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

Навчально-науковий інститут телекомунікаційних систем

Кафедра телекомунікацій

До захисту допущено:

В.о.завідувача кафедри

_____ Сергій КРАВЧУК

«___»_____2026 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Інженерія та програмування інфокомунікацій»

спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «Децентралізовані IoT-мережі для моніторингу пошкоджень інфраструктури»

Виконав:
студент IV курсу, групи ТЗ-22
Стадник Олександр Сергійович _____

Керівник:
Доцент кафедри ТК НН ІТС, к.т.н., доцент,
Явіся Валерій Сергійович _____

Рецензент:
Доцент кафедри ІТТ НН ІТС, к.т.н., доцент,
Правило Валерій Володимирович _____

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

Київ – 2026 року

Національний технічний університет України

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий інститут телекомунікаційних систем
Кафедра телекомунікацій

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інженерія та програмування інфокомунікацій»

ЗАТВЕРДЖУЮ
В.о.завідувача кафедри
_____ Сергій КРАВЧУК
«___»_____2026 р.

ЗАВДАННЯ

на дипломну роботу студенту
Стаднику Олександру Сергійовичу

1. Тема роботи «Децентралізовані IoT-мережі для моніторингу пошкоджень інфраструктури», керівник роботи Явіся Валерій Сергійович, к.т.н., доцент, затверджені наказом по університету від «26» травня 2026 р. № 1912-с.

2. Термін подання студентом роботи 10 червня 20265 р.

3. Вихідні дані до роботи:

1) сучасні концепції та архітектури Інтернету речей (IoT);

2) технології побудови децентралізованих мереж та систем розподіленого реєстру (DLT, Blockchain);

3) бездротові технології передачі даних LoRaWAN, NB-IoT, 4G/5G;

4) методи збору, обробки та передачі даних у бездротових сенсорних мережах;

5) принципи побудови mesh-мереж, edge computing та fog computing;

6) науково-технічні публікації, стандарти та технічна документація у сфері IoT та телекомунікацій;

7) вимоги до надійності, відмовостійкості та кібербезпеки систем моніторингу критичної інфраструктури;

8) програмні та апаратні засоби моделювання телекомунікаційних мереж.

4. Зміст роботи:

1) Аналіз сучасних підходів до побудови децентралізованих IoT-мереж для моніторингу інфраструктури.

2) Дослідження принципів функціонування IoT-систем та методів моніторингу інфраструктурних об'єктів.

3) Аналіз централізованих і децентралізованих архітектур мереж, технологій Blockchain та DLT.

4) Аналіз сучасних бездротових технологій передачі даних (LoRaWAN, NB-IoT, 4G/5G).

5) Розробка архітектури децентралізованої IoT-мережі для моніторингу пошкоджень інфраструктури.

6) Розробка алгоритмів взаємодії вузлів, маршрутизації та передачі тривожних повідомлень.

7) Дослідження методів забезпечення безпеки, надійності та відмовостійкості системи.

8) Моделювання роботи мережі та оцінка її ефективності.

9) Виконання розрахунків автономної роботи LoRaWAN-вузлів.

10) Проведення техніко-економічного обґрунтування та аналізу питань охорони праці.

11) Формування висновків та рекомендацій щодо впровадження розробленої системи.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо):

