Вінницький національний технічний університет
Факультет інформаційних електронних систем
Кафедра інфокомунікаційних систем і технологій

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Інтелектуальна сенсорна мережа Інтернету речей»

Виконав: студент 2-го курсу,
групи ТСМ-23м
спеціальності 172 – Електронні комунікації та радіотехніка
_____ Паламарчук М.С.

Керівник: к.т.н., доцент каф. ІКСТ
_____ Васильківський М.В.
«16» 12 2024 р.

Опонент: к.т.н., доцент каф. ІРТС
_____ Осадчук Я.О.
«16» 12 2024 р.

Допущено до захисту
Завідувач кафедри ІКСТ
д.т.н., проф. Кичак В.М.
«16» 12 2024 р.

Вінниця ВНТУ – 2024 рік

Вінницький національний технічний університет
факультет інформаційних електронних систем
Кафедра інфокомунікаційних систем і технологій
Рівень вищої освіти ІІ-й (магістерський)
Галузь знань - 17– Електроніка, автоматизація та електронні комунікації
(шифр і назва)
Спеціальність - 172 – Електронні комунікації та радіотехніка
(шифр і назва)
Освітньо-професійна програма - Телекомунікаційні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКСТ
д.т.н., професор В.М. Кичак
"24" 09 2024 року

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

Паламарчуку Максиму Сергійовичу .
(прізвище, ім'я, по батькові)

1. Тема роботи Інтелектуальна сенсорна мережа Інтернету речей
керівник роботи Васильківський Микола Володимирович, канд. техн. наук, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "17" 09 2024 року № 310
2. Строк подання студентом роботи 09 грудня 2024 року
3. Вихідні дані до роботи потужність передавача (для протоколів Bluetooth Low Energy, ZigBee, LoRaWAN): 0.1–100 мВт; дальність дії (залежно від технології, середовища та потужності передавача): 10–1000 м; діапазони робочих частот: 433 МГц, 868 МГц, 2.4 ГГц; енергоспоживання в активному режимі: 1–100 мВт; енергоспоживання у режимі сну: 1–10 мкВт; роздільна здатність сенсорів: від 8 до 24 біт; частота вибірки: 1 Гц – 1 кГц; обсяг пам'яті: ОЗП: 2–256 кБайт; обсяг пам'яті: ПЗП: 16 кБ – 2 МБайт; пропускна здатність (для ZigBee): 1–250 кбіт/с; пропускна здатність (для Wi-Fi 6, BLE 5.0): до 50 Мбіт/с; затримка для критичних систем: <10 мс; затримка для не критичних систем: 100–500 мс; щільність вузлів (для масового IoT): до 10^6 вузлів/км^2; тривалість роботи батареї (в залежності від частоти обміну даними, типу батареї, режиму енергозбереження): 1–10 років; частота передачі даних (при моніторингу руху) декілька разів на секунду; частота передачі даних (при моніторингу стану довкілля) декілька разів на місяць; рівень втрат пакетів (в залежності від мережі та інтерференцій): 1–5%; тривалість обробки локальних даних (алгоритми попередньої обробки даних, фільтрація): <100 мс; частота оновлення моделей (при використанні ШІ в залежності від обсягу даних і змін умов): 1–10 разів на добу; шифрування даних: 128-біт (AES); рівень помилок (BER): 10^{-5} – 10^{-9}.

4. Зміст текстової частини: дослідження методів підвищення енергоефективності безпровідних сенсорних мереж; дослідження методів оптимізації маршрутизації у мобільних Ad-hoc мережах та безпровідних сенсорних мережах в умовах IoT; агрегація даних в мережі інтернету речей; визначення ключових особливостей інтеграції ML та DL у IoT; економічна частина.

5. Перелік ілюстративного матеріалу (з точним зазначенням обов'язкових крес
структура системи Інтернету речей у WSN; блок-схема CZLAR;
маршрутизації та агрегації даних у мережі; схема агрегації даних на
вибірки; схема багатовимірного агрегування даних; схема агрегації да
основі блокчейну; архітектура MufHAS; архітектура запропонованої систем

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдан прийня
Спеціальна частина	Васильківський М.В., доцент кафедри ІКСТ	24.09.2024	16.12.2024
Економічна частина		24.09.2024	16.12.2024

7. Дата видачі завдання 02 вересня 2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Пр
1.	Розробка технічного завдання	09.09.2024р.	
2.	Дослідження методів підвищення енергоефективності безпровідних сенсорних мереж	16.09.2024р.	
3.	Дослідження методів оптимізації маршрутизації у мобільних Ad-hoc мережах та безпровідних сенсорних мережах в умовах IoT	12.10.2024р.	
4.	Агрегація даних в мережі інтернету речей	30.10.2024р.	
5.	Визначення ключових особливостей інтеграції ML та DL у IoT	11.11.2024р.	
6.	Економічна частина	22.11.2024р.	
7.	Оформлення пояснювальної записки та ілюстративної частини	02.12.2024р.	
8.	Нормоконтроль МКР	06.12.2024р.	
9.	Попередній захист МКР, опонування МКР	14.12.2024р.	
10.	Захист МКР ЕК	18.12.2024р.	

Студент (підпис) Паламарчук М.С.

Керівник роботи (підпис) Васильківський М.В.

АНОТАЦІЯ

УДК 621.396

Паламарчук М.С. Інтелектуальна сенсорна мережа Інтернету речей. Магістерська кваліфікаційна робота зі спеціальності 172 – електронні комунікації та радіотехніка, освітня програма – телекомунікаційні системи та мережі. Вінниця: ВНТУ, 2024. 118 с.

На укр. мові. Бібліогр.: 35 назв; рис.: 27; табл. 11.

Робота присвячена дослідженню інтелектуальних сенсорних мереж Інтернету речей (IoT), які відіграють ключову роль у формуванні сучасних технологій. Інтелектуальні сенсорні мережі IoT забезпечують автоматизований збір, передачу та обробку даних, що є основою для побудови розумних систем у різних галузях, таких як охорона здоров’я, розумний дім, промисловість 4.0, сільське господарство та екологічний моніторинг.

Основна увага приділяється розробці алгоритмів та моделей, які дозволяють підвищити точність роботи сенсорних пристроїв і зменшити затримки у передачі даних. Розглянуто потенційний вплив інтелектуальних сенсорних мереж на розвиток Інтернету речей, а також перспективи їх застосування в умовах урбанізації та цифровізації суспільства.

Метою роботи є розробка та дослідження ефективних методів і підходів до побудови, оптимізації та забезпечення функціонування інтелектуальних сенсорних мереж у середовищі Інтернету речей (IoT). Це дозволить забезпечити високу продуктивність, енергоефективність, надійність передачі даних і безпеку в умовах сучасних викликів цифровізації. Основні завдання наукової роботи: Дослідження методів підвищення енергоефективності безпровідних сенсорних мереж (WSN) шляхом використання рекурентних нейронних мереж довготривалої короткочасної пам’яті (LSTM) для прогнозування та оптимізації функціонування мережі. Дослідження методів оптимізації маршрутизації у

мобільних Ad-hoc мережах (MANET) та безпровідних сенсорних мережах (WSN) в умовах IoT, які забезпечують високу безпеку, енергоефективність та адаптивність до змінних умов мережі. Використання енергоефективних методів внутрішньомережевої агрегації даних для IoT-мереж з метою зменшення енергоспоживання, оптимізації використання пропускної здатності та підвищення надійності передачі інформації. Визначення ключових особливостей інтеграції машинного навчання (ML) та глибинного навчання (DL) у IoT, аналіз переваг, викликів та перспектив їх застосування. Оцінювання економічної ефективності впровадження інтелектуальної сенсорної мережі IoT.

Робота містить п’ять розділів. У першому розділі проведено дослідження методів підвищення енергоефективності безпровідних сенсорних мереж.

У другому розділі виконано аналіз методів оптимізації маршрутизації у мобільних Ad-hoc мережах та безпровідних сенсорних мережах в умовах IoT.

У третьому розділі дослідженні особливості використання енергоефективних методів внутрішньомережевої агрегації даних для IoT-мереж.

У четвертому розділі виконано визначення ключових особливостей інтеграції машинного навчання (ML) та глибинного навчання (DL) у IoT.

У п’ятому розділі виконано економічне обґрунтування доцільності реалізації даної науково-дослідної роботи.

ABSTRACT

UDC 621.396

Palamarchuk M.S. Intelligent sensor network of the Internet of Things. Master's thesis in the specialty 172 - electronic communications and radio engineering, educational program - telecommunication systems and networks. Vinnytsia: VNTU, 2024. 118 c.

In Ukrainian. Bibliography: 35 titles; Figures: 27; Table 11.

The work is devoted to the study of intelligent sensor networks of the Internet of Things (IoT), which play a key role in the formation of modern technologies. Intelligent IoT sensor networks provide automated data collection, transmission, and processing, which is the basis for building smart systems in various fields, such as healthcare, smart home, industry 4.0, agriculture, and environmental monitoring.

The main focus is on the development of algorithms and models that improve the accuracy of sensor devices and reduce delays in data transmission. The potential impact of intelligent sensor networks on the development of the Internet of Things, as well as the prospects for their application in the context of urbanization and digitalization of society are considered.

The aim of the work is to develop and study effective methods and approaches to the construction, optimization and maintenance of intelligent sensor networks in the Internet of Things (IoT) environment. This will ensure high performance, energy efficiency, data transmission reliability and security in the face of modern digitalization challenges. Main tasks of the research work: Investigation of methods for improving the energy efficiency of wireless sensor networks (WSNs) by using recurrent neural networks of long short-term memory (LSTM) to predict and optimize network operation. Investigation of routing optimization methods in mobile ad-hoc networks (MANETs) and wireless sensor networks (WSNs) in the IoT environment that provide high security, energy efficiency and adaptability to changing network conditions. Use of energy-efficient methods of intranet data aggregation for IoT networks to reduce

energy consumption, optimize bandwidth utilization and increase the reliability of information transmission. Identification of key features of machine learning (ML) and deep learning (DL) integration in IoT, analysis of advantages, challenges and prospects of their application. Evaluation of the economic efficiency of implementing an intelligent sensor network IoT.

The paper consists of five chapters. In the first section, we study methods for improving the energy efficiency of wireless sensor networks.

The second section analyzes the methods of optimizing routing in mobile Ad-hoc networks and wireless sensor networks in the IoT environment.

The third section studies the features of using energy-efficient methods of intra-network data aggregation for IoT networks.

Section 4 identifies the key features of machine learning (ML) and deep learning (DL) integration in IoT.

Section 5 provides an economic justification for the feasibility of this research work.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

AN - Адаптивні мережі

ШІ - Штучний інтелект

ШНМ - Штучна нейронна мережа

БС - Базова станція

ЦП - Центральний процесор

CDMA - Множинний доступ з кодовим поділом каналів

CNN - Згорткові нейронні мережі

CPS - Кіберфізичні системи

DL - Глибоке навчання

DMCAP - Багатоканальна модель навчання та захисту на основі глибокого навчання

DNN - Глибока нейронна мережа

DRDC - Глибоке навчання з підкріпленням

DWT - Дискретне вейвлет-перетворення

DCA - Дискримінантний кореляційний аналіз

DFRTP - Протокол динамічної тривимірної нечіткої маршрутизації

EDI - Електронні інтерфейси даних

ECC - Еліптична криптографія

EDACR - Енергоефективна розподілена адаптивна кооперативна маршрутизація

EESRP - Енергоефективний протокол захищеної маршрутизації

FFT - Швидке перетворення Фур'є

FANET - Літаючі спеціальні мережі

FCN - Мережі з вільними комірками

GPS - Глобальні системи позиціонування

GSM - Глобальна система мобільного зв'язку

GPU - Графічний процесор

HSPA - Високошвидкісний пакетний доступ

IEEE - Інститут інженерів з електротехніки та електроніки

ICRA - Інтелектуальний кластерний підхід до маршрутизації

MCE - Міжнародний союз електрозв'язку

IoMT - Інтернет медичних речей

IoT - Інтернет речей

KPI - Ключові показники ефективності

LAN - Локальна обчислювальна мережа

LSTM - Довга короткочасна пам'ять

MTC - Комунікації машинного типу

M2M - Зв'язок між машинами

MANET - Мобільні спеціальні мережі

MLRP - Багатоканальний протокол маршрутизації каналів

NOMA - Неортогональний множинний доступ

OWC - Оптичний бездротовий зв'язок

QoS - Якість обслуговування

RAN - Мережа радіодоступу

RSMA - Множинний доступ зі швидкісним розділенням каналів

RTRL - Рекурентне навчання в реальному часі

RNN - Рекурентні нейронні мережі

RWSN - Відновлювані бездротові сенсорні мережі

SOA - Сервіс-орієнтована архітектура

TDMA - Множинний доступ з часовим розділенням каналів

UMTS - Універсальна мобільна телекомунікаційна система

БПЛА - Безпілотні літальні апарати

VR - Віртуальна реальність

WBAN - Бездротові натільні мережі

WLAN - Бездротові локальні мережі

WMN - Бездротові комірчасті мережі

WMSN - Бездротові мультимедійні сенсорні мережі

WSN - Бездротові сенсорні мережі

ВСТУП

Актуальність теми. Сучасний розвиток бездротового зв’язку та комп’ютерних мереж базується на впровадженні інноваційних технологій, таких як бездротові сенсорні мережі (WSN) і Інтернет речей (IoT), що відіграють ключову роль у цифровій трансформації суспільства. Зростання кількості IoT-пристроїв та інтенсивне збільшення обсягів даних, які генеруються цими пристроями, формують нові виклики в галузях зберігання, обробки та аналізу інформації в режимі реального часу. Ці виклики стимулюють активний інтерес до розробки інтелектуальних, адаптивних і автоматизованих моделей прогнозування продуктивності WSN і IoT. Штучний інтелект (ШІ), машинне навчання (МН) і глибоке навчання (ГН) вже довели свою ефективність у розв'язанні задач аналізу даних, оптимізації процесів і прийняття рішень. Зокрема, їх використання сприяє підвищенню продуктивності в таких застосуваннях, як дрони, автоматичне водіння, розумні медичні пристрої, охоронні системи та інші реальні сценарії. Однак, незважаючи на значний прогрес, технології ML/DL мають обмеження, зокрема щодо забезпечення високої точності, енергоефективності та відповідності вимогам до часу обробки. Крім того, збільшення обсягу, різноманітності та достовірності даних створює нові проблеми, що не завжди можуть бути розв’язані існуючими підходами.

Впровадження нових рішень, зокрема квантових обчислень і квантових технологій у WSN, залишається відкритим питанням, яке вимагає систематичного вивчення. Аналогічно, розвиток криптографії та блокчейну забезпечує захист даних, що надходять від сенсорів, і має значний потенціал у сфері IoT завдяки простоті та безпеці цих технологій. Крім того, вдосконалення технологій зв'язку (5G і майбутнього 6G) створює нові можливості для побудови високошвидкісних і надійних мереж, що відповідають вимогам сучасних і перспективних сценаріїв. Завдяки стрімкому розвитку вбудованих пристроїв, що носяться, і їх інтеграції в IoT-екосистему, ці технології відкривають нові перспективи для охорони здоров'я, відстеження людської активності,

автоматизації виробництва та інших сфер. Таким чином, актуальність теми обумовлена необхідністю подолання сучасних технологічних викликів, що пов’язані із зростанням кількості пристроїв IoT, обробкою великих обсягів даних та забезпеченням їхньої безпеки, а також розвитком нових підходів до побудови інтелектуальних мереж та систем зв’язку [1-3].

Проектування та розробка інтелектуальних, адаптивних і автоматизованих моделей для підвищення продуктивності бездротових сенсорних мереж (WSN) та Інтернету речей (IoT) є однією з найважливіших задач сучасної науки і техніки. Постійне зростання кількості IoT-пристроїв і генерованих ними даних потребує нових підходів до надійного зберігання, швидкої обробки та ефективного аналізу великих обсягів інформації. Підходи на основі машинного (ML) і глибокого навчання (DL) демонструють значний потенціал у вирішенні задач аналізу, оптимізації і прийняття рішень у сфері IoT і WSN. Ці методи дозволяють підвищувати ефективність роботи систем, автоматизувати обробку даних та забезпечувати високий рівень адаптивності. У свою чергу, блокчейн і криптографія значно підвищують безпеку і цілісність переданих даних, що особливо важливо для захищених мереж і критично важливих додатків IoT.

Бездротові сенсорні мережі є критично важливими для моніторингу зон бойових дій, виявлення небезпечних об’єктів і забезпечення безпеки. Використання вузлів поглинання для управління даними і сенсорами дозволяє оптимізувати роботу мережі, але високі затримки та перевантаження в централізованих системах залишаються серйозною проблемою. Розвиток WSN і IoT відкриває значні можливості для сільськогосподарських додатків, включаючи моніторинг стану посівів, управління зрошенням та прогнозування кліматичних умов. Залучення AI, ML та DL у ці системи дозволяє вирішувати проблеми, пов’язані зі зміною клімату, посухами та ерозією ґрунтів, сприяючи підвищенню продуктивності сільського господарства. IoT-пристрої використовуються для моніторингу стану здоров’я пацієнтів у реальному часі, збираючи дані про кров’яний тиск, рівень цукру та кисню. Такі системи автоматизують медичні послуги, забезпечуючи лікарів актуальною інформацією

та підвищуючи якість обслуговування. Новітні технології зв’язку, такі як 5G і 6G, забезпечують надмалі затримки і високу пропускну здатність, необхідну для передачі великих обсягів даних у WSN та IoT. Проте незбалансовані з’єднання та географічні обмеження все ще створюють технічні бар’єри, які потребують розробки нових рішень. Сукупність цих технологій формує міждисциплінарний простір для інновацій у галузі IoT та WSN, спрямованих на подолання сучасних викликів. Інтеграція ML/DL, блокчейну та передових технологій зв’язку дозволяє створювати більш безпечні, ефективні та гнучкі системи, які відповідають вимогам сучасного суспільства [4-6].

Аналіз останніх досліджень. Останні наукові роботи в галузі бездротових сенсорних мереж (WSN) зосереджені на використанні методів штучного інтелекту (ШІ) для вирішення ключових проблем, пов'язаних із збором, агрегацією та поширенням даних. Розробка ефективних алгоритмів і стратегій оптимізації для вирішення цих проблем залишається актуальною, особливо в контексті енергоефективності, збільшення терміну служби мережі та підвищення швидкості передачі даних.

У численних роботах досліджується використання алгоритмів машинного навчання (ML) і глибокого навчання (DL) для оптимізації роботи WSN. Основні акценти:

- Зменшення затримки передачі даних.
- Покращення точності прогнозування стану мережі.
- Оптимізація маршрутизації даних для зниження енергоспоживання.

Агрегація є критичним аспектом для зменшення обсягу переданих даних і продовження терміну служби вузлів. Дослідники пропонують:

- Використання кластеризації даних за допомогою ШІ для зменшення надмірності.
- Моделі компресії даних, що базуються на ML, для мінімізації втрат енергії при передачі.

Алгоритми ШІ широко використовуються для вирішення задач:

- Балансування навантаження між вузлами.

- Прогнозування стану батареї вузлів і оптимального розподілу ресурсів.

- Виявлення і запобігання помилок вузлів у реальному часі.

Проблема обмеженого енергетичного ресурсу вузлів WSN є однією з найактуальніших. Методи оптимізації на основі ШІ, такі як генетичні алгоритми, нейронні мережі та методи рою частинок, показують високу ефективність у скороченні витрат енергії.

Використання моделей на основі глибоких нейронних мереж дозволяє передбачати динамічні зміни в топології мережі та адаптивно налаштовувати маршрутизацію. Це значно знижує ймовірність перевантаження каналів і втрат пакетів.

Застосування підходів ШІ у WSN значно покращує показники мережі, зокрема:

- Підвищення швидкості передачі пакетів.

- Збільшення терміну служби вузлів.

- Зменшення затримок у передачі даних.

- Оптимізація використання енергетичних ресурсів.

Проте, є певні виклики, які потребують подальшого дослідження:

- Інтеграція ШІ у вузли з обмеженими обчислювальними ресурсами.

- Забезпечення безпеки та захисту даних у мережах, які використовують алгоритми ШІ.

- Зниження залежності від централізованих обчислювальних вузлів у великих WSN.

Огляд останніх досліджень показує, що методи ШІ мають значний потенціал для вирішення поточних проблем WSN. Вибір оптимальних стратегій залежить від конкретних вимог до мережі, таких як енергоефективність, швидкість передачі даних або безпека. Подальші дослідження можуть зосередитися на створенні адаптивних та автономних систем, які поєднують різні методи ШІ для комплексного підходу до оптимізації WSN [7-9].

Мета і завдання роботи. Метою даної кваліфікаційної роботи є розробка та дослідження ефективних методів і підходів до побудови, оптимізації та

забезпечення функціонування інтелектуальних сенсорних мереж у середовищі Інтернету речей (IoT), що дозволяють забезпечити високу продуктивність, енергоефективність, надійність передачі даних і безпеку в умовах сучасних викликів цифровізації.

Задачами магістерської кваліфікаційної роботи є:

1. Дослідження методів підвищення енергоефективності безпровідних сенсорних мереж (WSN) шляхом використання рекурентних нейронних мереж довготривалої короткочасної пам’яті (LSTM) для прогнозування та оптимізації функціонування мережі.

2. Дослідження методів оптимізації маршрутизації у мобільних Ad-hoc мережах (MANET) та безпровідних сенсорних мережах (WSN) в умовах IoT, які забезпечують високу безпеку, енергоефективність та адаптивність до змінних умов мережі.

3. Використання енергоефективних методів внутрішньомережевої агрегації даних для IoT-мереж з метою зменшення енергоспоживання, оптимізації використання пропускної здатності та підвищення надійності передачі інформації.

4. Визначення ключових особливостей інтеграції ML та DL у IoT, аналіз переваг, викликів та перспектив їх застосування.

5. Оцінювання економічної ефективності впровадження інтелектуальної сенсорної мережі IoT.

Об’єктом дослідження є мережі сенсорів, інтегровані у системи Інтернету речей (IoT), що забезпечують збір, обробку, передачу та аналіз даних для прийняття автоматизованих рішень у реальному часі.

Предметом дослідження є процеси, методи та технології функціонування, управління та оптимізації інтелектуальних сенсорних мереж IoT.

Методи досліджень базуються на використанні: теоретичних методів для аналізу, моделювання та формалізації принципів роботи сенсорних мереж, розробки концепцій побудови архітектури IoT-систем, визначення оптимальних підходів до взаємодії пристроїв, а також для створення математичних моделей та

алгоритмів обробки даних; емпіричних методів для проведення експериментів, тестування та спостереження за роботою прототипів сенсорних мереж IoT; методів машинного та глибокого навчання для обробки великих обсягів даних, виявлення аномалій, класифікації подій, прогнозування та автономного прийняття рішень; методів обробки та аналізу даних для роботи з великими потоками даних у режимі реального часу, фільтрації шумів, очищення даних, їх візуалізації та пошуку прихованих закономірностей; методів оцінки ефективності та економічного обґрунтування для визначення економічної доцільності впровадження інтелектуальних сенсорних мереж IoT, розрахунку показників ефективності, аналізу витрат та вигод, прогнозування окупності інвестицій та управління фінансовими ризиками; методів кібербезпеки та захисту даних для захисту мереж IoT від кібератак, шифрування переданих даних, забезпечення конфіденційності та цілісності інформації, а також для розробки засобів автентифікації, контролю доступу до мережі та захисту від загроз типу DDoS.

Новизна одержаних результатів:

1. Досліджено особливості використання рекурентних нейронних мереж довготривалої короткочасної пам’яті (LSTM) для прогнозування навантаження та оптимізації функціонування WSN. Це дозволяє значно зменшити енергоспоживання мережі, підвищуючи її тривалість життя та ефективність.

2. Розглянуто застосування нових методів оптимізації маршрутизації для мобільних Ad-hoc мереж (MANET) та WSN, які забезпечують високу безпеку, енергоефективність та адаптивність до змінних умов. Ці методи сприяють більш стабільній та ефективній роботі мереж в умовах Інтернету речей (IoT).

3. Досліджено нові методи агрегації даних в IoT-мережах для зменшення енергоспоживання, оптимізації пропускної здатності та підвищення надійності передачі інформації. Це покращує загальну продуктивність та економічність мереж.

4. Здійснено визначення ключових особливостей інтеграції машинного навчання (ML) та глибинного навчання (DL) у IoT, аналіз переваг, викликів та

перспектив їх застосування. Це дослідження відкриває нові горизонти для розвитку інтелектуальних IoT-систем.

5. Виконано оцінювання економічної доцільності впровадження інтелектуальних сенсорних мереж в IoT, враховуючи їх потенціал для зниження витрат та підвищення ефективності в різних галузях. Це сприяє обґрунтованому прийняттю рішень щодо інвестицій у новітні технології IoT.

Кожен з цих напрямів досліджень сприяє покращенню енергоефективності, безпеки, надійності та економічної ефективності мереж IoT, що є актуальними та важливими для сучасних технологічних систем.

Апробація роботи та її основні результати роботи проводилися на Всеукраїнській науково-практичній інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2025)» у 2024 році.

Публікації результатів магістерської кваліфікаційної роботи. Основні положення кваліфікаційної роботи висвітлені у 2 тезах науково-технічної конференції.

1 ЕНЕРГОЕФЕКТИВНА WSN НА ОСНОВІ LSTM

1.1 Оптимізовані методи створення ефективної та стійкої мережі

Традиційні моделі прогнозування транспортного потоку дійсно мають певні обмеження [4]. Рекурентні нейронні мережі (RNN) стикаються з проблемами, коли часові лаги між даними є великими. Основні виклики пов'язані з наступними аспектами:

1. Проблеми з навчанням RNN при тривалих часових інтервалах: Коли розмір часового вікна (n) у транспортному потоці занадто великий, RNN важко зберігати інформацію про далекі залежності в часі. Це викликає проблему затухання або вибуху градієнтів, що призводить до погіршення точності моделі.

2. Вибір оптимального розміру часового інтервалу (n): Це складне завдання через вплив багатьох зовнішніх факторів, таких як погодні умови, швидкість руху, дорожні інциденти тощо. Визначити, як далеко в минуле потрібно дивитися для адекватного прогнозування, непросто.

Для подолання цих проблем застосовуються такі методи, як довготривала короткочасна пам'ять (LSTM), яка здатна краще працювати з тривалими часовими залежностями, оскільки LSTM блокує градієнт, дозволяючи йому не затухати при проходженні крізь час. CEC у блоках LSTM: Постійна похідна у комірках блоку пам'яті (CEC) дозволяє зберігати інформацію на тривалих часових інтервалах. Це досягається за допомогою комбінації методів зворотного поширення в часі (BPTT) і рекурентного навчання в реальному часі (RTRL). Важливим моментом є те, що певні похідні повинні постійно обчислюватися незалежно від того, чи використовується бажана оцінка на кожному конкретному етапі.

Таким чином, використання сучасних підходів, таких як LSTM або інші види покращених рекурентних мереж, допомагає подолати обмеження традиційних RNN, особливо при роботі з довготривалими часовими залежностями.

