method for calculating the duty cycle and queue determination increased from 3.8% to 11.25%.

2. The lifetime of the sensory network increased from 8.4% to 14.8%, compared to the asynchronous cycle of queues in the sensory networks of the Internet of Things.

Keywords: Internet of Things, coordinated vethod, energy saving, Wireless Sensor Network, architecture, network lifetime, random mode Cycle.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

IoT	Internet of Things
SNMP	Simple Network Management Protocol
АСКТП	Автоматизована система керування технологічним процесом
GSM(Global System for Mobile communication)	Технологія бездротового телефонного зв’язку
NB-IoT(Narrow band IoT)	Вузькосмуговий Інтернет речей
LPWAN	Широкосмуговий мережевий протокол малої потужності.
WSN(Wireless Sensor Network)	Бездротова сенсорна мережа

ВСТУП

Інтернет речей (IoT)[4] - це розширення підключення Інтернету до фізичних пристроїв і предметів повсякденного життя. З вбудованою електронікою, підключенням до Інтернету та іншими формами апаратних засобів (наприклад, датчиками), ці пристрої можуть спілкуватися та взаємодіяти з іншими через Інтернет, та їх можна дистанційно перевіряти та контролювати.

Актуальність. Визначення Інтернету речей з'явилось завдяки поєднанню декількох технологій, а саме: аналітиці в реальному часі, машинному навчанню, датчикам товарів і вбудованим системам. Традиційні галузі вбудованих систем, бездротові сенсорні мережі, системи управління, автоматизація (включаючи автоматизацію будинку й будівлі), та інші впливають на створення Інтернету речей. На споживчому ринку, технологія IoT є найближчим синонімом продуктів, що відносяться до концепції «розумного дому», що охоплює пристрої та прилади (наприклад, термостати, системи домашньої безпеки та камери, світильники та інші побутові прилади), які підтримують одну або більше загальних екосистем, і їх можна контролювати за допомогою пристроїв, пов'язаних з цією екосистемою, таких як смартфони та смарт-динаміки.

Проте незважаючи на велику кількість моментів, в яких Інтернет речей здатен спростити життя людству, існує маса проблем, які необхідно вирішити. Однією з таких проблем є питання енергозабезпеченості безпровідних сенсорів в мережах Інтернету речей.

Предмет дослідження: моделі та методи передачі даних в мережі Інтернету Речей.

Об'єкт дослідження: процес керування енергозбереженням вузлів збору та передачі інформації сенсорної мережі Inernet of Things.

Мета роботи: підвищити енергоефективність сенсорної мережі IoT за рахунок модифікації методу передачі інформації, що дозволить збільшити час роботи вузлів збору та передачі інформації сенсорної мережі IoT.

Для досягнення мети було поставлено та вирішено наступні задачі:

1. Проаналізувати проблеми архітектури мережі Інтернету речей.
2. Проаналізувати методи підвищення енергоефективності мережі Інтернету речей.
3. Вдосконалити метод передачі інформації для підвищення енергоефективності мережі Інтернету речей за рахунок додавання буферу та плануванням процесом передачі.
4. Вдосконалити спосіб функціонування мережі Інтернету речей з урахуванням запропонованого методу.
5. Провести порівняльний аналіз запропонованого методу з існуючими рішеннями з використанням математичного моделювання.

Наукова новизна:

Вдосконалено метод передачі інформації в сенсорній мережі IoT, який дозволяє підвищити енергоефективність даної мережі IoT та збільшити час роботи вузлів за рахунок додавання буферу та планування процесу передачі.

Практичний результат роботи:

Застосування запронованого методу дозволяє збільшити час життя сенсорної мережі на 14,8-20,6% порівняно з сенсорними мережами Інтернету речей, що застосовують асинхронний цикл черг.

РОЗДІЛ 1
АНАЛІЗ ПРОБЛЕМ ІНТЕРНЕТУ РЕЧЕЙ

1.1. Сучасна проблематика інтернету речей

Незважаючи на те що сегмент «Інтернету речей» зараз переживає період активного росту, схоже, світ досі не готовий сприйняти всі переваги даної концепції[34]. Потенційним замовникам не вистачає фахівців, інвестицій та знань.

Інтернет речей - це не тільки концепція; в її основі лежать цілком конкретні елементи і технології. Щоб внести більше ясності, перерахуємо основні з них.

По-перше, це сенсори і датчики – кінцеві пристрої IoT, збирають ті чи інші дані. Друга група, актуатори – також кінцеві пристрої, але вже мають вплив на навколишнє середовище, наприклад, освітлювальні прилади, електронні замки, динаміки і т.д.

Згадані елементи підключаються до шлюзів, які представляють собою спеціалізовані мікрокомп'ютери, здатні здійснювати первинний аналіз інформації від датчиків або давати певні команди актуаторами.

У масштабних системах шлюзи підключаються до повноцінних серверів, які відповідають за більш складну обробку і зберігання даних, а ті, в свою чергу, утворюють мережу або хмару.

Зв'язок між датчиками/актуаторами і шлюзами здійснюється за допомогою спеціалізованих енергоефективних технологій передачі даних, наприклад, LoRa або ZigBee. Шлюзи, в свою чергу, взаємодіють з серверами за класичними мережами Ethernet або Wi-Fi.

Коли тема «Інтернету речей» тільки починала розвиватися, то в широкому інформаційному полі досить швидко намітилося два напрямки її розвитку - «важкі» корпоративні рішення і рішення призначені для користувача системи. Прикладом першого з них є промисловий Інтернет речей (Industrial Internet of Things, IIoT), друга ж група об'єднує різну споживчу електроніку і рішення типу «розумний дім» (точніше навіть,

«розумне житло»). Довгий час здавалося, що це два відносно незалежних напрямки, кожен з яких буде формувати окремий ринок, де за вигоду від використання унікальних технологій будуть платити, відповідно комерційні компанії і кінцеві споживачі. Зараз же стає все більш очевидним, що головним вигодонабувачем залишається бізнес, в першу чергу - великий. Одна з головних особливостей систем IoT – збір і аналіз детальної інформації – була дуже доречною для багатьох компаній. У сучасному, високо конкурентному світі бізнесу, особливо в економічно розвинених країнах, на ринку перемагає той, хто краще знає свого клієнта і враховує найдрібніші нюанси, що впливають на його вибір. Отримати таке знання можна за допомогою технологій IoT, збираючи інформацію з мільярдів призначених для користувача пристроїв – смартфонів, розумних годинників, побутових приладів, датчиків розумного будинку і т.д. При цьому кінцеві споживачі теж отримують певну перевагу у вигляді додаткових сервісів і зручностей, котрі забезпечує їм «розумна» споживча електроніка, але компанії набувають саме фінансову вигоду – ту, що потім можна перетворити в гроші.

Але якщо компанії навчилися за допомогою Інтернету речей збирати дані і завертати їх собі на користь, значить, у них-то, швидше за все, справи йдуть чудово і за проектами IoT повинні буквально шикуватися черги замовників? У теорії начебто так, але, як завжди, хороші ідеї часто розбиваються об невблаганну практику. Інтернет речей – класичний приклад концепції, що обігнала свій час. Сьогодні у науковців існує маса підходів, ідей, навіть втілених розробок. Але не вистачає головного – універсальної інфраструктури передачі даних і єдиних стандартів. Домінуюча технологія також відсутня. Замість неї – десятки галузевих варіантів реалізації IoT. Логічно, що роль середовища передачі для основної маси пристроїв Інтернету речей повинні виконувати мережі операторів мобільного зв'язку, які охоплюють сьогодні більшу частину населення Землі. Але проблема в тому, що нинішні формати 3G і навіть 4G погано підходять для масового розгортання інфраструктур IoT – швидкості передачі даних повинні бути

більші (рис 1.1), а затримки менше. Наприклад, в США нормальною затримкою на мережах LTE вважається 50 мс – більш ніж достатньо для людського сприйняття, але в разі міжмашинних інтерфейсів, що використовуються пристроями IoT, бажано, щоб затримка була істотно менше – в межах декількох мілісекунд.

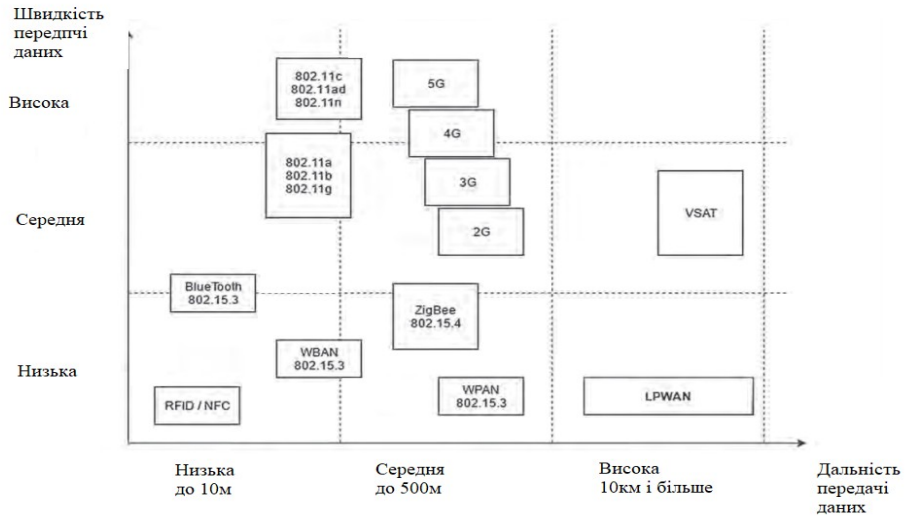

Рис. 1.1. Порівняння різних радіотехнологій, використовуванихдля побудови мереж IoT.

Це можуть забезпечити тільки мобільні мережі п'ятого покоління (5G). Власне, з їх повсюдним впровадженням багато виробників пов'язують майбутній швидкий розвиток IoT, та й оператори по всьому світу так чи інакше розгорнуть 5G, як універсальну технологію передачі даних, в перспективі найближчих декількох років. Тому галузеві технології, наприклад, LPWAN, швидше за все будуть мати досить вузьке застосування, оскільки для них буде потрібно розгортати власні спеціалізовані мережі, замість того щоб використовувати вже готову інфраструктуру операторів зв'язку.

Ще одна проблема полягає в можливості масштабування. Класична ситуація – інженери розробляють відмінний проект, створюють прототипи і все працює як задумано, поки мережа об'єднує всього кілька пристроїв. Коли

ж проект швидко зростає і кількість підключень обчислюється тисячами, виникають несподівані технологічні проблеми, які просто неможливо було виявити на стадії прототипу.

Крім того, фахівці, що зіткнулися на практиці з великими проектами IoT, говорять про те, що складність подібних впроваджень зростає експоненціально, у міру підключення нових пристроїв. В результаті все більше часу починає йти на пошук помилок і налагодження процесів – в якийсь момент витрати на підтримку мережі IoT (як тимчасові, так і фінансові) починають перевершувати вкладення в її розвиток. Подібної ситуації сьогодні вдається уникнути, як правило, в тих проектах, де витриманий збалансований підхід до вимог функціональності та збору даних, іншими словами там, де обходяться розумним мінімумом того і іншого.

Судячи з усього, Інтернет речей чекає перспективне майбутнє. Адже ця концепція дуже вдало вбирає в себе всі самі передові технології. Поява 5G відкриває нові перспективи щодо розвитку інфраструктури IoT, інструменти роботи з великими даними дають можливість здійснювати глибокий і ефективний аналіз інформації, граничні обчислення (Edge Computing) дозволять розвантажити дата-центри і магістральні канали зв'язку за рахунок локальних обчислень. Великі надії покладаються на майбутні досягнення в сфері штучного інтелекту, за допомогою якого вдасться забезпечити зручне управління мережами IoT і їх безшовне масштабування. Хмарні платформи стануть основою для обробки і надійного зберігання даних, а блокчейн забезпечить нові послуги з високим рівнем безпеки.

1.2. Класифікація проблем Інтернету речей

Інтернет речей починається або закінчується однією подією: звичайний рух, зміна температури або тиску, або, може бути, важіль замикає замок. На відміну від багатьох існуючих IT-пристроїв, Інтернет речей здебільшого пов'язаний з фізичною дією або подією. Він формує реакцію на певний фактор реального світу[35]. При цьому один-єдиний датчик може

згенерувати величезний обсяг даних, наприклад, акустичний датчик для профілактичного огляду обладнання. В інших випадках всього одного біта даних достатньо, щоб передати життєво важливі відомості про стан здоров'я пацієнта. Якою б не була ситуація, системи датчиків еволюціонували відповідно до закону Мура[17] та розділилися на класи в яких вони використовуються (Рис. 1.2). Закон Мура каже, що кількість транзисторів на кристалах мікросхем подвоюватиметься кожні 24 місяці починаючи з 1965 року. Після створення графіку(Рис. 1.3), було виявлено закономірність, а саме, що нові моделі випускалися через 18-24 місяці після виходу попередніх моделей. Також їх місткість кожного разу зростала майже в два рази. Варто зазначити, що системи датчиків зменшилися до субнанометрових розмірів і стали в рази дешевшими. Саме цим апелюють ті, хто прогнозує, що до Інтернету речей будуть підключені мільярди пристроїв, і саме тому ці прогнози виправдаються в майбутньому.

Тому, обговорюючи Інтернет Речей, необхідно розглядати мікро- та макро-електромеханічні системи, датчики і інші типи недорогих граничних пристроїв і їх електрофізичних властивостей. Також це стосується силових і енергетичних систем, що необхідні для живлення цих пристроїв. Буде неправильно вважати, що граничні пристрої забезпечуються енергією за замовчуванням. Мільярди маленьких датчиків все одно потребують великої кількості енергії[10].

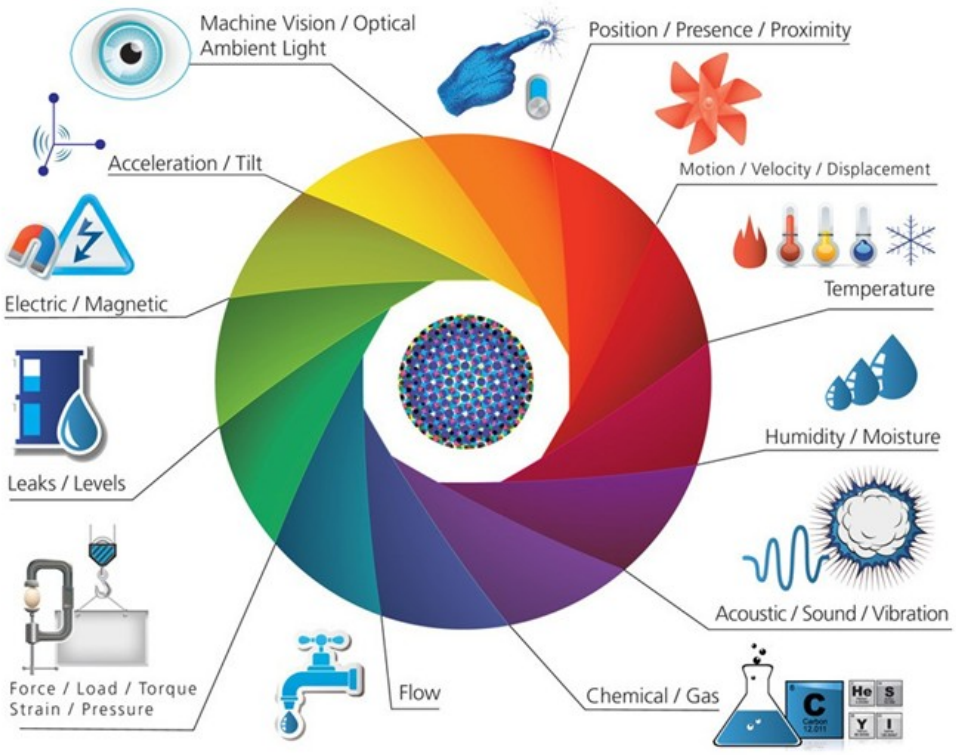

Рис. 1.2. Варіанти існуючих датчиків та сенсорів.