Слайд №1 Децентралізовані IoT-мережі для моніторингу пошкоджень інфраструктури

Слайд №2 Актуальність

Слайд №3 Мета та завдання

Слайд №4 Аналіз існуючих рішень

Слайд №5 Запропонована архітектура системи

Слайд №6 Взаємодія компонентів

Слайд №7 Алгоритм маршрутизації

Слайд №8 Передача тривожного повідомлення

Слайд №9 Аналіз надійності: централізована vs децентралізована

Слайд №10 Розрахунок автономної роботи LoRaWAN-вузлів

Слайд №11 Техніко-економічне обґрунтування і висновки

Слайд №12 Висновки

6. Дата видачі завдання 01.10.2025 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз завдання на дипломну роботу та формування плану дослідження	01.10.2025-12.10.2025	Виконано
2	Пошук та аналіз науково-технічної літератури за тематикою роботи	13.10.2025-17.10.2025	Виконано
3	Дослідження сучасних IoT-технологій та децентралізованих мереж	18.10.2025-07.11.2025	Виконано
4	Аналіз технологій передачі даних LoRaWAN, NB-IoT, 4G/5G	08.11.2025-03.12.2025	Виконано
5	Розробка архітектури децентралізованої IoT-мережі	04.12.2025-14.01.2026	Виконано
6	Розробка алгоритмів маршрутизації та передачі тривожних повідомлень	12.01.2022-12.02.2026	Виконано
7	Дослідження методів забезпечення безпеки та кіберстійкості системи	13.02.2026-19.03.2026	Виконано
8	Моделювання роботи мережі та оцінка її ефективності	20.03.2026-15.04.2026	Виконано
9	Виконання техніко-економічного обґрунтування та розділу з охорони праці	16.04.2026-07.05.2026	Виконано
10	Оформлення тексту роботи та графічних матеріалів	08.05.2026-14.05.2026	Виконано
11	Перевірка роботи керівником, усунення зауважень. Підготовка доповіді та презентації до захисту	15.05.2026-01.06.2026	Виконано

Студент Олександр СТАДНИК

Керівник Валерій ЯВІСЯ

РЕФЕРАТ

Дипломна робота містить: 85 сторінок, 4 рисунки, 2 таблиці, 15 джерел.

Об’єктом дослідження є процеси моніторингу технічного стану об’єктів інфраструктури з використанням децентралізованих IoT-мереж.

Предметом дослідження є методи, архітектури та технології побудови децентралізованих IoT-мереж для збору, передачі та обробки даних під час моніторингу пошкоджень інфраструктури.

Метою дипломної роботи є розробка та обґрунтування архітектури децентралізованої IoT-мережі для моніторингу пошкоджень об’єктів інфраструктури з підвищеною надійністю, відмовостійкістю та можливістю функціонування в умовах часткової втрати зв’язку.

У роботі проведено аналіз сучасних технологій Інтернету речей (IoT), принципів побудови централізованих і децентралізованих мереж, а також сучасних бездротових технологій передачі даних, зокрема LoRaWAN, NB-IoT та 4G/5G. Досліджено методи збору, обробки та передачі даних у сенсорних мережах, розглянуто підходи до забезпечення надійності, відмовостійкості та кібербезпеки IoT-систем.

У процесі виконання роботи використано методи системного аналізу, структурного та функціонального проєктування інформаційно-комунікаційних систем, а також методи порівняльного аналізу сучасних мережевих технологій.

Результатом роботи є запропонована архітектура децентралізованої IoT-мережі для моніторингу пошкоджень інфраструктури, що забезпечує підвищення надійності функціонування системи, зменшення ризиків втрати даних та можливість автономної роботи окремих вузлів мережі.

Отримані результати можуть бути використані під час створення систем моніторингу транспортної, енергетичної, промислової та міської інфраструктури, а також у проєктах «розумного міста». Результати роботи

можуть бути рекомендовані для подальшого використання у сфері проєктування сучасних телекомунікаційних та IoT-систем. [10]

Ключові слова: IoT, Інтернет речей, децентралізована мережа, моніторинг інфраструктури, сенсорна мережа, LoRaWAN, NB-IoT, 4G, 5G, mesh-мережа, бездротовий зв’язок, передача даних, відмовостійкість, кібербезпека, edge computing, телекомунікаційні системи, критична інфраструктура, блокчейн, DLT, моніторинг пошкоджень.

ABSTRACT

Bachelor’s thesis: 85 pages, 4 figures, 2 tables, 15 references.

The object of the research is the processes of monitoring the technical condition of infrastructure facilities using decentralized IoT networks.

The subject of the research is the methods, architectures, and technologies for building decentralized IoT networks for collecting, transmitting, and processing data during infrastructure damage monitoring.

The purpose of the thesis is to develop and justify the architecture of a decentralized IoT network for monitoring infrastructure damage with increased reliability, fault tolerance, and the ability to operate under conditions of partial communication loss.

The paper analyzes modern Internet of Things (IoT) technologies, principles of centralized and decentralized network construction, and modern wireless data transmission technologies, including LoRaWAN, NB-IoT, and 4G/5G. Methods of data collection, processing, and transmission in sensor networks are investigated, and approaches to ensuring reliability, fault tolerance, and cybersecurity of IoT systems are considered.

During the research, methods of system analysis, structural and functional design of information and communication systems, as well as comparative analysis of modern networking technologies were used.

The result of the work is the proposed architecture of a decentralized IoT network for infrastructure damage monitoring, which provides improved system reliability, reduced risk of data loss, and autonomous operation of network nodes.