При управлінні інформацією про часовий режим транспортного потоку традиційні моделі прогнозування мають два недоліки:

(1) Традиційні підходи, зокрема традиційні ШНМ, важко навчати, якщо серія транспортних потоків має тривалі часові лаги, а це означає, що якщо розмір часового вікна n в рівнянні (1) занадто великий, традиційні рекурентні нейронні мережі (РНМ) будуть працювати погано.

(2) Визначити ідеальний розмір часового інтервалу n досить складно, оскільки на зв'язок між транспортними потоками в різні періоди часу впливає безліч складних елементів, включаючи погоду, швидкість і непередбачені інциденти [1]. При збереженні СЕС в комірках блоків пам'яті LSTM (рис. 1.1) все ще використовуються дві методології дослідження: рекурентне навчання в реальному часі (RTRL) надихає компоненти системи до і включаючи комірки, і зворотне поширення в часі (BPTT) для навчання системних доступів після комірок. Останні сумісні з RTRL, оскільки певні часткові похідні (пов'язані зі станом клітини) повинні завжди обчислюватися на кожній фазі, незалежно від того, чи буде на цьому кроці задана бажана оцінка, чи ні. Наразі дослідники лише скорочують потік, щоб звільнити місце для додаткових рекурентних зв'язків і дозволити градієнту клітини змінюватися з часом.

Запропоновані технології призначені для створення бездротової натільної мережі, яка є високозахищеною, стійкою та енергоефективною. Завдяки застосуванню двох протоколів для передачі даних і планування за допомогою інтелектуальної мережі та систем відновлюваної енергетики, мета досягається. Загальна архітектура бездротової натільної мережі (WBAN) зображена на рисунку 1.2. Для забезпечення зв'язку всередині WBAN через інтелектуальну мережу та системи відновлюваної енергетики датчики підключені до пацієнтів, і кожен з них може взаємодіяти з тілесним координатором. Персональний пристрій-асистент (PDA), через який спілкується координатор, надсилає зібрані дані на медичний сервер для запису. Копія даних передається лікарю пацієнта. Лікар може отримати доступ до попередніх записів на медичному сервері і приймати рішення на їх основі [5].

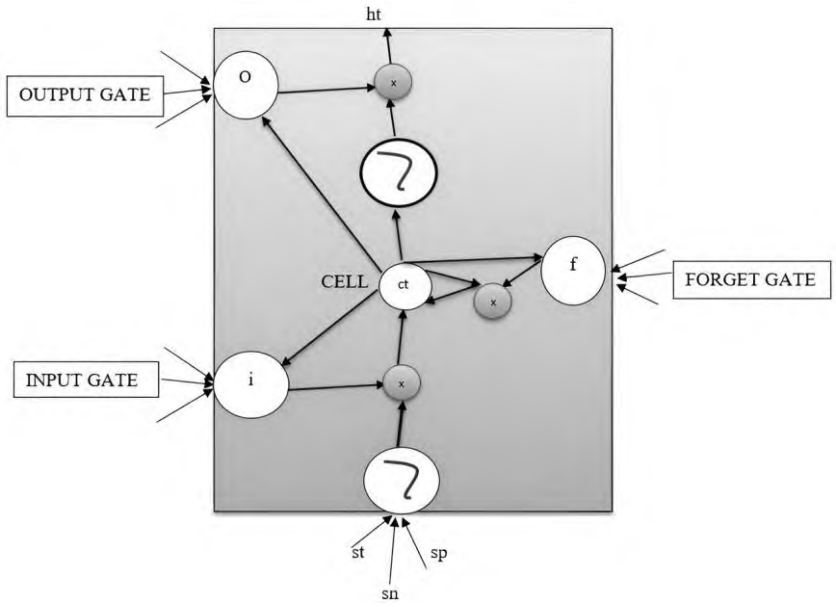

Рисунок 1.1 – Структура LSTM

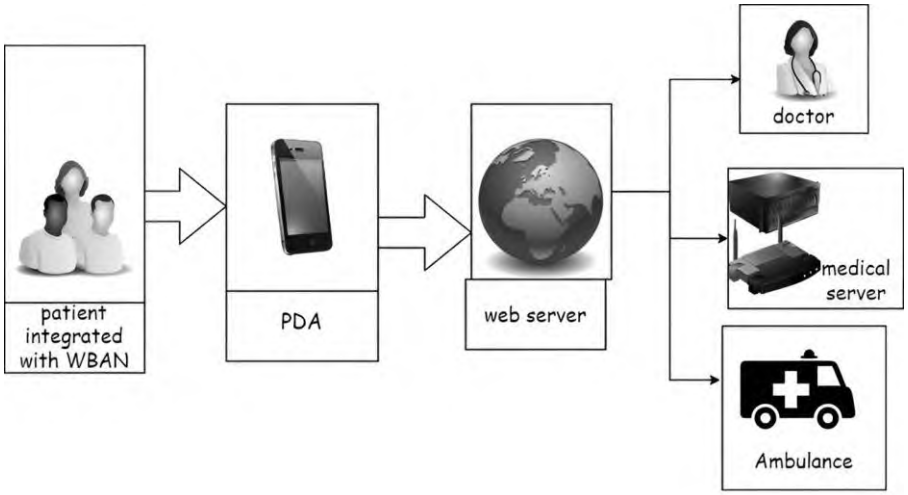

Рисунок 1.2 – Загальна архітектура бездротової IoT мережі

Щоб змінити рецепт або надати іншу дистанційну підтримку, лікар може зв'язатися з пацієнтом через КПК. У разі необхідності, лікар може отримати повідомлення з вказівкою транспортувати пацієнта в кареті швидкої допомоги.

Мережа WBAN може розширити своє покриття, використовуючи технології бездротових приватних мереж як шлюзи. Через шлюзові пристрої носимі технології можуть бути підключені до інтернету [2]. Оскільки медичний

персонал може отримати доступ до даних пацієнта онлайн, місцезнаходження пацієнта не має значення. Точну кількість енергії, яку використовує мережа, можна дізнатися за допомогою математичної функції, наприклад:

$$E = f(x) \tag{1.1}$$

де E - точна кількість енергії, яку споживає мережа, а x - різні параметри мережі, що впливають на енергоспоживання, такі як потужність передачі, протокол маршрутизації та методи агрегації даних.

$$\text{Minimize } E = f(x) \tag{1.2}$$

за умови:

- Підтримується зв'язок з мережею
- Дані передаються з певною затримкою
- Точність даних відповідає певному порогу
- Не порушуються обмеження на ресурси, такі як пам'ять вузла та обчислювальна потужність.

1.2 Оптимізація енергоефективних WSN

Оптимізація адаптивних методів зменшення обсягу даних в енергоефективних бездротових сенсорних мережах може бути досягнута за рахунок застосування методів глибокого навчання, зокрема використання стратегії розосередженого інтелектуального аналізу даних на основі нейронних мереж LSTM. Метою зменшення обсягу даних в WSNs є мінімізація обсягу даних, що передаються від датчиків до базової станції, при збереженні високого рівня точності зібраної інформації. Це важливо для енергоефективності у WSN, оскільки передача великих обсягів даних може швидко виснажити обмежені енергетичні ресурси сенсорних вузлів. Одним з підходів до зменшення обсягу

даних є використання адаптивних методів, які регулюють частоту дискретизації сенсорних вузлів на основі патернів даних, що спостерігаються в мережі. Однак ефективність цих методів значною мірою залежить від точності моделей даних, які використовуються для прогнозування майбутніх патернів даних [8]. Методи глибокого навчання, зокрема мережі LSTM, мають багатообіцяючі результати в оцінці моделей даних часових рядів. Застосовуючи стратегію розосередженого інтелектуального аналізу даних, LSTM-модель може навчатися на даних з декількох датчиків у мережі, що дозволяє більш точно прогнозувати майбутні моделі даних. Стратегія розосередженого інтелектуального аналізу даних передбачає навчання LSTM-моделі на даних з підмножини датчиків у мережі, де кожна підмножина представляє окремий регіон мережі. Це дозволяє моделі вивчати унікальні характеристики кожного регіону і робити більш точні прогнози на основі об'єднаних даних з усіх датчиків.

Оптимізований адаптивний метод зменшення обсягу даних в енергоефективних WSN з використанням глибокого навчання та стратегії розосередженого інтелектуального аналізу даних на основі LSTM буде включати наступні кроки:

1. Збір даних з датчиків у мережі.

2. Розділити мережу на регіони та створити підмножини даних з датчиків у кожному регіоні.

3. Навчити модель LSTM на даних з кожної підмножини.

4. Об'єднати LSTM-моделі для прогнозування майбутніх патернів даних для всієї мережі.

5. Відрегулюйте частоту дискретизації сенсорних вузлів на основі прогнозованих шаблонів даних, щоб мінімізувати обсяг переданих даних, зберігаючи при цьому високий рівень точності.

Використовуючи цей оптимізований підхід, мережі WSN можуть досягти енергоефективності, одночасно збираючи точні та змістовні дані [6].

1.3 Дослідження інформаційної та енергетичної ефективності мереж

Важливою темою досліджень є енергоефективні мережі WSN, які дозволяють ефективно і з найменшими витратами збирати дані. LSTM-мережі та інші алгоритми глибокого навчання (DL) можуть бути використані для аналізу даних, зібраних в БСМ, та отримання глибоких висновків. Підвищити ефективність збору та аналізу даних у WSN можна за допомогою методу розсіяного інтелектуального аналізу даних. Розподіляючи діяльність зі збору та аналізу даних між кількома вузлами мережі, ця тактика мінімізує кількість даних, які потрібно надсилати до центрального процесора. Як наслідок, мережа працюватиме довше і споживатиме менше енергії. Для реалізації цієї стратегії кожен вузол WSN може бути обладнаний мережею LSTM, яка відповідає за аналіз даних, зібраних цим вузлом. Результати аналізу можуть передаватися на центральний вузол, який агрегує результати і генерує вичерпний звіт про використання енергії в усій мережі.

Аналіз використання енергії різними технологіями є важливим етапом у розробці та оптимізації бездротових сенсорних систем. Він включає в себе розрахунок кількості енергії, необхідної для запропонованого методу для створення енергоефективних мереж, які можуть ефективно функціонувати в умовах, коли джерела електроенергії можуть бути дефіцитними або відсутніми. Споживання енергії можна розрахувати за наступною формулою [7]:

$$\text{Енергоспоживання} = \text{Потужність} * \text{Час} \tag{1.3}$$

Наприклад, якщо потужність, яку споживає бездротовий датчик, становить 10 Вт і він працює 10 годин, то споживання енергії можна розрахувати так:

$$\text{Енергоспоживання } 10 \text{ Вт} * 10 \text{ годин} = 100 \text{ Вт/год}$$

Потім споживання енергії можна порівняти з енергією, що споживається традиційними підходами, щоб визначити ефективність запропонованого підходу у зменшенні споживання енергії.

Мережі WSN набувають все більшого поширення в різних сферах застосування, таких як моніторинг навколишнього середовища, промислова автоматизація та «розумні» будинки. Однак, енергоспоживання мереж WSN викликає велике занепокоєння, оскільки більшість вузлів у цих мережах живляться від батарейок і мають обмежені енергетичні ресурси.

Одним з підходів до вирішення цієї проблеми є розробка енергоефективних алгоритмів для обробки та передачі даних у WSN. Методології обчислювального інтелекту, включаючи мережі LSTM, показали багатообіцяючі результати в різних додатках, включаючи WSN. ШНМ також мають потенціал для вивчення довгострокових залежностей, включаючи LSTM-мережі в послідовних даних.

Підхід розсіяного аналізу даних може бути використаний для зменшення обсягу даних, які необхідно надсилати за кордон, щоб підвищити енергоефективність мереж WSN. Ця стратегія передбачає обробку даних локально на кожному сенсорному вузлі і передачу лише зведених даних на базову станцію. Мережа LSTM може бути використана для генерації зведених даних, вивчаючи закономірності в даних і прогнозуючи майбутні значення. Ефективність запропонованої стратегії можна дослідити за допомогою аналізу коефіцієнта поширення. Цей аналіз передбачає порівняння обсягу даних, переданих за допомогою стратегії розосередженого інтелектуального аналізу даних, з обсягом даних, переданих за допомогою традиційного підходу, коли всі дані передаються на базову станцію. Результати аналізу можуть пролити світло на те, наскільки добре запропонована стратегія працює для зниження енергоспоживання мереж WSN.

Аналіз коефіцієнта передачі передбачає оцінку ефективності запропонованого підходу в зменшенні обсягу даних, що передаються від датчиків до базової станції. Коефіцієнт передачі можна розрахувати за наступною формулою [8]:

Коефіцієнт передачі = передані дані/загальний обсяг зібраних даних (1.4)

Наприклад, якщо сенсорна мережа збирає 1000 точок даних і передає лише 100 точок даних на базову станцію, то коефіцієнт передачі можна розрахувати наступним чином:

Коефіцієнт передачі = 100/1000 = 0.1

Низький коефіцієнт передачі вказує на те, що запропонований підхід є ефективним для зменшення обсягу переданих даних, що призводить до зменшення споживання енергії та подовження терміну служби мережі.

Таким чином, за рахунок зменшення обсягу переданих даних розподілений інтелектуальний аналіз даних, побудований на мережах LSTM, може підвищити обчислювальну ефективність мереж WSN. Ефективність запропонованої стратегії можна оцінити за допомогою аналізу коефіцієнта маршрутизації, який також може запропонувати пропозиції щодо подальшого вдосконалення.

Дещо довший термін служби літій-іонної батареї туманних вузлів робить енергоефективність цих мереж серйозною проблемою. Цю проблему можна вирішити, оптимізувавши аналіз співвідношення часу життя мережі за допомогою підходу на основі DL і позитивістського підходу до розосередженого інтелектуального аналізу даних на LSTM. RNN з довгими з'єднаннями можуть бути захоплені за допомогою LSTM, які можуть бути застосовані для аналізу часових рядів даних. В контексті WSN, LSTM можна використовувати для прогнозування майбутньої поведінки сенсорних вузлів на основі їх минулих даних [9].

Це передбачення може допомогти у прийнятті енергоефективних рішень, таких як вимкнення деяких вузлів або зменшення частоти їх зчитування, тим самим продовжуючи термін служби мережі. Стратегія розосередженого інтелектуального аналізу даних передбачає збір даних з декількох сенсорних вузлів, їх обробку та надсилання результатів назад на вузли для прийняття

рішень. Такий підхід може допомогти зменшити обсяг даних, що передаються, та енергію, що споживається кожним вузлом, тим самим збільшуючи термін служби мережі.

Аналіз коефіцієнту тривалості життя мережі передбачає оцінку того, наскільки запропонований підхід може продовжити термін служби бездротової сенсорної мережі.

Коефіцієнт тривалості життя мережі можна розрахувати за наступною формулою [10]:

Коефіцієнт терміну служби мережі = Термін служби мережі із запропонованим підходом / Термін служби мережі без запропонованого підходу (1.5)

Наприклад, якщо бездротова сенсорна мережа має термін служби 2 роки без запропонованого підходу і 5 років із запропонованим підходом, то співвідношення терміну служби мережі можна розрахувати наступним чином:

Коефіцієнт тривалості життя мережі = 5 / 2 = 2,5

Вищий коефіцієнт тривалості життя мережі вказує на те, що запропонований підхід є ефективним для продовження терміну служби мережі, що зменшує витрати на обслуговування та підвищує надійність мережі.

Для того, щоб розрахувати коефіцієнт тривалості життя інтернет-магістралі, необхідно порівняти залишкову енергію сенсорних вузлів з їх початковою енергією. Це співвідношення можна використовувати для оцінки тривалості життя мережі та визначення вузлів, які споживають більше енергії. Використовуючи стратегію розосередженого інтелектуального аналізу даних на основі LSTM, можна оптимізувати це співвідношення і збільшити термін служби мережі. Таким чином, підходи на основі глибокого навчання з використанням стратегії розосередженого інтелектуального аналізу даних на основі LSTM можуть бути застосовані для оптимізації енергоефективності WSN. Цей підхід

може допомогти продовжити термін служби мережі і зменшити навантаження на сенсорні вузли, тим самим сприяючи широкому впровадженню WSN в різних сферах застосування [11].

LSTM, ще одна технологія глибокого навчання, продемонструвала багатообіцяючу перспективу в підвищенні енергоефективності WSN. У цьому контексті, стратегія розосередженого пошуку даних на основі LSTM може бути використана для аналізу ефективності WSN. Стратегія розосередженого аналізу даних передбачає збір даних з різних датчиків в мережі та їх локальну обробку за допомогою легких алгоритмів. Потім оброблені дані передаються на центральний сервер або шлюз для подальшого аналізу з використанням методів глибокого аналізу. Така стратегія зменшує щільність мережі або кількість конфіденційних даних, які необхідно передавати через мережу, тим самим зменшуючи споживання енергії. Рекурентні штучні нейронні мережі з можливостями LSTM можуть виявляти часові залежності в минулому часі, що робить їх добре придатними для аналізу даних з датчиків. Вони можуть вивчати закономірності в даних і прогнозувати майбутні значення, що може бути використано для оптимізації енергоспоживання WSN.

Для застосування LSTM в аналізі ефективності WSN можна виконати наступні кроки:

Збір даних: Дані з різних датчиків в мережі збираються і обробляються локально з використанням легких алгоритмів.

Передача даних: Оброблені дані передаються на центральний сервер або шлюз для подальшого аналізу з використанням LSTM.

Навчання LSTM: LSTM-модель навчається, використовуючи зібрані дані для вивчення закономірностей і прогнозування майбутніх значень.

Оптимізація енергоспоживання: Навчена LSTM-модель використовується для оптимізації енергоспоживання WSN шляхом прогнозування оптимального часу передачі даних сенсорами та налаштування частоти їх дискретизації.

Аналіз ефективності передбачає оцінку загальної продуктивності запропонованого підходу. Ефективність може бути розрахована за допомогою

різних показників, таких як точність, пропускна здатність або енергоефективність. У цьому випадку ефективність можна оцінити на основі споживання енергії на одну точку зібраних даних, яке можна розрахувати за такою формулою [12]:

$$\text{Споживання енергії на одну точку даних} = \text{Споживання енергії}/\text{Загальна кількість зібраних даних} \quad (1.6)$$

Наприклад, якщо сенсорна мережа споживає 100 Вт-год енергії для збору 1000 точок даних, то споживання енергії на одну точку даних можна розрахувати наступним чином:

$$\text{Енергоспоживання на одну точку 100 Вт/год} /1000 = 0{,}1 \text{ Вт/год на одну точку}$$

Нижче споживання енергії на точку даних свідчить про вищу ефективність і кращу продуктивність запропонованого підходу.

Використовуючи стратегію розосередженого інтелектуального аналізу даних на основі LSTM, можна зменшити споживання енергії, зберігаючи при цьому точність і надійність роботи мереж WSN. Цей підхід може бути застосований до різних додатків WSN, таких як моніторинг навколишнього середовища, охорона здоров'я та розумні міста, для підвищення їх енергоефективності та подовження терміну служби [13].

1.4 Застосування LSTM в рекурентних нейронних мережах

Використання LSTM (Long Short-Term Memory) поверх RNN (Recurrent Neural Networks) допомагає подолати ключові проблеми традиційних рекурентних нейронних мереж. Звичайні RNN мають обмеження, пов'язані з затухаючим градієнтом та складнощами у зберіганні довгострокових

залежностей. LSTM — це різновид RNN, який краще справляється з задачами, що потребують роботи з послідовними даними, такими як обробка тексту, прогнозування часових рядів та розпізнавання мови.

LSTM містить спеціальну комірку пам'яті та механізми керування інформацією (входи, виходи, забування), які дозволяють зберігати важливу інформацію на тривалих проміжках часу.

Завдяки своєму дизайну, LSTM забезпечує стабільніший градієнт під час навчання, що зменшує втрату важливих залежностей, які трапляються у довгих послідовностях.

Можна будувати багатошарові мережі, використовуючи кілька LSTM-шарів поверх базової RNN, щоб навчати модель складнішим закономірностям у даних. Базову RNN-мережу можна ускладнити, додаючи кілька шарів LSTM. Наприклад:

- Вхідні дані → RNN-шар → LSTM-шар → Вихідний шар (Softmax / Dense)

У цьому підході LSTM виконує роль "удосконаленої пам'яті", яка зберігає довготривалі залежності, тоді як звичайний RNN-шар може бути відповідальним за початкове згортання та вивчення базових послідовностей.

Переваги застосування LSTM поверх RNN:

- Краще розуміння контексту: Зберігається інформація навіть із довгих послідовностей.

- Менше помилок при довгих вхідних даних: Проблема затухаючого градієнта значно знижується.

- Більш глибокі моделі: LSTM дозволяє створювати глибші архітектури, які ефективні для обробки великих наборів даних. Отже, застосування LSTM поверх RNN робить такі мережі набагато потужнішими та придатними для складних послідовних задач, що потребують роботи з довгими залежностями [14].

Ранні дослідження показали, що LSTM-мережі здатні навчатися завданням, які колись вважалися неможливими, включаючи завдання, що вимагають точного хронометражу та підрахунку, вивчення контекстних мов та обробку високоточних дійсних чисел над зашумленими послідовностями. Більше того,

дослідники успішно створили метазаробіток у LSTM-мережах, використовуючи завдання пошуку подкастів для наближення підходу до навчання квадратичних функцій, а також застосували навчання з підкріпленням для вирішення немарковських проблем навчання, пов'язаних зі стійкими залежностями. Ці висновки підкреслюють потенціал LSTM-мереж для вирішення складних проблем машинного навчання, які включають довготривалі залежності та зашумлені вхідні послідовності, що дозволяє розробляти більш ефективні моделі та алгоритми, які можуть бути використані для вирішення широкого спектру реальних проблем [9].

LSTM- RNNs виявилися винятковими у виконанні різноманітних когнітивних навчальних завдань. Найпоширеніші технології розпізнавання аудіо та рукописного тексту, а також, останнім часом, машинного перекладу, застосовуються в літературі.

Інші завдання когнітивного навчання включають синтаксичний аналіз, моделювання конверсійних ситуацій, категоризацію текстів, генерування почерку, ідентифікацію почуттів за мовленням і створення текстів.

Попередня оцінка можливостей нейронних мереж у ситуаціях, що вимагають природної мови, була зроблена за допомогою звичайного тесту нейронного моделювання. У 2003 році ефективних результатів було досягнуто, коли для задач розпізнавання мови було застосовано стандартні LSTM з комбінацією довгих короткочасних і поліноміальних блоків ядра. Кращі результати було отримано після мультимодального навчання з двонаправленим довгим короткочасним (BLSTM) порівняно з системами на основі секретної прихованої марковської моделі (RNNs). І останнє, але не менш важливе: варіація, відома як BLSTM-CTC (коннекціоністська тимчасова класифікація), перевершила HMM; подальші досягнення висвітлюються, і відмінні результати були отримані як у 2013 році, так і після використання глибокої форми як складеної BLSTM-CTC, так і еталонної цільової функції CTC, що налаштовується.

Гібридний дизайн LSTM/HMM показав найкращі результати, згідно з дослідженнями ефективності різних топологій LSTM для задач розпізнавання голосу з великим лексиконом. Продуктивність LSTM нещодавно було покращено за допомогою навчання на основі уваги та фреймворку послідовності до послідовності. У 2015 році було представлено спеціальний фреймворк синтезу мовлення з двома функціями - «слухач» і «слухач і орфографія». Функція «слухач» використовує BLSTM з пірамідальною структурою і базується на раніше описаних годинникових RNNs (pBLSTM). Нещодавно розроблений LSTM-перетворювач, що базується на увазі, використовується в іншій функції - «слухати і писати». Для тренування обох функцій використовуються методи з фреймворку навчання, що базується на увазі, та фреймворку навчання від послідовності до послідовності [10].

BLSTM-CTC вперше був використаний для виявлення віртуальних рукописів у 2007 році і в кінцевому підсумку перевершив приховані марковські методи. Тоді, поєднуючи BLSTM-C TC та ймовірнісну мовну модель, було створено систему, яка могла миттєво перекладати рукописні дані в Інтернеті. Ця система продемонструвала неймовірно високі показники SCADA з частотою помилок, подібною до людської при виконанні цього виду діяльності в реальному сценарії використання. У задачі відстеження почерку в автономному режимі інший метод, що поєднує BLSTM-C TC і багатовимірний LSTM, перевершив класифікатори, засновані на прихованій моделі Маркова.

Було рекомендовано відмовитися від використання високоефективного підходу регуляризації з 2013 року.

Автори дослідження 2014 року використали архітектуру нейронної мережі кодер-екодер RNN для підвищення продуктивності стохастичної системи машинного перекладу, що призвело до покращення точності та швидкості перекладу.

На основі представленої методології побудовано макет прийомопередавача RNN. Ці результати було підтверджено, і було досліджено архітектуру глибокого LSTM, що заробляє шаблони. Здатність перекладати терміни, яких не було в

лексиконі, була покращена завдяки використанню еквівалентності sequence-t-to-s, що також вирішило проблему з рідкісними словами. Дизайн був значно покращений завдяки вирішенню проблем з перекладом довгих фраз шляхом включення в декодер механізму уваги. Використання послідовності до послідовності покращило можливості перекладу термінів, яких не було в словнику, і вирішило проблему з рідкісними словами. Додавання механізму уваги до декодера дозволило вирішити проблеми з перекладом довгих слів, що значно покращило архітектуру [15].

Здатність двонаправленої довготривалої короткочасної пам'яті розрізняти різні форми даних у текстових даних, таких як тексти, математика, схеми та ілюстрації, дозволила їй у 2012 році перевершити HMM та SVM у визначенні ключових слів та розпізнаванні режиму. Приблизно в той самий час дослідники також вивчали класифікацію злегка піднятих зображень з топової колекції, що дало значно кращі результати, ніж попередні підходи. Для того, щоб створювати справжні англійські речення, що виражають фотографії, у 2015 році була успішно навчена найновіша версія LSTM, заснована на методі послідовності до послідовності. Крім того, у 2015 році автори створили модель, об'єднавши LSTM з ієрархічним високорівневим екстрактором ознак для класифікації та інтерпретації зображень, таких як виявлення активності та опис зображень/відео.

1.5 Висновки до розділу 1

Отже, використання методів глибокого аналізу даних, таких як LSTM, може значно підвищити енергоефективність бездротових сенсорних мереж. Стратегія розосередженого інтелектуального аналізу даних, запропонована в цьому дослідженні, також дозволяє зменшити передачу даних і подовжити термін служби мережі, особливо у віддалених місцях, де технічне обслуговування є складним завданням. Експериментальний аналіз показав, що запропонований підхід перевершує традиційні технології за вимогами до використання енергії, коефіцієнту передачі, терміну служби мережі та ефективності. Це дослідження є

перспективним рішенням проблем, з якими стикаються при створенні стійких бездротових сенсорних мереж, особливо у віддалених районах.