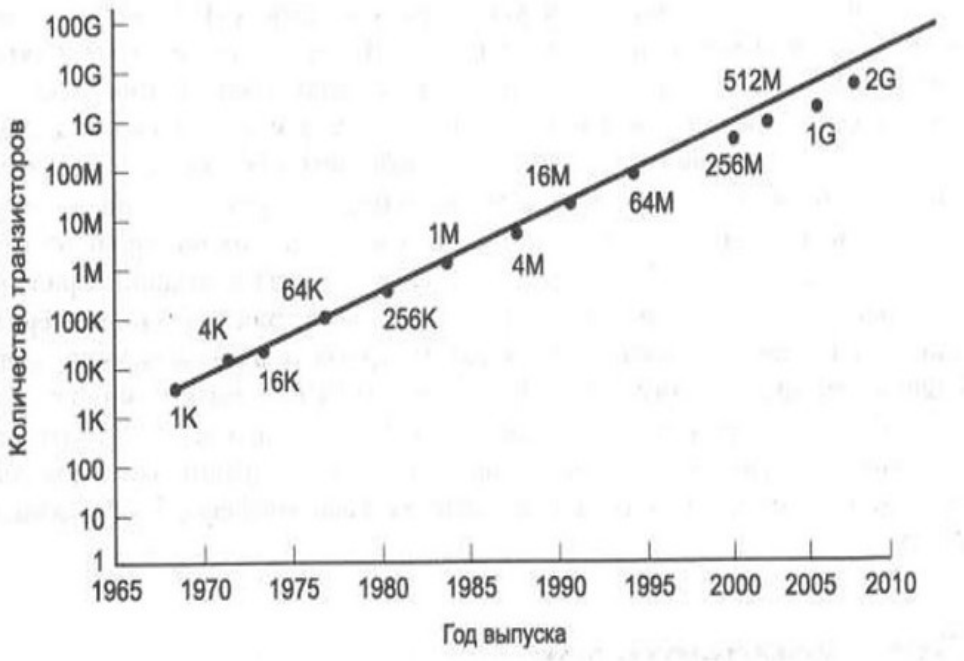

Рис. 1.3. Графік закону Мура Крапки на графіку – об’єм пам’яті в бітах.

Концепція Інтернету речей(IoT) зіткнулася з вираженою критикою, особливо стосовно проблем в області конфіденційності та безпеки, пов'язаних з цими пристроями, та можливості проникнення до певної екосистеми з їх допомогою[22]. Також була висунута на обговорення проблема енергозбереження в бездротових сенсорних датчиках в мережах.

1.3. DoS-атаки в Інтернеті речей

Оскільки з кожним днем збільшується кількість пристроїв, що підключаються до мережі, вони вносять вклад в категорію пристроїв, які легко захоплюються в ботнети і можуть бути використані для розподілених атак зловмисників. Використання розподілених атак робить відстеження джерел атаки більш важким, в той же час полегшуючи можливість знищення пристроїв і додатків, на які вони орієнтовані. Наприклад, розподілені атаки стали варіантом нападу для здирників і активістів на мережі Інтернету речей[20]. Одним з способів атаки є використання Simple Network Management Protocol (SNMP, Простий протокол керування мережею) як особливу форму DoS-атак, які дозволяють зловмисникові захопити незахищені мережеві пристрої: датчики, камери, принтери, роутери і тому подібні пристрої. Надалі їх використовують як ботів для атаки на третіх осіб. Ця форма DDoS-атаки збільшує кількість пристроїв, які можуть бути скомпрометовані, а також віддалених пристроїв, таких як датчики і принтери, які з найменшою вірогідністю оснащені необхідним програмним забезпеченням для захисту, що робить їх більш схильними до атак. Simple Network Management Protocol (SNMP) використовує протокол призначених для користувача датаграм.

Ідентифікуються DoS-атаки, які використовують SNMP як якусь форму посилення стандартної атаки, в зв'язку з тим, що SNMP-запити можуть призводити до відповідей, які в три рази частіше, ніж можна було б очікувати раніше. «У три рази частіше» в даному випадку означає, що число відповідей на запит SNMP-протоколу в три рази більше звичайного числа. Зловмисник,

таким чином має можливість сканувати масив IP-адрес з метою виявлення SNMP-вузлів, які потім можуть бути використані для відправки SNMP-запиту, що використовує цільовий сервер для підміни IP-адрес, після чого відповіді від вузла повністю заповнюють пропускну здатність мережі, роблячи її тим самим недоступною.

Вважається, що для захисту від DoS-атак необхідно ввести ідентифікацію всіх пристроїв, які можуть бути доступні через свою мережу і при цьому є чутливими до злому. Віддалений доступ до пристроїв і управління пристроями надають більшу зручність у використанні, додають компромісні рішення, які повинні бути надійно захищені і керовані. Як правило, обмежені обчислення і жорстка пам'ять девайсу означають, що вона відкрита для ресурсномістких атак. Це надає можливість зловмисникам безперервно відправляти запити для обробки конкретного пристрою в силу виснаження його ресурсів. До того ж, виявленно, що внесення фізичних перешкод в канали зв'язку може бути використано для запуску DoS-атаки, яка буде відключати канали зв'язку між пристроями. Нарешті, було встановлено, що використання великої кількості пакетів, що переповнюють мережу, може також порушити доступність мережі.

1.4. Прослуховування в Інтернеті речей

Було виявлено, що пасивні атаки можуть призначатися для каналів зв'язку, таких як Інтернет, локальні провідні мережі і бездротові мережі, для отримання даних з потоку певної інформації. Очевидно, що якщо зловмисник отримає доступ до певної інфраструктури, то він може відновити інформацію, що проходить через неї та використовувати її в своїх цілях. Поки заходи безпеки не спрямовані на захист даних і інформації, ймовірність того, що зловмисник зможе отримати доступ до самої системи і вкрасти дані, є реальною. Однією з найбільш серйозних проблем в масштабному прийнятті Інтернету речей, з точки зору користувача, є управління даними. Варто зазначити, що обережність не слід плутати з власними даними. В

найближчому часі, розвиток Інтернету речей призведе до ситуації, коли доступ і керування даними будуть важливішими, ніж володіння інформацією. І на данний момент, можна стверджувати, що захист особистих даних в Інтернеті речей має величезні проблеми.

Ще одна проблема, з якою зіткнеться Інтернет речей – це спільне використання даних. У парадигмі Інтернету речей всі дані важливі, хоча забезпечення даними – це результат соціального договору між клієнтами і компаніями. Компанія забезпечує формальні ціни або безкоштовні послуги в обмін на особисті дані замовника. Потім ці дані можуть бути використані в подальшому розвитку послуг і продуктів, які будуть задовольняти потреби споживача, а також будуть продані маркетологам і рекламодавцям. Можна використовувати сторонні додатки, що основані на базовому обслуговуванні, особливо при переманюванні клієнтів і певних даних з таких же програм. Для великих корпорацій і визнаних мереж це може стати згубною практикою, так як ці програми в кінцевому випадку можуть переманити клієнтів. Великі корпорації в таких випадках повинні збалансувати комерційні міркування з точки зору їх відкритого вихідного коду.

1.5. Вузол захоплення в Інтернеті речей

Такі речі, як вуличні ліхтарі і побутова техніка, фізично знаходяться в специфічних умовах, і замість того щоб вивести їх з ладу, зловмисники можуть спробувати витягти інформацію з цих речей. Замість атаки на сам пристрій зловмисник може бути націлений на інфраструктуру, яка використовується для зберігання даних організації або для обробки даних. Якщо, з іншого боку, фактичні дані в Інтернеті речей розподілені, то для створення і обробки інформації будуть використовуватися різні об'єкти. Це означає, що хакерам знадобиться багато часу і сил, щоб контролювати таку кількість ресурсів. Проте було встановлено, що розподіл ресурсів діє як двосічний меч. Якщо зловмисники зацікавлені в тій чи іншій частині інформації, то вони можуть орієнтуватися на системи, що керують

конкретною інформацією, розташованою в центральних об'єктах. Дійсно, зловмисники можуть використовувати «партизанську» стратегію, взявши під свій контроль невелику ділянку мережі, і потай впливати на всю систему.

Через обмеженість ресурсів вузлів, розподіленої організованої структури і динамічної зміни топології мережі існує безліч загроз, в тому числі можливість фізичного захоплення, адже багато вузлів нерухомі і можуть бути легко скомпрометовані за допомогою фізичного доступу. Інша загроза виходить від атаки «грубою силою» (метод повного перебору, brute force), що особливо критична в разі, коли розмір сховища вузла і його обчислювальні потужності сильно обмежені. Крім того, структура апаратних засобів деяких вузлів проста і зрозуміла, що визначає можливості для нападника скомпрометувати її. Маршрутизовані атаки також можливі в Інтернеті речей, особливо у випадках, коли ретрансляція і пересилання даних здійснюються в рамках уразливого процесу збору даних. Вузли також уразливі для захоплення при DoS-атаці у зв'язку з їх здатністю кінцевої обробки, в той час як зловмисники можуть активно або пасивно красти конфіденційну інформацію.

1.6. Фізична безпека датчиків

Фізичні атаки можуть пошкодити датчики пристроїв Інтернету речей або навіть привести їх до повної непрацездатності, що являє собою явну загрозу безпеці. Наприклад, зловмисник може увійти в будинок, де розташований датчик, і виявити супутні електронні та фізичні сигнали інших сенсорів за допомогою обладнання для виявлення радіо-, тепло-, магнітних, візуальних та інших електронних сигналів. Потім зловмисник може визначити розташування датчиків на підставі властивостей сигналів, після чого вони можуть бути відключені фізично, знищені або вкрадені. Фізичне руйнування може бути здійснено з використанням нагрівання, фізичної сили або порушення цілісності ланцюга датчиків, що робить датчики не функціонуючими. Крім того, легко запустити фізичні атаки з використанням

старих технологій через уразливість датчиків, особливо невеликих. Атаки такого роду неминучі для сенсорних мереж Інтернету речей. Оскільки зловмисник знаходиться в безпосередній близькості до мережі при атаці такого роду, у нього є можливість реагувати на захисні механізми, на відміно від віддалених атак.

1.7. Проблеми вибору хмарного сервісу для обробки данних

На сьогоднішній день, кількість IoT проектів зростає та стають вони більш масштабними, тому тепер розробники мають можливість стикатись з новим полем для створення інфраструктури. Куди відправляти дані, отримані від різних датчиків, і яка правильна архітектура для їх аналізу?

Першою на думку спадає «хмара». Хмарні технології дають можливість масштабованості та можливості просто підключення, що, безумовно, є необхідними функціями для IoT-платформи, проте тільки цих можливостей недостатньо. Для успішного створення IoT-додатків необхідний комплексний підхід, що базується на знаннях як в області операційних технологій, так і в області інформаційних технологій.

На теперішній момент існує три види хмарних сервісів:

- Публічна хмара (Public Cloud);
- Приватна хмара (Private Cloud);
- Гібридна хмара (Hybrid Cloud).

Для кращого розуміння хмарних сервісів в IoT, необхідно розглянути функціональні властивості кожного з сервісів.

Публічна хмара має такі переваги як технологічна та фінансова гнучкість, простота та ефективність використання, легке масштабування, надійність та відмовостійкість. Проте існують певні недоліки даної моделі хмарних сервісів, такі як залежність від швидкості і стабільності доступу в Інтернет та контроль IT-інфраструктури сторонньою компанією (сервіс-провайдером).

Приватний хмарний сервіс відрізняється покращенням у таких аспектах як висока швидкість роботи, використання ресурсів тільки однією компанією власником, високий рівень безпеки та повним контролем обладнання та програмного забезпечення.

Гібридна хмара з’являється все частіше, у зв’язку з необхідністю одночасного використання як публічних, так і приватних хмарних сервісів, так як саме гібридний хмарний сервіс об’єднує переваги обох згаданих підходів. Публічна хмара надає гнучкість, приватна – високий рівень безпеки та кращий контроль ресурсів. Ключовою особливістю гібридного підходу є те, що існує можливість функціонування всієї хмарної інфраструктури як єдиної системи під загальним централізованим управлінням; ідеальний випадок централізованого управління є створення однорідного пулу, що надає можливість динамічно виділяти ресурси за необхідною вимогою в повній відповідності до внутрішніх регламентів безпеки та політик доступу.

Для наочності, можна звести порівняння трьох видів хмарних сервісів в невелику таблицю (таблиця 1) – чим більше «зірочок», тим вище відповідність зазначеному показнику[24]:

Таблиця 1.1

Порівняння публічної, приватної та гібридної хмар

Характеристика/тип хмари	Публічна	Приватна	Гібридна
Перетворення CapEx в OpEx		-	
Продуктивність і доступність			
Гнучкість конфігурацій			
Масштабованість			
Прогнозованість витрат			
Підтримка застарілих додатків	-		
Безпека даних			
Продуктивність при роботі з потужними аналітичними онлайн-системами			
Продуктивність при роботі з «важкою» графікою			
Контроль над IT-інфраструктурою з боку власника даних	-		

У зв’язку з гарними показниками масштабованих гібридних IoT-хмар, було продовжено їх модернізацію та створено нову архітектуру – конвергентний модульний сервер[7]. Порівняно зі звичним сервером з масштабованим процесором, конвергентні модульні сервери надають більш потужні і в той же час гнучкі обчислювальні ресурси. Модульні сервери, використовуючи багатоядерні процесори з більш низьким енергоспоживанням, мають можливість знизити загальне енергоспоживання, а також зменшити простір необхідний для одночасного масштабування продуктивності всередині платформ та покращення взаємодії між ними. Такі сервери спеціально розроблені для легких робочих навантажень на веб-рівні. Архітектура конвергентного модульного сервера дозволяє збалансувати навантаження між процесорними ядрами при малій затримці, завдяки

з’єднанню кількох процесорів в одному корпусі за допомогою швидкої, настроюваної структури з низькою затримкою.

Також, перевага, якою володіють модульні сервери в питанні енергоспоживання – це динамічний режим очікування, який управляє потужністю для кожного сервера[21]. Ретельно розподіляючи завдання, дає можливість процесорам перебувати в режимі сну або відключати живлення, коли вони не задіяні.

1.8. Проблема енергоефективності

На даний момент, вчені вважають, що однією з найбільших проблем в Інтернеті речей є проблема енергоефективності [2],[3],[13],[26] та часу життя бездротових сенсорних датчиків в мережах Інтернету речей. Дана проблема з'являється при розгортанні систем в місцях, що віддалені від необхідного постійного енергопостачання (наприклад, поля, гори, печери, ліси). Енергія кожного вузла є обмеженою та не завжди є можливісь замінити джерело живлення на інше. В ситуації з розгортанням системи в важкодоступних місцях, наприклад відкритий космос або навколо орбіти землі, неможливо буде часто та за терміновою неодхідністю замінювати батареї вузлів, а також це буде не дуже доцільно з фінансового питання.

Тож визначивши дану проблему, вчені запропонували використання різниз алгоритмів та режимів роботи і очікування систем. Дані режими спрямовані на підвищення часу життя системи, так як, саме передача пакетів з інформацією споживає близько 70% всієї енергії вузлів.

1.9. Загальні положення архітектури Інтернету речей

Архітектура Інтернету речей[5],[10],[16],[19] відрізняється в залежності від реалізації. Тим не менше вона дещо схожа на архітектуру класичних систем АСКТП (Автоматизована система керування технологічним процесом)[13],[18]. Один із прикладів архітектури показаний на рис.1.4.