The obtained results can be used in the development of monitoring systems for transport, energy, industrial, and urban infrastructure, as well as in smart city projects. The results of the work can be recommended for further use in the design of modern telecommunication and IoT systems.

Keywords: IoT, Internet of Things, decentralized network, infrastructure monitoring, sensor network, LoRaWAN, NB-IoT, 4G, 5G, mesh network, wireless

communication, data transmission, fault tolerance, cybersecurity, edge computing, telecommunication systems, critical infrastructure, blockchain, DLT, damage monitoring.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

IoT	Internet of Things – Інтернет речей
DLT	Distributed Ledger Technology – технологія розподіленого реєстру
WSN	Wireless Sensor Network – бездротова сенсорна мережа
LoRaWAN	Long Range Wide Area Network
NB-IoT	Narrowband Internet of Things
MQTT	Message Queuing Telemetry Transport
CoAP	Constrained Application Protocol
BLE	Bluetooth Low Energy
LPWAN	Low Power Wide Area Network
TLS	Transport Layer Security
SSL	Secure Sockets Layer
DDoS	Distributed Denial of Service
UML	Unified Modeling Language
CAPEX	Capital Expenditure – капітальні витрати
OPEX	Operational Expenditure – експлуатаційні витрати
Edge Computing	Периферійні обчислення
Fog Computing	Туманні обчислення
Mesh	Багатохопова децентралізована топологія мережі
4G	Fourth Generation Mobile Network
5G	Fifth Generation Mobile Network

ВСТУП

У сучасних умовах стрімкого розвитку цифрових технологій та зростання навантаження на критичну інфраструктуру особливої актуальності набуває питання оперативного моніторингу технічного стану інженерних об’єктів. Транспортні мережі, мости, тунелі, лінії електропередач, промислові споруди, системи водопостачання та інші елементи інфраструктури постійно піддаються впливу природних факторів, техногенних навантажень, зношування матеріалів, аварійних ситуацій і зовнішніх загроз. Несвоєчасне виявлення пошкоджень може призводити до значних економічних збитків, порушення функціонування важливих систем та виникнення небезпечних ситуацій для населення. [6, 7]

Особливо важливим є питання контролю стану інфраструктури в умовах зростання кількості надзвичайних ситуацій, природних катастроф та воєнних дій, які суттєво впливають на цілісність об’єктів інфраструктури. Традиційні методи моніторингу, що передбачають регулярні перевірки та ручний збір даних, часто не забезпечують необхідної швидкості реагування, точності або безперервності управління. Додатково, централізовані системи моніторингу мають свої недоліки, такі як значна залежність від центрального контрольного вузла, труднощі з масштабуванням і вразливість до збоїв окремих компонентів мережі. [6, 12]

Одним із перспективних рішень цієї проблеми стало широке впровадження технологій Інтернету речей (IoT). Завдяки IoT-системам можна автоматизувати процеси збору, передачі та аналізу великих обсягів даних із сенсорів у реальному часі. За допомогою датчиків температури, вібрації, деформації, вологості, тиску та інших параметрів можна постійно контролювати технічний стан об’єктів інфраструктури та оперативно виявляти потенційні пошкодження. Проте більшість існуючих IoT-рішень побудовані за централізованою архітектурою, що створює ризики

перевантаження серверів, втрати даних або зупинки системи у разі відмови центрального вузла. [6, 12]

У зв’язку з цим значний науковий та практичний інтерес становлять децентралізовані IoT-мережі, які забезпечують підвищену стійкість, автономність та надійність функціонування систем моніторингу. Децентралізований підхід передбачає розподіл обчислювальних ресурсів і функцій обробки даних між вузлами мережі без використання єдиного центру керування. Така архітектура дозволяє зменшити ризик відмови всієї системи, підвищити швидкість обробки інформації та забезпечити безперервність роботи навіть у випадку пошкодження окремих елементів мережі. [1, 5]

Додатково перспективність децентралізованих систем посилюється використанням технологій розподіленого реєстру (DLT) та блокчейн, які забезпечують захист даних від несанкціонованого втручання, прозорість обміну інформацією та підвищення рівня довіри між вузлами мережі. Використання таких технологій дозволяє створювати безпечні системи моніторингу, здатні функціонувати в умовах нестабільного зв’язку або часткової недоступності окремих вузлів. [2–4]