2 ОПТИМІЗАЦІЯ МАРШРУТИЗАЦІЇ ДЛЯ МОБІЛЬНИХ AD-HOC І WSN В IOT

2.1 Бездротова сенсорна мережа

Бездротові сенсорні мережі (WSN) — це системи просторово розподілених спеціалізованих датчиків, які відстежують і реєструють змінні навколишнього середовища та передають отриману інформацію до централізованого пункту. Температура, рівень забруднення, звук, вологість та вітер — це лише деякі з змінних, які можуть відстежувати WSN. Останнім часом WSN привертають багато уваги завдяки появі передових технологій мікроелектромеханічних систем (MEMS), які дозволяють створювати сенсорні вузли, що можуть виконувати багато функцій, будучи при цьому невеликими, дешевими і вимагаючи лише невеликої кількості обчислювальної потужності. Вони можуть виявляти фізичні величини, а також змінні навколишнього середовища, що дозволяє їм аналізувати інформацію локально, бездротово спілкуватися і співпрацювати.

Огляд загальної структури WSN показано на рисунку 2.1. Сенсорний вузол складається з радіопередавача, сенсорного пристрою, мікроконтролера і джерела живлення, яким зазвичай є батарея, а також інших компонентів. Вартість сенсорних вузлів може становити від кількох доларів до кількох сотень доларів, залежно від їхніх можливостей. В результаті обмежень ціни та розміру сенсорних вузлів, доступні ресурси системи, включаючи енергію, передачу та обчислення, також були обмежені [16].

Вузол-поглинач є джерелом енергії та ресурсоємним вузлом, який має необмежені комунікаційні та обчислювальні можливості. Він може бути як фіксованим, так і динамічним, і служить інтерфейсом між сенсорною мережею і центральним адміністративним центром. Залежно від застосування WSN, активність, за якою ведеться спостереження, може бути як стаціонарною, так і мобільною. Рухомі сенсорні вузли використовуються, наприклад, для

спостереження за поведінкою диких тварин, коли вони рухаються у нестандартний спосіб. У порівнянні з сенсорними вузлами, фіксовані та добре відомі місця є кращими [11].

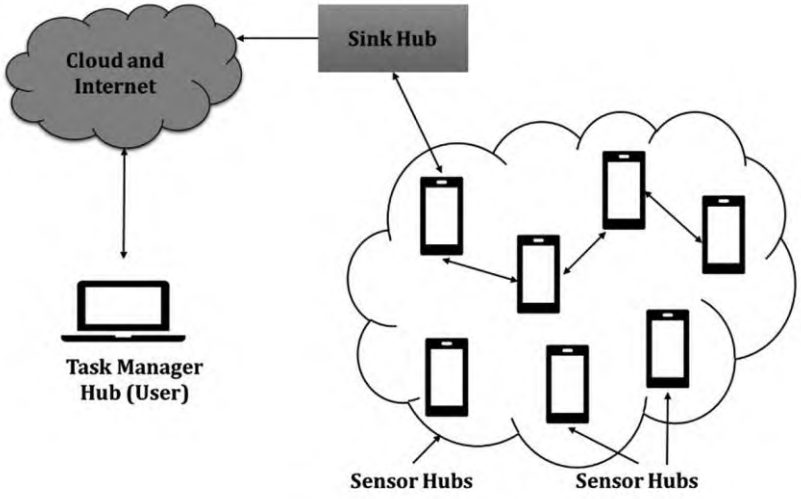

Рисунок 2.1 – Структура мережі WSN

Бездротова сенсорна мережа (WSN) — це різновид бездротової мережі, в якій велика кількість сенсорних вузлів (також відомих як моти) вільно циркулюють, самонаправляються і використовують мінімальну потужність. Ці мережі включають безліч невеликих, географічно розподілених вбудованих пристроїв, що працюють від батарейок, які об'єднані в мережу з метою ретельного збору, обробки та передачі даних користувачам. Окрім збору даних, вони також контролюють обчислювальні та обробні потужності. Невеликі комп'ютери, відомі як вузли, використовуються в мережах для з'єднання інших вузлів.

Сенсорний вузол є енергоефективним бездротовим пристроєм з широким спектром функцій. Моти мають широкий спектр промислового використання. Для досягнення конкретних цілей застосування мережа сенсорних вузлів збирає дані з навколишнього середовища. Для зв'язку між собою моти використовують трансивери. Кількість сенсорів у WSN може обчислюватися сотнями або навіть тисячами. Спеціальні мережі, на відміну від сенсорних, матимуть менше вузлів,

але не матимуть жодної організації. В результаті їх широкого використання бездротові сенсорні мережі пропонують безліч нових концептуальних і оптимізаційних проблем, включаючи розгортання, розташування і відстеження.

Одним з важливих аспектів є покриття, яке дає відповіді на питання щодо здатності сенсорної мережі надавати якісні послуги (спостереження). Важливо, щоб сенсорні вузли були розміщені таким чином, щоб забезпечити ефективне і надійне покриття для збору даних з навколишнього середовища, забезпечуючи при цьому мінімальні витрати енергії та обчислювальних ресурсів [12].

2.2 Мобільні спеціальні мережі (MANET)

Мобільна ad hoc мережа (MANET) переміщується між різними місцями. У загальній бездротовій мережі весь географічний регіон має кілька базових станцій, і кожна з них має фіксоване покриття в цьому географічному регіоні. Мобільний вузол передає будь-які сигнали, які вузли можуть почути на базовій станції. Будь-який мобільний вузол завжди буде приєднуватися до якоїсь базової станції, а базові станції передають будь-який сигнал або дані. Це середовище є загальним уявленням про бездротові мережі.

Вузли MANET, навпаки, беруть участь у кооперативній передачі пакетів, причому кожен мобільний вузол бере участь як у передачі, так і в прийомі, з метою передачі пакета іншому вузлу. Операція індивідуальної маршрутизації не обов'язково повинна виконуватися через бездротовий маршрутизатор. Щоб передати пакет на потрібний вузол, кожен мобільний вузол може виконати маршрутизацію і вибір маршруту. Мобільні мережі ad hoc вимагають кооперативної передачі пакетів. Причиною кооперативного зв'язку є те, що, на відміну від інших типів бездротових мереж, немає базової станції для координації процесу маршрутизації та передачі пакетів. Оскільки в MANET відсутня фіксована топологія, для пересилання пакетів необхідна колективна передача [13]. На рисунку 2.2 зображено загальну мобільну спеціальну мережу.

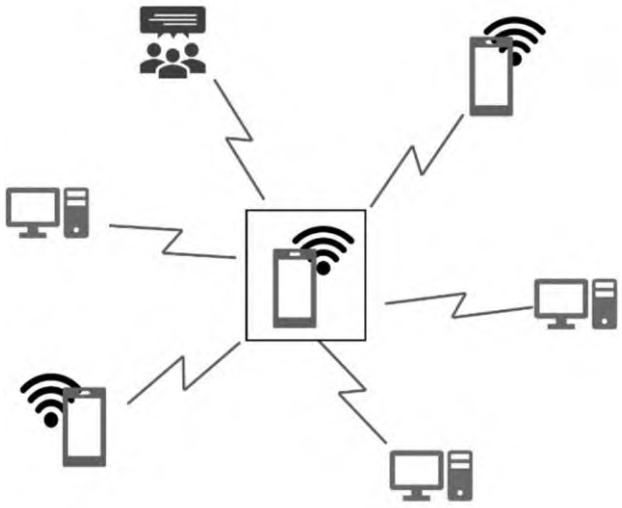

Рисунок 2.2 – Мобільна спеціальна мережа

Таким чином, MANET характеризується децентралізованою природою і вимагає від кожного вузла здатності до самостійної маршрутизації, що дозволяє мережі адаптуватися до змін у топології та забезпечує гнучке і надійне передавання даних навіть в умовах мобільності вузлів. Подібно до топології, існують інші обмеження на мобільні вузли в цьому типі мережі. Найважливішим з них є те, що вузли мають єдиний радіоприймач з фіксованим діапазоном передачі. Дальність передачі радіостанції визначає, наскільки далеко можна почути сигнал, переданий мобільним вузлом. Крім того, кожен вузол має певну постійну потужність у ватах, яка необхідна для активації радіо для передачі та прийому сигналів. Незалежно від процесу, чи то передача, чи то прийом сигналу, вузол втрачає певну кількість енергії, і час життя вузла дорівнює часу, який він має в запасі.

Мобільний вузол має інші властивості, такі як швидкість мобільності; вузол може рухатися з будь-якою швидкістю і в будь-якому напрямку. Ця властивість часто змінює топологію мережі, що сильно впливає на передачу пакетів [14]. Фактори, що впливають на функціонування мобільної ad hoc мережі та маршрутизацію, детально розглядаються в цьому розділі. Серед таких факторів:

1. Оскільки вузли мають фіксовану дальність передачі, зв’язок між вузлами можливий лише в межах цієї дальності. Це створює необхідність у

багатоступеневій передачі даних, де вузли передають пакети через посередницькі вузли для досягнення кінцевого пункту призначення.

2. Енергоефективність є критично важливою, оскільки вузли живляться від батарейок. Це вимагає оптимізації енергоспоживання під час передачі та прийому даних для продовження терміну служби вузлів і, як наслідок, всієї мережі.

3. Постійна зміна розташування вузлів у просторі впливає на маршрутизацію, оскільки зв’язки між вузлами можуть утворюватися і розриватися через рух. Це потребує динамічного адаптування маршрутів для забезпечення безперебійного передавання даних.

4. Швидка зміна топології може призвести до частих перебудов маршрутів, що може створювати додаткове навантаження на мережу і знижувати ефективність передачі даних. Вказані фактори вимагають від MANET використання спеціальних алгоритмів і протоколів маршрутизації, які можуть адаптуватися до змін і забезпечувати надійну передачу даних навіть в умовах мобільності та обмежених ресурсів.

2.3 Особливості технологій IoT

Інтернет речей (IoT) значною мірою покладається на датчики, коли мова йде про дані в режимі реального часу. Використання цих електронних гаджетів у кожному секторі призведе до величезного потоку великих даних, оскільки вони поширюються на все населення світу. При розробці електричних систем важливо враховувати зворотні аспекти низького заряду батареї та високої продуктивності. На рисунку 2.3 відображено огляд IoT.

Існує два підходи до розробки IoT:

1. Створення окремої мережі, яка складається лише з фізичних речей:

- Цей підхід передбачає створення автономної мережі, що об'єднує фізичні пристрої, сенсори та інші компоненти, які взаємодіють між собою без підключення до Інтернету.

- Така мережа може бути корисною для певних специфічних завдань, де необхідно забезпечити високу безпеку та конфіденційність даних, або в умовах, де підключення до Інтернету неможливе чи небажане.

2. Розширення охоплення Інтернету:

- Цей підхід вимагає інтеграції фізичних пристроїв у глобальну мережу Інтернету, що дозволяє використовувати переваги хмарних обчислень, великих сховищ даних та інших інноваційних технологій.

- Хоча цей підхід є дорогим, він відкриває великі можливості для обробки і аналізу даних у реальному часі, забезпечуючи високий рівень продуктивності та ефективності.

- Застосування хмарних обчислень дозволяє централізовано обробляти великі обсяги даних, отриманих від сенсорів, що є критично важливим для багатьох додатків IoT.

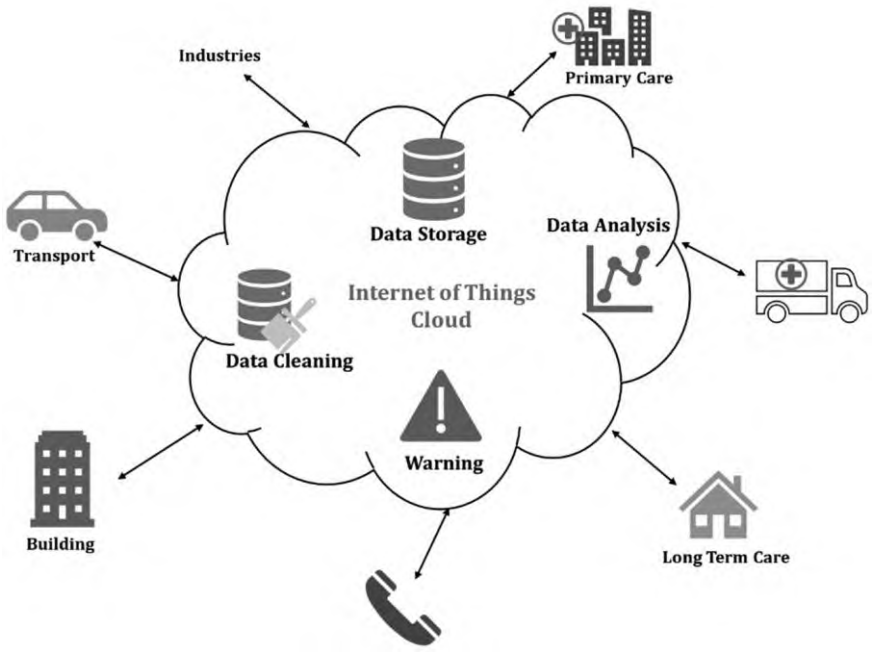

Рисунок 2.3 – Сегмент мережі IoT

Важливі аспекти розробки IoT.

- Енергоспоживання: Однією з головних проблем IoT є низький заряд батареї пристроїв, тому важливо розробляти енергоефективні рішення.

- Висока продуктивність: Пристрої IoT повинні забезпечувати високу продуктивність для обробки та передачі великих обсягів даних.

- Безпека: Забезпечення безпеки даних та пристроїв є критичним аспектом у розвитку IoT.

- Масштабованість: Інфраструктура IoT повинна бути здатна підтримувати величезну кількість підключених пристроїв, які можуть рости експоненційно. Отже, мережа IoT має величезний потенціал для трансформації різних секторів, але вимагає ретельного планування та розробки для подолання технічних викликів та забезпечення безперебійного функціонування систем.

Пристрої Інтернету речей (IoT) генерують величезну кількість даних, які потребують надійного зберігання та обробки. Хмарні технології відіграють важливу роль у цій ситуації, надаючи масштабовані рішення для зберігання та обробки даних. Завдяки хмарним обчисленням ми можемо більш ефективно аналізувати ці дані, що дозволяє краще розуміти стан системи та виявляти, наприклад, електричні несправності. Для зв'язку пристроїв необхідне підключення до Інтернету, оскільки кожен фізичний об'єкт має свою IP-адресу в мережі Інтернет. Однак поточна схема іменування IP-адрес дозволяє використовувати обмежену кількість адрес, що може стати проблемою зі зростанням кількості IoT-пристроїв. Через це дослідники шукають альтернативні системи іменування для ефективного опису кожного фізичного об'єкта, щоб зберегти час та ресурси [15].

2.4 Розробка WSN в IOT

Виконаємо опис технології Інтернету речей (IoT) та її архітектури, використаної в даному дослідженні. Окрім того, розглядаються прикладні формули, що використовуються для розрахунків у різних системах. Детальне проектування та розробка архітектури на основі додатків розглядаються в цьому

розділі, як показано на рисунку 2.4. Архітектура сенсорної мережі широко використовується у бездротових сенсорних мережах (WSN). Цей тип архітектури може бути застосований у різних сферах, таких як лікарні, дороги, школи та будинки, а також у управлінні катастрофами, безпекою та кризовому менеджменті. Оскільки WSN є системою, що базується на конкретних застосуваннях, опис проектів з точки зору вимог та обмежень застосування є відносно простим.

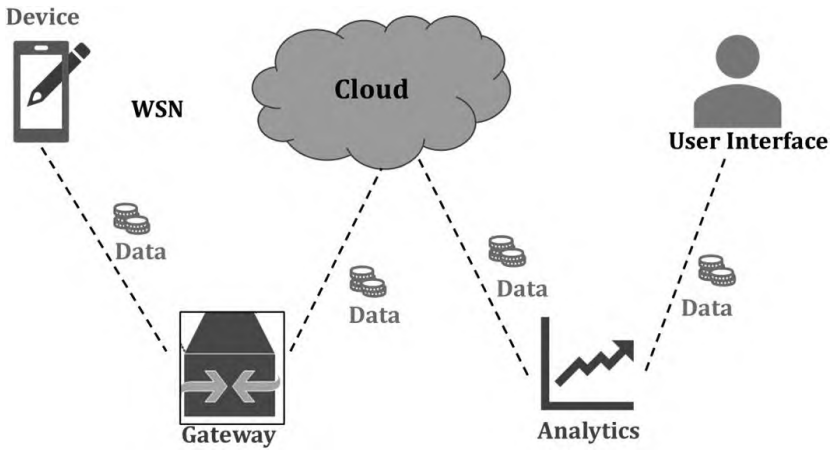

Рисунок 2.4 – Структура системи Інтернету речей у WSN

Незважаючи на швидкий розвиток технологій, суспільство рухається до парадигми, яка забезпечує постійну взаємозв'язаність. Фіксовані та мобільні мережі стали звичним явищем, а відкриті стандарти для певних процедур адресації вже розроблені та доступні [16].

Концепції майбутнього Інтернету вивчаються, розробляються і постійно адаптуються до повсякденного життя. Інтернет речей (IoT) є новою ідеєю, яка пов'язана з «майбутнім Інтернетом». Впроваджуючи IoT, ми уявляємо майбутнє, в якому повсякденні об'єкти інтегровані в Інтернет, їхнє місцезнаходження і статус можуть бути розпізнані, а інтелектуальні функції додаються для ефективного розширення можливостей Інтернету. Ця безшовна інтеграція віртуального середовища з фізичною сферою значно впливає на індивідуальне та міжособистісне середовище людей.

IoT об'єднує в мережу об'єкти реального світу, які мають електроніку як частину своєї конструкції. Це надає цим об'єктам можливість спілкуватися один з одним і розуміти, як вони взаємодіють з навколишнім середовищем. У найближчі роки «технології, засновані на Інтернеті речей, забезпечать просунутий рівень обслуговування і кардинально змінять те, як люди займаються бізнесом і живуть повсякденним життям». IoT добре зарекомендував себе у різних сферах, включаючи медицину, агробізнес, генну терапію, розумні міста, електроенергетику та розумні будинки. Коли йдеться про промислову автоматизацію Інтернету речей, першим кроком є встановлення великих локальних бездротових сенсорних мереж з тривалим часом автономної роботи та найкращою операційною системою для їхніх потреб. Розвиток і розширення мереж IoT включає використання різних типів пристроїв, а також розробку і вдосконалення протоколів бездротового зв'язку та систем розшарування, щоб краще відповідати вимогам ринку WSN [17].

2.5 Інтеграція WSN в IoT

В останні роки Інтернет перетворився з мережі людей на мережу Інтернету речей (IoT). Інтеграція бездротових сенсорних мереж (WSN) в Інтернет речей призвела до значної складності в управлінні функціональною сумісністю. Шлюз IoT відіграє ключову роль у додатках IoT, оскільки він з'єднує WSN зі звичайними комунікаційними мережами або Інтернетом. Це дозволяє управляти і контролювати бездротові сенсорні мережі, а також забезпечує безперешкодну інтеграцію WSN з мобільними комунікаційними мережами або Інтернетом (див. рис. 2.5). Шлюз IoT виконує кілька важливих функцій:

1. Забезпечує зв'язок між WSN та іншими мережами.

2. Перетворює дані з одного протоколу в інший, забезпечуючи сумісність між різними мережами.

3. Захищає дані, передані між WSN і зовнішніми мережами, шляхом шифрування та аутентифікації.

4. Збирає, обробляє і передає дані від сенсорів до центрів обробки даних.

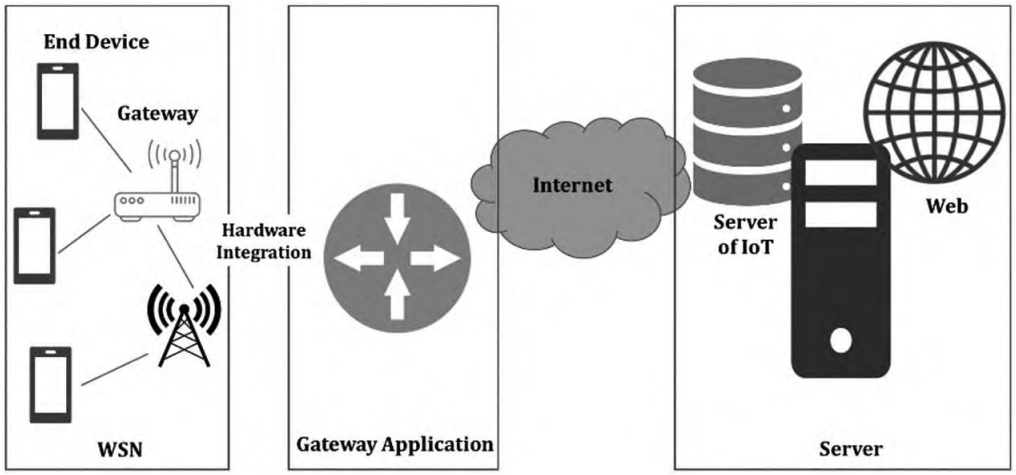

Рисунок 2.5 – Структура WSN з системою IoT

Таким чином, шлюз IoT є критично важливим компонентом для забезпечення ефективної та надійної роботи систем IoT, сприяючи більш глибокій інтеграції та функціональній сумісності між різними мережами і пристроями.

Мережі WSN були відкриті для Інтернету, що дозволяє зловмисникам здійснювати свої злочинні операції з будь-якої точки світу. Як наслідок, глобальні мережі повинні докладати значних зусиль для вирішення проблем, що виникають внаслідок такого підключення до Інтернету, таких як шкідливе програмне забезпечення та інші загрози. Для забезпечення ефективного захисту існуючих мереж, їх було оснащено потужним центральним шлюзом. Цей шлюз виконує унікальну і важливу роль у захисті мережі, забезпечуючи централізовану точку контролю і управління. Проте існують значні виклики, пов'язані з дефіцитом обчислювальних ресурсів, потребою в енергії і необхідністю економії пам'яті, що ускладнює перепрофілювання поточних механізмів безпеки.

Використання WSN дозволяє користувачам контролювати та керувати системним середовищем. Однак для забезпечення безпеки цих мереж необхідні наступні заходи:

1. Використання легких криптографічних алгоритмів, які можуть працювати в умовах обмежених ресурсів.

2. Встановлення систем моніторингу для виявлення та реагування на підозрілу активність.

3. Забезпечення своєчасного оновлення для виправлення вразливостей.

4. Розробка рішень, що мінімізують енергоспоживання, зберігаючи при цьому високий рівень безпеки.

5. Підвищення обізнаності користувачів щодо потенційних загроз і методів їх уникнення. Ці заходи допоможуть забезпечити надійну і безпечну роботу WSN в умовах глобального підключення до Інтернету.

2.6 Застосування WSN та IoT

Проект IoT, проведений у 2010 році, виявив, що сценарії застосування Інтернету речей (IoT) можна розділити на 14 різних категорій. Ці категорії охоплюють широкий спектр сфер, включаючи транспорт, розумні міста, розумні будинки, спосіб життя, сільське господарство та роздрібну торгівлю, а також розумні фабрики. Деякі з найбільш відомих додатків IoT включають:

- Інфраструктура для оптимізації ресурсів, підвищення ефективності послуг і покращення якості життя мешканців.

- Системи для моніторингу та управління енергоспоживанням, зниження витрат і впливу на навколишнє середовище.

- Віддалений моніторинг пацієнтів, управління медичними пристроями та підтримка здоров'я.

- Технології для відстеження ідентифікації та аутентифікації смартфонів.

- Системи для контролю і управління водопостачанням, виявлення витоків і забезпечення якості води.

- Розумні пристрої, які відстежують здоров'я, фізичну активність і інші показники користувача.

- Автоматизація домашніх систем для підвищення комфорту, безпеки та енергоефективності.

- Системи для моніторингу рівня радіації і виявлення небезпечних матеріалів.

- Мережі сенсорів для виявлення сейсмічної активності і раннього попередження.

- Технології для управління трафіком, зниження заторів і покращення безпеки на дорогах.

Більшість додатків Інтернету речей використовуються на підприємствах, які застосовують датчики та інші IoT-пристрої в різних галузях, таких як промисловість, торгівля та комунальні послуги. Технологія IoT також знайшла своє застосування в сільському господарстві, архітектурі та автоматизації будівель, сприяючи діджиталізації цих сфер. Зокрема, IoT допомагає підприємствам:

- Оптимізація виробничих процесів, зниження витрат і підвищення ефективності через автоматизацію та моніторинг в реальному часі.

- Покращення управління запасами, аналіз поведінки покупців і оптимізація логістики.

- Ефективне управління інфраструктурою, забезпечення надійного постачання послуг і зниження експлуатаційних витрат. Таким чином, технологія IoT не тільки покращує існуючі процеси, але й відкриває нові можливості для інновацій та діджиталізації в різних галузях.

На рисунку 2.6 показано, що мережі WSN та IoT мають багато застосувань. Інтернет речей (IoT) і бездротові сенсорні мережі (WSN) мають широке застосування завдяки своїй здатності збирати, обробляти та передавати дані. Їх використання класифікується за кількома критеріями, такими як:

- Мобільність: здатність сенсорів або пристроїв переміщуватися в межах мережі.

- Гетерогенність: інтеграція різних типів пристроїв і технологій.

- Покриття: площа, яку охоплюють датчики.

- Топологія: структура організації мережі.

- Якість обслуговування (QoS): ефективність передачі даних і стабільність системи.

Рисунок 2.6 – Особливості застосування WSN

Приклади застосувань IoT і WSN [18]:

1. Сільське господарство:

Завдяки IoT фермери можуть автоматизувати і вдосконалювати процеси. Наприклад, датчики вимірюють:

- Температуру.

- Вологість повітря.

- Кількість опадів.

- Вміст ґрунту.

Це дозволяє точніше керувати поливом, добривами та іншими методами, оптимізуючи використання ресурсів.

2. Контроль інфраструктури:

Датчики можуть відстежувати:

- Стабільність будівель.

- Стан доріг і мостів.

- Інші елементи критичної інфраструктури.

Це сприяє попередженню аварій, економії коштів на ремонті та забезпечує безпеку.

3. Інші сфери:

IoT має вплив і в інших галузях, таких як:

- Охорона здоров'я: моніторинг стану пацієнтів, управління медичним обладнанням.

- Банківська справа: безпечні платежі та моніторинг транзакцій.

- Роздрібна торгівля: управління запасами, покращення клієнтського досвіду.

- Промисловість: автоматизація виробничих процесів.

Переваги IoT:

- Економія ресурсів і грошей.

- Підвищення продуктивності.

- Покращення якості життя.

- Оптимізація робочих процесів.

IoT є революційною технологією, яка впливає на всі аспекти сучасного життя та господарської діяльності.

Процедура знаходження маршруту в протоколі демонструє ефективний підхід до організації мережі з мобільними вузлами [19].