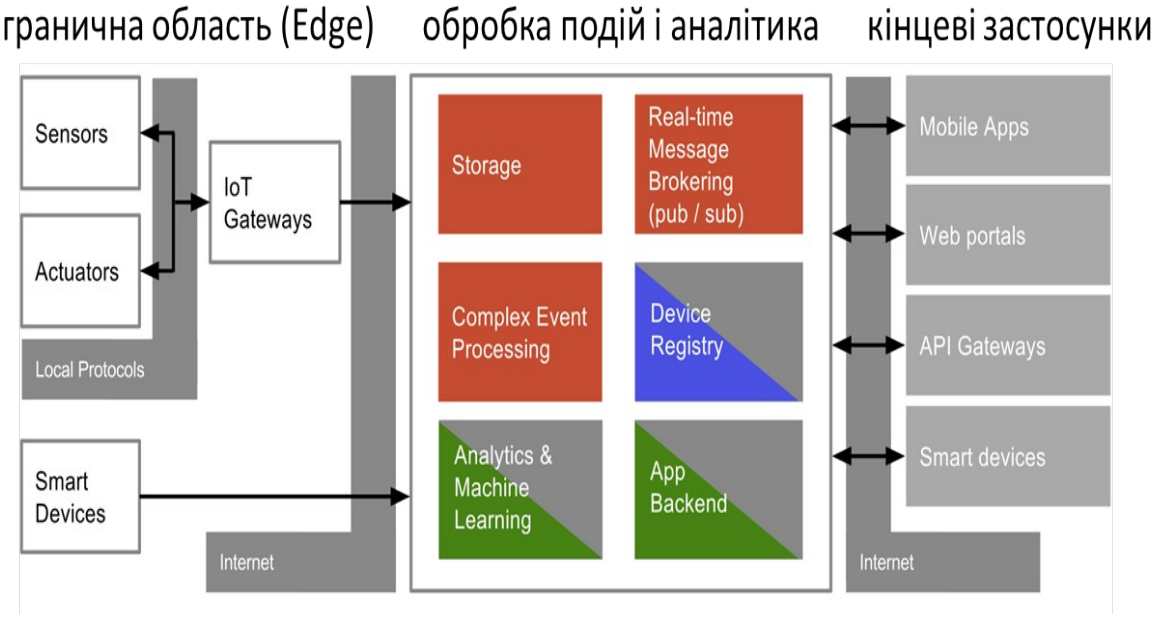

Рис. 1.4. Загальна архітектура Інтернету речей

Взаємодія з «речами» відбувається через датчики (sensors) та виконавчі механізми (Actuators), аналогічно як це робиться в АСКТП для будь якого об’єкту керування. Ці датчики разом з усією інфраструктурою для інтеграції з рівнем обробки подій через мережу Internet формують так звану граничну область (Edge).

Події (дані) що поступають з граничної області зберігаються і обробляються відповідно до задачі (рівень обробки подій і аналітики, event processing, Platform). На цьому рівні події зберігаються (storage), обробляються (Event Processing), перенаправляються потрібним додаткам (Real-Time Message Brokering, Stream Processing). Також на цьому рівні відбувається керування та адміністрування пристроями з граничної області (Device Registry, Edge Device Management). Події обробляються з

використанням аналітичних сервісів (Analytics) на основі них проводиться машинне навчання (Machine Learning), що дозволяє зробити певні висновки про об’єкт. Цей рівень як правило реалізований з використанням хмарних (Cloud) або туманних (Fog) обчислень. Якщо провести аналогію с АСКТП, то це рівень контролерів та SCADA (за виключенням функцій HMI). Отримання результатів, контроль, віддалене керування та адміністрування системи проводиться через кінцеві застосунки з використанням Internet. Цей рівень можна умовно порівняти з HMI в АСУТП.

На рис. 1.5 показана подібна наведеній вище архітектура, однак у вигляді сервісів. На ньому область Edge представлений у вигляді датчиків (Sensors), Device Hub/Gateway (збір та маршрутизація даних) та Device Management (керування пристроями). Останні частково виконуються як хмарні обчислення так і на граничних пристроях. Усі функції збереження та первинної обробки подій (даних) зведені до Data Management. Усі інші функції обробки, в тому числі аналітичні показані як додатки PaaS, що взаємодіють з сервісами керування даних через API (Application Program Interface).

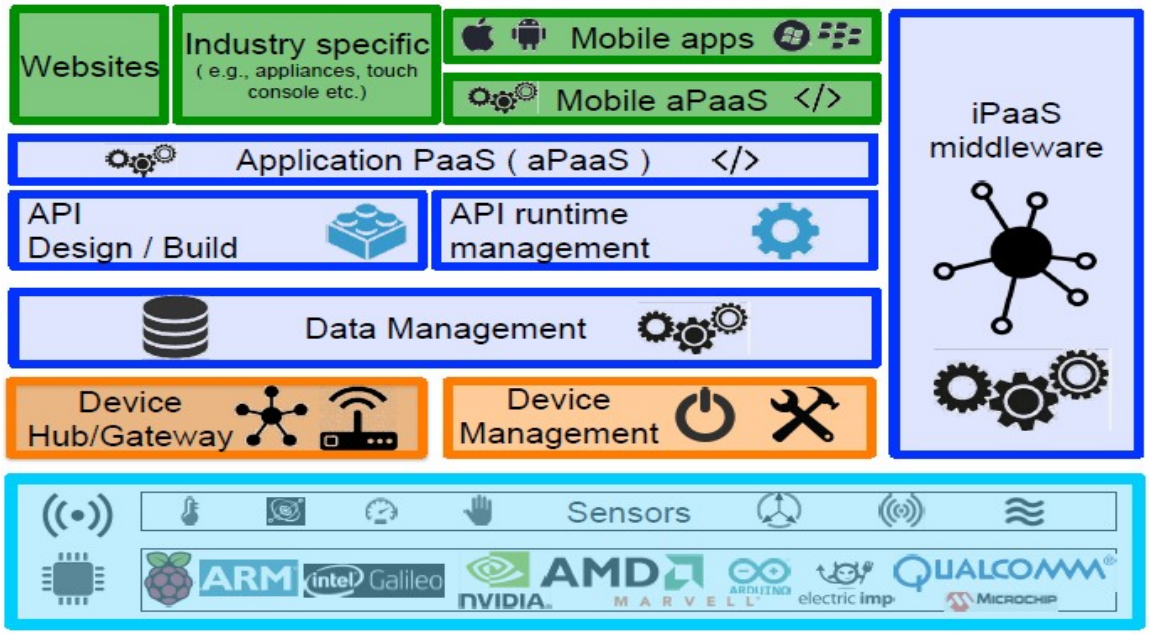

Рис. 1.5. Архітектура Інтернету речей у вигляді сервісів

Висновки

1. Проаналізовано та виділено основні існуючі проблеми Інтернету речей, як в питаннях комп’ютерної безпеки, так і в питаннях фізичної безпеки вузлів та систем.

2. Виділено проблему енергоефективності та часу життя систем Інтернету речей при передачі пакетів інформації між вузлами.

3. Приведено загаліні положення в архітектурі Інтернету речей та пояснено які саме задачі виконують елементи систем в залежності від їх знаходженні в відповідному з трьох рівнів. Також представлена архітектура у вигляді сервісів.

РОЗДІЛ 2

АНАЛІЗ ІСНУЮЧИХ ТЕХНОЛОГІЧНИХ РІШЕНЬ З ПИТАННЬ ПОДОВЖЕННЯ ЧАСУ ЖИТТЯ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

Щодня перед жителями планети Землі постають нові виклики і завдання: то нависне всесвітньою загрозою глобальне потепління, то з'ясується, що існуючі методи «очищення» (або, скоріше, не забруднення) навколишнього середовища є, якщо не шкідливими, то, принаймні, не в тій мірі, в якій вважали раніше, приносять реальну користь [27]. Для тих, хто робить гроші, і для тих, хто підраховує збитки, завдані природі першими, постає питання оптимізації різних процесів, в тому числі під ракурсом визначення можливостей, а саме:

1) витрачати менше енергії на підтримку того ж рівня енергетичного забезпечення;

2) позбутися від непотрібних процесів, або скоротити рівень споживання до мінімально прийнятного.

Для досягнення нових економічних висот, а також порятунку екології, підходить безліч рішень, але сьогодні ми спробуємо зупинитися на тому, чи можуть технології Інтернету речей дозволити вивести енергетичну ефективність та енергозбереження на новий рівень, а також оцінити необхідність таких рішень.

2.1. Що повинно бути відомо про енергетичну економію «споживачеві»?

Можна припустити, що про проблеми ефективного та ощадливого споживання енергії люди стали замислюватися з часів усвідомлення, що деякі ресурси є невідновні, однак процес піддався формалізації фактично лише в 70х роках минулого століття, під час енергетичної кризи. [28] Як ілюструє приклад рішень того періоду, фахівцями наводиться еволюція технологій будівництва житлових будинків - від «мають величезні запаси для підвищення теплової ефективності» до будинків-термосів. [29] Хоча зараз

стоять завдання іншого характеру – нові інструменти гіпотетично можуть принести навіть більш відчувану користь[30].

Законодавчо ці поняття є наступними: під енергетичною ефективністю розуміються показники, що відображають ставлення корисного ефекту від використання енергетичних ресурсів до витрат енергетичних ресурсів, виробленими з метою отримання такого ефекту; під терміном енергозбереження мається на увазі реалізація організаційних, правових, технічних, технологічних, економічних та інших заходів, спрямованих на зменшення обсягу використовуваних енергетичних ресурсів при збереженні відповідного корисного ефекту від їх використання. Для зручності в подальшому визначимо ці терміни як енергетичну економію.

Але головним «споживачем» технологій, які дозволять економити енергію, є організації промислового і енергетичного сектора, як приватні бізнес-структури, так і ті, що знаходяться під управлінням держави. Досить складно звабити учасників ринку новою тенденцією одними лише нормами, заборонами і підвищенням тарифів. Для цих цілей, ймовірно, відбувається активна «розкрутка» з метою показати, що IoT вже зарекомендував себе в даній сфері економії.

Для бізнесу, як для «споживача» таких рішень, складається красива картинка, а бажання наздогнати двох зайців вже здається реальною перспективою. Але не все так гладко, як здається на перший погляд, і деякі експерти обережно роблять припущення про те, що IoT може стати свого роду білим слоном, якого індійські правителі дарували неугодним підданим: з таким слоном можна було робити нічого, крім як утримувати [31] Основна проблема полягає в тому, що ефект від впровадження таких технологій потрібно розрахувати, а от таки з розрахунками в публічному доступі відчувається недостатність. Одним з небагатьох прикладів є аналіз від фахівців з PricewaterhouseCoopers, однак і вони оцінюють економічний ефект, який може бути наданий на галузь за допомогою впровадження IoT-технологій, за допомогою масштабування конкретних прикладів окремих

організацій, при цьому не розкриваючи самі вихідні дані. [32] Але як же новачкові вирушити в дорогу до енергоефективності, якщо інструментом обраний Інтернет речей?

2.2. Про що повинен задуматися «споживач» при використанні енергоефективних технологій з IoT?

Рішення «споживача» перейти до використання технологій Інтернету речей супроводжується велико. кількістю питань, головні з яких: «які технології існують?» і «якій віддати перевагу?». Необхідно дати відповідь на них з боку спостерігачів.

На даний момент, на ринку енергоефективних технологій представлено декілька стандартів зв'язку, в основі яких лежить поєднання провідних і бездротових каналів, а саме:

1. GSM/GPRS є буквально «технологію бездротового телефонного зв'язку» (Global System for Mobile communication). Іншими словами, даний вид зв'язку використовується багатьма з нас вже більше десятиліття і не сприймається як передове явище.

Саме через те, що даний вид зв'язку являє собою стандарт мобільного зв'язку, передача сигналу на далекі відстані має певну специфіку(Таблиця 2.1):

Таблиця 2.1

Плюси	Мінуси
Висока якість сигналу	Можливе спотворення сигналу
Конфіденційність	Невеликий(середній) радіус дії базової станції

Недоліки, в даному випадку, пояснюються саме первинною метою розробки зазначеного стандарту – мобільний зв'язок був створений з розрахунком на достатньо велику кількість функцій – відправка СМС, голосова та факсимільна пошта. Дані функції для передачі сигналу лічильника на базову станцію залишаються незатребуваними.

На даний момент, такий вид зв'язку застосуються компаніями для збору і передачі інформації з лічильників. ТОВ «Водоканал» на своєму сайті описує роботу інтелектуальних приладів обліку наступним чином: інформацію з приладу обліку води зчитує пристрій, що обладнаний системою збору даних протоколу M-Bus. У свою чергу, зібрані дані по бездротовому каналу зв'язку (GSM/GPRS) передаються на сервер.

Таку модель також застосовує ТОВ «Ленсвет» для збору і передачі показників лічильників, які входять в автоматизовану інформаційно-вимірювальну систему комерційного обліку електроенергії. Процес автоматизованого збору показників описується наступним чином: з лічильника електроенергії, за допомогою інтерфейсу RS232, дані надходять на модем, потім використовуючи GSM зв'язок і технології CSD (протокол v.110) дані надходять на модем сервера, звідки вже по RS232 надходять на COM-сервер і далі по локальній мережі Ethernet на сервер бази даних. Після обробки, дані по запитам надходять на АРМ (Автоматизовані Робочі Місця). Здійснення запитів і виведення даних відбувається за допомогою сертифікованого програмного забезпечення «Альфа-Центр». При цьому, в даний момент до складу автоматизованої системи входять 1594 вузла обліку.

Описана модель збору та передачі даних використовує провідні та безпровідні канали зв'язку і є стандартною для більшості ресурсонадаючих організацій, хоча і не є єдиною. У зв'язку з появою нової потреби передачі інформації маленького обсягу, на великі відстані, з використанням надійного сигналу, з'явилася задача розробки нових стандартів. Саме для цього були розроблені мережі LPWAN, а також спеціальні стандарти стільникового зв'язку, розраховані на далекі відстані і містять невеликий набір використовуваних функцій.

2. NB-IoT (Narrow band IoT - вузькосмуговий Інтернет речей) - стандарт, який був розроблений на базі існуючих стандартів мобільного зв'язку, як більш адаптована версія до згаданого GSM.

Для роботи NB-IoT в рамках мережі стільникового зв'язку виділяються вузькі смуги частот на існуючих базових станціях. Пристрої NB-IoT під’єднуються до мережі, проходять процедуру реєстрації в мережі, аналогічну звичайних мобільних телефонів, після чого можуть здійснювати обмін даними з мережею.

Стандарт NB-IoT забезпечує значно вищу енергоефективність пристроїв, в порівнянні зі звичайними мобільними стандартами мереж другого, третього і четвертого покоління, за рахунок значного зниження швидкості обміну даними і спрощення стека протоколів, наближаючись по ефективності до мереж LPWAN. Окрім того, стандарт надає можливість пристроям передавати дані з великими часовими проміжками не втрачаючи реєстрацію в мережі. Пристрої NB-IoT авторизуються при підключенні до мережі за допомогою стандартних SIM карт, аналогічно до звичайних мобільних телефонів.

У зв'язку з тим, що NB-IoT - це стандарт стільникового зв'язку, тому для роботи базових станцій необхідно отримати ліцензію. У зв'язку з цим, ймовірно протокол NB-IoT використовуватимуть компанії, присутні на ринку мобільного зв'язку, інакше будівництво мережі з нуля для охоплення мегаполісу вимагає істотних інвестицій.

3. LPWAN мережі. Переходячи до мереж, слід розуміти, що під ними мається на увазі кілька технологій, завдяки яким відбувається з'єднання датчиків і контролерів з Інтернетом. Мережі Wi-Fi і стільникового зв'язку при цьому не використовуються. Розглядаючи дані мережі, можна виділити їх наступні переваги і недоліки (Таблиця 2.2):

Таблиця 2.2

Плюси	Мінуси
Великий радіус дії (більше 10км)	Відносно низька пропускна здатність, як наслідок використання низької частоти радіо каналу. Варіюється в залежності від використовуваємої технології пердачі данних на фізичному рівні.
Енергоємність (час використання батареї – декілька років)	Затримка передачі даних від датчика/сенсора до кінцевого додатку, пов'язана з часом передачі радіосигнала, що може досягати від декількох секунд до декількох десятків секунд.
Масштабність (багато девайсів від однієї базової станції)	Відсутність єдиного стандарта, який визначає фізичний шар і управління доступом до середовища для безпровідних LPWAN-мереж.
Виділений канал зв'язку (не GSM, і не Інтернет)	–

При цьому з точки зору розгортання LPWAN мереж, крім технічних особливостей також має значення організація бізнес процесів. Власники патенту зазвичай хочуть контролювати не тільки фізичний рівень, але і виробництво (реалізацію) кінцевих пристроїв і базових станцій.