Аналіз сучасних наукових досліджень і практичних рішень провідних компаній у сфері IoT, таких як Cisco Systems, IBM, Siemens та Huawei, свідчить про активний розвиток технологій розподіленого моніторингу та інтелектуальних сенсорних мереж. Значна увага приділяється питанням енергоефективності IoT-пристроїв, оптимізації передачі даних, підвищення надійності мережевої взаємодії та впровадження алгоритмів автоматичного виявлення аномалій. Однак проблема побудови ефективних децентралізованих IoT-мереж для моніторингу пошкоджень інфраструктури залишається актуальною та потребує подальших досліджень. [3, 6, 7]

Актуальність теми дипломної роботи полягає у необхідності створення сучасної системи моніторингу інфраструктурних об’єктів, яка забезпечуватиме безперервний контроль технічного стану, оперативне виявлення пошкоджень, високу надійність передачі даних та стійкість до

зовнішніх впливів. Використання децентралізованої архітектури дозволяє підвищити ефективність функціонування IoT-мереж і забезпечити їхню адаптивність до складних умов експлуатації.

Новизна роботи полягає у дослідженні можливостей поєднання IoT-технологій із децентралізованими методами обробки та передачі даних для створення системи моніторингу пошкоджень інфраструктури. Передбачається аналіз архітектури децентралізованої мережі, принципів взаємодії сенсорних вузлів, методів збору та агрегації інформації, а також способів забезпечення надійності та безпеки даних. Особлива увага приділяється питанням автономності вузлів мережі, оптимізації навантаження та забезпечення стійкості системи до відмов.

У межах дипломної роботи планується обґрунтувати основні проєктні рішення щодо побудови децентралізованої IoT-мережі для моніторингу інфраструктурних об’єктів, дослідити можливості використання бездротових технологій зв’язку, розглянути методи передачі та обробки даних, а також оцінити ефективність застосування розподілених систем для виявлення пошкоджень у режимі реального часу. Також передбачається аналіз існуючих протоколів взаємодії IoT-пристроїв та визначення оптимальних підходів до організації мережевої архітектури.

Результати роботи можуть бути використані у сферах моніторингу транспортної, енергетичної, промислової та міської інфраструктури, системах контролю стану будівель і споруд, а також у проєктах створення «розумних міст». Практичне застосування розроблених рішень дозволить підвищити ефективність виявлення пошкоджень, зменшити витрати на обслуговування інфраструктурних об’єктів та покращити рівень безпеки експлуатації критично важливих систем. [1, 5, 6]

Метою дипломної роботи є розробка та обґрунтування архітектури децентралізованої IoT-мережі для моніторингу пошкоджень об’єктів інфраструктури з підвищеною надійністю, відмовостійкістю, кіберстійкістю

та можливістю функціонування в умовах часткової втрати зв’язку або руйнування центральних вузлів.

Для досягнення поставленої мети необхідно вирішити такі завдання:

— проаналізувати сучасний стан та основні напрями розвитку технологій Інтернету речей (IoT);
— дослідити принципи побудови централізованих і децентралізованих мереж та визначити їх основні переваги і недоліки;
— розглянути архітектуру децентралізованих IoT-мереж та особливості їх функціонування;
— проаналізувати сучасні бездротові технології передачі даних (LoRaWAN, NB-IoT, 4G/5G) для використання в системах моніторингу;
— дослідити методи збору, обробки та передачі даних у сенсорних мережах;
— визначити підходи до забезпечення надійності, відмовостійкості та безпеки функціонування IoT-мереж;
— розглянути можливості застосування децентралізованих IoT-мереж для моніторингу пошкоджень об’єктів інфраструктури;

Об’єктом дослідження є процеси моніторингу технічного стану об’єктів інфраструктури з використанням децентралізованих IoT-мереж. Предметом дослідження є методи, архітектури та технології побудови децентралізованих IoT-мереж для збору, передачі та обробки даних під час моніторингу пошкоджень інфраструктури.