ALGORITHM FOR CZLER

Step 1: Every node's neighbor and zone are initially determined and kept in node N, destination D.
Step 2: To create a zone (Z), obtain the number of hops as a radius (R).
Step 3: Analyze the transaction log to choose a controller.
Step 4: If (certain node N can receive traffic T,
Step 5: The mode of Node A is active.
Step 6: If (node N = destination D) then
Step 7: Accept and send an acknowledgment (ACK).
Step 8: Else
Step 9: Check that Destination D is located in zone (Z), and then send the packet using the inter-zone routing method if that is the case.
Step 10: Else, employ the intra-zone routing mechanism.
Step 11: End

Наведемо детальний опис цієї процедури:

Ключові аспекти процесу маршрутизації:

1. Обмеження зони маршрутизації:

Для визначення маршруту враховуються лише вузли, розташовані в межах півмісяця (як показано на рис. 2.7). Це дозволяє уникати вузлів, які можуть бути поза досяжністю через мобільність. Радіус зони обчислюється у кількості переходів між вузлами, наприклад, радіус дорівнює 8.

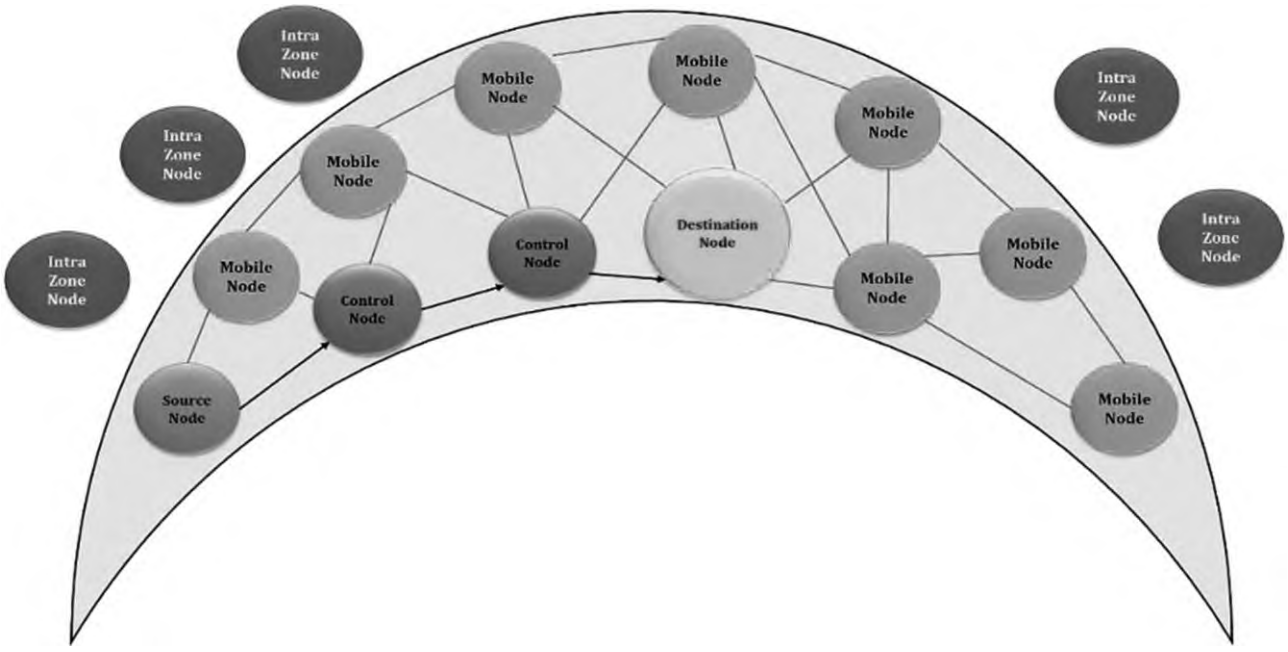

Рисунок 2.7 – Особливості застосування маршруту CZLAR

2. Роль контролера:

Контролер забезпечує передачу даних до цільового вузла, виконуючи функції управління маршрутом. Якщо кількість мобільних вузлів менша, довжина хвилі (зона покриття) також зменшується, що підвищує ефективність передачі.

3. Алгоритм вибору контролера (CZLAR):

Процедура вибору контролера передбачає регулярне ініціювання мобільними вузлами процесів, спрямованих на:

- Збір інформації про сусідів (сусідні вузли визначаються на першому етапі).

- Оцінку залишкової енергії кожного вузла для підвищення якості обслуговування (QoS).

4. Обмін повідомленнями «HELLO»:

Мобільні вузли обмінюються повідомленнями типу "HELLO", які містять:

- Інформацію про сусідів.

- Дані про залишкову енергію.

- Загальні метрики стану мережі.

5. Обчислення періоду очікування:

Для кожного вузла визначається час затримки перед оголошенням координатора.

Фактори, що впливають на тривалість періоду:

- Кількість сусідів: більше сусідів → менша затримка.

- Залишкова енергія: більше енергії → менша затримка (рис. 2.8).

Процес вибору координатора:

- Кожен вузол зважує свою енергетику та кількість сусідів.

- Найбільш енергоефективний вузол із найменшою затримкою оголошується координатором.

- Роль координатора забезпечує підтримання якості обслуговування (QoS) при передачі даних.

Переваги CZLAR:

- Оптимізоване використання ресурсів енергії вузлів.

- Підтримка стабільності мережі навіть за умов мобільності вузлів.

- Зменшення затримок і підвищення ефективності передачі даних.

Цей підхід є важливим для мобільних сенсорних мереж, оскільки враховує їх динамічну природу, забезпечуючи збалансовану роботу та тривалий час життя мережі.

Результати моделювання показують, що запропонований протокол CZLER споживає менше енергії, досягаючи при цьому покращеної пропускної здатності та коефіцієнту передачі пакетів. У дослідженні розглядаються реальні сценарії

випадкового розгортання та випадкового розподілу вузлів у таких контекстах, як заклади охорони здоров'я, торгові зони та спортивні стадіони.

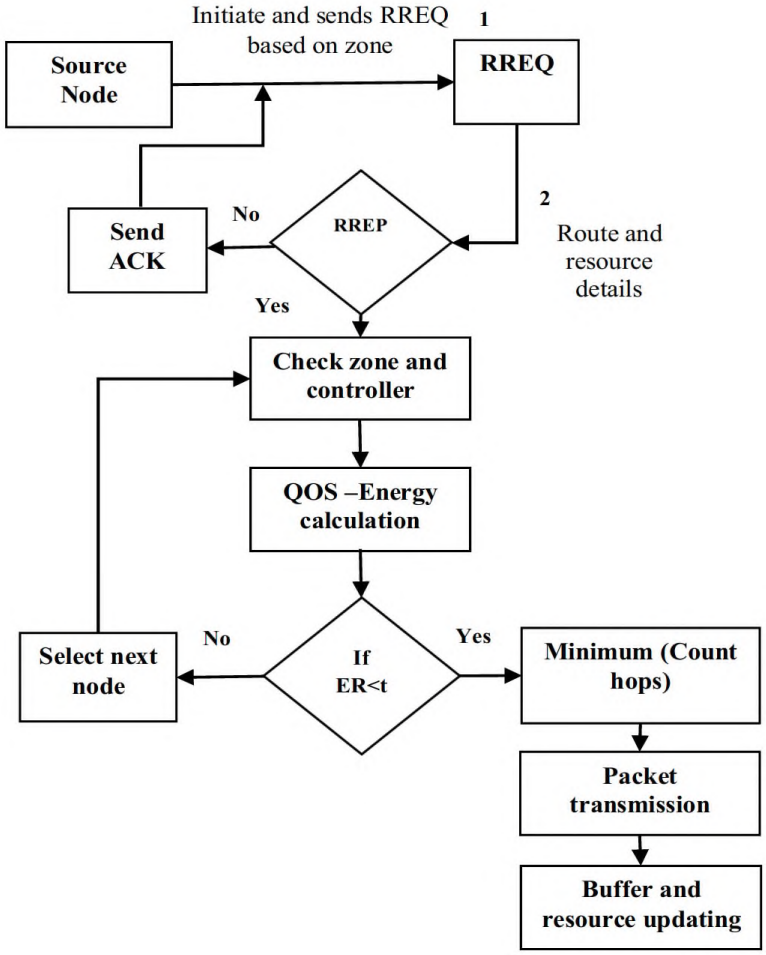

Рисунок 2.8 – Блок-схема CZLAR

Також передбачається поширення цієї роботи на медичні сенсори на основі Інтернету речей. Основні переваги протоколу CZLER включають [20]:

1. Зменшення споживання енергії дозволяє вузлам працювати довше.
2. Забезпечення надійної передачі даних з мінімальними втратами.
3. Зниження витрат на енергію та ресурси.
4. Забезпечення швидкої та захищеної передачі даних між вузлами.

Розробка та впровадження такого протоколу можуть значно покращити ефективність та надійність MANET у різних сферах, включаючи медицину,

торгівлю та спорт, а також сприяти розвитку медичних сенсорів на основі Інтернету речей [21].

2.7 Оцінювання продуктивності сегменту сенсорної мережі

Продуктивність оцінювалася за такими основними метриками: наскрізна затримка (E2D), коефіцієнт доставки пакетів (PDR), пропускна здатність та енергоспоживання. Для оцінки масштабованості протоколів кількість вузлів варіювалася від 20 до 100.

Наскрізна затримка (E2D) для запропонованого CZLER коливається від 12 до 104 мілісекунд. Оскільки CZLER виконує балансування навантаження, що зменшує час очікування в черзі під час перевантаження, затримка запропонованого CZLER є меншою у порівнянні з ArcRect та TWRDASR. Це показано на рисунку 2.9.

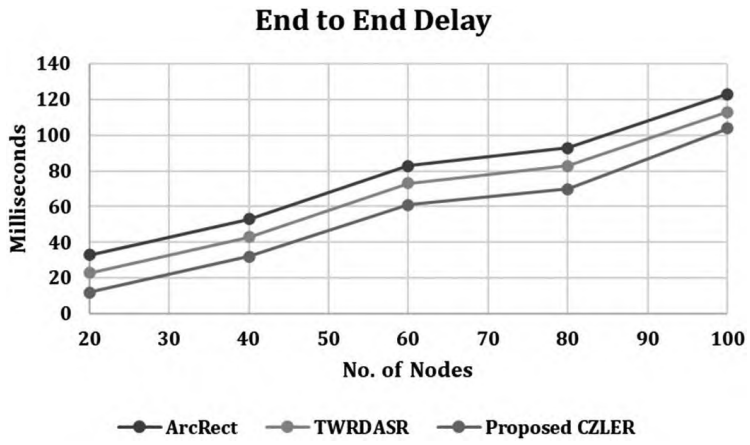

Рисунок 2.9 – Наскрізна затримка

Пропускна здатність

Графік пропускної здатності для різної кількості вузлів показано на рисунку 2.10. Видно, що пропускна здатність CZLER коливається від 432 до 532. Завдяки балансуванню навантаження у CZLER, втрати пакетів, спричинені

перевантаженням вузлів мережі, зменшуються. Отже, пропускна здатність CZLER є вищою, ніж у ArcRect та TWRDASR.

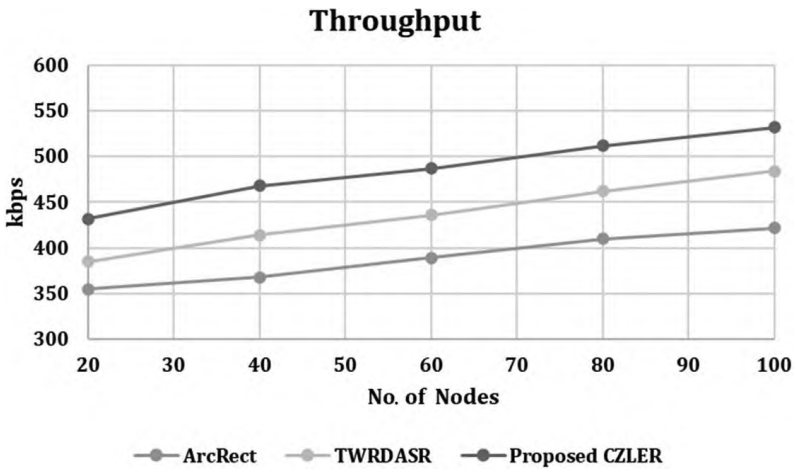

Рисунок 2.10 – Пропускна здатність

Коефіцієнт доставки пакетів (PDR) для різної кількості вузлів показано на рисунку 2.11. PDR для запропонованого CZLER коливається від 0,62 до 0,26. Завдяки балансуванню навантаження у CZLER втрати пакетів через перевантаження зменшуються. Таким чином, PDR CZLER є вищим, ніж у ArcRect та TWRDASR.

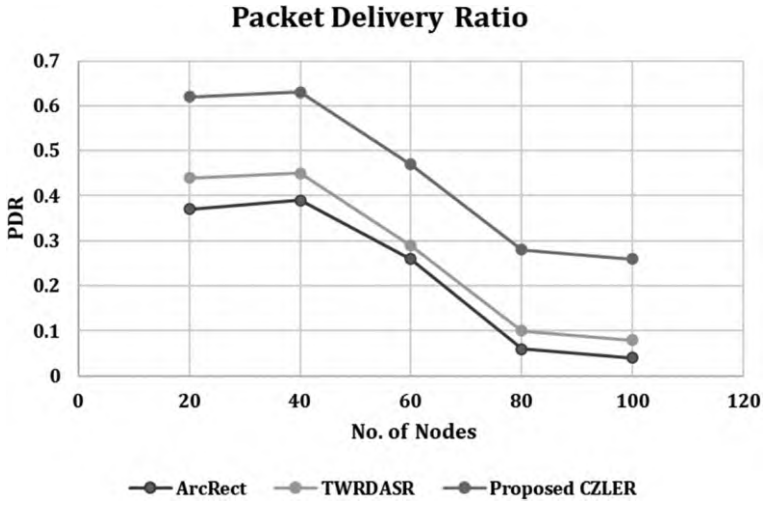

Рисунок 2.11 – Коефіцієнт доставки пакетів

Графік енергоспоживання для різної кількості вузлів показано на рисунку 2.12. Енергоспоживання CZLER коливається від 9,55 до 13,19 джоулів. Завдяки енергоефективному вибору маршруту в CZLER, енергоспоживання CZLER є меншим у порівнянні з ArcRect та TWRDASR.

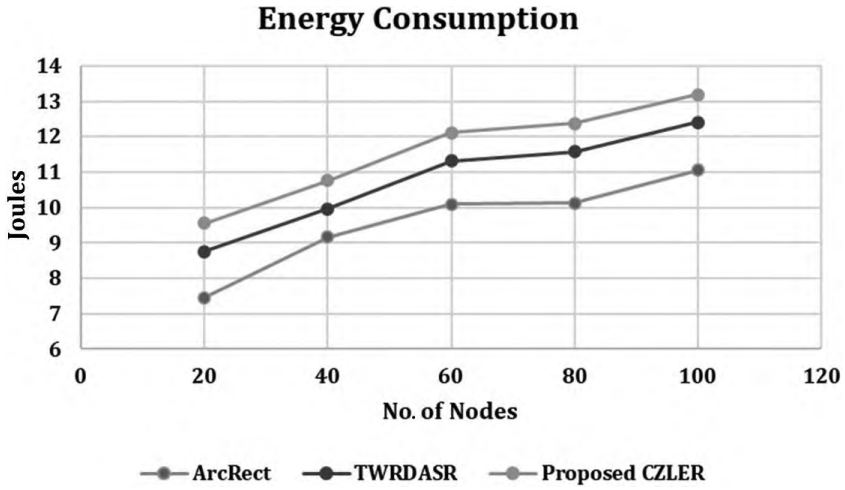

Рисунок 2.12 – Енергетичне споживання

Результати моделювання демонструють переваги протоколу CZLER у порівнянні з ArcRect і TWRDASR. CZLER забезпечує меншу затримку, вищу пропускну здатність, кращий коефіцієнт доставки пакетів і менше енергоспоживання, що робить його ефективним рішенням для використання у реальних сценаріях випадкового розгортання та випадкового розподілу вузлів у контексті закладів охорони здоров'я, торгових зон та спортивних стадіонів. Це також свідчить про перспективи його поширення на медичні сенсори на основі Інтернету речей [22].

2.8 Висновки до розділу 2

Мобільні мережі (MANET) мають ряд унікальних якостей, які відрізняють їх від інших мереж. Основною проблемою у реалізації архітектури протоколу маршрутизації в MANET є те, що ці мережі є портативними і мають багато

специфічних рис, які ускладнюють управління споживанням енергії, використанням ресурсів та доставкою пакетів.

При успішній побудові протоколу маршрутизації в MANET ці труднощі можуть бути подолані. Метою цього дослідження є створення протоколу маршрутизації, який є енергоефективним і зберігає якість обслуговування (QoS). Протокол CZLER (Cross-Layer Energy-efficient Routing) розроблений для подовження терміну служби вузла, зменшення споживання енергії, забезпечення високого коефіцієнта доставки пакетів і низького рівня втрат пакетів. Крім того, цей протокол є економічно ефективним і забезпечує швидкий і безпечний внутрішньовузловий зв'язок.

3 АГРЕГАЦІЯ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

3.1 Методи агрегації даних у мережі

Інтернет речей (IoT) протягом останніх років значно змінив спосіб взаємодії людини з технологіями, підвищуючи якість повсякденного життя. Застосування IoT у таких сферах, як "розумні міста", "розумні будинки" та "розумна охорона здоров'я", демонструє його широкий потенціал. Основою успіху цієї технології є гнучка архітектура, яка включає чотири ключові рівні: зондування, мережевий зв'язок, хмарні обчислення та прикладний рівень. Завдяки цьому IoT інтегрує реальний і віртуальний світи, постійно розширюючи кількість підключених пристроїв (рис. 3.1) [23].

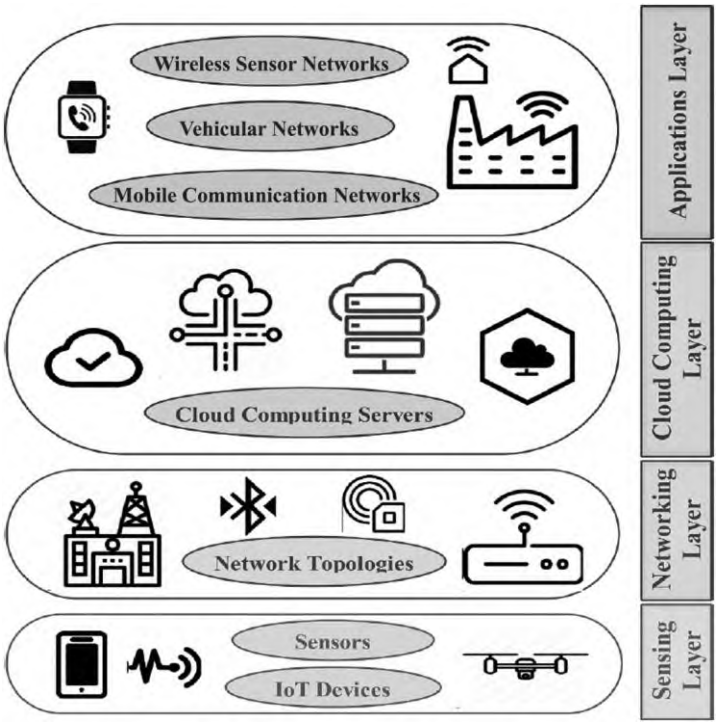

Рисунок 3.1 – Архітектура Інтернету речей

Однак широке впровадження IoT породжує значні виклики, зокрема у сфері енергоефективності. Більшість IoT-пристроїв працюють від батарей, а енергетичні витрати на передачу даних перевищують витрати на обчислення, що

скорочує термін служби пристроїв і знижує загальну ефективність мережі. З огляду на це, зменшення обсягу трафіку даних стає ключовим завданням. Мінімізація трафіку дозволяє економити енергію, збільшуючи тривалість роботи пристроїв, що, в свою чергу, покращує продуктивність систем IoT. Для досягнення цієї мети дослідники активно розробляють нові методи управління енергоспоживанням та оптимізації передачі даних. Це підхід, який відкриває перспективи для сталого розвитку Інтернету речей, забезпечуючи його довгострокову ефективність.

Агрегація даних у системах на основі Інтернету речей (IoT) є важливим механізмом оптимізації, який дозволяє усувати надлишкові дані та об'єднувати інформацію з різних пристроїв у компактний формат. Використовуючи функції агрегації (суму, середнє значення, підрахунок, мінімум, максимум тощо), дані пересилаються як єдиний пакет на проміжний пристрій, базову станцію (БС) або в хмарний центр обробки даних (ЦОД). Це суттєво зменшує обсяг трафіку, покращуючи ефективність мережі [24].

Особливості та переваги агрегації даних:

1. У сценарії без агрегації кожен пристрій передає дані окремо, що створює значне навантаження на мережу. Агрегація дозволяє зменшити кількість передач даних, об’єднуючи їх на проміжних вузлах. Наприклад, у мережі з п’ятьма пристроями кількість передач може скоротитися з 11 до 5 (рис. 3.2).

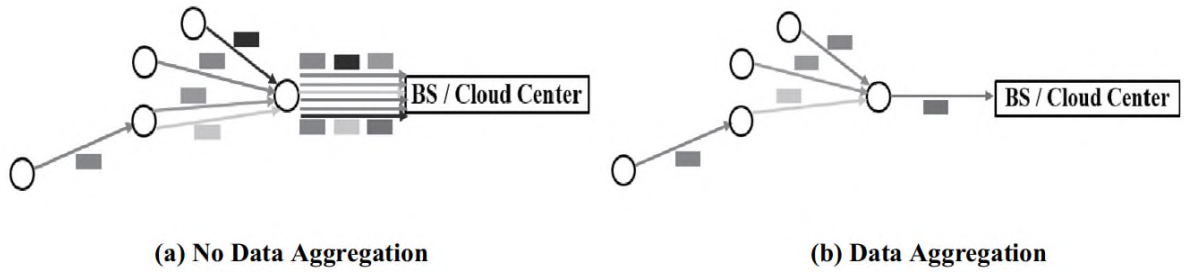

Рисунок 3.2 – Особливості передачі даних в IoT

2. Оскільки передачі даних споживають значно більше енергії, ніж обчислення, агрегація сприяє економії енергії, подовжуючи термін служби батарей IoT-пристроїв.

3. Замість того щоб передавати численні пакети даних, агреговані дані доставляються швидше, що знижує затримку.

4. Агрегація сприяє ефективній роботі великих мереж, дозволяючи інтегрувати більше пристроїв без втрати продуктивності.

5. Ефективніше використання енергії та ресурсів мережі загалом продовжує її термін служби. Виклики агрегації даних:

- Зростання швидкості генерації даних підвищує вартість обробки на проміжних вузлах. Це вимагає балансування між ефективністю та витратами.

- Тип мережі, її топологія, обсяг даних і модель зв’язку впливають на вибір методів агрегації. Агрегація даних є основою внутрішньомережевої обробки в системах IoT, дозволяючи не лише знижувати навантаження, а й підвищувати ефективність. Оптимальні протоколи агрегації орієнтовані на збереження енергії, мінімізацію трафіку та забезпечення точності даних, що робить цей процес ключовим для побудови стійких та ефективних IoT-систем.

У системах на основі Інтернету речей (IoT) оптимізація агрегації даних залежить від кількох ключових аспектів: маршрутизації, планування роботи пристроїв і забезпечення конфіденційності даних. Ці фактори є вирішальними для ефективного зниження трафіку, мінімізації затримок та підтримання безпеки даних.

Протоколи маршрутизації спрямовані на оптимальний вибір шляху передачі даних у мережі IoT. Вони допомагають:

- Мінімізувати трафік даних за рахунок використання енергоефективних маршрутів і об’єднання даних на проміжних вузлах.

- Протоколи обирають шляхи з мінімальними витратами енергії, що дозволяє зменшити навантаження на пристрої та продовжити їхній термін служби.

- У великих мережах маршрутизація допомагає знизити перевантаження трафіку, забезпечуючи стабільну роботу системи.

Сучасні маршрутизуючі протоколи, такі як RPL (Routing Protocol for Low-Power and Lossy Networks), часто інтегрують механізми агрегації, що підвищує їхню ефективність.

Планування роботи IoT-пристроїв спрямоване на оптимізацію часу їхньої активності, щоб мінімізувати затримки агрегації та забезпечити своєчасність отриманих даних:

- Планування дозволяє узгоджувати час передачі даних між вузлами, що сприяє зменшенню затримки.

- Обмеження часу роботи пристроїв у активному режимі знижує енергетичні витрати.

- Планування забезпечує актуальність агрегованої інформації, що важливо для критично залежних від часу застосунків, таких як охорона здоров’я та транспорт.

Забезпечення конфіденційності є ключовим викликом під час агрегації даних, оскільки IoT-системи часто працюють із чутливою інформацією. Методи захисту включають:

- Передачу даних у зашифрованому вигляді запобігає їхньому несанкціонованому доступу.

- Деякі протоколи забезпечують анонімізацію даних, щоб захистити особисту інформацію користувачів.

- Використання блокчейн-технологій для забезпечення цілісності та захисту даних від модифікації.

Провідні експерти розробляють нові моделі та алгоритми, що враховують маршрутизацію, планування та безпеку. Наприклад:

- Протоколи на основі машинного навчання для адаптивної маршрутизації.

- Алгоритми оптимального планування для зниження затримок.

- Методи конфіденційної агрегації, що поєднують шифрування з енергозберігаючими технологіями.

Таким чином, інтеграція маршрутів, планування та забезпечення безпеки під час агрегації даних робить IoT-системи більш стійкими, ефективними та безпечними. Агрегація даних у мережах IoT значною мірою залежить від ефективності використовуваної структури маршрутизації, яка визначає, як дані передаються від сенсорних вузлів до базової станції (БС). Зважаючи на динамічний характер IoT-мереж, де пристрої часто змінюють своє розташування, структура маршрутизації повинна бути адаптивною, енергоефективною та здатною впоратися зі зміною топології. Основні підходи до агрегації даних залежно від структури маршрутизації (рис. 3.3) [25].

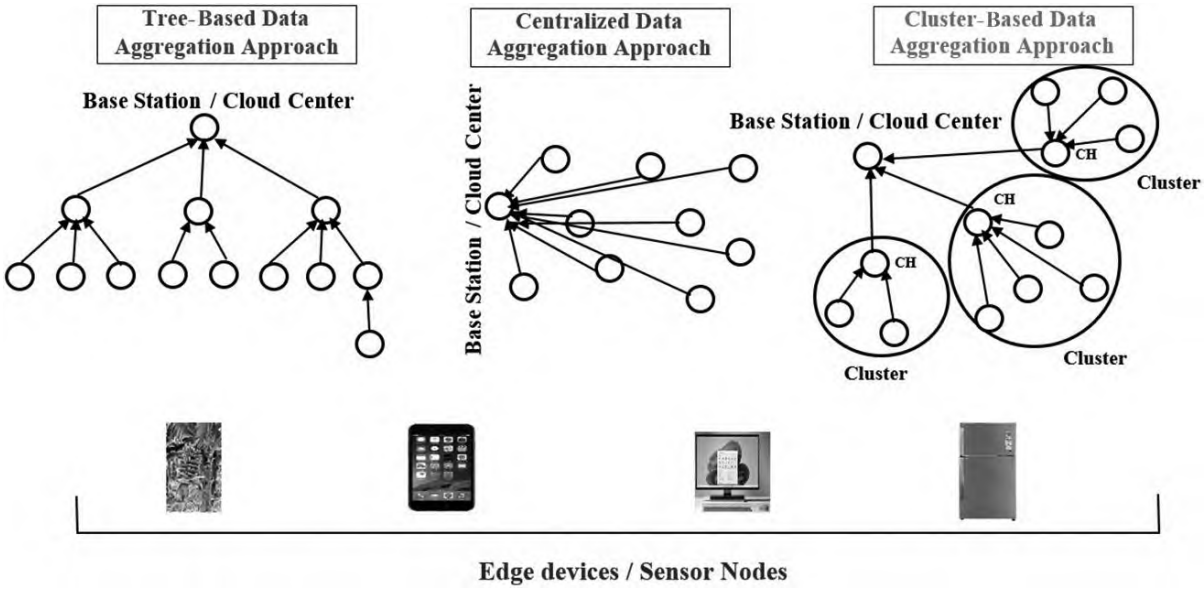

Рисунок 3.3 – Методи маршрутизації та агрегації даних у мережі

У кластерних мережах вузли групуються у кластери, кожен з яких має "головний вузол" (cluster head, CH), відповідальний за збирання, агрегацію та пересилання даних від інших вузлів до БС.