Однією з мереж LPWAN є LoRaWAN (протокол мережі LoRa), яка обмінюється даними тільки тоді, коли їм є, що передати. У звичайних мобільних мережах пристрої часто змушені «прокидатися» для синхронізації з мережею і перевірки повідомлень для отримання і/або відправки. Така синхронізація призводить до значної витрати енергії і скорочує автономний

термін роботи пристрою від акумулятора. Аналітики GSM провели безліч досліджень мереж LPWAN, в результаті чого прийшли до висновку: автономність LoRaWAN-пристроїв в 3-5 разів вище в порівнянні з іншими технологіями. Більш, того у даній мережі висока пропускна здатність, що означає можливість отримувати повідомлення з дуже великого числа пристроїв.

Організація зв'язку за допомогою технології LoRa для «споживача» не складає труднощів - чіпи LoRa для кінцевих пристроїв присутні у вільному доступі, документація на них відкрита, створювати пристрої з їх використанням можуть усі бажаючі.

Інший представник мережі LPWAN - «Стриж», від компанії «Стриж Телематика». Серед загальних позитивних рис, «Стриж» виділяється надійністю передачі сигналу: сигнал від модему надходить відразу на кілька базових станцій. При цьому стіни і конструкції не є серйозною перешкодою для сигналу. Крім того, за рахунок дальності передачі даних і особливостей протоколу «Стриж» обслуговує сотні тисяч датчиків однієї радіоточкою безпосередньо. Це в рази зменшує загальну вартість обладнання та робіт по його установці. При цьому, для розгортання мережі «Стриж» необхідно враховувати, що компанія «Стриж Телематика» самостійно виробляє практично всі компоненти, необхідні для користування даною технологією. Іншими словами, базова станція, кінцеві пристрої, а також послуги з підключення, встановлення та надання сервера виявляються виключно «Стриж Телематика», зі стягненням абонентної плати.

Така степінь закритості не тільки не дозволяє реалізувати багато проектів взагалі, а й навіть там, де реалізація можлива, представляє серйозний ризик для бізнесу – користувач прив'язаний до єдиного постачальника на всіх рівнях рішення.

Останнім з «великої трійки» стандартів виступає стандарт Sigfox - історично перша велика компанія на даному ринку. Розробником системи є французька компанія, заснована в 2009 році. Sigfox, як і інші мережі LPWAN,

забезпечує просту, надійну і економічно ефективний зв'язок для пристроїв, які передають малий обсяг інформації.

З точки зору організації системи з використання даного стандарту, то у компанії виробника необхідно придбати базові станції, а також укласти договір на розгортання мережі з платним доступом абонентів. При цьому, Sigfox не став узурпувати ринок чіпів і кінцевих пристроїв - він домовився з іншими виробниками про підтримку своєї мережі, тому проблем придбання пристрою, що підтримується Sigfox, виникнути не повинно. Однак, з підключенням такого пристрою до мережі в Україні, ймовірно, виникнуть труднощі – якщо в Європі Sigfox встиг розгорнути свої мережі, то зараз, з появою LoRa, його експансія фактично зупинилася.

Таким чином, поява нових завдань провокує нові технічні рішення, що створює конкуренцію на ринку стандартів зв'язку, де кожна з розглянутих технологій має свої недоліки і переваги. Як би там не було, LPWAN-мережі в Україні при всій їх перспективності поки знаходяться на етапі тестування.

2.3. Що хвилює «споживачів» технологій насправді?

За словами начальника виробничо-технічного управління «КиївГаз» Євгена Живлюка «інтернет речей», застосовуваний в області енергетики (в широкому її розумінні) носить неповноцінний характер. Фактично використання IoT зводиться до диспетчерських функція або, іншими словами, до збору даних. Ні про яку управлінську та виконавчу функції IoT-пристроїв мови поки не йде і на це є кілька причин. По-перше, люди не знають до чого застосувати IoT-технології і перше питання, яке ви почуєте: чому не використовувати Wi-Fi? Незрозумілі, перш за все, переваги та перспективи IoT-рішень. По-друге, існують певні нормативні обмеження, особливо в сфері, яка належить до компетенції МНС. Ідеологія нормативного регулювання в сфері енергетичної безпеки полягає в тому, що у всіх випадках повинна забезпечуватися незалежність роботи енергетичних систем. З одного боку, це означає, що всі технічні пристрої повинні мати

«ручний» режим управління і регулювання, але, з іншого боку, в будь-якому випадку зовнішнє втручання в роботу таких пристроїв необхідно повністю виключити. Тому говорити про IoT-технологіях доводиться тільки в гіпотетичному ключі.

Створення інтелектуальної системи управління транспортуванням газу, в тому числі з використанням IoT-рішень, безумовно, можливо - за аналогією з чайником і кавоваркою, які домовляються про те, коли готувати каву, координувати свою роботу могли б і газорегуляторні пункти. Однак впровадження такої системи навряд чи виправдано ще й тому, що газорозподільний комплекс має властивість саморегуляції через «гідравлічну» взаємодію його елементів.

IoT-технологію доцільно використовувати в рамках однієї організації, в «закритих системах» і, перш за все, в частині реалізації диспетчерських функцій. Наприклад, з використанням «Інтернету Речей» цілком можливо було б забезпечувати безпеку в будинках, в яких не перебувають постійно люди, здійснювати перевірку загазованості приміщень дистанційно. Ще більш актуальним збір даних про транспортування газу і визначенні витрати газу конкретними споживачами. Мабуть, тільки в останньому випадку на поточний момент можна говорити про використання IoT-технологій в контексті вирішення завдання підвищення енергоефективності.

Опитані експерти також наголошують, що IoT-технології цікаві «споживачеві» перш за все в контексті вирішення економічних завдань - збору даних про спожитих ресурсах і їх оплаті відповідно, набагато рідше інтерес викликає сама «енергоефективність» проектів.

Сенсорні мережі Інтернету речей складаються з сотень до тисяч сенсорних вузлів, кожен вузол має батарею єдиного джерела енергії. Оскільки батареї більшості вузлів датчиків не є акумуляторними, однією з ключових проблем є планування використання вузлів для мінімізації споживання енергії. Проблема з вузлами бездротової мережі сенсорних датчиків полягає в тому, що вони живляться батареями, які, як правило, не

можна перезаряджати, що обмежує їх термін служби самої мережі. Вузли мереж, як правило, переводять в режим сну, коли вони не використовується, і переводять в режим роботи, коли це необхідно, щоб зменшити ці затримки, розробляючи схеми пересилання пакетів на основі "будь-якого відправлення", де кожен вузол опортуністично пересилає пакет до першого

Спочатку ми вивчаємо, як оптимізувати будь-які схеми переадресації для мінімізації очікуваних затримок доставки пакетів від вузлів датчиків до стоку. Будь-яка подача чітко знижує очікувану затримку одного стрибку. За традиційними схемами переадресації пакетів, кожен вузол має один призначений наступний вузол ретрансляції стрибку по сусідству, і він повинен чекати, поки вузол наступного переходу не прокинеться, коли йому потрібно передати пакет. На відміну від цього, при асинхронних схемах передачі пакетів кожен вузол має кілька вузлів ретрансляції наступного стрибку в наборі кандидатів (це також можна назвати набором переадресації) і пересилає пакет на перший вузол, який прокидається в наборі пересилання.

2.4. Впровадження бездротової сенсорної мережі

Серед функціональних компонентів вузла датчика радіозв'язок споживає значну частину енергії. Для мінімізації споживання даної енергії пропонуються різні напрямки вирішення цього питання. У цій роботі увага була зосереджена на Основному Розкладі (Backbone Scheduling(BS)), який динамічно вимикає радіоприймачі вузлів датчиків для економії енергії. Основний розклад дозволяє частці деяких вузлів датчиків в сенсорній мережі увімкнути радіозв'язок для відправки повідомлень, інші вузли датчиків вимикають радіостанції для економії енергії. Цей метод [1] не впливає на якість зв'язку, оскільки бездротові сенсорні мережі Інтернету речей мають надмірність. Під дублюванням мається на увазі, що вимкнення радіоприймачів деяких датчиків в сенсорній мережі не впливає на підключення мережі. Ця надмірність призводить до більш ніж необхідних бездротових зв'язків. Таким чином, можна побудувати комунікаційні

магістралі для економії енергії. Зокрема, використовується алгоритм Підключеного Домінуючого Набору (CDS - Connected Dominating Set) для побудови таких магістралей.

Проте єдина магістральна мережа не продовжує строк служби мережі. Ідея полягає в тому, щоб побудувати кілька роз'єднаних CDS і дозволити їм працювати альтернативно. Цей підхід був визначений і сформульований як проблема підключеного доматичного розділу (CDP). Таким чином, використовується віртуальне планування масштабування (VBS), новий алгоритм, що дозволяє здійснювати тонкий графік сну. VBS планує декілька перекритих магістральних мереж, так що споживання енергії мережі рівномірно розподіляється між усіма вузлами датчиків. Таким чином, енергія всіх вузлів датчиків в мережі повністю використовується, що, у свою чергу, продовжує строк служби мережі.

2.5. Обмеження існуючої системи

2.5.1. Обмеження потужності

Обмеження потужності бездротових сенсорних вузлів підвищується через їх невеликі фізичні розміри та відсутність проводів. Оскільки відсутність проводів призводить до відсутності постійного джерела живлення вузлів, то залишається не так багато варіантів живлення. Вузли датчиків зазвичай керуються батареєю[35]. Однак, оскільки мережа датчиків містить від сотні до тисяч вузлів, і тому, що часто бездротові сенсорні мережі розгортаються у віддалених або ворожих середовищах, то важко замінити або перезарядити батареї. Потужність використовується для різних операцій в кожному вузлі, таких як запуск датчиків, обробка зібраної інформації і передача даних. Обмеження потужності сильно впливає на безпеку, оскільки алгоритми шифрування вводять накладні комунікації між вузлами, які повинні обмінюватися більшою кількістю повідомлень, тобто для цілей керування ключами.

2.5.2. Обмежена обчислювальна потужність

Для обмеженої обчислювальної потужності обчислення безпосередньо пов'язані з наявною величиною потужності. Так як існує обмежена кількість енергії, обчислення також обмежені. Хоча визнається, що датчики не повинні мати обчислювальної потужності робочих станцій або навіть мобільних портативних пристроїв, дослідники і розробники дуже стурбовані цим питанням. Більша частина потужністі використовується для зв'язку, ніж для обчислення. Тому, оскільки потужність для обчислень ще більш обмежена, ніж загальна кількість енергії, то комплексні рішення безпеки заборонені. Обмеження обчислювальної потужності зменшує кількість можливих прийнятих сильних криптографічних алгоритмів, таких як алгоритм відкритого ключа RSA, який є обчислювально дорогим.

Замість цього використовуються симетричні алгоритми шифрування для захисту комунікаційних вузлів датчиків, оскільки симетричне шифрування не вимагає таких вимог до обчислень, як асиметричне шифрування. Однак, з асиметричним шифруванням, функції, такі як цифрові підписи, не підтримуються. Тому ще однією проблемою для дослідників і розробників є розробка відповідних алгоритмів для встановлення та перевірки довіри серед вузлів, що беруть участь у комунікації. Крім того, інші рішення безпеки повинні бути прийняті для покриття слабких сторін симетричного шифрування; коли противник компрометує вузол, він може отримати спільний ключ, який використовується для шифрування повідомлень, а потім скомпрометувати всю комунікацію датчиків.

2.6. Запропонована система

Планування режиму сну та режиму роботи є ефективним механізмом для продовження терміну служби бездротових сенсорних мереж в Інтернеті речей, що обмежені енергією. Тим не менш, планування даного режиму може призвести до значних затримок, оскільки передавальний вузол повинен чекати, поки його наступний крок, він є ретрансляційний вузол, прийде до

дії. Дана система намагається зменшити ці затримки, розробляючи схеми пересилання пакетів, де кожен вузол опортуністично пересилає пакет до першого сусіднього вузла, який прокидається серед декількох вузлів-кандидатів. Протокол планування Sleep\wake і будь-який протокол пересилання пакетів використовуються для максимізації терміну служби мережі за умови обмеження очікуваної затримки доставки пакетів.

2.7. Бездротова сенсорна мережа в Інтернеті речей

Виникаюче поле бездротових сенсорних мереж поєднує в собі зондування, обчислення та комунікацію в єдиний маленький пристрій. Критично важливим для розгортання будь-якої бездротової сенсорної мережі є очікуваний час життя. Метою застосування сценаріїв моніторингу навколишнього середовища та безпеки є наявність вузлів, розміщених у полі, без нагляду, протягом місяців або років. Основним обмежувальним фактором для терміну служби сенсорної мережі є енергозабезпечення. Кожен вузол повинен бути спроектований таким чином, щоб самостійно керувати своєю локальною енергією, щоб максимізувати загальний термін служби мережі. У багатьох, що розгортаються, важливим параметром є не середній час життя вузла, а мінімальний час життя вузла. Найбільш істотним фактором при визначенні терміну служби даного енергопостачання є споживання радіосигналу. У бездротовому сенсорному вузлі радіозв'язок споживає більшу частину енергії системи.

Споживана потужність може бути зменшена за рахунок зменшення вихідної потужності передачі або зменшення робочого циклу. Обидві ці альтернативи включають в себе жертву інших системних показників. При збільшенні терміну служби мережі різними методами з'являється проблема низького часу реагування. Тривалість роботи мережі може бути збільшена, якщо вузли працюють лише на радіостанціях протягом короткого періоду часу. Якщо вузол вмикає радіостанцію лише один раз на хвилину для передачі та прийому даних, то неможливо виконати вимоги до додатків для

часу відгуку системи безпеки. Час відгуку можна поліпшити, включаючи вузли, які постійно живляться. Ці вузли можуть прослуховувати повідомлення і пересилати їх по ходу маршрутизації, коли це необхідно. Це, однак, зменшує простоту розгортання системи.

2.8. Режими роботи та очікування

Планування сплячого режиму є ефективним механізмом для продовження терміну служби цих бездротових сенсорних мереж. Енергія, необхідна для сприйняття подій, зазвичай є постійною і її не можна контролювати. Отже, енергія, витрачена на увімкнення системи зв'язку (для прослуховування середовища і для прийняття та передачі пакетів управління), є домінуючою складовою споживання енергії, яку можна контролювати для продовження терміну служби мережі. Таким чином, динаміка сплячого режиму стає ефективним механізмом для продовження терміну служби енергозахищених подій сенсорних мереж. Поміщаючи вузли в сплячий режим, коли в них немає необхідності, енерговитрати сенсорних вузлів можуть бути значно зменшені.

Запропонована система є асинхронним методом планування сплячого режиму. У цих протоколах кожен вузол прокидається незалежно від сусідніх вузлів для економії енергії. Припускається, що сенсорна мережа використовує асинхронний графік сплячого режиму для підвищення енергетичної ефективності, а вузли вибирають вузол наступного переходу і пересилають пакет до вибраного вузла, використовуючи наступний основний протокол планування режиму Sleep/wake. Перевагою планування Пуассонівських режимів сну та роботи є те, що у зв'язку з малим об'ємом пам'яті, вузли датчиків можуть використовувати оптимальну для часу політику, щоб максимізувати час життя мережі. Тож аналіз вище описаного способу зменшення енергетичних витрат сенсорних мереж в Інтернеті речей зосереджується на випадку, коли пробудження вузлів слідує за процесом Пуассона[23].

Тобто, якщо розглядається послідовність проміжків часу між подіями пуассонівського процесу, а саме увімкненням та вимкненням вузлів бездротової сенсорної мережі за необхідністю пересилання пекетів інформації, то така послідовність буде послідовністю абсолютно незалежних випадкових велечин, та матиме назву пуассонівського потоку.

Висновки

Енергетична економія як глобальне завдання має багато різних напрямків вирішення. В ідеальному варіанті їх об'єднує одна загальна властивість - технологічність[35]. І IoT треба сказати є не єдиною технологією, яка повинна (знову ж таки в ідеальному варіанті) істотно підвищити енергоефективність. Однак на шляху до енергоефективності та енергозбереження не можна, та й неможливо нехтувати вимогами безпеки та економічної доцільності, які в своїй сукупності навіть не завжди виступають противагами. Як наслідок, IoT-технології ще належить доводити свою спроможність у цій сфері і, ймовірно, не варто чекати послаблень - існують дуже вагомі перешкоди на шляху у розвитку технологій, які на забобони і не спишеш.