У ході виконання роботи застосовуються сучасні методи дослідження, аналізу та проєктування інформаційно-комунікаційних систем. Використовуються інструменти системного аналізу для вивчення структури та принципів функціонування децентралізованих IoT-мереж, а також методи порівняльного аналізу для оцінки ефективності централізованих і децентралізованих моделей побудови мереж моніторингу. [1, 5]

Для моделювання архітектури системи застосовуються методи структурного та функціонального проєктування, що дають змогу визначити

склад ключових компонентів, їх взаємодію та механізми обміну даними між вузлами. Крім того, використовуються методи обробки даних — фільтрація, агрегація та попередня обробка інформації на рівні периферійних пристроїв (edge computing). [1, 5, 11]

Особливу увагу приділено організації бездротового зв’язку в IoT-мережах із використанням технологій LoRaWAN, NB-IoT та мобільних мереж 4G/5G, а також принципів побудови mesh-мереж для забезпечення децентралізованої взаємодії вузлів. Розглядаються підходи до підвищення надійності та відмовостійкості системи, включаючи резервування вузлів, багатохопову передачу даних і розподілену обробку інформації. Практичне значення одержаних результатів полягає у можливості використання запропонованих підходів та архітектурних рішень для створення ефективних систем моніторингу технічного стану об’єктів критичної інфраструктури. Результати роботи можуть бути застосовані під час проєктування систем контролю мостів, транспортних мереж, промислових об’єктів, енергетичної інфраструктури та елементів «розумного міста». [9, 12, 13]

Запропоновані рішення дозволяють підвищити надійність функціонування IoT-мереж, забезпечити безперервний збір даних навіть у випадку часткової відмови вузлів мережі, а також зменшити ризики втрати інформації завдяки використанню децентралізованого підходу. Практичне впровадження результатів роботи сприятиме підвищенню рівня безпеки експлуатації інфраструктурних об’єктів та оперативності виявлення пошкоджень.

РОЗДІЛ 1
АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО ПОБУДОВИ ДЕЦЕНТРАЛІЗОВАНИХ IoT-МЕРЕЖ ДЛЯ МОНІТОРИНГУ ІНФРАСТРУКТУРИ

1.1. Основні принципи функціонування IoT-систем

Інтернет речей (Internet of Things, IoT) є одним із ключових напрямів розвитку сучасних інформаційно-комунікаційних технологій. Концепція IoT передбачає об’єднання фізичних пристроїв, сенсорів, програмного забезпечення та засобів зв’язку в єдину мережу для автоматизованого збору, передачі, обробки та аналізу даних без постійного втручання людини. Основною метою IoT-систем є забезпечення взаємодії між різними об’єктами та створення інтелектуального середовища для моніторингу, контролю та автоматизації процесів. [9, 12]

Стрімкий розвиток технологій IoT пов’язаний із появою недорогих сенсорних пристроїв, розвитком бездротових мереж, збільшенням обчислювальних можливостей мікроконтролерів та поширенням хмарних сервісів. [8, 9, 12] Сучасні IoT-системи активно використовуються у промисловості, транспорті, енергетиці, медицині, аграрному секторі, системах безпеки та концепціях «розумного міста» (Smart City). [10]

Основу IoT-систем становлять сенсорні вузли, які здатні збирати інформацію про стан навколишнього середовища або контрольованого об’єкта. Залежно від сфери застосування використовуються датчики температури, вологості, тиску, освітленості, вібрації, деформації, руху, газоаналізатори та інші типи сенсорів. Отримані дані передаються через канали зв’язку до систем обробки інформації, де виконуються їх аналіз, зберігання та формування керуючих рішень. [8, 10]

Типова IoT-система складається з декількох основних рівнів:

— рівень пристроїв (сенсорний рівень);

— мережевий рівень;

— рівень обробки даних;
— прикладний рівень. [8, 12]

Сенсорний рівень включає фізичні пристрої та датчики, які здійснюють вимірювання параметрів об’єкта моніторингу. На цьому рівні відбувається первинний збір інформації та її попередня обробка. Як правило, сенсорні вузли мають обмежені обчислювальні ресурси та працюють із мінімальним енергоспоживанням.

Мережевий рівень забезпечує передачу даних між пристроями та обчислювальними вузлами. Для цього використовуються різні технології зв’язку, зокрема Wi-Fi, Bluetooth Low Energy, ZigBee, LoRaWAN, NB-IoT, LTE та 5G. Вибір технології залежить від дальності передачі даних, швидкості обміну, енергоспоживання та умов експлуатації системи. Для систем моніторингу інфраструктури особливо важливими є енергоефективність, велика зона покриття та стійкість до втрати зв’язку.