- Переваги:

- Зменшення обсягу трафіку за рахунок локальної обробки даних у межах кластера.

- Енергозбереження завдяки розподіленню навантаження між вузлами.

- Недоліки:

- Балансування енергоспоживання між вузлами CH є викликом.

- Часті зміни топології можуть ускладнювати процес вибору CH.

- Приклад: Протоколи, такі як LEACH (Low-Energy Adaptive Clustering Hierarchy).

У деревовидній структурі вузли організовані у вигляді ієрархічного дерева, де листові вузли передають дані до вузлів вищого рівня (батьківських), які, у свою чергу, агрегують дані та пересилають їх далі.

- Переваги:

- Ефективне використання енергії завдяки ієрархічній передачі даних.

- Мінімізація дублювання даних.

- Недоліки:

- Вразливість до відмов вузлів, що може порушити роботу дерева.

- Часті зміни топології ускладнюють підтримку дерева.

- Приклад:** Протоколи, такі як PEGASIS (Power-Efficient GAthering in Sensor Information Systems).

У централізованих системах дані безпосередньо передаються до центрального вузла або БС, де вони обробляються та агрегуються.

- Переваги:

- Спрощена структура без необхідності локальної обробки на вузлах.

- Підходить для мереж із низькою динамічністю.

- Недоліки:

- Високе енергоспоживання на етапі передачі даних.

- Менша масштабованість для великих мереж.

- Приклад: Системи, що використовують централізовані хмарні обчислення.

Виклики маршрутизації в агрегації даних. Часті зміни в положенні пристроїв ускладнюють підтримку стабільних маршрутів. Низька ємність батарей і обчислювальних ресурсів вузлів вимагає енергоефективних рішень. Необхідно уникати перевантаження окремих вузлів, таких як CH або вузли верхніх рівнів у дереві. Уникнення втрати або спотворення даних під час їх агрегації.

Структури маршрутизації відіграють центральну роль у процесі агрегації даних, впливаючи на енергоспоживання, затримки та продуктивність мережі IoT. Вибір між кластерним, деревовидним та централізованим підходами залежить від характеристик мережі, її масштабів, динамічності та вимог до енергозбереження. Подальші дослідження в цій галузі спрямовані на створення гібридних рішень, які поєднують переваги різних структур маршрутизації [26].

3.2 Агрегація даних з урахуванням затримки сигналів в мережі

Циклічний режим роботи сенсорів є ключовим підходом для зменшення енергоспоживання в мережах IoT, оскільки він дозволяє датчикам переходити в сплячий режим, коли вони не виконують завдань. Водночас використання циклічного режиму створює виклики у вигляді затримки агрегації даних, особливо коли активний період значно коротший за період сну (рис. 3.4) [27].

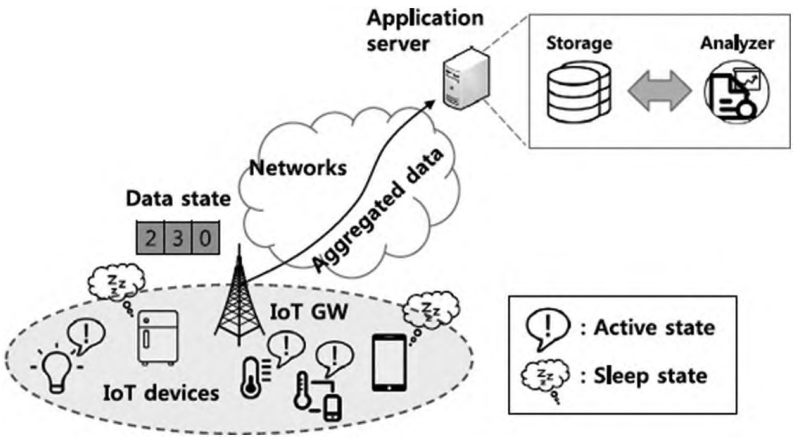

Рисунок 3.4 – Схема агрегації даних за сценарієм циклічності роботи пристроїв

Основні аспекти циклічного режиму роботи та затримки агрегації. Ефективне управління активними слотами:

- Традиційні методи агрегації, такі як "знизу вгору" або "дві фази", не завжди ефективно використовують активні часові слоти сенсорів, що збільшує затримку.

- Запропонований підхід до планування конвеєра поєднує побудову дерева агрегації та розподіл часових інтервалів для передачі даних у межах одного процесу [12].

Методика побудови дерева агрегації:

- Побудова дерева здійснюється шляхом вибору вузлів-відправників із невибраних сенсорів і їхньої прив'язки до вузлів-одержувачів, які вже є частиною дерева.

- Одночасно для кожної пари відправник-одержувач призначається часовий інтервал для передачі даних.

- Це зменшує затримку, оскільки мінімізується кількість циклів, необхідних для завершення агрегації.

Багаторівнева стратегія ранжування:

- Пари вузлів обираються на основі:

- Для забезпечення зваженого вибору вузлів із найкращим потенціалом для агрегації.

- Для мінімізації часу передачі між вузлами.

- Стратегія побудована на аналізі двостороннього графа, де вузли-кандидати розділені на відправників і одержувачів.

Переваги підходу [12]:

- Завдяки паралельному плануванню передачі та побудові дерева.

- Завдяки оптимальному використанню активних слотів сенсорів.

Недоліки та обмеження:

- Для кожного вузла встановлено фіксовану максимальну кількість дочірніх вузлів. Це може зменшити ефективність, особливо в густих мережах.

- У великих мережах підхід може потребувати значних обчислювальних ресурсів для ранжування та планування.

Можливі напрями вдосконалення. Використання адаптивного підходу, де кількість дочірніх вузлів залежить від їхніх ресурсів та топології. Використання алгоритмів для прогнозування часу активності вузлів та оптимізації побудови дерева агрегації. Зменшення залежності від централізованих процесів для

побудови дерева, що дозволить підвищити масштабованість системи. Таким чином, циклічний режим роботи у поєднанні з удосконаленими методами планування та агрегації даних здатний значно покращити енергоефективність IoT-мереж, зберігаючи при цьому низьку затримку передачі даних.

Агрегація даних на канальному рівні є важливим методом оптимізації в мережах IoT, спрямованим на зменшення затримки передачі. У підході, описаному [13], використовується багатоканальне планування та побудова дерева агрегації для підвищення ефективності передачі даних. Розглянемо основні аспекти цієї методики:

1. Побудова дерева агрегації.

- Початковою точкою є вузол-поглинач, який стає коренем дерева.

- Інші вузли додаються поступово, ґрунтуючись на значенні затримки зв’язку. Вузли, що мають найменшу затримку з обраним вузлом, включаються першими.

- Цей процес продовжується до моменту, коли всі вузли стануть частиною дерева агрегації.

2. Призначення часових інтервалів.

- Після завершення побудови дерева часові інтервали розподіляються за принципом «знизу-вгору».

- Листові вузли отримують часові інтервали першими, далі процес піднімається до кореня дерева.

- Використання активних часових інтервалів дозволяє зменшити час простою вузлів і забезпечує ефективне використання доступних ресурсів.

3. Оптимізація розкладу.

- Запропоноване планування враховує невикористані часові інтервали та канали, залишені основним алгоритмом, що дає змогу скоротити довжину розкладу.

- Як наслідок, зменшується затримка агрегації, що є критично важливим для масових IoT-мереж. Переваги підходу.

- Використання багатоканального планування та дерева агрегації дозволяє суттєво зменшити наскрізну затримку.

- Включення невикористаних часових інтервалів і каналів сприяє зменшенню конфліктів і простою.

Попри зменшення затримки, запропонована схема не враховує енергоспоживання вузлів, що є критично важливим для тривалості життя IoT-мереж. Інтеграція енергозберігаючих механізмів є важливим напрямком подальших досліджень. Хоча метод ефективний для невеликих модельних мереж (наприклад, із 12 вузлів), його ефективність у великих, динамічних мережах залишається відкритим питанням (рис. 3.5) [28].

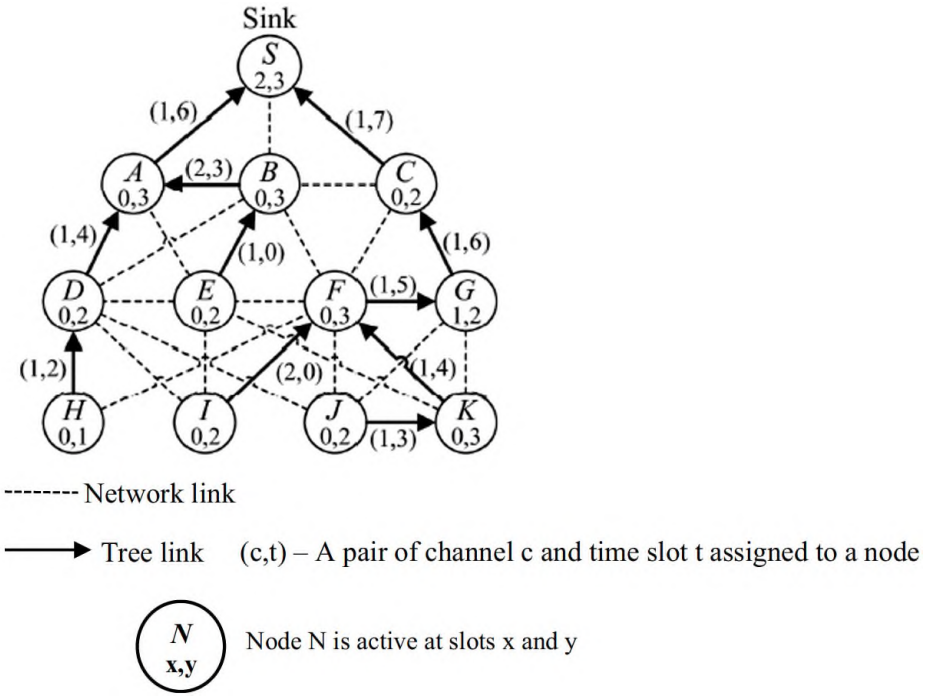

Рисунок 3.5 – Схема агрегації даних на дереві вибірки

У роботі не розглянуто сценарії з різнорідними пристроями, які можуть мати різні вимоги до енергії та затримки. Перспективи подальших досліджень:

- Розробка алгоритмів, які одночасно мінімізують затримку та енергоспоживання.

- Адаптація методики для роботи з гетерогенними пристроями.

- Масштабування підходу на великі мережі з динамічною топологією.

- Інтеграція з механізмами машинного навчання для адаптивного управління ресурсами та прогнозування змін у мережі. Цей підхід демонструє, як ефективне планування може суттєво покращити продуктивність IoT-мереж, але також підкреслює важливість врахування комплексних потреб мережевої інфраструктури.

3.3 Інформаційна безпека агрегації даних в IoT мережі

Агрегація даних в IoT передбачає, що всі пристрої є чесними та надійними. Однак через відкриту природу IoT та бездротове середовище зловмисники можуть здійснювати різні атаки під час агрегації даних. Тому необхідно впроваджувати механізми захисту для забезпечення безпечної агрегації даних.

Одним із основних методів забезпечення безпечної агрегації даних є їх шифрування. Гомоморфні схеми шифрування дозволяють виконувати агрегацію зашифрованих даних, що забезпечує безпечність процесу агрегації. Використовуючи методи шифрування, автентифікації та цифрового підпису, можна досягти конфіденційності та цілісності агрегованих даних.

Безпечна схема агрегації даних, розроблена [14], використовується для агрегації сенсорних даних пристроїв Інтернету речей. Для захисту конфіденційності даних, сенсорні дані, що містять конфіденційну інформацію користувача, шифруються за допомогою гомоморфної схеми шифрування Пайєра. Процес агрегації виглядає наступним чином:

1. Сенсорні дані шифруються за допомогою відкритого ключа криптосистеми Пайєра.

2. Отриманий зашифрований текст додається до цифрового підпису та надсилається на периферійний сервер.

3. Периферійний сервер, що діє як агрегатор, перевіряє підписи всього зашифрованого тексту для забезпечення цілісності даних.

4. Якщо всі підписи дійсні, сервер агрегує зашифрований текст (рис. 3.6).

5. Після агрегації сервер додає підпис до агрегованого шифрованого тексту і надсилає його до центрального контролера (ЦК).

6. ЦК розшифровує агрегований шифротекст, використовуючи приватний ключ криптосистеми Пайєра, для прийняття інтелектуальних рішень [29].

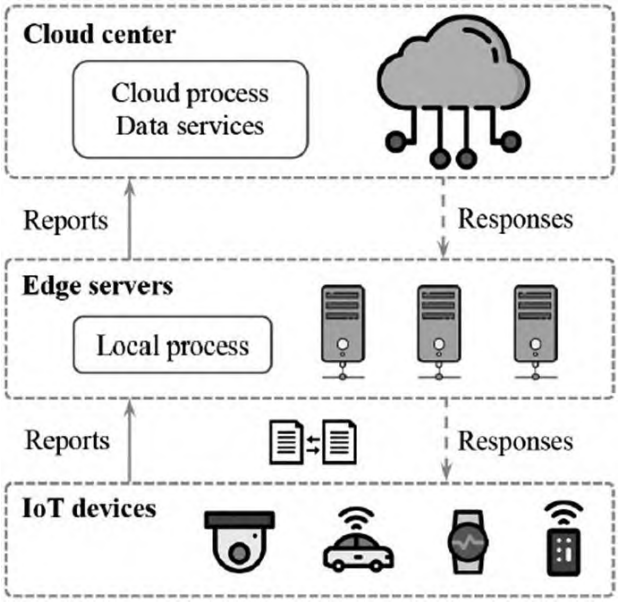

Рисунок 3.6 – Схема агрегації даних зі збереженням конфіденційності

Незважаючи на те, що запропонована схема є легкою, перевіреною та захищеною від атаки обраним повідомленням, вона все ще вразлива до атак змови. Атаки змови можуть бути здійснені, якщо декілька зловмисних вузлів співпрацюють між собою для порушення цілісності даних або розкриття конфіденційної інформації. Для забезпечення безпечної агрегації даних в IoT необхідно використовувати сучасні криптографічні методи, такі як гомоморфне шифрування, автентифікація та цифровий підпис. Однак, навіть перевірені та захищені схеми можуть мати певні вразливості, що вимагає подальших досліджень та вдосконалень для захисту від нових типів атак [15].

Медичні пристрої, підключені до Інтернету речей (IoT), генерують величезні обсяги даних. Зважаючи на обмежені ресурси цих пристроїв, агрегація даних є важливою для збереження їхніх ресурсів. Однак, агрегація даних

супроводжується проблемами безпеки, такими як порушення цілісності та конфіденційності медичних даних [16]. Для вирішення цих проблем пропонується новий механізм, що поєднує криптосистему з відкритим ключем та методи секретного обміну.

Новий механізм безпечної агрегації даних про стан здоров'я, отриманих пристроями IoT, складається з наступних кроків:

1. Підпис даних пацієнтами:

- Пацієнти підписують свої дані про стан здоров'я за допомогою приватних ключів.

- Підписані дані надсилаються до медичних центрів.

- Підпис дозволяє медичним центрам визначати дублікати даних і відповідно нагороджувати пацієнтів.

2. Шифрування та агрегація даних медичними центрами:

- Медичні центри шифрують дані за допомогою криптосистеми Boneh-Goh-Nissim.

- Після цього зашифровані дані агрегуються.

- Перед передачею даних до хмарного центру медичні центри додають шум до агрегованих даних, що запобігає диференціальним атакам.

3. Агрегація даних хмарним центром:

- Хмарний центр отримує агреговані дані від медичних центрів.

- Дані додатково агрегуються та надсилаються кінцевим користувачам для контролю за станом здоров'я громади або наукових досліджень [17].

Багато досліджень щодо безпечної агрегації даних зосереджуються на одновимірних даних. Однак пристрої IoT генерують багатовимірні дані, які також потребують захисту. Схема гомоморфного шифрування на основі китайської теореми про залишок (CRT) (рис. 3.7) [18]:

1. Шифрування даних:

- Багатовимірні дані шифруються за допомогою гомоморфної схеми шифрування на основі CRT.

- До зашифрованого тексту додається підпис.

2. Агрегація даних периферійними центрами:

- Периферійний центр перевіряє всі підписи.

- Якщо підписи дійсні, центр агрегує зашифрований текст та відправляє дані до хмари для подальшого аналізу. Запропоновані методи забезпечують високий рівень безпеки при агрегації медичних даних IoT:

- Конфіденційність та цілісність даних забезпечуються за рахунок використання сучасних криптографічних методів.

- Захист від диференціальних атак досягається шляхом додавання шуму до агрегованих даних.

- Підтримка багатовимірних даних завдяки використанню гомоморфного шифрування на основі CRT.

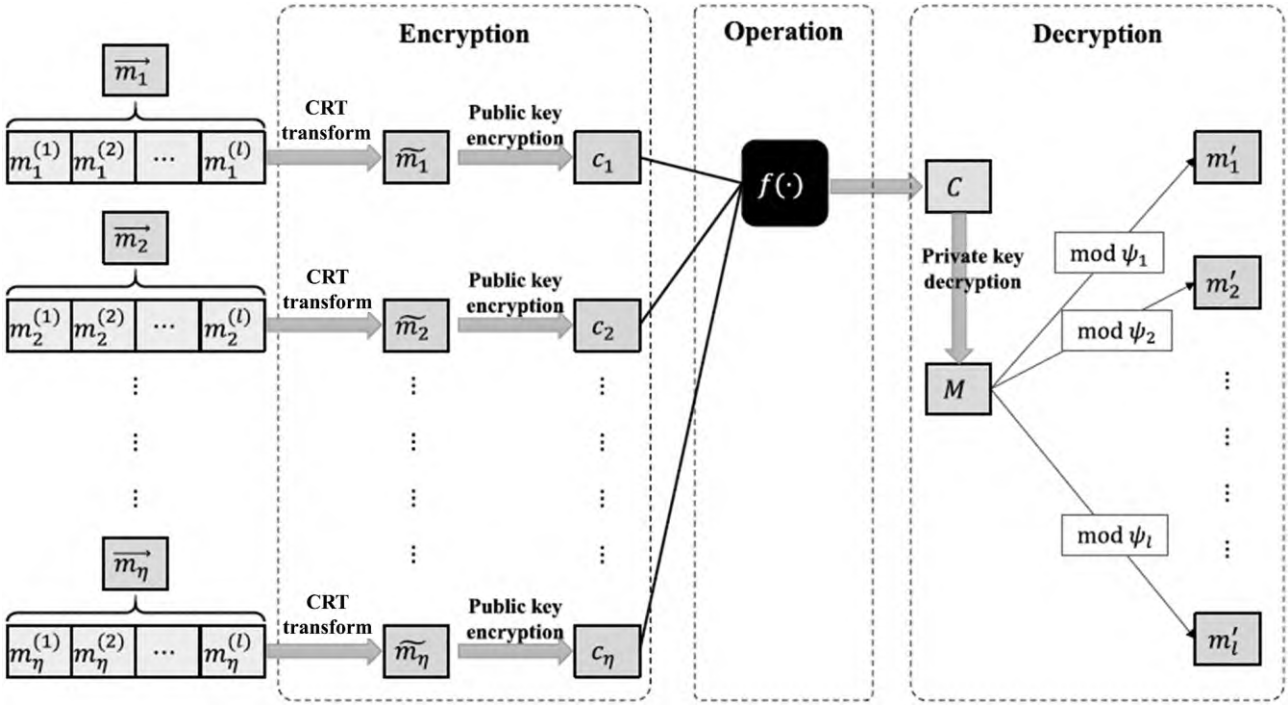

Рисунок 3.7 – Схема багатовимірного агрегування даних

Розглянуті методи забезпечують прийнятний рівень безпеки з точки зору комунікаційних та обчислювальних витрат, що робить їх придатними для використання в реальних сценаріях агрегації медичних даних IoT.

Основна ідея іншої запропонованої моделі полягає в кластеризації вузлів мережі [19]. У цій моделі вузол-поглинач надсилає в систему мультиатрибутивні запити, які передаються до голови кластера, а потім до членів кластерів. Модель використовує гомоморфне шифрування Пайєра для забезпечення безпеки даних. Процес агрегації виглядає наступним чином:

1. Відправка запитів:

- Вузол-поглинач відправляє мультиатрибутивні запити.

- Голови кластерів отримують ці запити та пересилають їх членам кластерів.

2. Шифрування та передача даних: Члени кластера генерують дані, шифрують їх за допомогою гомоморфного шифрування Пайєра та відправляють зашифровані тексти голові кластера.

3. Агрегація даних:

- Голови кластерів отримують зашифровані тексти від усіх членів кластера та агрегують їх, враховуючи кореляцію між кількома атрибутами та припущення про порядок комбінації атрибутів.

- Агрегований шифротекст відправляється вузлу-поглиначу.

4. Розшифрування та відповідь: Вузол-поглинач розшифровує агреговані дані та надсилає відповіді користувачу для прийняття інтелектуальних рішень.

Обмеження моделі. Модель потребує довіреної особи для забезпечення безпеки, що знижує її ефективність. Кількість атрибутів, що можуть бути агреговані, обмежена, що може зменшувати гнучкість системи.

Механізм безпеки [19] спрямований на запобігання підслуховуванню приватних даних під час агрегації. Модель використовує кластерну топологію та шифрування на основі еліптичної кривої. Процес включає наступні етапи:

1. Вибір голови кластера: Голови кластерів (ЦН) обираються залежно від залишкової енергії та відстані між смарт-пристроєм та базовою станцією (БС).

2. Шифрування даних:

- Члени кластера шифрують сенсорні дані за допомогою схеми шифрування еліптичної кривої.

- Генерується гомоморфний код автентифікації повідомлення (MAC), який додається до зашифрованого тексту.

3. Передача даних:

- Зашифрований текст разом з MAC надсилається до голови кластера.

- Центральна станція перевіряє MAC і, якщо він дійсний, агрегує шифротекст своїх дочірніх станцій.

4. Агрегація та розшифрування:

- Агрегований шифротекст надсилається на вузол-поглинач.

- Вузол-поглинач розшифровує агреговані дані для відновлення вихідних даних.

Переваги:

- Висока точність агрегації даних.

- Захист від підслуховування приватних даних завдяки шифруванню та автентифікації.

Недоліки: Високе споживання енергії смарт-пристроями через складність криптографічних обчислень. Різні підходи до безпечної агрегації даних в IoT мають свої переваги та обмеження. Модель на основі парадигми запит-відповідь [20] є залежною від довіреної особи та обмеженою кількістю атрибутів. Механізм безпеки [21] забезпечує високий рівень безпеки та точності, але потребує значних енергетичних витрат. Обидві моделі вимагають подальших досліджень для оптимізації та підвищення ефективності в реальних умовах використання.

3.4 Агрегація даних на основі блокчейну

Для забезпечення надійної і контрольованої взаємодії між пристроями Інтернету речей (IoT), дослідники впровадили технологію блокчейн. Оскільки блокчейн забезпечує захист конфіденційності даних користувачів, його використовують у процесі агрегації даних IoT для захисту цих даних.

На основі технології блокчейн можна захистити процес агрегації даних, як зазначено в дослідженні [22]. Для збереження конфіденційності блокчейн було модифіковано шляхом додавання мітки безпеки у заголовок блоку. Ця мітка безпеки складається з двох частин: рівня безпеки та вимог, які необхідно виконати. Завдяки цій мітці були розроблені нові правила для генерації блоків, які покращують їх обчислювальні можливості. Це, в свою чергу, зменшує затримку і збільшує пропускну здатність процесу агрегації даних. Крім того, для захисту конфіденційності, транзакції та отримувачі транзакцій розбиваються на групи. Для забезпечення енергоефективності маршрути будуються за допомогою методів навчання з глибоким підкріпленням. Хоча ця схема є стійкою до атак типу collusion, вона не є масштабованою з точки зору латентності.

Технологія блокчейн також уникає проблеми єдиної точки довіри під час процесу агрегації даних [23], як показано на рис. 3.8.

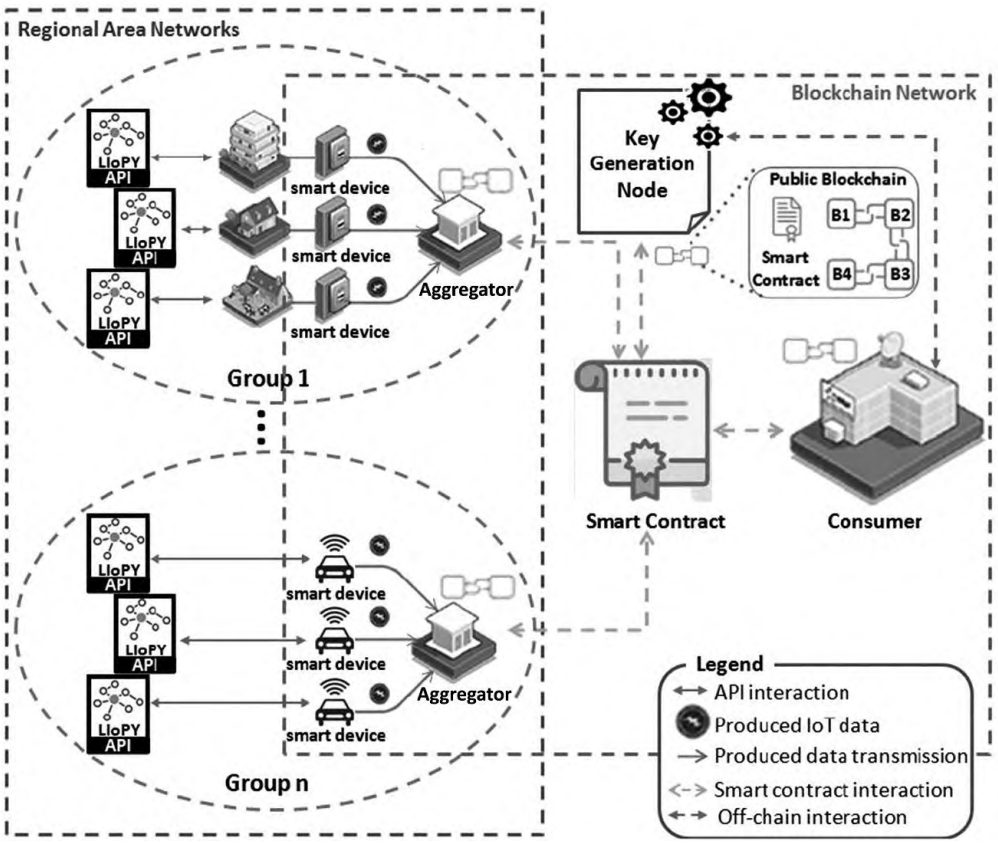

Рисунок 3.8 – Схема агрегації даних на основі блокчейну

Для захисту конфіденційності агрегованих даних блокчейн поєднується з гомоморфним шифруванням. Сирі сенсорні дані шифруються за допомогою гомоморфної схеми шифрування, а потім зберігаються в блокчейні, який діє як розподілене сховище даних і, зрештою, дозволяє уникнути проблеми довіри.