У розділі описано випадковий (асинхронний) робочий цикл режиму роботи та сну вузлів, за використанням процесу Пуассона для пробудження вузлів при передачі пакетів інформації між ними. Висвітлено процес ретрансляції та поняття набору переадресації. Описано використання асинронного циклу в питанні енергозбереження на часу життя вузлів.

РОЗДІЛ 3
МОДИФІКОВАНИЙ МЕТОД ПЕРЕДАЧІ ІНФОРМАЦІЇ ДЛЯ ПІДВИЩЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ

Величезні досягнення в техніці в цілому і в бездротових комунікаціях надають людству здатність виготовляти маленькі, дешеві датчики, які з'єднуватимуться один з одним бездротово[35]. Датчики, що розгорнуті, незалежно від того, під час випадкового або попереднього методу вони можуть з'єднуватися один з одним в системі і вводити мережу бездротового сенсорного елемента (WSN), цей продукт одиниці площі датчиків розгортається під час попередньо визначення простору. Датчики адаптують зняту фізичну інформацію у тип, який може полегшити для користувача їх розуміння. Технологія WSN швидко зростає, перетворюючись на дешевшу та простішу у користуванні, і дозволяє повне застосування різних додатків в таких мережах. WSN часто використовуються для великої кількості додатків, що керують спостереженням (середовища охорони здоров'я, сейсмічні тощо), управлінням (виявлення та відстеження об'єктів) та роботою поліції (спостереження на полі бою).

3.1 Координований метод в сенсорних мережах Інтернету речей

Мережі бездротового зондування складаються з діапазону вузлів чутливих елементів, які розташовані в зонах спостереження (пустелях, льодовиках, зонах з підвищенною небезпекою і т.д.) та трансіверів експлуатації, які є методом транспортування інформації. У кожному зчитувальному елементі вузла енергія батареї обмежується тим, що значне підвищення споживання енергії стає основною проблемою[7]. Кількісне співвідношення між активним режимом і сплячим режимом називається робочим циклом. Теоритично, вузли можуть заощаджувати енергію між активним і сплячим режимами[9]. Під час цієї методології WSN є адаптованим, а ці вузли чутливого елемента вмикаються і вимикаються під час впливу та необхідності у використанні. Використовується техніка

кодування мережі, що дає можливість забезпечити більш захищене використання інформації і додатково кодує вхідні пакети інформації і тим самим передає кодований пакет до стокового вузлу мережевих програмних вузлів, використовуючи єдиний стрибок для зв'язку, в той же час інші різновиди вузлів чутливого елемента використовують багатоканальний зв'язок.

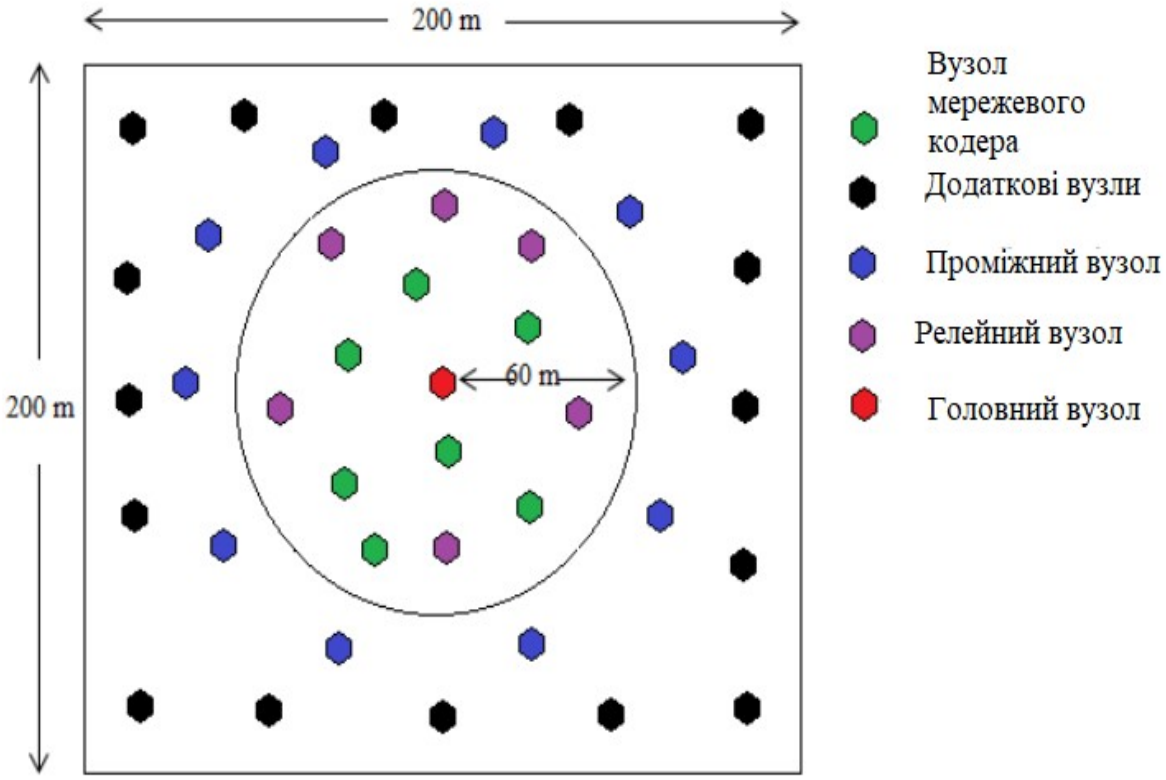

Рис. 3.1. Схема сенсорної мережі Інтернету речей

Коефіцієнт робочого циклу WSN розділений на три основні типи: випадковий WSN, координований WSN, пристосований WSN по циклу чергування – вузли звичайних елементів вмикаються або вимикаються у випадковому порядку. Випадковий квадратичний WSN є квадратно-мірним прямолінійним, оскільки не потрібні додаткові накладні витрати. Однак недолік випадкового WSN-циклу в тому, що він не перейде в стан сну, підтримуючи стан мережі. Такий розвиток подій буде генерувати значний

трафік. Він не використовуватиме більш високий рівень використання інформації. При координованому робочому циклі речовина чутливого елемента взаємодіє між собою через обмін інформацією та повідомленнями.

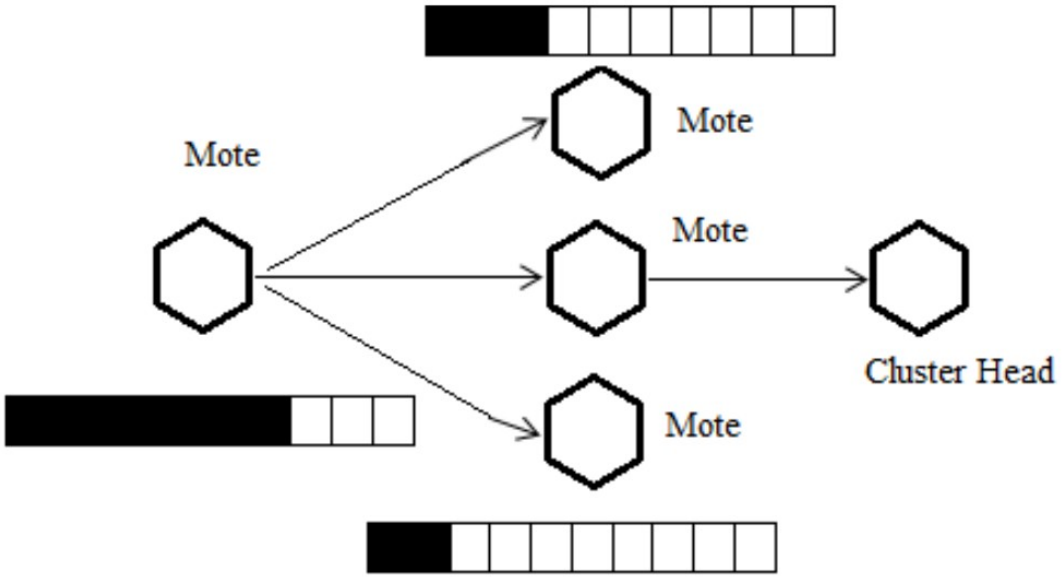

Рис. 3.2. Довжина черги та варіації вузла чутливого елемента

Тим не менш, він потребує подальшого обміну інформацією для трансляції активних графіків сну кожного вузла. Це призведе до значного додаткового трафіку та накладних витрат тільки для підтримки функціонування системи. Як правило, пропонується виявлення черг і скоординований механізм управління робочим циклом, що надає можливість управління чергою з метою збереження енергії та зменшення затримки. Для проектованого методу немає необхідності отримувати конкретну інформацію про стан з сусідніх вузлів, однак він використовує тільки присвійні довжини черги, які можна отримати на вузлі. Зміни в умовах мережі неявно відбуваються в результаті станів черг, які мають ризик або потужність станів мережі[35]. Обробляючи довжину черги та її варіації вузла чутливого елемента(Рис.3.2), прагнеться надати режим розподіленого мережного контролера для робочого циклу. Таким чином, розпізнавання черг і скоординований WSN з базовим циклом, пов'язаним з виконанням обов'язкових операцій є окремим режимом.

3.2 Моделювання розрахунку використаної енергії

Вузол пристрою споживає енергію в абсолютно різних станах, таких як збирання та генерування інформації, стан відправки, прийому та сну. Економія енергії здійснюється на рівні вузла за рахунок переключення між активним та режимом сну.

Споживання енергії вузлом передачі в секунду на відстань d з показником втрат шляху n становить:

$$E_{tx} = R_d(\alpha_{11} + \alpha_2 d^n)$$

Де R_d швидкість передачі даних ретранслятора, α_{11} це споживання енергії на біт передавачем і a_2 – споживання енергії на біт в операційному підсилювачі передачі [33]. Загальне споживання енергії за час t вузлом джерела (листовим вузлом) без дії реле (проміжний вузол) дорівнює:

$$E_s = t[p(r_s e_s + E_{tx}) + (1-p)E_{sleep}] ,$$

де E_{sleep} – споживання енергії в режимі холостого ходу вузла датчика в секунду, r_s – середня швидкість зондування датчика, і вона дорівнює для всіх вузлів, e_s – енергоспоживання мотора; ймовірність P є середнім частки часу t, яку вузол датчика використовує в активному режимі. Таким чином, p – робочий цикл. Вузол датчика залишається в режимі очікування з імовірністю (1-p) до часу t. Споживання енергії в секунду проміжним вузлом, який виконує функцію релейного елемента, визначається[23]:

$$E_{txr} = R_d(\alpha_{11} + \alpha_2 d^n + \alpha_{12}) ,$$

де a_{12} – споживання енергії вузлом датчика для отримання біта. Загальна енергія, спожита за час t проміжним (релейним) вузлом, становить:

$$E_r = t[p(r_s e_s + E_{txr}) + (1-p)E_{sleep}] ,$$

Загальне споживання енергії в зоні вузького місця за час t для p-циклу робочого циклу WSN визначається [23]:

$$E_d = E_{agd} + E_{2gd} + E_{3gd} + (1-p)tN\frac{B}{A}E_{sleep}$$

$$E_d = \left[\frac{m+1}{2}\right]Npr_s t\frac{A-B}{A}\left(\alpha_1\frac{D}{d_m}\frac{n}{n-1}\right) + Npe_s r_s t\frac{B}{A} + pr_s\frac{N}{A}t\iint\left(\alpha_1\frac{x}{d_m}\frac{n}{n-1} - \alpha_{12}\right)d_S + (1-p)tN\frac{B}{A}E_{sleep}$$

(1)

Коли p = 1 (усі вузли активні) і m = 1, споживання енергії в зоні вузького місця для ретрансляції бітів даних, що генеруються всередині, а також поза зоною вузького місця, стає таким самим, як у загальному або безчерговому циклі WSN [6]. Таким чином, дане рівняння(1) також охоплює загальний мережевий сценарій без урахування робочого циклу вузлів.

Термін служби бездротової мережі значно залежить від споживання енергії на рівні вузла. Нехай E_b - початкова енергія батареї, доступна на кожному вузлі датчика. У мережі з N вузлів, запас енергії на початку становить $N \cdot E_b$.

Продуктивність WSN суворо залежить від існуючої статистики відмов вузлів кожного датчика. Загальна картина відмов вузлів датчиків залежить від швидкості використання енергії. Термін служби мережі вимагає, щоб загальне споживання енергії не перевищувало початковий запас енергії в мережі. Верхня межа ресурсу мережі може бути досягнута, коли загальна енергія акумулятора (NE_b), що доступна в WSN, повністю вичерпається. Наступна нерівність виконується для оцінки верхньої межі часу життя мережі для робочого циклу на основі WSN [23]:

$$E_D \leq \frac{NB}{A}E_b$$

$$t \leq \frac{d_m B E_b}{S_x} = T_u D$$

,

Де знаменник S_x задано формулою:

$$S_x = p\alpha_1\frac{n}{n-1}r_s\left[D(A-B)\frac{m+1}{2} + \int\int x d_s\right] + Bd_m[p - r_s(e_s - \alpha_{12}) + (1-p)E_{sleep}]$$

а T_uD – верхня межа мережі WSN із робочим циклом (p). Величина споживання енергії є максимальною, коли p=1 (тобто всі станції в активному стані), і час життя стає мінімальним в WSN. Енергоефективність мережі збільшується при низькому робочому циклі, що збільшує термін служби мережі. r_s визначається як:

$$r_s = \frac{H}{(A-B)\frac{N}{A}},$$

де H – інформація, котра була зібрана сенсором за одну сесію збирання, $B = \pi D^2$ – площа стоку.

Таким чином, вимальовується залежність між величиною буфера та зміною кількості циклів передачі пакетів, а в наслідок цього – часом життя сенсорної мережі. Тобто, існує два обмеження при мінімальному та максимальному розмірі буфера.

Перша цільова функція – розмір буфера прямує до максимально можливого. В даному випадку, коли буфер буде заповнений і почнеться передача пакеті, то збільшується час активної передачі за одну сесію.

Друга цільова функція – розмір буферу прагне до мінімально можливого. Даний варіант має обернений вигляд, проте результат – загальна витрата енергії мережі – аналогічний першому обмеженню. Наприклад, за умови використання буферу з меншою ємністю, ніж довжина відправного пакету данних, то вузол матиме довгі активні стани передачі та призведе до збільшення кількості робочих сесій.

3.3 Виявлення черги та координація робочого циклу

Система враховується при однорідному розподіленні N пристроїв в просторі A. Всі N вузлів пристроїв є адаптивним циклом Duty Enabled, тобто перемикання між активним і сплячим станом підтримує їх значення черги в межах зони B, вузли розрізняються на дві команди, що нагадують пристрої ретрансляції і вузли пристроїв лінійних мережевих програм [7],[35]. Вузли

активних пристроїв ретрансляції (R) передають інформацію, яка генерується зовні, так само, як і в зоні вузького місця. В зоні вузького місця ретрансляційні вузли зв'язуються зі стоком, використовуючи зв'язок одним кроком, ретрансляційний вузол передає на інший вузол ретрансляції і вузол програми, що використовує зв'язок з декількома каналами. Активні лінійні мережі програмних вузлів пристрою записують в код інформацію ретрансляційного вузла перед передачею до стоку. Він буде використовувати один крок, щоб виходити на контакт зі стоком. Вузли листового пристрою спорадично відчувають інформацію і передають їх до сусідніх вузлів у бік стоку. Вузли проміжного пристрою спорадично відчувають інформацію і передають виявлену інформацію і отримані дані в напрямку раковини S.

Зміна часу життя сенсорної мережі в залежності від розміру буферу визначається наступним чином:

$$t \leq \frac{d_m B E_b}{S_x} = T_u D$$

Де значення S_x взято з:

$$S_x = p\alpha_{31}\frac{n}{n-1} r_s \left[D(A-B)\frac{m+1}{2} + \int\int x d_s\right] + B d_m [p - r_s(e_s - \alpha_{12}) + (1 - p)E_{sleep}]$$

Кожен вузол пристрою охоплює різноманітність отриманої черги і виявляє чергу, що приєднана до нього, одну або декілька з альтернативних вузлів. На кожному вузлі пристрою пакети надходять і відходять, за винятком листового (або) термінального вузла і раковинного вузла. Плановий підхід полягає в тому, щоб виділити буфер на кожному вузлі на одну чергу обліку запасів. Після того, як буферна зайнятість перевищує поріг, передавач починає працювати на вузлі пристрою в активному стані, щоб спробувати таким чином, до того моменту як зайнятість буфера опуститься нижче межі, передати всю інформацію. Якщо розмір буфера буде нижче порогового значення, то пристрій переходить до стану сну[12].