Рівень обробки даних виконує функції аналізу, агрегації, зберігання та візуалізації інформації. У традиційних IoT-системах обробка даних зазвичай здійснюється у централізованих хмарних сервісах. Проте сучасні системи дедалі частіше використовують концепції edge computing та fog computing, які передбачають часткову обробку інформації безпосередньо на периферійних вузлах мережі або на локальних проміжних серверах. Це дозволяє зменшити затримки передачі даних, знизити навантаження на мережу та підвищити відмовостійкість системи. [5, 7, 11]

Прикладний рівень відповідає за взаємодію користувача із системою. На цьому рівні реалізуються програмні інтерфейси, системи візуалізації, аналітичні модулі та механізми прийняття рішень. Користувач отримує доступ до інформації у вигляді графіків, повідомлень, статистики або аварійних сповіщень.

Однією з основних особливостей IoT-систем є можливість функціонування у режимі реального часу. [8, 9] Це особливо важливо для систем моніторингу інфраструктури, де оперативне виявлення пошкоджень

дозволяє мінімізувати ризики аварій та забезпечити безпечну експлуатацію об’єктів. Для цього використовуються алгоритми автоматичного аналізу даних, виявлення аномалій та прогнозування можливих відмов.

Сучасні IoT-системи також характеризуються високою масштабованістю, що дозволяє об’єднувати велику кількість пристроїв у межах єдиної мережі. [9, 12] Однак збільшення кількості підключених вузлів створює додаткові проблеми, пов’язані з кібербезпекою, захистом даних, перевантаженням мережі та забезпеченням надійності функціонування системи.

Одним із перспективних напрямів розвитку IoT є використання децентралізованих архітектур, у яких відсутній єдиний центр керування. У таких системах вузли можуть взаємодіяти між собою безпосередньо, а обробка даних виконується розподілено між елементами мережі. Це дозволяє підвищити стійкість системи до відмов, забезпечити автономність окремих сегментів мережі та зменшити ризики втрати інформації.

Для забезпечення безпеки IoT-систем активно досліджуються технології блокчейн та розподіленого реєстру (DLT). Їх використання дозволяє забезпечити цілісність даних, захист від несанкціонованого доступу та підвищити рівень довіри між вузлами мережі. Особливо актуальним це є для систем моніторингу критичної інфраструктури, де достовірність і захищеність інформації мають важливе значення.

Таким чином, IoT-системи є важливою складовою сучасних інформаційно-комунікаційних технологій та забезпечують ефективний моніторинг і керування різноманітними об’єктами. Розвиток децентралізованих підходів, edge/fog computing та сучасних бездротових технологій створює передумови для побудови надійних систем моніторингу пошкоджень інфраструктури з високим рівнем автономності та відмовостійкості.

1.2. Сучасні методи моніторингу інфраструктури

Моніторинг технічного стану інфраструктурних об’єктів є важливою складовою забезпечення безпечної та безперервної роботи транспортних, енергетичних, промислових і міських систем. [10, 12] Своєчасне виявлення пошкоджень, деформацій або аварійних станів дозволяє запобігати надзвичайним ситуаціям, зменшувати витрати на ремонт та продовжувати термін експлуатації об’єктів.

До об’єктів інфраструктури належать мости, тунелі, дороги, лінії електропередач, трубопроводи, промислові споруди, системи водопостачання, енергетичні об’єкти та інші критично важливі елементи. [10] У процесі експлуатації вони постійно піддаються впливу механічних навантажень, погодних умов, корозії, вібрацій, температурних змін та техногенних факторів. У сучасних умовах додатковими ризиками є надзвичайні ситуації, природні катастрофи та пошкодження, спричинені воєнними діями.

Традиційні методи моніторингу базуються на періодичних візуальних інспекціях та ручному контролі стану об’єктів. Такі підходи використовуються протягом тривалого часу та дозволяють виявляти очевидні дефекти, тріщини, корозію або механічні пошкодження. Проте ручний моніторинг має низку недоліків:

- значні витрати часу та ресурсів;
- залежність від людського фактору;
- обмежена точність вимірювань;
- відсутність безперервного контролю;
- складність оперативного реагування на аварійні ситуації.