Процес агрегації даних контролюється смарт-контрактами, які приймають запит, групують смарт-пристрої на основі цього запиту для отримання відповіді та публікують результат агрегації. Хоча блокчейн долає проблеми довіри, він пов'язаний з витратами на зберігання даних. Оскільки пристрої Інтернету речей обмежені в ресурсах, використання технології блокчейн обмежує кількість додатків, які можуть виконувати агрегацію даних за допомогою технології блокчейн.

3.5 Висновки до розділу 3

Агрегація даних в Інтернеті речей (IoT) є важливою областю досліджень, яка має потенціал для зниження витрат енергії, підвищення ефективності та забезпечення масштабованості систем IoT. У наведеному тексті виокремлено ключові аспекти, пов’язані з поточним станом і викликами в цій галузі.

У статичних середовищах алгоритми агрегації можуть бути добре оптимізовані, оскільки топологія мережі залишається незмінною. Проте у динамічному середовищі, де вузли можуть переміщуватись, змінювати своє місцезнаходження або з’являтись/зникати, агрегація стає складнішою. Це відкриває питання створення адаптивних алгоритмів, здатних реагувати на ці зміни. У IoT мережах пристрої можуть суттєво відрізнятися за обчислювальною потужністю, енергетичними ресурсами, протоколами зв’язку та типами даних. Більшість існуючих підходів орієнтовані на однорідні мережі, тоді як гетерогенність ускладнює процеси агрегації. Рішення для роботи в таких умовах повинні враховувати сумісність різних пристроїв і стандартів. Для мобільних пристроїв з обмеженими ресурсами критично важливо мінімізувати обчислювальні навантаження. Це включає розробку легких алгоритмів, які

споживають менше процесорного часу та енергії, зберігаючи при цьому ефективність агрегації.

Стандартні методи агрегації здебільшого зосереджені на простих операціях, таких як сума або середнє значення. Для виконання складних операцій, таких як медіана, квантиль, мода або ранжування, потрібні нові підходи, які б не надмірно збільшували обчислювальні та енергетичні витрати. Більшість сучасних методів агрегації покладаються на єдиний вузол-поглинач, який збирає всі дані. Проте в розподілених мережах з кількома поглиначами виникають нові виклики, такі як координація між поглиначами, зменшення дублювання даних та оптимізація маршрутизації. Подолання зазначених викликів вимагає розробки нових алгоритмів, методів моделювання та інструментів. Водночас, інтеграція сучасних технологій, таких як штучний інтелект, машинне навчання та блокчейн, може забезпечити прорив у цій галузі, зокрема в аспектах безпеки та ефективності.

4 ОСОБЛИВОСТІ IOT З МАШИННИМ НАВЧАННЯМ/ГЛИБОКИМ НАВЧАННЯМ

4.1 Архітектура інтелектуального інтернету речей

Інтернет речей (IoT) — це зв'язок між різними пристроями та користувачами. Пристрої збирають дані з різних джерел, обробляють ці дані і надсилають їх на сервер. Центри обробки даних виконують додатковий аналіз, забезпечуючи автоматизацію та дії. Проте існує складна архітектурна структура, яка залежить від різних компонентів і взаємодії між командуванням та виконанням завдань.

Технологія Інтернету речей останнім часом набуває все більшої популярності і має широкий спектр застосувань. Додатки IoT працюють відповідно до свого призначення, залежать від багатьох областей застосування, але не існує стандартів, що визначають архітектуру роботи. Залежно від конкретного бізнес-завдання використовуються різні архітектурні рівні та рівні складності. Найбільш поширеною і прийнятною є чотирирівнева архітектура.

Різні рівні архітектури IoT:

1. Рівень зондування/сприйняття: Перший рівень системи IoT — фізичний рівень, де всі пристрої з'єднані для забезпечення зв'язку між реальним світом і цифровим. Фізичний рівень містить датчики і виконавчі механізми, здатні збирати, приймати і обробляти дані через мережу. Цей рівень називається рівнем сприйняття (рис. 4.1). Для підключення датчиків і виконавчих механізмів можуть використовуватися як дротові, так і бездротові з'єднання. Радіус дії та місце розташування компонентів не обмежуються конструкцією.

2. Системний рівень: Датчики збирають дані у реальному часі на сенсорному рівні, які передаються на системний рівень. На цьому рівні знаходяться мережеві шлюзи та системи збору даних (DAS). DAS відповідає за агрегування даних, які збирає сенсорний рівень. Він вимірює, збирає, упорядковує та агрегує дані з датчиків, а потім перетворює ці аналогові дані у

цифрові. Системний рівень забезпечує зв'язок між цими пристроями та серверами, хмарними і мережевими пристроями, контролюючи передачу даних кожним пристроєм.

3. Рівень уточнення: Рівень уточнення працює подібно до обробного рівня людського мозку. Дані перед передачею в центр обробки даних оцінюються, попередньо обробляються (видаляються зашумлені дані), аналізуються і зберігаються. Подальші дії виконуються за допомогою програмних додатків, які обробляють і готують дані. Це здійснюється за допомогою периферійної аналітики або периферійних ІТ.

4. Прикладний рівень: Прикладний рівень забезпечує користувальницький інтерфейс рішень IoT, корисний для адміністраторів для управління пристроями IoT і створення нових правил для операцій IoT. Приклади включають інформаційну панель, яка відображає стан гаджетів у системі, або додаток для розумного будинку, де користувачі можуть увімкнути кавоварку, натиснувши кнопку в додатку. Існує багато способів використання Інтернету речей [30].

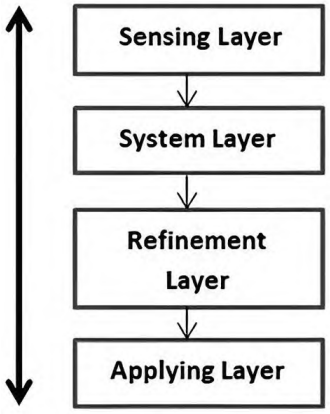

Рисунок 4.1 – Рівні архітектури Інтернету речей

Таким чином, чотирирівнева архітектура IoT забезпечує всебічний підхід до збору, обробки, аналізу та використання даних, забезпечуючи ефективність та гнучкість систем IoT у різних сферах застосування [24].

4.2 Моделювання поведінки та аналіз IoT за допомогою глибокого навчання

Ідентифікація зображень та інтерпретація часових рядів для додатків Інтернету речей (IoT) широко використовують методи глибокого навчання, такі як нейронні мережі, згорткові нейронні мережі (CNN), навчання з підкріпленням і довготривала пам'ять (LSTM) [25]. Наприклад, сучасні системи допомоги водієві та автономні транспортні засоби використовують ці методи для реалізації функцій, таких як попередження про зіткнення, моніторинг сліпих зон, допомога водієві, забезпечення безпеки руху, управління інфраструктурою та контролювання переповненості (рис. 4.2).

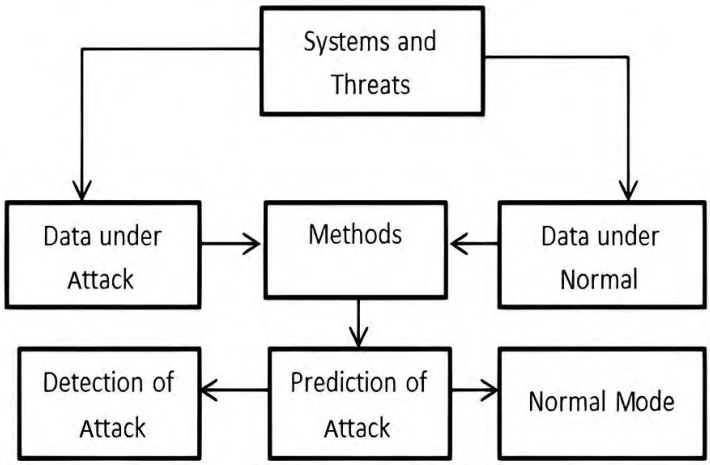

Рисунок 4.2 – Методи DL в IoT

За допомогою автомобільних систем зв'язку, таких як спеціалізовані системи зв'язку короткого радіусу дії (DSRC), VANET, довгострокові розробки і мобільні мережі п'ятого покоління (5G), автономні транспортні засоби можуть співпрацювати один з одним. Вони обмінюються виявленою інформацією, такою як дорожні знаки, події зіткнення і так далі, що дозволяє створювати більш безпечні та ефективні транспортні системи. Методи глибокого навчання в IoT використовуються не тільки в автомобільній індустрії, але і в багатьох інших

галузях, забезпечуючи високу точність і ефективність при обробці великих обсягів даних та прийнятті рішень на їх основі. Наведемо кілька прикладів застосування методів глибокого навчання в IoT [26]:

1. Ідентифікація зображень:

- Аналіз зображень для моніторингу стану врожаю, виявлення хвороб рослин і оцінки родючості ґрунту.

- Виявлення та розпізнавання осіб для систем контролю доступу та моніторингу громадських місць.

- Аналіз медичних зображень для діагностики захворювань, таких як рак, і моніторинг стану пацієнтів.

2. Інтерпретація часових рядів:

- Прогнозування споживання енергії та управління розподілом ресурсів.

- Аналіз фінансових даних для прогнозування ринкових тенденцій та управління ризиками.

- Моніторинг життєвих показників пацієнтів для виявлення аномалій і своєчасного надання медичної допомоги. Завдяки цим методам глибокого навчання IoT-системи стають більш інтелектуальними і здатними до самоорганізації, що сприяє покращенню якості життя та підвищенню ефективності в різних сферах.

Глибинне навчання (DL) значно сприяло розвитку сучасного штучного інтелекту (AI). Воно знаходить широке застосування в багатьох прикладних дисциплінах, таких як робототехніка, комп'ютерний зір та розпізнавання мови. У порівнянні з традиційними методами машинного навчання (ML), DL має кілька важливих переваг (рис. 4.3).

Переваги глибинного навчання:

1. DL використовує численні приховані шари в структурі нейронної мережі, що дозволяє витримувати складні нелінійні зв'язки між атрибутами.

2. Популярні топології, такі як згорткові нейронні мережі (CNN) і мережі з довготривалою пам'яттю (LSTM), здатні витягувати та ідентифікувати відповідні ознаки безпосередньо з необроблених даних, замість залежності від вручну

побудованих статистичних характеристик, як у традиційному ML (наприклад, автоматичні кодувальники).

3. DL особливо ефективне для вирішення проблем, пов'язаних з великими обсягами даних, що робить його дуже важливим у сучасних додатках.

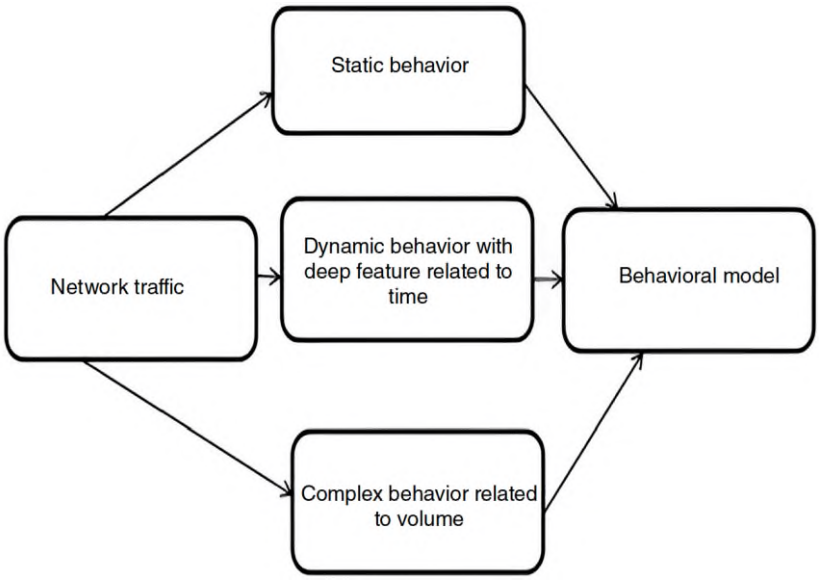

Рисунок 4.3 – Аналіз IoT за допомогою глибинного навчання

IoT застосовується в багатьох галузях, включаючи:

- Розумну енергетику
- Розумні будинки
- Індустрію 4.0
- Охорону здоров'я.

Переваги та виклики IoT:

- Підвищена гнучкість та мобільність
- Вища продуктивність та ефективність
- Проблеми конфіденційності даних
- Проблеми безпеки
- Інтероперабельність

Мережі IoT є ситуативними за своєю природою, і управління IoT зараз стикається з істотними проблемами в області безпеки і конфіденційності (рис.

4.2). Сучасні дослідження показали, що алгоритми DL є досить ефективними і мають численні переваги в порівнянні з попередніми підходами для оцінки безпеки пристроїв IoT [27].

Алгоритми глибинного навчання можуть використовуватися для:

- Виявлення аномалій у поведінці пристроїв IoT, що може вказувати на злом чи неправомірні дії.

- Аналізу мережевого трафіку, щоб ідентифікувати потенційні загрози або несанкціоновані доступи.

- Автоматичного оновлення моделей безпеки у відповідь на нові загрози, що виникають у середовищі IoT. Завдяки цим можливостям, DL допомагає підвищити рівень безпеки і конфіденційності в середовищах IoT, що стає критично важливим з огляду на зростаючу кількість підключених пристроїв та обсяги оброблюваних даних.

4.3 Аналіз інформаційної безпеки IoT

Завдяки підключенню до Інтернету, IoT поєднує фізичні об'єкти та їхнє середовище, що відкриває нові можливості, але водночас і нові загрози. Більшу частину часу гаджети працюють у небажаному і небезпечному інтернет-середовищі. Як наслідок, хакери та зловмисники можуть використовувати слабкі місця Інтернету речей (рис. 4.4), щоб розголошувати персональні дані та паролі з датчиків. Загрози можна розділити на дві категорії: пасивні та активні [28].

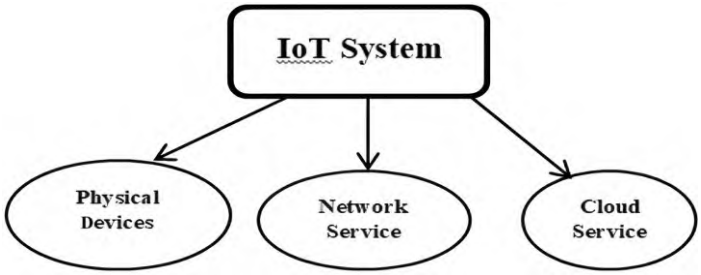

Рисунок 4.4 – Аналіз IoT за допомогою глибинного навчання

Пасивні загрози намагаються отримати доступ до даних та інформації системи без втручання в її ресурси. Прикладом пасивної загрози є підслуховування, де зловмисник просто отримує доступ до передаваних даних, але не змінює їх. Активні загрози виникають, коли зловмисник або хакер намагається змінити інформацію або заволодіти апаратним забезпеченням. До активних загроз належать:

- Sybil атаки: Зловмисник створює кілька фальшивих ідентичностей для отримання неправомірного контролю над мережею.

- Розподілена відмова в обслуговуванні (DDoS): Атака, що призводить до недоступності сервісу шляхом перевантаження його численними запитами.

- Відмова в обслуговуванні (DoS): Атака, яка призводить до недоступності сервісу шляхом відправки надмірної кількості запитів до системи.

- Трояни: Шкідливе програмне забезпечення, яке маскується під легітимні програми для отримання несанкціонованого доступу до системи.

- Спуфінг: Підробка ідентичності для обману системи та отримання доступу до конфіденційної інформації.

- Фішинг: Спосіб обману користувачів для отримання їх конфіденційних даних, таких як паролі.

- Смішинг: Фішинг через SMS-повідомлення.

Потенційні атаки на безпеку, які можуть вплинути на вимоги до безпеки, включають:

- Авторизація: Незаконне отримання прав доступу.

- Автентифікація: Підробка ідентичності для отримання доступу.

- Конфіденційність: Неправомірний доступ до конфіденційної інформації.

- Доступність: Перешкоджання доступу до послуг.

- Цілісність: Зміна або знищення даних.

- Квазі: Порушення часової послідовності або затримки в обробці даних.

Для захисту пристроїв IoT від зазначених загроз необхідні комплексні заходи безпеки:

- Шифрування даних: Захист даних під час передачі та зберігання.

- Механізми автентифікації: Використання надійних методів автентифікації для перевірки користувачів та пристроїв.

- Контроль доступу: Забезпечення доступу тільки авторизованим користувачам та пристроям.

- Моніторинг та аудит: Постійний моніторинг мережі та аудит безпекових подій.

- Оновлення програмного забезпечення: Регулярне оновлення програмного забезпечення для виправлення вразливостей. Завдяки цим заходам можна значно зменшити ризики та підвищити рівень безпеки систем IoT, що стає критично важливим у сучасному цифровому світі [29].

4.4 Ієрархічна схема підвищення інформаційної безпеки в системах інтернету речей

Архітектура MufHAS (Multi-Factor Hierarchical Authentication Scheme) представляє собою багаторівневу ієрархічну схему аутентифікації, розроблену для забезпечення високого рівня безпеки в системах Інтернету речей (IoT). Ця архітектура орієнтована на подолання проблем конфіденційності та безпеки, які виникають в середовищах IoT, де численні пристрої взаємодіють один з одним і з користувачами через інтернет.

Основні компоненти архітектури MufHAS:

1. Сенсорний рівень (Perception Layer) складається з різноманітних датчиків і виконавчих механізмів, які безпосередньо збирають дані з фізичного світу. Пристрої цього рівня можуть включати в себе різні типи сенсорів, такі як температурні датчики, датчики вологості, камери, мікрофони тощо. Для забезпечення аутентифікації на цьому рівні можуть використовуватися легкі криптографічні алгоритми, що враховують обмежені обчислювальні ресурси пристроїв.

2. На мережевому рівні (Network Layer) дані, зібрані сенсорами, передаються до центральних вузлів для подальшої обробки. Це включає в себе

різні мережеві протоколи і технології, такі як Wi-Fi, Bluetooth, Zigbee, LoRaWAN тощо. Для забезпечення безпеки на цьому рівні використовуються методи шифрування даних під час передачі, а також аутентифікація вузлів мережі.

3. Рівень обробки (Processing Layer) відповідає за агрегування, фільтрацію та попередню обробку даних, отриманих з сенсорів. Тут дані можуть бути збережені, проаналізовані та передані на вищі рівні для подальшої обробки. Для аутентифікації на цьому рівні можуть використовуватися більш потужні методи криптографії, зважаючи на наявність більших обчислювальних ресурсів.

4. На прикладному рівні (Application Layer) користувачі взаємодіють з системою через різні додатки та сервіси. Це можуть бути веб-додатки, мобільні додатки, аналітичні платформи тощо. Аутентифікація на цьому рівні може включати багатофакторні методи, такі як поєднання паролів, біометричних даних, одноразових паролів (OTP) тощо.

Основні функції та характеристики MufHAS:

- MufHAS використовує кілька рівнів аутентифікації для забезпечення безпеки на кожному етапі взаємодії пристроїв IoT. Це включає в себе використання різних методів аутентифікації на різних рівнях архітектури.

- Архітектура організована у вигляді ієрархії, що дозволяє ефективно управляти аутентифікацією та забезпечувати безпеку на різних рівнях системи.

- Завдяки використанню багатофакторної аутентифікації та різних методів шифрування, MufHAS забезпечує високий рівень захисту від різноманітних атак, таких як підслуховування, спуфінг, DDoS тощо.

- Архітектура MufHAS враховує обмежені обчислювальні ресурси пристроїв IoT та оптимізує процес аутентифікації для забезпечення високої продуктивності системи. Архітектура MufHAS є ефективним рішенням для забезпечення безпеки в системах IoT, поєднуючи багаторівневу аутентифікацію та ієрархічну структуру. Вона забезпечує захист конфіденційності даних, автентифікацію користувачів та пристроїв, а також захист від різноманітних загроз, що робить її важливим елементом сучасних систем IoT [30].

Автоматизація, зокрема домашня автоматизація, стає все більш важливою як у повсякденному житті, так і в світовій економіці. Завдяки поєднанню автоматизованого обладнання з числовими та організаційними інструментами інженери створюють складні системи, що відповідають зростаючому різноманіттю застосувань і людської діяльності.

Сучасні системи домашньої автоматизації спрямовані на зняття відповідальності за управління електроприладами з кінцевих користувачів, надаючи мешканцям ефективні, практичні та безпечні засоби для управління їхніми домівками. Незалежно від змін в очікуваннях користувачів або розвитку технологій, існуючі системи автоматизації, такі як мікроконтролери та платформи на базі Raspberry Pi, продовжують забезпечувати передачу даних і управління.

Одним з основних викликів у домашній автоматизації є висока вартість будівництва та налаштування систем для вже існуючих будівель. Незважаючи на це, сучасні технології значно спрощують процес автоматизації та підключення пристроїв.

1. Автоматизація будівель за допомогою програмної платформи IoS: Ці системи використовують програмні платформи для інтеграції та управління різними пристроями в будинку, забезпечуючи централізований контроль і управління.

2. Система домашньої автоматизації на основі смартфона: Смартфони дозволяють користувачам контролювати різні аспекти свого будинку через спеціальні додатки, забезпечуючи зручність та доступність управління.

3. Система підключеного будинку на основі Zigbee: Zigbee є протоколом для бездротового підключення, що забезпечує низьку потужність та високу ефективність передачі даних між пристроями в "розумному" будинку (рис. 4.5).

4. Система підключеного будинку на основі локальної мережі: Використання локальних мереж для підключення та управління пристроями дозволяє забезпечити високу швидкість передачі даних та надійність системи.

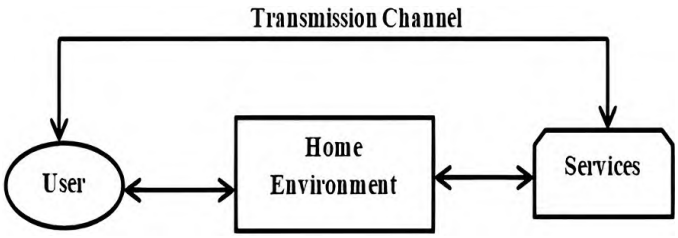

Рисунок 4.5 – Архітектура MufHAS

Автоматизація, зокрема в домашньому середовищі, значно вплинула на те, як люди взаємодіють зі своїми домівками. З розвитком технологій та впровадженням нових рішень, таких як програмні платформи IoS, системи на основі смартфонів, Zigbee та локальних мереж, автоматизація стає ще більш доступною та ефективною, забезпечуючи комфорт, безпеку та зручність для користувачів [31].

4.5 Архітектура запропонованої сенсорної системи

Використання Інтернету речей (IoT) має значний потенціал для покращення якості життя, особливо в бідних країнах, де технологічні інновації можуть сприяти підвищенню ефективності, безпеки та економічного розвитку. Розумні будинки, які є частиною цієї концепції, забезпечують можливість інтеграції різних пристроїв і технологій, спрямованих на автоматизацію процесів і полегшення життя.

Основні особливості розумних будинків:

- Керування побутовими пристроями (освітленням, опаленням, безпекою) за допомогою датчиків і програмованих алгоритмів.

- Контроль через смартфони або ноутбуки, підключені до Інтернету.

- Моніторинг активності в будинку, використовуючи мережеві рішення, що реагують на потенційні загрози.

Локальні мережі, які об'єднують пристрої IoT, можуть бути основою для впровадження розумних будинків. Вони сприяють:

- Ефективному управлінню процесами.

- Розподілу завдань між підсистемами (наприклад, мережі транспортних засобів).

- Зберіганню та обробці даних на серверах, які виконують функції домашніх шлюзів для координації пристроїв.

Запропонований підхід проектування мереж домашньої автоматизації об'єднує IoE і сучасні мережеві технології, щоб забезпечити вирішення конкретних завдань, таких як економія енергії, моніторинг здоров'я мешканців або управління домашніми ресурсами (рис. 4.6).

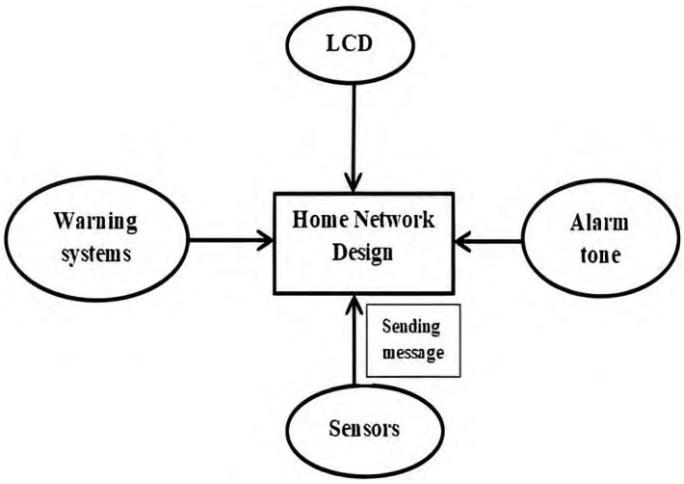

Рисунок 4.6 – Архітектура запропонованої системи

У країнах з низьким рівнем доходу такі технології можуть:

- Підвищити доступність базових послуг (вода, електроенергія) через ефективне управління ресурсами.

- Забезпечити нові можливості для освіти та зайнятості завдяки навчанню використанню IoT-технологій.

- Зменшити витрати на комунальні послуги завдяки енергоощадним рішенням.

Розвиток IoT у цьому напрямі має не лише економічний, але й соціальний вплив, підвищуючи якість життя та відкриваючи нові можливості для самореалізації.

Домашня автоматизація в сучасних умовах забезпечує значно більше, ніж просто безпека. Вона надає користувачам широкий набір інструментів для управління та оптимізації домашніх процесів [32].

Основні функції домашньої автоматизації

1. Програмована безпека:

- Системи попередження з використанням звукових сигналів, рідкокристалічних дисплеїв та текстових сповіщень.

- Інформування авторизованих користувачів про загрози безпеці.

- Використання інтегрованих сенсорів для швидкого реагування на потенційні ризики.

2. Домашня комп'ютеризація:

- Управління побутовою технікою та іншими пристроями через ПК або мікроконтролери.