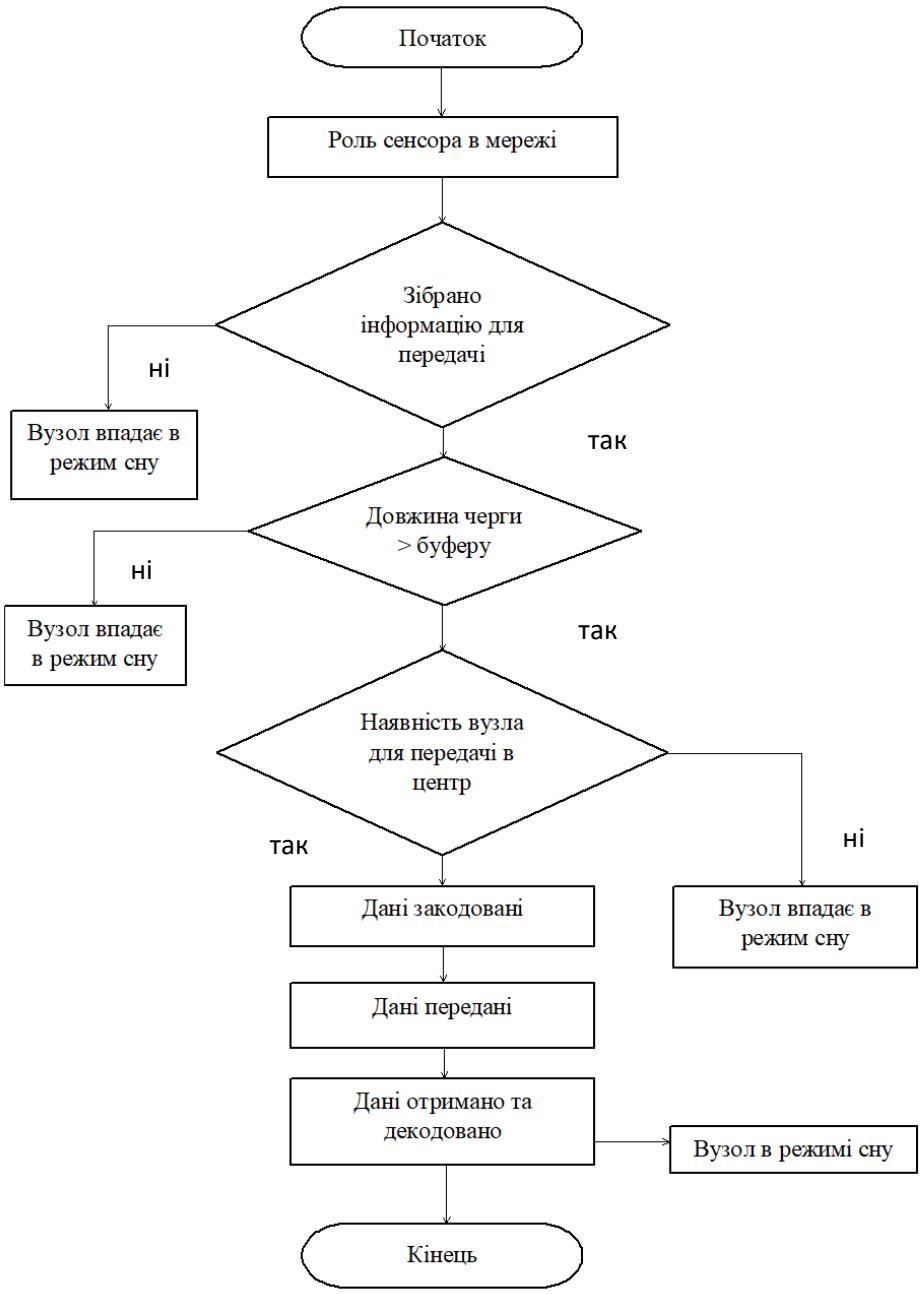

Рис. 3.3 Загальна схема проекту

Висновки

1. Модифіковано метод передачі інформації для підвищення енергоефективності мережі.

2. Висвітлено необхідність виділення буферу черг на кожному з вузлів та пояснення роботи вузла з використанням буферу черг.

3. Створено схему проекту з використанняммодифікованого алгоритму Sleep/Wake.

РОЗДІЛ 4
МОДИФІКОВАНИЙ МЕТОД В АРХІТЕКТУРІ ІНТЕРНЕТУ РЕЧЕЙ

4.1. Пояснення модифікації архітектури

Змінений та модифікований – координований - режим роботи сенсорної системи Інтернету речей має переваги в проблемі енергозбереження та часу життя системи, порівняно з асинхронним методом передачі пакетів інформації через вузли системи. Використовуючи координований метод можна підвищити час життя як одного елемента/вузла системи, так і всієї системи вцілому, та знизити необхідність в обслуговуванні чи заміни блоків живлення елементів системи.

Як видно з рис. 5.1., концептуальних змін [13],[14],[35], за умови використання координованого методу передачі пакетів інформації, архітектура не зазнала. Всі наведені архітектури, що згадуються в даній роботі, мають спільні риси: наявність трьох рівнів, подібні функції, наявність хмарних обчислень, використання Інтернету як інтеграційного рівня.

4.2. Місце використання координованого алгоритму в архітектурі Інтернету речей

Місце використання координованого методу передачі пакетів інформації можна побачити на рис. 5.1. Якщо звернути увагу на один з трьох рівнів архітектури Інтернету речей, а саме, на рівень, так називаємої, Граничної області (Edge), то видно що на цьому рівні знаходяться вузли з сенсорами та виконавчі механізми. Саме в вузлах з “Smart” IoT Device, відбуваються зміни Sleep/Wake алгоритму для підвищення енергоефективності та збільшення часу життя системи. Так як, “Smart” IoT Device[10] найкраще та найбільше співпрацюють з життєвим циклом людини[9], то для них[11],[25] було більш доцільно використовувати модифікований метод передачі інформації, тим самим підвищивши енергоефективність та час життя мереж.

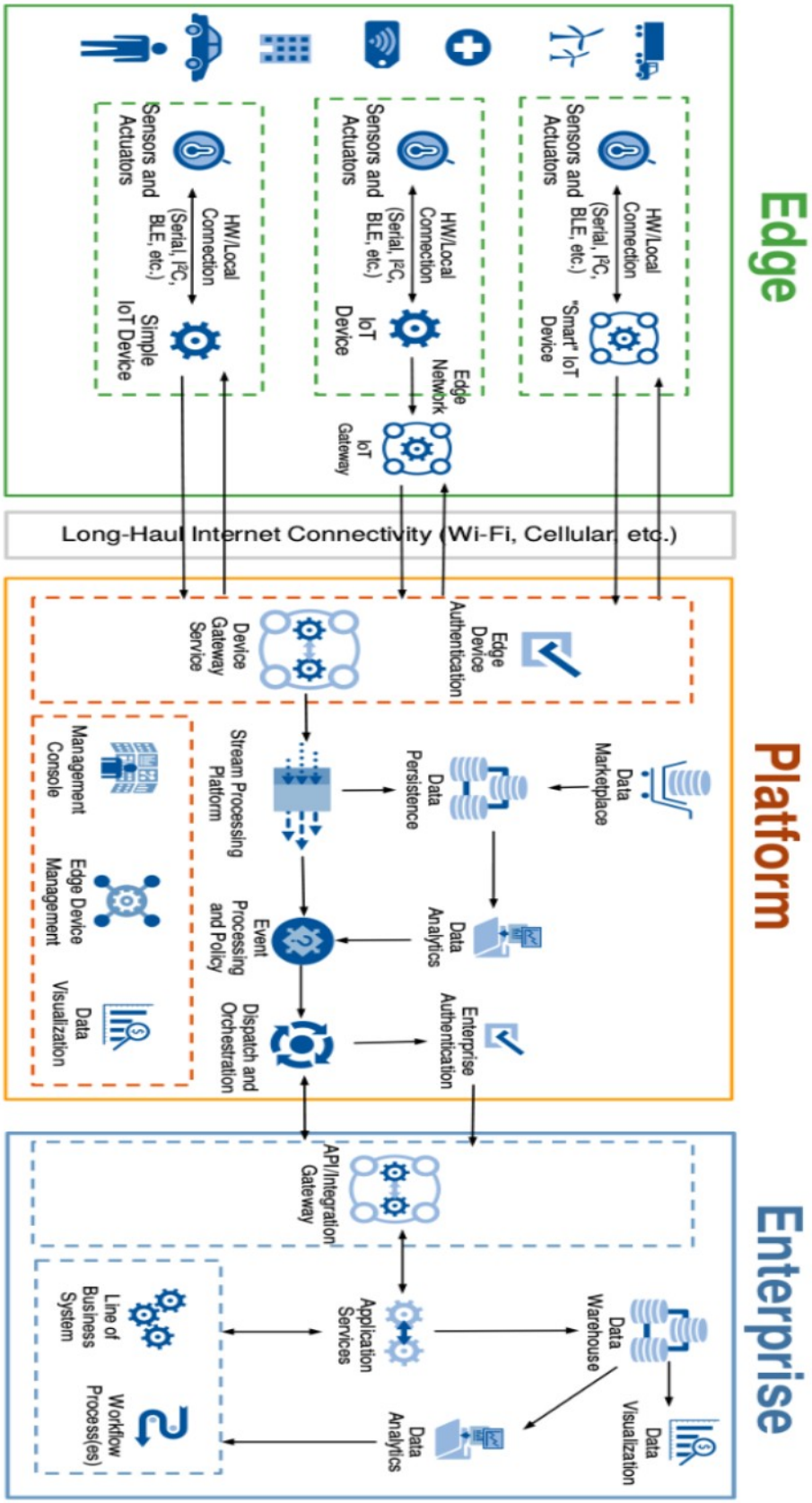

Рис. 4.1. Архітектура Інтернету речей з використанням координованого методу

Висновки

1. Викладено та пояснено модифікацію архітектури при використанні координованого режиму роботи в сенсорних мережах Інтернету речей.

2. Висвітлено в якому з трьох рівнів загальної архітектури Інтернету речей та в яких вузлах відбулися зміни алгоритму для підвищення енергоефективності та збільшення часу життя системи.

РОЗДІЛ 5
ОЦІНКА ЗАПРОПОНОВАНОГО МЕТОДУ

5.1. Мережеве життя за допомогою циклу випадкового режиму

В даній роботі розглянуто область бездротової сенсорної мережі 200x200 квадратних метрів, діаметр вузької зони 60м, кількість вузлів 1000, енергія батареї 25кДж, енергія сну 30Дж, довжина переходу 2, кількість бітів 96 і поріг буферу 12 біт[8],[35].

Рис. 5.1 показує енерговитрати на вузол в бездротовій сенсорній мережі зі зміною робочого циклу. Коли величина робочого циклу дорівнює 0,01, споживання енергії є мінімальним, тобто 30,1Дж, а робочий цикл 0,1, споживання енергії становить 1000Дж. Зі збільшенням робочого циклу збільшується споживання енергії.

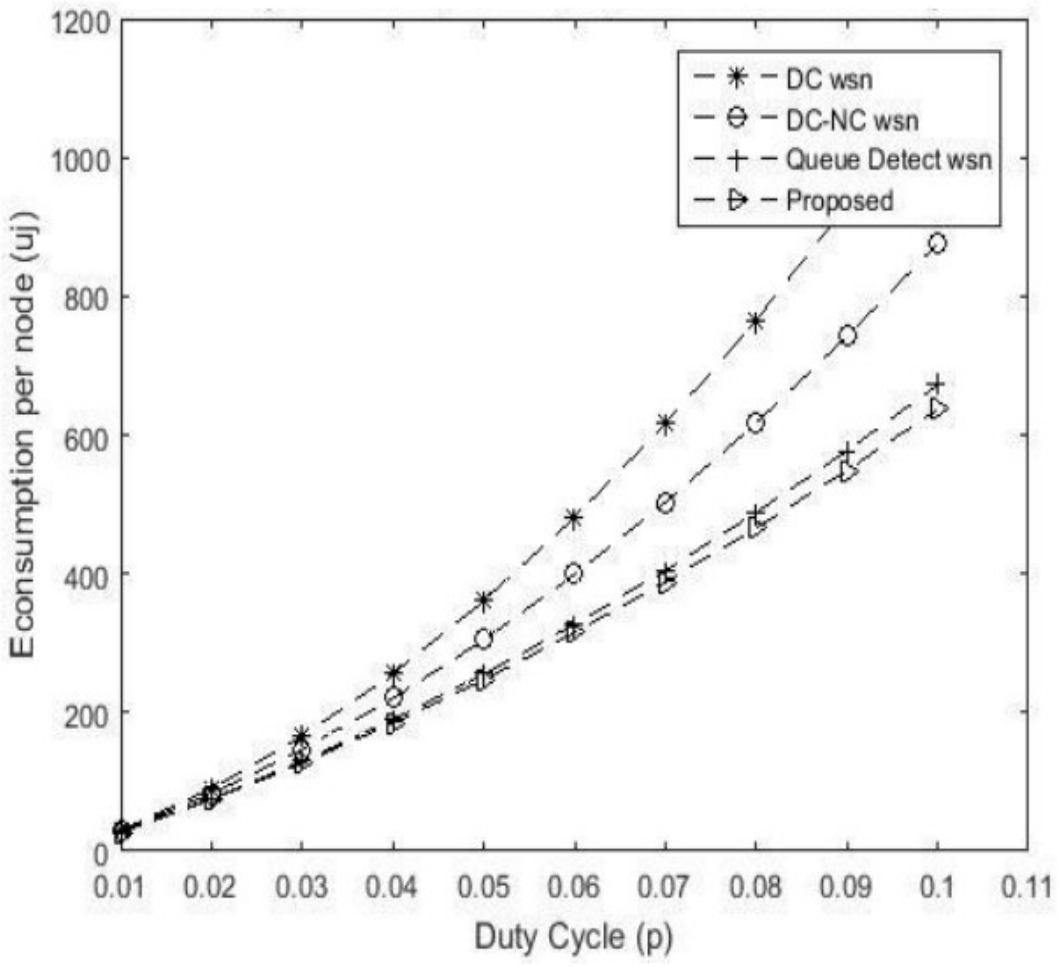

Рис. 5.1 Споживання енергії сенсорної мережі з використанням випадкового циклу

З малюнка спостерігається, що споживання енергії є максимальним для випадкових циклів, що використовуються в бездротових сенсорних мережах і мінімальним для виявлення черги з координованою мережею з циклічним циклом. У таблиці 5.1 зіставлено споживання енергії для різних технологій.

Таблиця 5.1

Споживання енергії для різних методів

Методи в бездротових сенсорних мережах в Інтернеті речей	Використання енергії для p=0.01	Використання для p=0.1
Довільний Робочий Цикл	30.1	1110.5
Мережевий кодований цикл	28.59	876.31
Виявлення черги за допомогою кодування в мережі	27.26	672.10
Запропонований метод (виявлення черги та координований робочий цикл)	27.04	637.12

5.2. Мережевий термін служби для координованого циклу виконання та виявлення черги

Техніка рис. 5.2 показує зміну часу життя бездротової сенсорної мережі зі зміною робочого циклу. Коли значення робочого циклу дорівнює 0,01, m=1, час життя становить 8,31×10^8 секунд. Зі збільшенням значення робочого циклу термін служби зменшується, а зі збільшенням величини m (щільність руху) термін служби знову зменшується. Для m = 9 і p = 0,01 час життя становить 8,0051x10 ^ 8 секунд.

З графіка можна спостерігати, що при щільності трафіку більш тривалий термін служби бездротової сенсорної мережі нижче. Використання

скоординованого циклу та методу виявлення черги збільшує термін служби у випадку більш високої щільності трафіку в порівнянні з терміном служби, досягнутої в бездротовій мережі бездротових датчиків з бездротовим та безконтактним бездротовим зв'язком.