- Ефективність, безпека та прибутковість завдяки автоматизації.

3. oT та IoE:

- IoT (Інтернет речей): Фокус на підключених пристроях, які збирають дані та виконують завдання автоматично.

- IoE (Інтернет усього): Включає не лише пристрої, але й людей і процеси для створення інтегрованих рішень.

Інтеграція технологій у розумному будинку [33].

1. Датчики та зв'язок:

- Датчики забезпечують моніторинг ключових параметрів: температура, рух, відкриття дверей тощо.

- Бездротові з'єднання через протоколи DHCP для побутової техніки, що дозволяє легко розширювати мережу.

- Дротові з'єднання використовуються для серверів, ПК та маршрутизаторів, які потребують стабільного зв'язку.

2. Програмне забезпечення Cisco Packet Tracer Simulator: Моделювання роботи розумного будинку, включаючи налаштування маршрутизаторів, серверів та підключення IoE-пристроїв.

3. Міжмашинна комунікація (M2M): Автоматизація обміну даними між пристроями для виконання завдань без втручання людини.

Переваги розумного будинку.

- Відстеження загроз, швидке реагування.

- Зменшення витрат енергії завдяки оптимізації роботи побутових пристроїв.

- Віддалений доступ до управління будинком через смартфони чи ПК.

- Можливість додавання нових пристроїв та функцій без порушення основної інфраструктури.

Реалізація концепції розумного будинку потребує інвестицій у розробку технологій, навчання користувачів та забезпечення кібербезпеки. Проте її впровадження має потенціал значно покращити якість життя, особливо у великих містах і регіонах з високим рівнем урбанізації. Розвиток розумних приладів дійсно є однією з найбільш динамічних сфер технологій. У контексті описаних напрямків варто уточнити деякі деталі [33]: Різні виробники використовують власні стандарти та протоколи, що ускладнює їхнє об'єднання в одну екосистему. Універсальні стандарти, такі як Matter (підтримується Google, Apple, Amazon тощо), можуть змінити ситуацію, забезпечуючи сумісність між різними екосистемами. Фокус на протоколах передачі даних, які працюють з мінімальними затримками та високим рівнем захисту. Вже зараз пристрої, такі як голосові помічники (наприклад, Alexa, Google Assistant), адаптуються до користувачів. Використання передбачувальної аналітики для автоматизації завдань. Наприклад, системи "розумного дому" можуть автоматично налаштовувати освітлення чи температуру на основі часу дня або поведінки користувача. Розробка розумних термостатів (Nest, Tado), енергомоніторів та сенсорів, що знижують споживання енергії. Алгоритми машинного навчання

для оптимізації енергоспоживання без втрати зручності. Зростання кількості підключених пристроїв збільшує ймовірність кіберзагроз. Рішення:

- Децентралізовані методи зберігання даних (наприклад, блокчейн).

- Інноваційні методи аутентифікації, такі як біометрія чи токенізація даних.

- Розробка систем захисту в реальному часі, які можуть виявляти аномальні дії.

Штучний інтелект. Можливості:

- Інтелектуальні рекомендації на основі аналізу великих даних.

- Розширені можливості голосового управління, що включають контекстуальне розуміння.

- Виявлення потенційних проблем (наприклад, поломок) у пристроях за допомогою діагностичних алгоритмів.

- Виклики: Забезпечення точності рішень при збереженні швидкодії та енергоефективності алгоритмів. Усі ці напрями взаємопов'язані. Наприклад, розробка інтероперабельних рішень може полегшити персоналізацію, а безпечні платформи дозволять користувачам більш активно впроваджувати нові пристрої у свої повсякденні життя. Реалізація цих ідей буде залежати від колаборації між компаніями, науковцями та регуляторами [34].

4.6 Висновки до розділу 4

Зазначені перспективи безпеки в розумних приладах відображають важливість збалансування між інноваціями та захистом конфіденційності й даних користувачів. Зокрема: Сучасні алгоритми шифрування (AES, RSA, ECC) використовуються для захисту даних, які передаються між пристроями та платформами. Протоколи на зразок HTTPS, MQTT з TLS забезпечують безпечну передачу даних. Інтеграція додаткових рівнів перевірки користувачів, таких як біометрія або одноразові паролі (OTP). Смарт-пристрої повинні мати функції автоматичного оновлення для закриття вразливостей у системі без необхідності ручного втручання користувачів. Використання технологій

штучного інтелекту для виявлення нових типів атак в реальному часі. Компанії можуть впроваджувати програми винагороди за виявлення вразливостей, що стимулює етичних хакерів працювати на благо.

Існує потреба в глобальних стандартах (ISO/IEC 27001, NIST), які охоплюватимуть питання безпеки IoT-пристроїв. Введення чітких регуляцій для виробників, які нестимуть відповідальність за безпеку своїх продуктів.

Користувачів необхідно навчати, як правильно використовувати смарт-пристрої, захищати свої дані та виявляти потенційні загрози. З огляду на майбутнє квантових обчислень, індустрія починає досліджувати методи захисту, які витримають атаки таких систем. Використання децентралізованих систем для зберігання та передачі даних, які забезпечують прозорість і надійність.

Загалом, захист розумних приладів – це безперервний процес, який вимагає участі виробників, споживачів та регуляторів. Впровадження цих підходів дозволить зберегти довіру користувачів до новітніх технологій та забезпечити їх безпечну інтеграцію в повсякденне життя.

5 ЕКОНОМІЧНА ЧАСТИНА

Виконання науково-дослідної роботи завжди передбачає отримання певних результатів і вимагає відповідних витрат. Результати виконаної роботи завжди дають нам нові знання, які в подальшому можуть бути використані для удосконалення та/або розробки (побудови) нових, більш продуктивних зразків техніки, процесів та програмного забезпечення.

Дослідження на тему «Інтелектуальна сенсорна мережа Інтернету речей» може бути віднесено до фундаментальних і пошукових наукових досліджень і спрямоване на вирішення наукових проблем, пов’язаних з практичним застосуванням. Основою таких досліджень є науковий ефект, який виражається в отриманні наукових результатів, які збільшують обсяг знань про природу, техніку та суспільство, які розвивають теоретичну базу в тому чи іншому науковому напрямку, що дозволяє виявити нові закономірності, які можуть використовуватися на практиці.

Для цього випадку виконаємо такі етапи робіт:

1) здійснимо проведення наукового аудиту досліджень, тобто встановлення їх наукового рівня та значимості;

2) проведемо планування витрат на проведення наукових досліджень;

3) здійснимо розрахунок рівня важливості наукового дослідження та перспективності, визначимо ефективність наукових досліджень.

5.1 Оцінювання наукового ефекту

Основними ознаками наукового ефекту науково-дослідної роботи є новизна роботи, рівень її теоретичного опрацювання, перспективність, рівень розповсюдження результатів, можливість реалізації. Науковий ефект НДР на тему «Інтелектуальна сенсорна мережа Інтернету речей» можна охарактеризувати двома показниками: ступенем наукової новизни та рівнем теоретичного опрацювання.

Значення показників ступеня новизни і рівня теоретичного опрацювання науково-дослідної роботи в балах наведені в табл. 5.1 та 5.2.

Таблиця 5.1 – Показники ступеня новизни науково-дослідної роботи виставлені експертами

Ступінь новизни	Характеристика ступеня новизни	Значення ступеня новизни, бали		
		Експерти (ПІБ, посада)		
		1	2	3
Принципово нова	Робота якісно нова за постановкою задачі і ґрунтується на застосуванні оригінальних методів дослідження. Результати дослідження відкривають новий напрям в даній галузі науки і техніки. Отримані принципово нові факти, закономірності; розроблена нова теорія. Створено принципово новий пристрій, спосіб, метод	0	0	0
Нова	Отримана нова інформація, яка суттєво зменшує невизначеність наявних значень (по-новому або вперше пояснені відомі факти, закономірності, впроваджені нові поняття, розкрита структура змісту). Проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів	60	58	60
Відносно нова	Робота має елементи новизни в постановці задачі і методах дослідження. Результати дослідження систематизують і узагальнюють наявну інформацію, визначають шляхи подальших досліджень; вперше знайдено зв’язок (або знайдено новий зв’язок) між явищами. В принципі відомі положення розповсюджені на велику кількість об’єктів, в результаті чого знайдено ефективне рішення. Розроблені більш прості способи для досягнення відомих результатів. Проведена часткова раціональна модифікація (з ознаками новизни)	0	0	0
Традиційна	Робота виконана за традиційною методикою. Результати дослідження мають інформаційний характер. Підтверджені або поставлені під сумнів відомі факти та твердження, які потребують перевірки. Знайдено новий варіант рішення, який не дає суттєвих переваг в порівнянні з існуючим	0	0	0
Не нова	Отримано результат, який раніше зафіксований в інформаційному полі, та не був відомий авторам	0	0	0
Середнє значення балів експертів		59,3		

Згідно отриманого середнього значення балів експертів ступінь новизни характеризується як нова, тобто отримана нова інформація, яка суттєво зменшує невизначеність наявних знань (по-новому або вперше пояснені відомі факти, закономірності, впроваджені нові поняття, розкрита структура змісту) та проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів.

Таблиця 5.2 – Показники рівня теоретичного опрацювання науково-дослідної роботи виставлені експертами

Характеристика рівня теоретичного опрацювання	Значення показника рівня теоретичного опрацювання, бали		
	Експерт (ПІБ, посада)		
	1	2	3
Відкриття закону, розробка теорії	0	0	0
Глибоке опрацювання проблеми: багатоаспектний аналіз зв'язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу	70	72	70
Розробка способу (алгоритму, програми), пристрою, отримання нової речовини	0	0	0
Елементарний аналіз зв'язків між фактами та наявною гіпотезою, класифікація, практичні рекомендації для окремого випадку тощо	0	0	0
Опис окремих елементарних фактів, викладення досвіду, результатів спостережень, вимірювань тощо	0	0	0
Середнє значення балів експертів	70,7		

Згідно отриманого середнього значення балів експертів рівень теоретичного опрацювання науково-дослідної роботи характеризується як глибоке опрацювання проблеми: багатоаспектний аналіз зв'язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу.

Показник, який характеризує рівень наукового ефекту, визначаємо за формулою [35]:

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор}, \quad (5.1)$$

де $k_{нов}, k_{теор}$ - показники ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи, $k_{нов} = 59,3, k_{теор} = 70,7$ балів;

0,6 та 0,4 – питома вага (значимість) показників ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи.

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор} = 0,6 \cdot 59,3 + 0,4 \cdot 70,67 = 63,87 \text{ балів.}$$

Визначення характеристики показника $E_{нау}$ проводиться на основі висновків експертів виходячи з граничних значень, які наведені в табл. 5.3.

Таблиця 5.3 – Граничні значення показника наукового ефекту

Досягнутий рівень показника	Кількість балів
Високий	70…100
Середній	50…69
Достатній	15…49
Низький (помилкові дослідження)	1…14

Відповідно до визначеного рівня наукового ефекту проведеної науково-дослідної роботи на тему «Інтелектуальна сенсорна мережа Інтернету речей», даний рівень становить 63,87 балів і відповідає статусу - середній рівень. Тобто у даному випадку можна вести мову про потенційну фактичну ефективність науково-дослідної роботи.

5.2 Розрахунок витрат на здійснення науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи на тему «Інтелектуальна сенсорна мережа Інтернету речей», під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

5.2.1 Витрати на оплату праці

До статті «Витрати на оплату праці» належать витрати на виплату основної та додаткової заробітної плати керівникам відділів, лабораторій, секторів і груп, науковим, інженерно-технічним працівникам, конструкторам, технологам, креслярам, копіювальникам, лаборантам, робітникам, студентам, аспірантам та іншим працівникам, безпосередньо зайнятим виконанням конкретної теми, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці.

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою [35]:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \qquad (5.2)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дн.;

T_p – середнє число робочих днів в місяці, T_p=21 дні.

$$З_о = 18200{,}00 \cdot 7 / 21 = 5409{,}11 \; грн.$$

Проведені розрахунки зведемо до таблиці.

Таблиця 5.4 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник науково-дослідної роботи	18200,00	772,73	7	5409,11
Старший науковий співробітник (фахівець дослідник телекомуні-каційних мереж)	17860,00	750,00	21	15750,00
Технік	8100,00	681,82	3	2045,46
Всього				23204,57

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Інтелектуальна сенсорна мережа Інтернету речей» розраховуємо за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i , \qquad (5.3)$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}}, \qquad (5.4)$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо $Мм$=8000,00 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. Б.2, додаток Б) [35];

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об'єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

T_p – середнє число робочих днів в місяці, приблизно T_p = 21 дн;

$t_{зм}$ – тривалість зміни, год.

$C_1 = 8000{,}00 \cdot 1{,}35 \cdot 1{,}15 / (21 \cdot 8) = 73{,}93$ *грн.*

$З_{р1} = 73{,}93 \cdot 8{,}00 = 591{,}43$ *грн.*

Таблиця 5.5 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Встановлення дослідного обладнання	8,00	3	1,35	73,93	591,43
Інсталяція програмного забезпечення	6,80	5	1,70	93,10	633,05
Компіляція програмних моделей елементів сенсорної мережі	9,00	5	1,70	93,10	837,86
Формування бази даних цифрового експерименту	13,00	3	1,35	73,93	961,07
Всього					3023,40

Додаткова заробітна плата дослідників та робітників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (5.5)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 10%.

$З_{дод}$ = (23204,57 + 3023,40) · 10 / 100% = 2622,80 грн.

5.2.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (5.6)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

Зн = (23204,57 + 3023,40 + 2622,80) · 22 / 100% = 6347,17 грн.

5.2.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за темою «Інтелектуальна сенсорна мережа Інтернету речей».

Витрати на матеріали на даному етапі проведення досліджень в основному пов’язані з використанням моделей елементів та моделювання роботи і досліджень за допомогою комп’ютерної техніки та створення

експериментальних математичних моделей або програмного забезпечення, тому дані витрати формуються на основі витратних матеріалів характерних для офісних робіт.

Витрати на матеріали (*М*), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$M = \sum_{j=1}^{n} H_j \cdot Ц_j \cdot К_j - \sum_{j=1}^{n} B_j \cdot Ц_{вj}, \qquad (5.7)$$

де H_j – норма витрат матеріалу *j*-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу *j*-го найменування, грн/кг;

$К_j$ – коефіцієнт транспортних витрат, ($К_j = 1,1 \ldots 1,15$);

B_j – маса відходів *j*-го найменування, кг;

$Ц_{вj}$ – вартість відходів *j*-го найменування, грн/кг.

$М_1 = 3,0 \cdot 210,00 \cdot 1,12 - 0 \cdot 0 = 705,60$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 5.6 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, грн	Норма витрат, кг	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Папір офісний А4 білий (500, 80%, 80 г/м)	210,00	3,0	0	0	705,60
Диск оптичний (CD-R)	27,50	4,0	0	0	123,20
Органайзер офісний ЕКО-81ВІС	185,00	3,0	0	0	621,60
Канцелярське приладдя	155,00	3,0	0	0	520,80

продовження таблиці 5.6 - Витрати на матеріали

Картридж змінний EPSON STYLUS	1025,00	1,0	0	0	1148,00
USB-FLASH-пам’ять 64 Gb	219,00	1,0	0	0	245,28
Папір для заміток А5 (65 г/м)	111,00	6,0	0	0	745,92
Тека для паперів	85,00	4,0	0	0	380,80
Всього					4491,20

5.2.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему «Інтелектуальна сенсорна мережа Інтернету речей», розраховуємо, згідно з їхньою номенклатурою, за формулою:

$$К_в = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j \qquad (5.8)$$

де $Н_j$ – кількість комплектуючих *j*-го виду, шт.;

$Ц_j$ – покупна ціна комплектуючих *j*-го виду, грн;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ *= 1,1 … 1,15*).

$К_в = 1 \cdot 3810,00 \cdot 1,12 = 4267,20$ грн.

Проведені розрахунки зведемо до таблиці.

Таблиця 5.7 – Витрати на комплектуючі

Найменування комплектуючих	Кількість, шт.	Ціна за штуку, грн	Сума, грн
Комплект блоків АЦП сигналу	1	3810,00	4267,20
Інше	1	500,00	560,00
Всього			4827,20

5.2.5 Спецустаткування для наукових (експериментальних) робіт

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування необхідного для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування, монтаж та встановлення.

Балансову вартість спецустаткування розраховуємо за формулою:

$$B_{спец} = \sum_{i=1}^{k} Ц_i \cdot C_{пр.i} \cdot K_i \ , \qquad (5.9)$$

де $Ц_i$ – ціна придбання одиниці спецустаткування даного виду, марки, грн;

$C_{пр.i}$ –кількість одиниць устаткування відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує доставку, монтаж, налагодження устаткування тощо, ($K_i = 1,10…1,12$);

k – кількість найменувань устаткування.

$B_{спец} = 10599,00 \cdot 1 \cdot 1,12 = 11870,88$ *грн.*

Отримані результати зведемо до таблиці:

Таблиця 5.8 – Витрати на придбання спецустаткування по кожному виду

Найменування устаткування	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Блок інтерфейсний	1	10599,00	11870,88
Імітатор передавача сигналу (програмований)	1	6259,00	7010,08
Імітатор приймача сигналу (програмований)	1	4380,00	4905,60
Всього			23786,56

5.2.6 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та придбання спеціальних програмних засобів і програмного забезпечення, (програм, алгоритмів, баз даних) необхідних для проведення досліджень, також витрати на їх проектування, формування та встановлення.

Балансову вартість програмного забезпечення розраховуємо за формулою:

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \ , \qquad (5.10)$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу даного виду, грн;

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, ($K_i = 1,10…1,12$);

k – кількість найменувань програмних засобів.

$B_{прг} = 9020,00 \cdot 1 \cdot 1,1 = 9922,00$ грн.

Отримані результати зведемо до таблиці:

Таблиця 5.9 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Прикладний пакет моделювання процесів MatLab	1	9020,00	9922,00
Пакет Quartus II	1	6380,00	7018,00
Всього			16940,00

5.2.7 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \quad (5.11)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$A_{обл} = (45299{,}00 \cdot 1) / (3 \cdot 12) = 1258{,}31$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 5.10 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Обчислювальний центр та комп'ютеризована система проектування	45299,00	3	1	1258,31
Вимірювальний комплекс	27266,00	3	1	757,39
Всього				3717,52

Продовження таблиці 5.10 - Амортизаційні відрахування по кожному виду обладнання

Комплект офісного програмного забезпечення (Microsoft Offise 2019)	9640,00	3	1	267,78
Лабораторія досліджень	400000,00	25	1	1333,33
Робоче місце дослідника	8460,00	7	1	100,71
Офісна оргтехніка	0,00	30	1	0,00
Всього				3717,52

5.2.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \quad (5.12)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо Ц$_e$ = 10,98 грн;

$K_{вni}$ – коефіцієнт, що враховує використання потужності, $K_{вni} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$B_e = 0,32 \cdot 160,0 \cdot 10,98 \cdot 0,95 / 0,97 = 562,18$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 5.11 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Обчислювальний центр та комп'ютеризована система проектування	0,32	160,0	562,18
Вимірювальний комплекс	0,03	80,0	26,35
Імітатори передавача/приймача сигналу (програмований)	0,12	80,0	105,41
Робоче місце дослідника	0,10	160,0	175,68
Офісна оргтехніка	0,40	3,0	13,18
Всього			882,79

5.2.9 Службові відрядження

До статті «Службові відрядження» дослідної роботи на тему «Інтелектуальна сенсорна мережа Інтернету речей» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов'язані з проведенням випробувань машин та приладів, а також витрати на відрядження на наукові з'їзди, конференції, наради, пов'язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» відсутні.

5.2.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» відсутні.

5.2.11 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (5.13)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 60%.

$I_в$ = (23204,57 + 3023,40) · 60 / 100% = 15736,78 грн.

5.2.12 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов’язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов’язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$В_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (5.14)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 100%.

$$В_{нзв} = (23204,57 + 3023,40) \cdot 100 / 100\% = 26227,97 \text{ грн.}$$

Витрати на проведення науково-дослідної роботи на тему «Інтелектуальна сенсорна мережа Інтернету речей» розраховуємо як суму всіх попередніх статей витрат за формулою:

$$В_{заг} = З_{о} + З_{р} + З_{дод} + З_{н} + М + К_{в} + В_{спец} + В_{прг} + А_{обл} + В_{е} + В_{св} + В_{сп} + І_{в} + В_{нзв}. \quad (5.15)$$

$$В_{заг} = 23204,57 + 3023,40 + 2622,80 + 6347,17 + 4491,20 + 4827,20 + 23786,56 + 16940,00 + 3717,52 + 882,79 + 0,00 + 0,00 + 15736,78 + 26227,97 = 131807,97 \text{ грн.}$$

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{В_{заг}}{\eta}, \quad (5.16)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,95.

$$ЗВ = 131807,97 / 0,95 = 138745,24 \text{ грн.}$$

5.3 Оцінювання важливості та наукової значимості науково-дослідної роботи

Оцінювання та доведення ефективності виконання науково-дослідної роботи фундаментального чи пошукового характеру є достатньо складним процесом і часто базується на експертних оцінках, тому має вірогідний характер.

Для обґрунтування доцільності виконання науково-дослідної роботи на тему «Інтелектуальна сенсорна мережа Інтернету речей» використовується спеціальний комплексний показник, що враховує важливість, результативність роботи, можливість впровадження її результатів у виробництво, величину витрат на роботу.

Комплексний показник K_P рівня науково-дослідної роботи може бути розрахований за формулою:

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t}, \tag{5.17}$$

де I – коефіцієнт важливості роботи. Приймемо $I = 3$;

n – коефіцієнт використання результатів роботи; $n = 0$, коли результати роботи не будуть використовуватись; $n = 1$, коли результати роботи будуть використовуватись частково; $n = 2$, коли результати роботи будуть використовуватись в дослідно-конструкторських розробках; $n = 3$, коли результати можуть використовуватись навіть без проведення дослідно-конструкторських розробок. Приймемо $n=2$;

T_C – коефіцієнт складності роботи. Приймемо $T_C = 2$;

R – коефіцієнт результативності роботи; якщо результати роботи плануються вище відомих, то $R = 4$; якщо результати роботи відповідають відомому рівню, то $R = 3$; якщо нижче відомих результатів, то $R = 1$. Приймемо $R = 4$;

B – вартість науково-дослідної роботи, тис. грн. Приймемо B =138745,24 грн;

t – час проведення дослідження. Приймемо t = 0,08 років, (1 міс.).

Визначення показників I, n, T_C, R, B, t здійснюється експертним шляхом або на основі нормативів [35].

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t} = 3^2 \cdot 2 \cdot 4 \,/\, 138{,}7 \cdot 0{,}08 = 6{,}23.$$

Якщо $K_P > 1$, то науково-дослідну роботу на тему «Інтелектуальна сенсорна мережа Інтернету речей» можна вважати ефективною з високим науковим, технічним і економічним рівнем.

5.4 Висновок до розділу 5

Витрати на проведення науково-дослідної роботи на тему «Інтелектуальна сенсорна мережа Інтернету речей» складають 138745,24 грн. Відповідно до проведеного аналізу та розрахунків рівень наукового ефекту проведеної науково-дослідної роботи на тему «Інтелектуальна сенсорна мережа Інтернету речей» є середній, а дослідження актуальними, рівень доцільності виконання науково-дослідної роботи $K_P > 1$, що свідчить про потенційну ефективність з високим науковим, технічним і економічним рівнем.

ВИСНОВКИ

У магістерській кваліфікаційній роботі досліджені методи забезпечують високий рівень продуктивності, енергоефективності, надійності передачі даних і безпеки функціонування інтелектуальних сенсорних мереж IoT. Це дозволяє ефективно реагувати на сучасні виклики цифровізації, сприяючи розвитку інноваційних рішень для смарт-технологій, індустрії 4.0 та інфраструктури "розумних" міст.

Основні результати магістерської роботи та випливаючі з них теоретичні та практичні висновки можуть бути сформульовані таким чином:

У першому розділі досліджено методи оптимізації споживання енергії у безпровідних сенсорних мережах. Встановлено, що використання методів управління живленням вузлів, розробка енергоефективних протоколів MAC-рівня та динамічне налаштування радіочастот дозволяють суттєво збільшити час роботи мережі. Визначено, що кластеризація та чергування режимів роботи вузлів є ключовими підходами для зниження енергоспоживання.

Аналіз у другому розділі підтвердив, що використання інтелектуальних алгоритмів маршрутизації для мобільних Ad-hoc мереж і сенсорних мереж IoT покращує якість зв’язку і забезпечує мінімізацію затримок. Застосування децентралізованих методів маршрутизації та алгоритмів, що враховують енергетичні обмеження, дозволяє збалансувати завантаження вузлів і підвищити надійність передачі даних.

Третій розділ присвячений розробці методів зменшення обсягу переданих даних шляхом використання внутрішньомережевої агрегації. Застосування компресії, об’єднання схожих даних та фільтрації на рівні вузлів дозволило оптимізувати обмін інформацією в мережі. Це зменшило витрати енергії на передачу та підвищило ефективність роботи IoT-систем.

У четвертому розділі встановлено, що інтеграція машинного та глибинного навчання у IoT відкриває нові можливості для автоматизації процесів. Використання ML/DL для аналізу даних у реальному часі,

прогнозування збоїв та адаптивного управління ресурсами дозволяє підвищити продуктивність IoT-систем. Особливу увагу приділено технікам розподіленого навчання для збереження конфіденційності даних.

У п’ятому розділі виконано економічну оцінку реалізації досліджуваних технологій. Доведено, що впровадження розроблених рішень сприяє зниженню експлуатаційних витрат, забезпечує масштабованість мереж та створює потенціал для впровадження комерційних IoT-рішень. Виявлено доцільність інвестицій у впровадження енергоефективних технологій для підвищення економічної ефективності.

Дослідження продемонструвало перспективність розробки та впровадження інтелектуальних сенсорних мереж IoT. Застосування енергоефективних методів, оптимізованої маршрутизації, технологій агрегації даних та інтеграція ML/DL дозволяють забезпечити надійну, економічну та масштабовану роботу таких систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Roberts, MK, P Ramasamy 2023, An improved high performance clustering based routing protocol for wireless sensor networks in IoT. Telecommun Syst, vol. 82, pp. 45–59. https://doi.org/10.1007/s11235- 022- 00968- 1

2. Технології інтернету речей. Навчальний посібник [Електронний ресурс]: навч. посіб. Для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані. – Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с.

3. Jiao, Xianlong, Wei Lou, Songtao Guo, Yong Li, Junmei Yao, Fuqiang Gu, and Junchao Ma. “Energy-a ware concurrent data aggregation scheduling for wire-less powered IoT leveraging hypergraph theory.” IEEE Wireless Communications Letters 10, no. 11 (2021a): 2464–2468.

4. Jiao, Xianlong, Wei Lou, Songtao Guo, Ning Wang, Chao Chen, and Kai Liu. “Hypergraph- based active minimum delay data aggregation scheduling in wireless-powered IoT.” IEEE Internet of Things Journal 9, no. 11 (2021b): 8786–8799.

5. Khan, Ab Rouf, and Mohammad Ahsan Chishti. “βDSC 2 DAM: beta-dominating set centered Cluster-B ased Data Aggregation mechanism for the Internet of Things.” Journal of Ambient Intelligence and Humanized Computing 13 (2022): 4279–4296.

6. Liu, X., X. Wang, K. Yu, X. Yang, W. Ma, G. Li, and X. Zhao. “Secure data aggrega-tion aided by privacy preserving in Internet of Things.” Wireless Communications and Mobile Computing 2022 (2022): 1–14.

7. Невлюдов І.Ш. Технології Інтернету речей в управлінні пристроями на мікроконтролерах: Навчальний посібник [Електронний ресурс] / І.Ш. Невлюдов, В.А. Андрусевич, С.П. Новоселов, О.Г. Резніченко. – Електронне видання. –Харків: ХНУРЕ, 2023. – 214 с.

8. Mohseni, Milad, Fatemeh Amirghafouri, and Behrouz Pourghebleh. “CEDAR: A cluster-b ased energy-a ware data aggregation routing protocol in the

internet of things using capuchin search algorithm and fuzzy logic.” Peer- to- Peer Networking and Applications (2022): 1–21.

9. Nguyen, Tien-D ung, Duc-T ai Le, and Hyunseung Choo. “Sensory data aggrega-tion in Internet of Things: Period-d riven pipeline scheduling approach.” IEEE Transactions on Mobile Computing 21, no. 9 (2021): 3326–3341.

10. Peng, Cong, Min Luo, Huaqun Wang, Muhammad Khurram Khan, and Debiao He. “An efficient privacy-p reserving aggregation scheme for multidimensional data in IoT.” IEEE Internet of Things Journal 9, no. 1 (2021): 589–600.

11. Vo, Van-V i, Tien-D ung Nguyen, Duc-T ai Le, Moonseong Kim, and Hyunseung Choo. “Link-d elay-a ware reinforcement scheduling for data aggregation in mas-sive IoT.” IEEE Transactions on Communications 70, no. 8 (2022): 5353–5367.

12. Wang, Xiaoding, Sahil Garg, Hui Lin, Georges Kaddoum, Jia Hu, and M. Shamim Hossain. “A secure data aggregation strategy in edge computing and blockchain-empowered Internet of Things.” IEEE Internet of Things Journal 9, no. 16 (2020): 14237–14246.

13. Невлюдов І.Ш. Технологія програмування промислових контролерів в інтегрованому середовищі CODESYS: Навчальний посібник/ І.Ш. Невлюдов, С.П. Новоселов, О.В. Сичова. –Харків: ХНУРЕ, 2019 . –286с.

14. Zhang, Jiale, Yanchao Zhao, Jie Wu, and Bing Chen. “LVPDA: A lightweight and verifiable privacy-p reserving data aggregation scheme for edge-e nabled IoT.” IEEE Internet of Things Journal 7, no. 5 (2020): 4016–4027.

15. Salil S. Kanhere, Sherali Zeadally, Mehmet A. Orgun. 2021. Machine Learning Techniques for IoT Security: A Comprehensive Survey. IEEE Communications Surveys & Tutorials, 15, 9231–9253.

16. Muhammad Usama, Sheraz Ahmed, Khaled Salah. 2021. Intrusion Detection Systems for IoT: A Comprehensive Survey. IEEE Communications Surveys & Tutorials, 15, 8845–8872.

17. Tong Li, Jiawei Chen, Guanbo Bao. 2020. Machine Learning for Security and Privacy in the Internet of Things: A Survey. IEEE Internet of Things Journal, 13, 287–312.

18. V. Dankan Gowda, S. B. Sridhara, K. B. Naveen, M. Ramesha, G. Naveena Pai. 2020. Internet of Things: Internet Revolution, Impact, Technology Road Map and Features. Advances in Mathematics: Scientific Journal, 9(7), 4405–4414 ISSN:1857- 8365.

19. Технології створення інтернету речей. Комп'ютерний практикум/ Жураковський Б. Ю., Федорова Н. В., Гаврилко Є. В., Зенів І. О. ; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 127 с.

20. Сторчак К.П. Технології Інтернет речей. Навчальний посібник / К.П. Сторчак, А.М. Тушич, І.М. Срібна, Н.Д. Яковенко, Д.В. Кравець. – К.: ДУТ, 2021. – 68 с.

21. Fatima Hussain, Rasheed Hussain, Syed Ali Hassan, Ekram Hossain. 2020. Machine Learning in IoT Security: Current Solutions and Future Challenges. IEEE Communications Surveys & Tutorials, 22(3), 386–410.

22. Naercio Magaia, Ramon Fonseca, Khan Muhammad, Afonso H. Fontes N. Segundo, Aloísio Vieira Lira Neto, Victor Hugo C. De Albuquerque. April 15, 2021. Industrial Internet-o f-T hings Security Enhanced With Deep Learning Approaches for Smart Cities. IEEE Internet of Things Journal, 8(8), 119–132.

23. Hao Lin, Wenwen Zhang, Ruikai Miao. 2020. Deep Learning for IoT, Big Data and Streaming Analytics: A Survey. IEEE Communications Surveys & Tutorials, 16, 982–1015.

24. Mohammed Ali Al-G aradi, Amr Mohamed, Abdulla Khalid Al-A li, Xiaojiang Du, Ihsan Ali, Mohsen Guizani. 2020. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. IEEE Communications Surveys & Tutorials, 22(3), 652–683.

25. Олещенко Л. М. Хіцко Я. В. Програмування пристроїв Інтернету речей: лабораторний практикум: навчальний посібник для студентів

спеціальності 121 «Інженерія програмного забезпечення». Київ : КПІ ім. Ігоря Сікорського, 2019. 47 с.

26. Yiwen Zhang, Youhuizi Li, Mingkui Wei, Jianxin Li, Laurence T. Yang, Albert Y. Zomaya. 2020. Edge Computing: A Survey on Recent Developments and Future Directions. ACM Computing Surveys, 11, 8852–8873.

27. 8. Васильківський, М., Прикмета, А., Олійник, А., & Нікітович, Д. (2023). Оптимізація інтелектуальних телекомунікаційних мереж. Вісник Хмельницького національного університету, Технічні науки. – 2023. – № 1. (317). – С. 33–41. doi: 10.31891/2307-5732-2023-317-1-33-41

28. Khan Muhammad, Afonso H. Fontes N. Segundo, Aloísio Vieira Lira Neto, Victor Hugo C. de Albuquerque. April 15, 2021. Industrial Internet-o f-T hings Security Enhanced With Deep Learning Approaches for Smart Cities. IEEE Internet of Things Journal, 8(8), 95–114.

29. М. Васильківський, О. Болдирева, Г. Варгатюк, і М. Будаш, «Керування телекомунікаційними мережами з використанням технологій AI/ML», ВОТТП, вип. 1, с. 89–100, Бер 2023. doi: 10.31891/2219-9365-2023-73-1-13

30. М. Васильківський, Д. Нікітович, О. Болдирева, Н. Якубівська. «Інтелектуальні технології коригування фізичного рівня мобільних мереж», КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ: ОСВІТА, НАУКА, ВИРОБНИЦТВО, (51), 148-160. https://doi.org/10.36910/6775-2524-0560-2023-51-19

31. М. Васильківський, Д. Нікітович, Н. Грабчак, і Н. Якубівська, «Оптимізація адаптивних радіосистем із використанням алгоритмів ШІ та МН», ВОТТП, вип. 2, с. 112–124, Чер 2023. doi.org/10.31891/2219-9365-2023-74-15

32. K. Jothimani, N. Gowsalya, S. Logeshwaran, E. Monika, M. Vinothini et al. 2022. A Deep Learning Approach For LSTM Based Covid-1 9 Forecasting System. Journal of Science Technology and Research (JSTAR), 3(1), 568–583.

33. K. Jothimani, S. Thangamani, K. Ushmansherif, P. Manojkumar, S. Gowrishankar. 2022. Artificial Intelligent Based Computational Model For Detecting

Chronic-K idney Disease. Journal of Science Technology and Research (JSTAR), 3(1), 723–735.

34. Васильківський, М., Прикмета, А., Олійник, А. і Ксьондз, Н. 2023. Оптимізація програмно-конфігурованих літаючих мереж доступу. КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ: ОСВІТА, НАУКА, ВИРОБНИЦТВО. 52 (Вер 2023), 128-139. DOI:https://doi.org/10.36910/6775-2524-0560-2023-52-16.

35. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

Додаток А

(обов’язковий)

ІЛЮСТРАТИВНА ЧАСТИНА

ІНТЕЛЕКТУАЛЬНА СЕНСОРНА МЕРЕЖА ІНТЕРНЕТУ РЕЧЕЙ

назва магістерської кваліфікаційної роботи

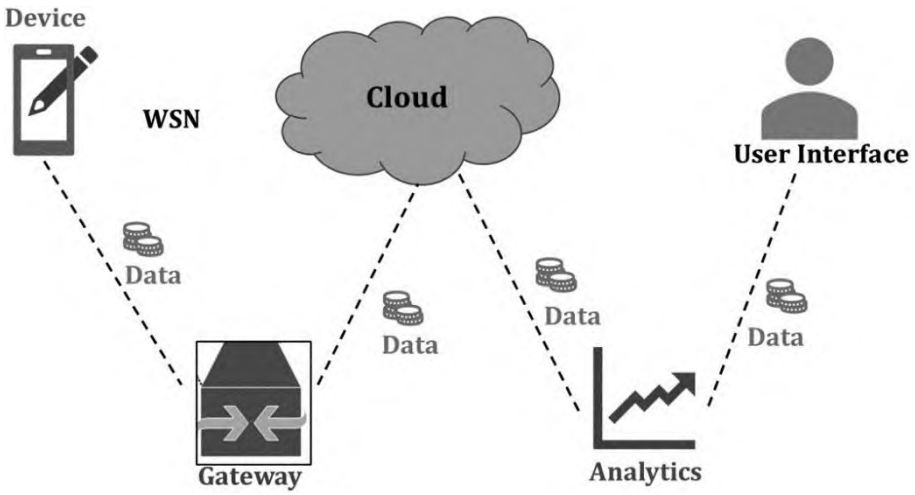

Рисунок 1 – Структура системи Інтернету речей у WSN

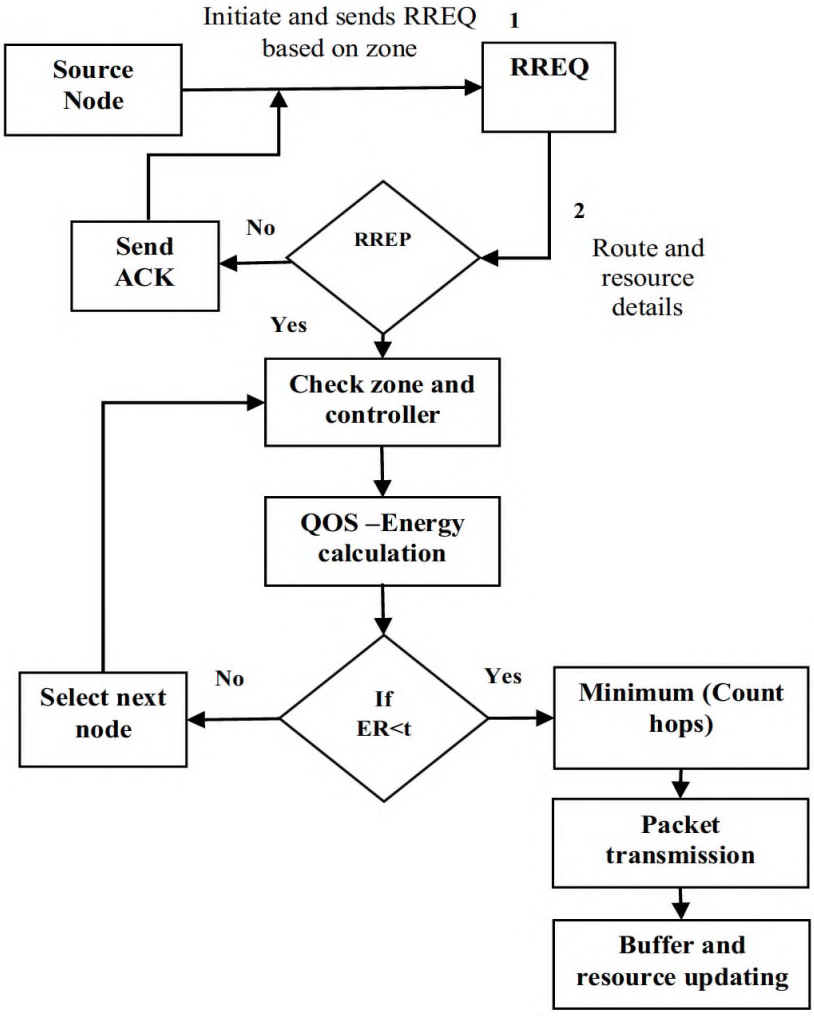

Рисунок 2 – Блок-схема CZLAR

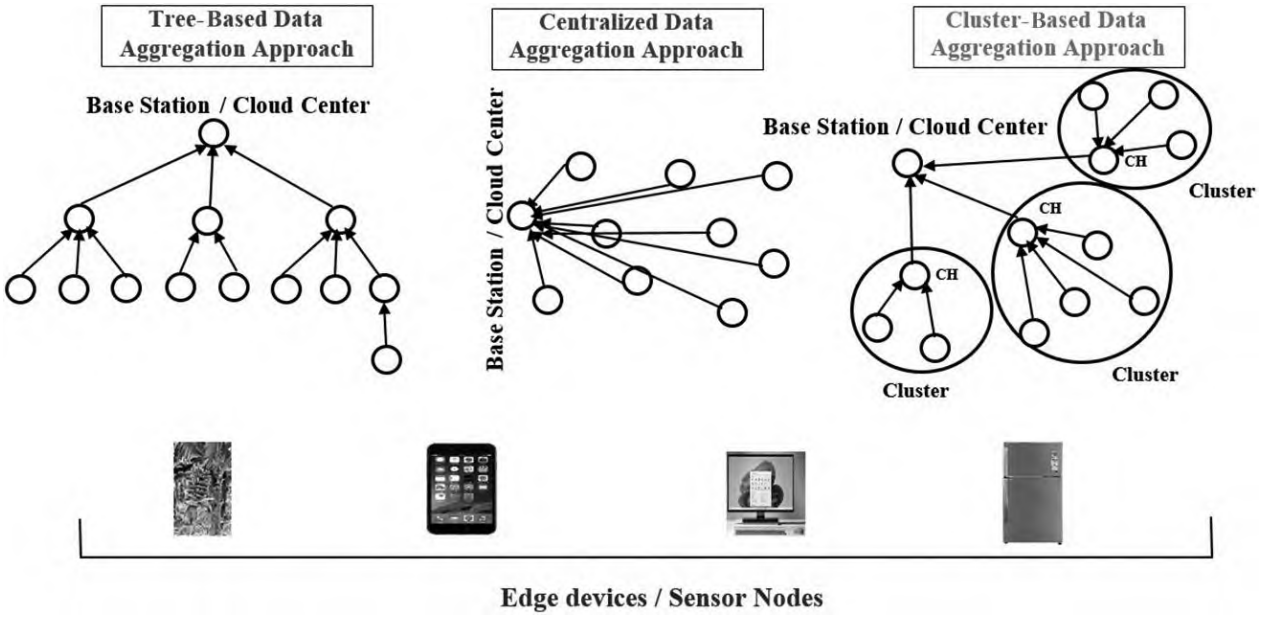

Рисунок 3 – Методи маршрутизації та агрегації даних у мережі

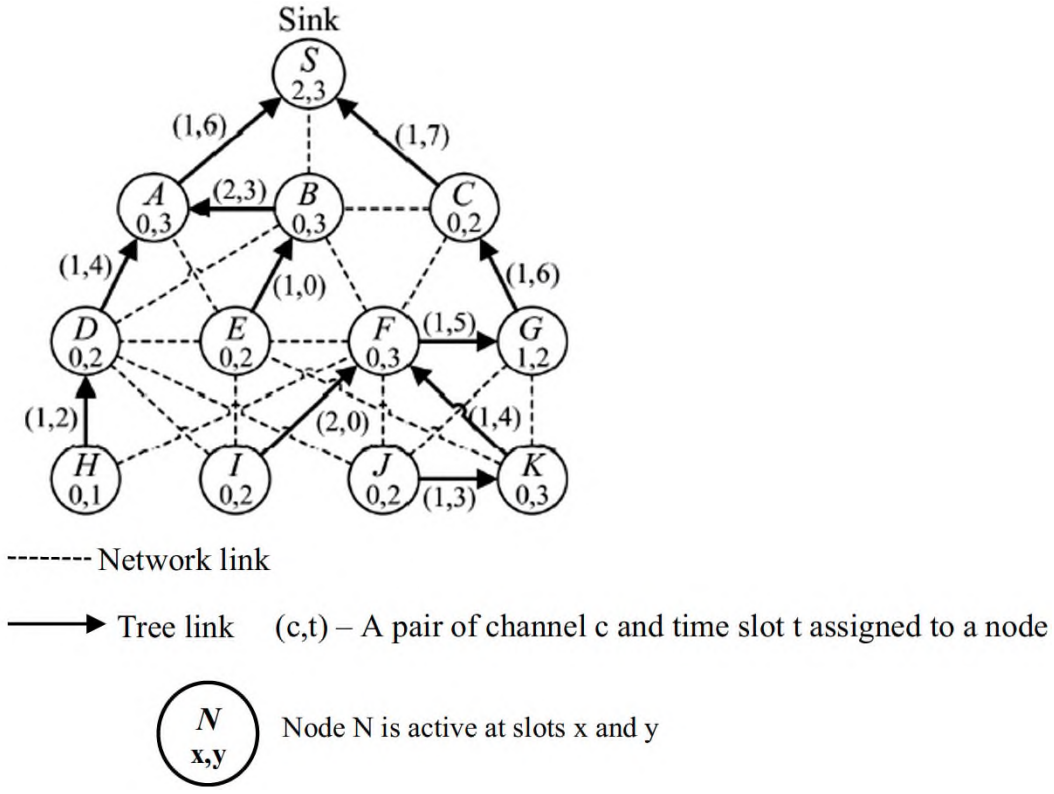

Рисунок 4 – Схема агрегації даних на дереві вибірки

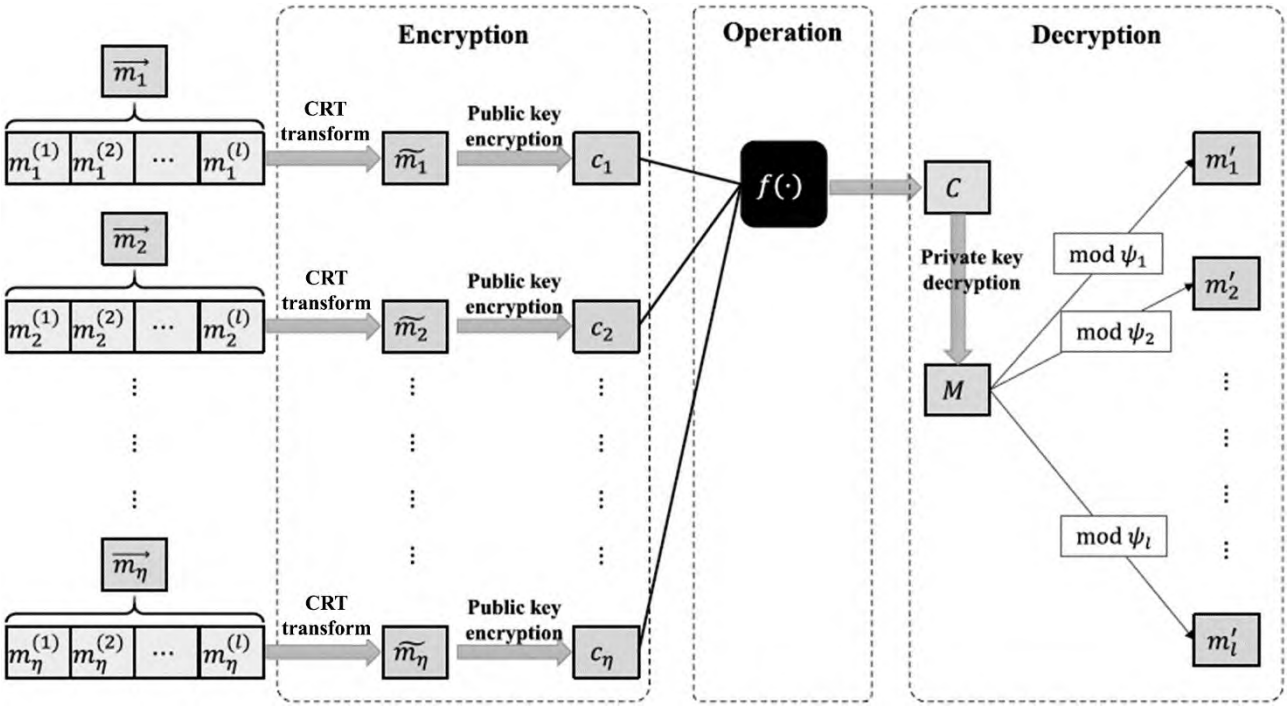

Рисунок 5 – Схема багатовимірного агрегування даних

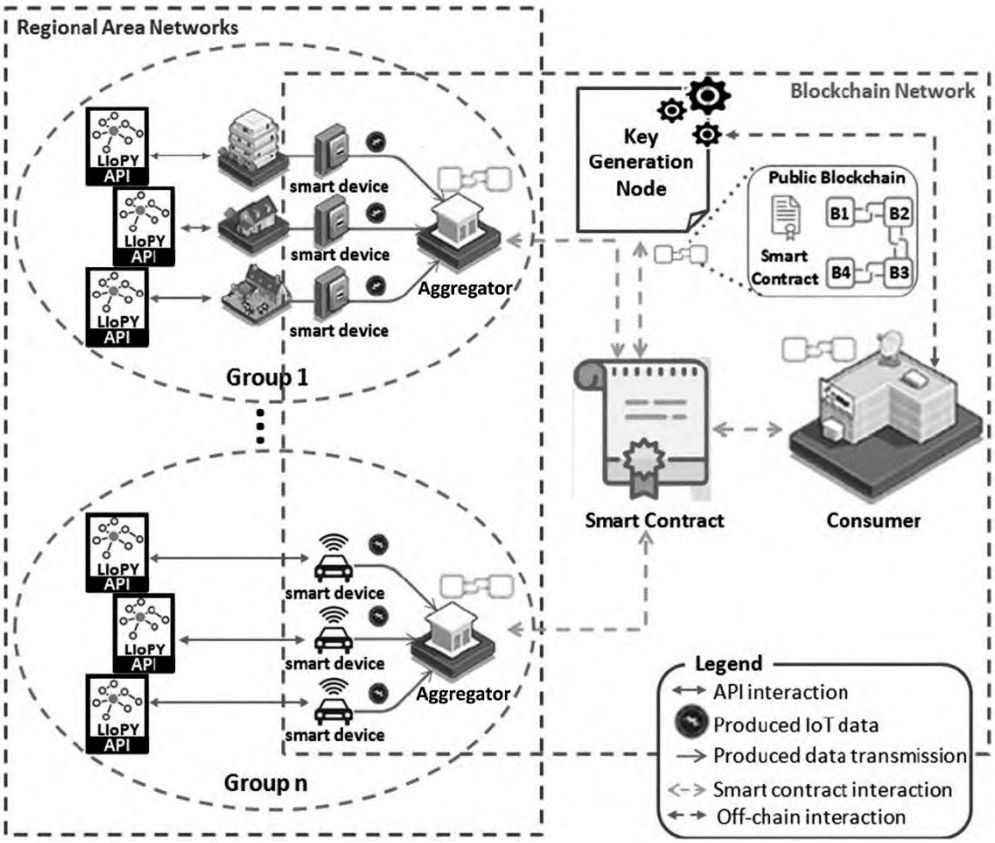

Рисунок 6 – Схема агрегації даних на основі блокчейну

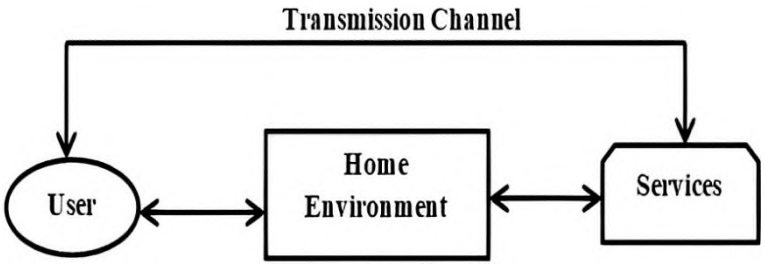

Рисунок 7 – Архітектура MufHAS

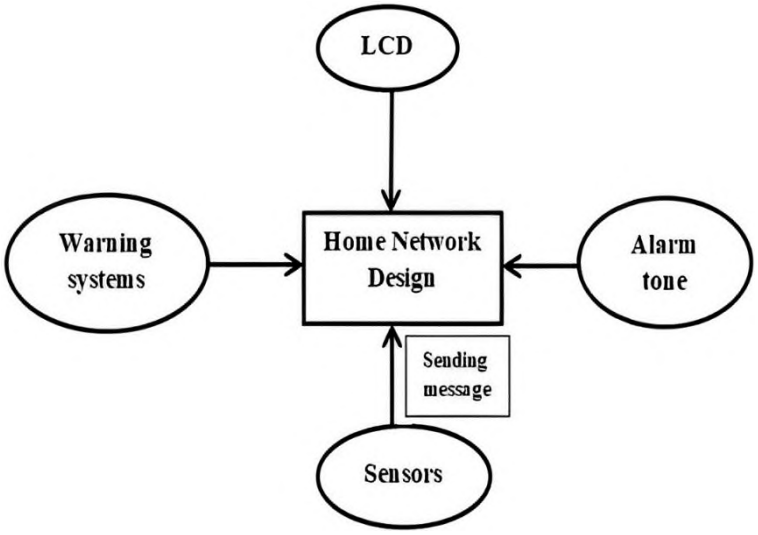

Рисунок 8 – Архітектура запропонованої системи

Додаток Б

ПРОТОКОЛ ПЕРЕВІРКИ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Назва роботи: Інтелектуальна сенсорна мережа Інтернету речей

Тип роботи: Магістерська кваліфікаційна робота

Підрозділ кафедра ІКСТ, факультет ІЕС

Керівник Васильківський М.В., к.т.н., доцент

Показники звіту подібності

Turnitin	
Оригінальність	98 %
Загальна схожість	2 %

Аналіз звіту подібності (відмітити потрібне)

- ▪ Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.
- ☐ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її автора. Роботу направити на доопрацювання.
- ☐ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Заявляю, що ознайомлений (-на) з повним звітом подібності, який був згенерований Системою щодо роботи (додається)

Автор _____ Паламарчук М.С.
(підпис) (прізвище, ініціали)

Опис прийнятого рішення

Особа, відповідальна за перевірку _____ Васильківський М.В.
(підпис) (прізвище, ініціали)

Експерт _____ _____
(за потреби) (підпис) (прізвище, ініціали, посада)