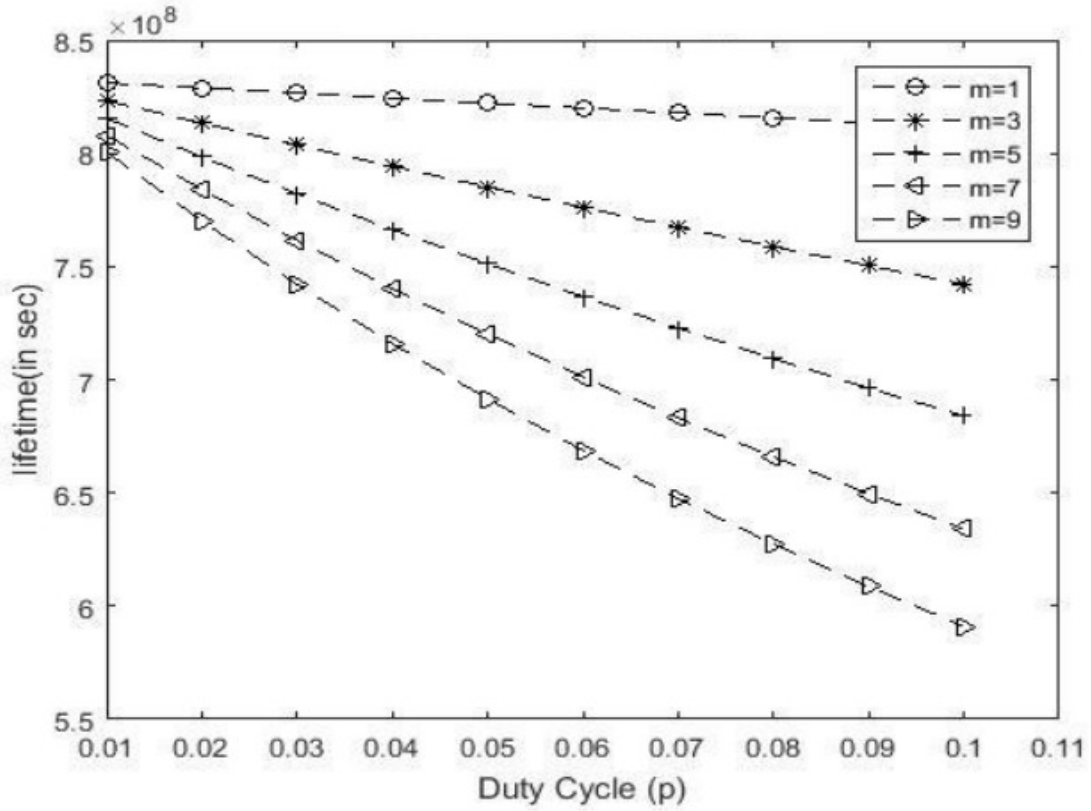

Рис. 5.2 Термін служби сенсорної мережі для запропонованого wsn при різних значеннях m.

Таблиця 5.2 показує час життя запропонованої сенсорної мережі в Інтернеті речей для змінної щільності руху. Після аналізу можна зробити висновок, що тривалість життя при низькій щільності руху є максимальною, а за великою щільністю руху – мінімальною.

Таблиця 5.2

Порівняння термінів дії для запропонованого WSN

	Тривалість життя при p=0.01	Тривалість життя p=0.1
m=1	8.31*10^8	8.11*10^8
m=3	8.23*10^8	8.11*10^8
m=5	8.15*10^8	7.42*10^8
m=7	8.08*10^8	6.34*10^8
m=9	8.005*10^8	5.91*10^8

5.3. Залежність терміну служби мережі для координованого циклу та методу виявлення черги на h параметрі

На рис.5.3 показано, як час життя мережі залежить від параметра h. Можна спостерігати, що зі збільшенням значення h час життя зменшується. Для більш високих значень h час життя майже постійний.

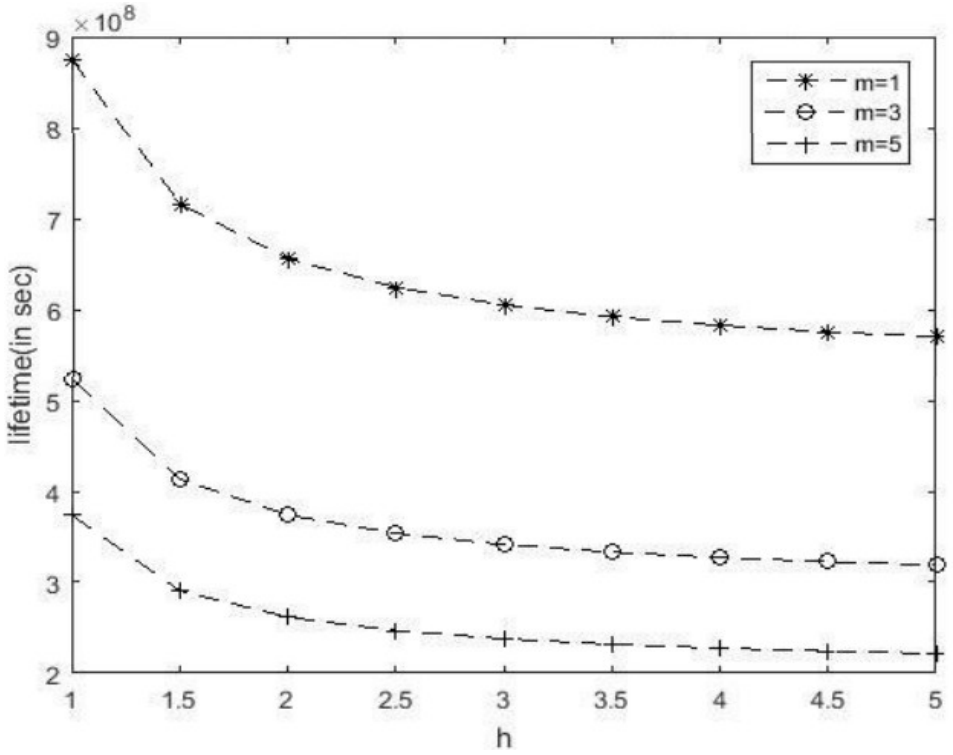

Рис. 5.3 Термін служби сенсорної мережі для запропонованого алгоритму в бездротовій сенсорній мережі Інтернету речей при різних значеннях m для різних параметрів h

Таблиця 5.3

Термін служби змінної щільності трафіку

	Тривалість життя при h=1	Тривалість життя при h=5

m=1	8.31*10^8	8.11*10^8
m=3	8.23*10^8	8.11*10^8
m=5	8.15*10^8	7.42*10^8

5.4. Мережеве життя за допомогою мережевого кодованого координованого циклу

На рис 5.4 показано порівняння терміну служби для випадкового циклу, кодованого мережевого циклу, мережевого кодування з технікою виявлення черг і виявлення черги з координованим циклом WSN. У формі таблиці 5.4 можна зробити висновок, що виявлення черг з координованим циклом wsn є найкращою технікою для поліпшення життя мережі.

Таблиця 5.4

Параметри сенсорної мережі

Кількість вузлів	1000
Зона сенсорної мережі	200m^2
Радіус зони обмеження пропускної здатності	60m
Експотенційні втрати при передачі	2
α_{11}	0,937кДж
α_{12}	0.787кДж
α_{2}	0.0172кДж
Режим сну	30Дж
α_{31}	1.2кДж

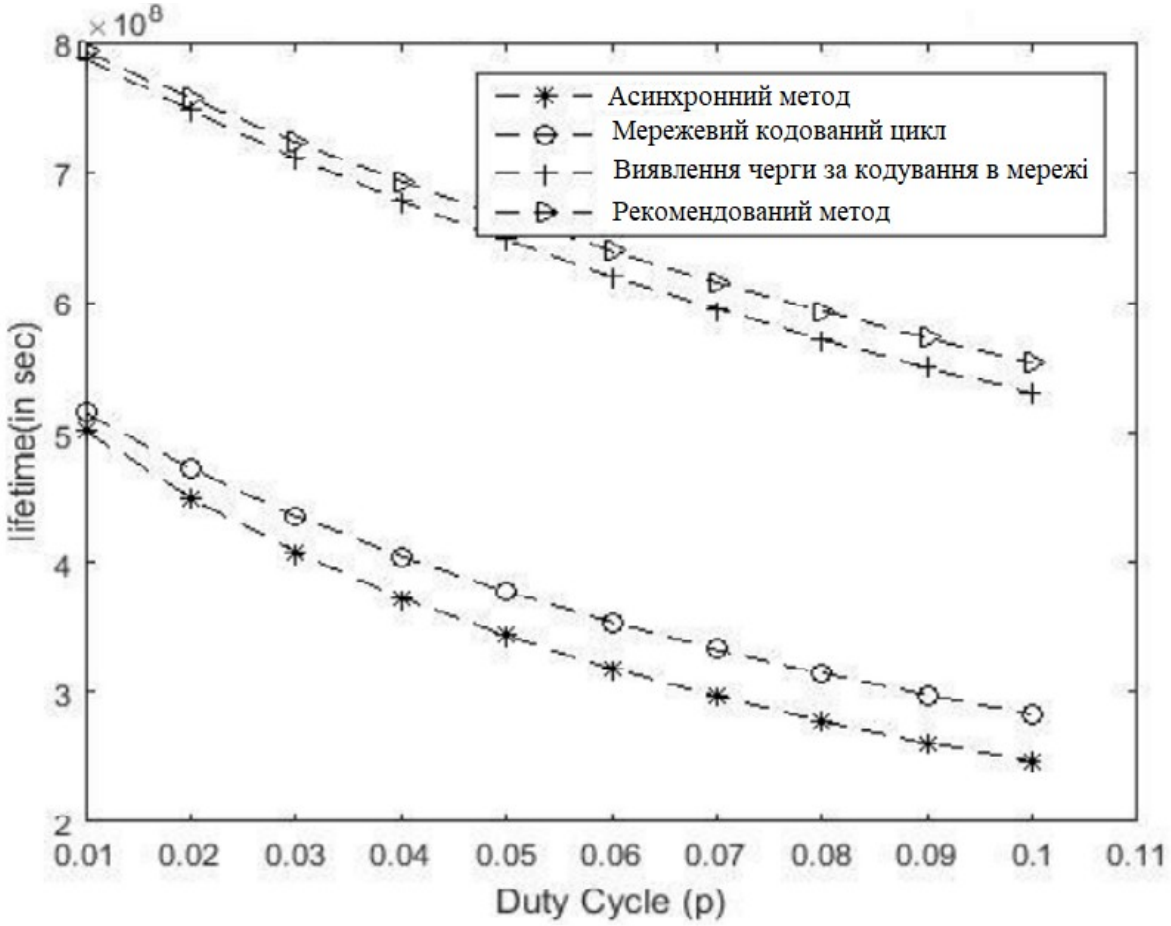

Рис. 5.4 Термін служби сенсорної мережі з використанням циклу випадкового режиму, мережевого кодування з циклом, методом виявлення черги та пропонованої системи

Таблиця 5.5

Порівняння тривалості життя для різних методів

	Тривалість життя при p=0.01	Тривалість життя при p=0.1
Довільний Робочий Цикл	5.01*10^8	2.46*10^8
Мережевий кодований цикл	5.15*10^8	2.82*10^8
Виявлення черги за допомогою кодування в мережі	7.88*10^8	5.29*10^8
Запропонований метод (виявлення черги та координований робочий цикл)	7.93*10^8	5.53*10^8

Порівнюючи два методи передачі пакетів даних в сенсорних мережах, а саме асинхронного та координованого методу з буфером черги обліку запасів (модифікованого методу), було отримано Рис.5.5:

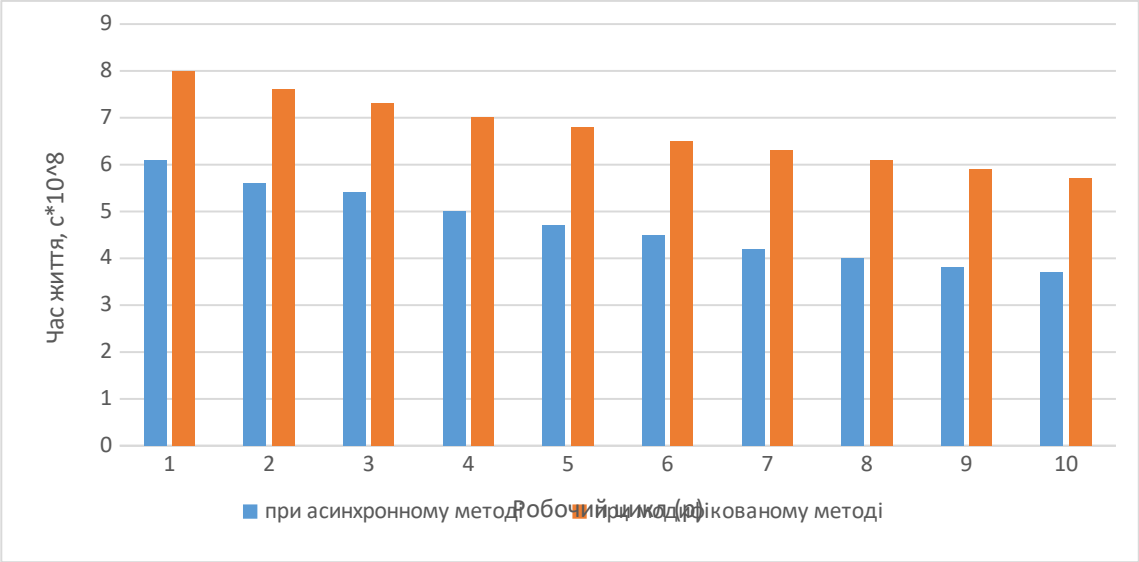

Рис. 5.5. Час життя сенсорної мережі за використання асинхронного та модифікованого методів передачі пакетів даних.

Таким чином, з рисунку 5.5 видно зміни часу життя системи від кількості робочих циклів за використання двох методів передачі пакетів даних. Можна спостерігати збільшення часу життя сенсорної мережі на 20% при використанні модифікованого методу порівняно з асинхронним методом передачі.

Висновки

1. З допомогою графіків та таблиць показано енерговитрати сенсорної мережі та споживання енергіїодного вузла з використанням різних методів.

2. Графіком висвітлено мережевий термін служби для координованого циклу виконання та виявлення черги.

3. Показано та порівняно термін служби сенсорної мережі з використанням циклу випадкового режиму, мережевого кодування з циклом, методом виявлення черги та пропонованої системи.

4. Процес вибору методу передачі інформації в сенсорні мережі Інтернету речей відіграє важливу роль при проектуванні мережі, так як в наслідку вибору методу залежить не тільки швидкість отримання пакетів інформації, а і час життя незалежної від енерголіній сенсорної мережі. Головна ідея методу полягає в тому, щоб на кожному вузлі виділяти буфер з певним пороговим значенням, при перевищенні якого буде запускатись передача пакетів інформації. Даний метод надає виграш в терміні використання на 14,8…20,6% вище порівняно з сенсорними мережами Інтернету речей, що застосовують асинхронний цикл черг.

РОЗДІЛ 6

РОЗРАХУНОК СТАРТАП ПРОЕКТУ З ВИКОРИСТАННЯ МОДИФІКОВАНОГО МЕТОДУ

Для розрахунку фінансового боку стартапу було виділено настапні вхідні данні:

1. Місце розгортання – Київська область.
2. Кількість клієнтів, що можуть використовувати мережу в своїх цілях – 4000.
3. Тип доступу – 4G.
4. Ємність транспортного каналу – 55Мбіт/с.
5. Оператор телекомунікаційних послуг для передачі пакетів даних від центрального вузла до серверу зберівгання та обробки інформації – Lifecell.

Для більш детального розрахунку та ознайомлення з фінаносовою складовою проекту було створено розрахункові таблиці 6.1 та 6.2. Розрахунок було проведено на період в 3роки поквартально. Були вирахувані наступні пункти:

1. Вартість використання – включає в себе вартість підключання, абонентські плати на саму сенсорну мережу та використання алгоритму.
2. Вартість обслуговування мережі – аренда місця встановлення мережі(вузлів мережі) та технічне обслуговування.
3. Адміністративні та технічні витрати – заробітня плата співробітникам, витрати на рекламу, аренда офісу, канцелярія і тд.
4. Були підраховані сумарні витрати на кожен з блоків проекту.
5. Вирахувані доходи проекту, витрати проекту, грошовий потік проекту та прибуток проекту після вирахування податків.

Таблиця 6.1.

Вихідні данні	Місце - Київська область											
	Кількість можливих клієнтів	4000										
	Ємність транспортного каналу, Мбіт/с	55										
	Тип доступу	4G										
	Оператор доступу	Lifecell										
	Загальна к-сть сенсорних мереж				1	2	2	3	3	4	5	5
	Сумарна пропускна здатність, Мбіт/с				55	110	110	165	165	220	275	275
	Відносна активність в-ння сенсорних мереж				60%	60%	60%	60%	60%	60%	60%	60%
	Число активних передач в мережі				120	192	240	336	408	528	672	792
	Середня ємність каналу, Мбіт/с				0.4583333	0.572917	0.458333	0.491071	0.4044118	0.4166667	0.409226	0.347222
Період					1кв	2кв	3кв	4кв	1кв	2кв	3кв	4кв
					К-сть клієнтів в сервісі				К-сть клієнтів в сервісі			
	Потенціал, %				5%	3%	2%	4%	3%	5%	6%	5%
Клієнти	Клієнти				200	120	80	160	120	200	240	200
Заг. к-ть клієнтів	Клієнти				200	320	400	560	680	880	1120	1320
	Сервіси											
Інтернет	Інтернет				200	120	80	160	120	200	240	200
Заг. к-ть девайсів	Інтернет				200	320	400	560	680	880	1120	1320
Фінансова інформація												
Вартість використання												
	Вартість підключення			200	200	200	200	200	200	200	200	200
	абон плата за сенсорну мережу			150	450	450	450	450	450	450	450	450
	абон плата за в-ння алгоритму			280	840	840	840	840	840	840	840	840
Дохід за використання												
	Плата за підключення				0	64000	80000	112000	136000	176000	224000	264000
	абон плата за сенсорну мережу				0	144000	180000	252000	306000	396000	504000	594000
	абон плата за в-ння алгоритму				0	268800	336000	470400	571200	739200	940800	1108800
Загальний дохід за використання					0	476800	596000	834400	1013200	1311200	1668800	1966800

Таблиця 6.2.

Вартість обслуговування мережі											
	Аренда місця встановлення на 1 сенсорну мережу			2500	7500	15000	15000	22500	22500	30000	37500
	Тех.обслуговування на 1 сенсорну мережу			250	750	1500	1500	2250	2250	3000	3750
	Аренда трафіку на 1 сенсорну мережу			1000	3000	6000	6000	9000	9000	12000	15000
Собівартість обслуговування					11250	22500	22500	33750	33750	45000	56250
Валовий дохід					-11250	454300	573500	800650	979450	1266200	1612550
Адміністративні та технічні витрати											
Заробітня плата, за місяць				150000	450000	450000	450000	450000	450000	450000	450000
Витрати на рекламу, за квартал				10000	10000	10000	10000	10000	10000	10000	10000
Доставка платіжок, за квартал				3000	3000	3000	3000	3000	3000	3000	3000
Аренда офісу, за місяць				25000	75000	75000	75000	75000	75000	75000	75000
Канцелярія і тд, за квартал				5000	5000	5000	5000	5000	5000	5000	5000
Купівля та встановлення мережі				25000	25000	25000		25000		25000	25000
Сумарні адміністративні та технічні витрати					568000	568000	543000	568000	543000	568000	568000
ВИТРАТИ СУМАРНІ					579250	590500	565500	601750	576750	613000	624250
ДОХОДИ											
	відсоток налогу			0.195							
	дохід до уплати налогів				-579250	-113700	30500	232650	436450	698200	1044550
Чистий дохід	дохід після уплати налогів				-692203.75	-142860.3	27711.5	187283.25	351342.25	562051	840862.75
NPV	чиста потокова вартість			5%	5,318,473.77						
IRR	Внутрішня норма прибутку				39%						
Період					1кв	2кв	3кв	4кв	1кв	2кв	3кв
Дохід проекту					0	476800	596000	834400	1013200	1311200	1668800
Витрати проекту					579250	590500	565500	601750	576750	613000	624250
Грошовий потік проекту					-579250	-113700	30500	232650	436450	698200	1044550

Після прорахування всіх необхідних аспектів був складений узагальнюючий графік фінансових затрат проекту. Рис. 6.1 надає змогу побачити кореляцію між такими параметрами як: дохідність проекту, витрати проекту та грошовий потік проекту.

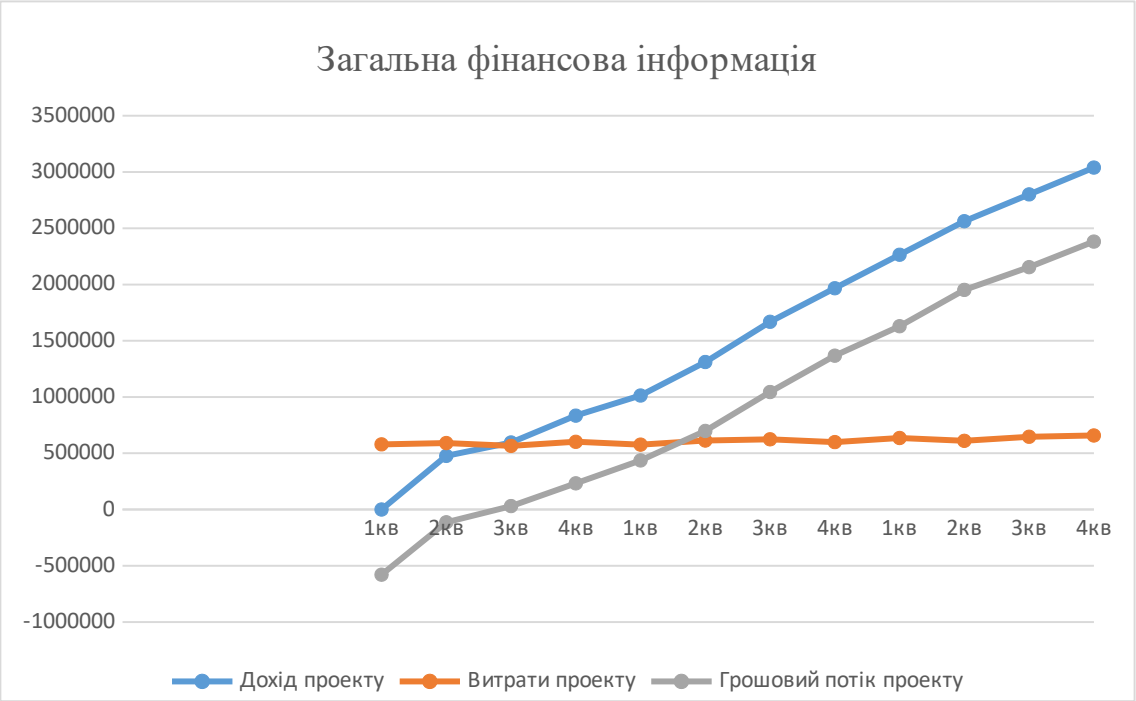

Рис.6.1 Загальна фінансова інформація по стартап проекту.

Висновки

Виконавши розрахунок фінансового плану поквартально на термін в три роки була визначена рентабельність впровадження модифікованого методу передачі пакетів інформації в мережах Інтернету Речей, що не мають постійного джерела живлення. Даний проект має термін окупності 2 квартали, за 1,17млн. грн. витрат за цей самий період. Дохід за весь період стартапу, а саме три роки, з вирахуванням податків та коштів необхідних на підтримування функціонування становитиме 8,76млн. грн., що робить його прогресивним та вигідним для первинного фінансування.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

1. Проаналізовано проблеми Інтернету речей, протоколів безпеки інформації при прийомі, збереженні та передачі, та енергоефективності і часу життя системи. Виявлено проблему енергоефективності вузлів мережі Інтернету речей.

2. Проаналізовано існуючі алгоритми та режими підвищення часу життя системи. Виділено асинхронний варіант протоколу Sleep/Wake для зменшення енерговитрат систем, як найбільш продуктивний.

3. Модифіковано метод передачі інформації, що відрізняється від методу Sleep/Wake на основі асинхронного увімкнення та вимкнення вузла, що дозволило підвищити час життя останнього.

4. Модифіковано архітектуру мережі Інтернету речей за рахунок використання буферу в вузлах передачі пакетів інформації (“Smart” IoT Device), що дозволило застосовувати модифікований режим роботи в сенсорних мережах Інтернету речей та підвищити енергоефективність мережі.

5. Проведено оцінку запропонованої архітектури. В результаті застосування запронованого методу підвищення енергоефективності сенсорна мережа має термін служби на 14,8...20,6% вище в порівнянні з сенсорними мережами Інтернету речей, що застосовують асинхронний цикл черг.

Роботу виконано в рамках НДР 0116U005092 "Підвищення ефективності обробки даних зі споживчих пристроїв в телекомунікаційній мережі Інтернету Речей". Результати дослідження апробовано на конференції Перспективи Телекомунікації 2019, 2020 та 2021.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dhar D. Energy Efficient Routing Algorithm with sleep scheduling in Wireless Sensor Network [Електронний ресурс] / D. Dhar, K. Praveen // International Journal of Computer Science and Information Technologies – Режим доступу до ресурсу: https://pdfs.semanticscholar.org/a7b3/bd02a2ceb6b6f7b4ba1c897d38055146a137.pdf.

2. Gottheil A. Energy Efficiency with IoT [Електронний ресурс] / Avrohom Gottheil. – 2017. – Режим доступу до ресурсу: https://theiotmagazine.com/energy-efficiency-with-iot-99afb953579a .

3. How can we improve energy efficiency in IOT? [Електронний ресурс]. – 2019. – Режим доступу до ресурсу : https://www.quora.com/How-can-we-improve-energy-efficiency-in-IOT

4. Internet of things [Електронний ресурс]. – 2019. – Режим доступу до ресурсу : https://en.wikipedia.org/wiki/Internet_of_things.

5. IOT (ІНТЕРНЕТ РЕЧЕЙ): Детальний Аналіз [Електронний ресурс]. – 201701. – Режим доступу до ресурсу: https://vkt.ua/articles/mnogogrannyj-internet-veshhej/.

6. D. Estrin, R. Govindan, J. Heidemann, S. Kumar, Next century challenges: scalable coordination in sensor networks, in: Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, Seattle, Washington, USA, August 1999, pp. 263-270.

7. Kontron. Інтернет речей:гіпер'обєднання інфраструктури [Електронний ресурс] / Kontron – Режим доступу до ресурсу: https://vkt.ua/articles/internet-veshhej-giperobedinenie-infrastruktury/.

8. C. F. Hsin and M. Liu, “Randomly duty-cycled wireless sensor networks: dynamic of coverage,” IEEE Trans. Wireless Commun., vol. 5, no. 11, pp. 3182– 3192, 2006.

9. Narsingh G. Lifetime Improvement Of Wireless Sensor Network Using Co-Ordinated Duty Cycle And Queue Detect Technique [Електронний

ресурс] / G. Narsingh, K. Rajeev // International Research Journal of Engineering and Technology (IRJET). – 2016. – Режим доступу до ресурсу: https://pdfs.semanticscholar.org/2c85/f004a4373bf4b41fe5070eb7ba44f7e4eff2.pdf.

10. Overview of the Most Popular Smart Home Devices [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: http://iotlineup.com/ .

11. Potthuri S. Lifetime Improvement in Wireless Sensor Networks using Hybrid Differential Evolution and Simulated Annealing (DESA) [Електронний ресурс] / Sweta Potthuri // Ain Shams Engineering Journal Volume. – 2018. – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S2090447916300284#f0005.

12. H. Zhang and J. C. Hou, “On the upper bound of α−lifetime for large sensor networks,” ACM Trans. Sen. Netw., vol. 1, no. 2, pp. 272–300, 2005.

13. Pupena O. Основи Інтернету Речей [Електронний ресурс] / Oleksandr Pupena. – 2019. – Режим доступу до ресурсу: http://edu.asu.in.ua/mod/book/tool/print/index.php?id=112#ch230.

14. Rouse M. IoT devices (internet of things devices) [Електронний ресурс] / Margaret Rouse. – 2018. – Режим доступу до ресурсу: https://internetofthingsagenda.techtarget.com/definition/IoT-device .

15. S. Slijepcevic. Power efficient organization of wireless sensor networks [Електронний ресурс] / S. Slijepcevic, M. Potkonjak. – 2002. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/abstract/document/936985/authors#authors .

16. SIAGRI R. Основа архитектуры интернета вещей [Електронний ресурс] / ROBERTO SIAGRI // CONTROL ENGINEERING. – 2017. – Режим доступу до ресурсу : https://www.prosoft.ru/cms/f/470105.pdf.

17. Закон Мура [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%BA%D0%BE%D0%BD_%D0%9C%D1%83%D1%80%D0%B0 .

18. Автоматизована система керування технологічним процесом [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BA%D0%B5%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%87%D0%BD%D0%B8%D0%BC_%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D0%BE%D0%BC .

19. Борейко О. Ю. Проектування IoT [Електронний ресурс] / Олег Юрійович Борейко. – 2017. – Режим доступу до ресурсу: https://www.slideshare.net/ssuserf405bc/iot-79608563 .

20. Иванов К. Интернет вещей и безопасность: проблемы и решения [Електронний ресурс] / Константин Иванов. – 2017. – Режим доступу до ресурсу : http://android.mobile-review.com/articles/49826/.

21. Міхненко Я. О. Порівняння видів хмарних сервісів в IoT [Електронний ресурс] / Я. О. Міхненко, В. В. Курдеча // «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ». – 2019. – Режим доступу до ресурсу: http://conferenc.its.kpi.ua/proc/article/view/168186 .

22. Проблемы и перспективы Интернета вещей [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://rb.ru/opinion/russian-iot/.

23. Пуассонівський процес [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%9F%D1%83%D0%B0%D1%81%D1%81%D0%BE%D0%BD%D1%96%D0%B2%D1%81%D1%8C%D0%BA%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81 .

24. Публічна, Приватна І Гібридна Хмари — Порівняння Підходів [Електронний ресурс]. – 201811. – Режим доступу до ресурсу: https://www.de-novo.biz/blog/publichna-privatna-i-gibridna-hmari-porivnyannya-pidhodiv-20.

25. Разработка IOT устройств [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://evergreens.com.ua/ru/products/development/iot-devices.html .

26. Як зменшити споживання енергії при використанні з'єднання IoT [Електронний ресурс]. – 2017. – Режим доступу до ресурсу : https://www.embedded-computing.com/embedded-computing-design/how-to-reduce-energy-consumption-when-using-an-iot-connection– .

27. Гранатштейн М. Чому пластикова тара і бензиновий транспорт не шкідливіше паперового пакета і електромобіля? Міфи і факти про екологічне побут // https://knife.media/eco-myths/

28. Практичні питання реалізації державної політики у сфері енергозбереження та підвищення енергетичної ефективності // http://teach.khti.ru/mod/resource/view.php?id=493

29. Волков А.А., Вахидова Б.Р. Енергозбереження в будівництві: з досвіду країн ЄС // Інтерактивна наука. 2016. №7. С. 33-35.

30. Огляд електроенергетичної галузі Росії // https: //www.ey.com/Publication/vwLUAssets/EY-power-market-russia-2018/$File/EY-power-market-russia-2

31. Інтернет речей: а чи не застрягли ми на місці? // https://habr.com/post/427035/

32. «Інтернет речей» (IoT) в Росії Технологія майбутнього, доступна вже зараз // https://www.pwc.ru/ru/publications/iot/IoT-inRussia-research_rus.pdf

33. M. Bhardwaj, T. Garnett, and A. Chandrakasan, “Upper bounds on the lifetime of sensor networks,” in Proc. 2001 IEEE ICC, pp. 785–790.

34. Міхненко Я.О., Курдеча В.В. Сучасна проблематика Інтернету Речей. [Електронний ресурс] / Я. О. Міхненко, В. В. Курдеча // «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ». – 2021. – Режим доступу до ресурсу: http://conferenc.its.kpi.ua/2021/paper/view/23192/12516

35. Міхненко Я.О. Модифікована архітектури Internet of Things.