У зв’язку з цим сучасні системи моніторингу дедалі частіше використовують автоматизовані технології збору та аналізу даних. Одним із найбільш перспективних напрямів є застосування сенсорних мереж та технологій Інтернету речей (IoT), які забезпечують безперервний контроль стану об’єктів у режимі реального часу. [8, 10, 12]

У системах моніторингу інфраструктури використовуються різні типи датчиків залежно від контрольованих параметрів. [8, 10] Для контролю механічного стану конструкцій застосовуються датчики деформації, вібрації, нахилу та прискорення. У системах контролю навколишнього середовища використовуються сенсори температури, вологості, рівня води, концентрації газів та тиску. Для енергетичної інфраструктури важливими є системи контролю електричних параметрів, навантаження та стану обладнання.

Одним із сучасних напрямів є використання бездротових сенсорних мереж (Wireless Sensor Networks, WSN). [12] Такі мережі складаються з великої кількості автономних сенсорних вузлів, які здатні збирати інформацію та передавати її через бездротові канали зв’язку. Основними перевагами WSN є:

— можливість розгортання у важкодоступних місцях;
— масштабованість;
— низьке енергоспоживання;
— гнучкість конфігурації;
— підтримка віддаленого моніторингу.

Для передачі даних у системах моніторингу широко використовуються сучасні бездротові технології, зокрема LoRaWAN, NB-IoT, ZigBee, Wi-Fi, LTE та 5G. Технологія LoRaWAN забезпечує передачу даних на великі відстані при мінімальному енергоспоживанні, що робить її ефективною для розподілених систем моніторингу. NB-IoT дозволяє використовувати інфраструктуру мобільних операторів для обслуговування великої кількості IoT-пристроїв. Мережі 4G/5G забезпечують високу швидкість передачі даних та підтримку систем реального часу. [6, 9, 13]

Окрему увагу приділяють використанню технологій edge computing та fog computing у системах моніторингу. Традиційні централізовані моделі передбачають передачу всіх даних до хмарного сервера для подальшої обробки. Проте у великих IoT-системах це може створювати значне навантаження на мережу та збільшувати затримки передачі даних.

Edge computing дозволяє виконувати первинну обробку інформації безпосередньо на периферійних вузлах мережі, тобто поблизу джерела даних. Fog computing передбачає використання проміжних вузлів між сенсорами та хмарною інфраструктурою для локальної обробки та агрегації інформації. Такі підходи дозволяють:

— зменшити затримки;
— скоротити обсяг переданих даних;
— підвищити швидкість реагування системи;
— забезпечити автономну роботу окремих сегментів мережі. [5, 7, 11]

Для сучасних систем моніторингу інфраструктури також характерне використання алгоритмів машинного навчання та аналізу великих даних (Big Data). Такі методи дозволяють автоматично виявляти аномалії, прогнозувати можливі відмови обладнання та оцінювати технічний стан об’єктів на основі накопичених даних. Використання інтелектуальних алгоритмів підвищує точність діагностики та дозволяє переходити від планового обслуговування до прогнозованого технічного обслуговування (predictive maintenance). [10, 11]

Важливим аспектом сучасних систем моніторингу є забезпечення надійності та кібербезпеки. Централізовані архітектури мають ризики, пов’язані з перевантаженням серверів, втратою даних або відмовою центрального вузла. Для вирішення цих проблем активно досліджуються децентралізовані IoT-мережі та технології блокчейн. [1–5] Використання розподілених систем дозволяє підвищити стійкість мережі до відмов, забезпечити захист інформації та підвищити рівень довіри між вузлами системи.

У сучасних проєктах «розумного міста» системи моніторингу інтегруються з іншими інформаційно-комунікаційними системами, включаючи транспортну інфраструктуру, енергетичні мережі, системи відеоспостереження та служби екстреного реагування. Це створює єдине

цифрове середовище для управління міською інфраструктурою та підвищення ефективності її функціонування. [10]

Таким чином, сучасні методи моніторингу інфраструктури базуються на використанні IoT-технологій, бездротових сенсорних мереж, edge/fog computing, аналітики даних та децентралізованих підходів до обробки інформації. Їх застосування дозволяє забезпечити безперервний контроль стану об’єктів, підвищити оперативність реагування на пошкодження та покращити рівень безпеки критичної інфраструктури.

1.3. Централізовані та децентралізовані мережі

Архітектура мережі є одним із ключових факторів, що визначають ефективність функціонування сучасних IoT-систем моніторингу інфраструктури. Від способу організації взаємодії між вузлами мережі залежать надійність передачі даних, масштабованість системи, швидкість обробки інформації та стійкість до відмов. У сучасних інформаційно-комунікаційних системах найбільш поширеними є централізовані та децентралізовані підходи до побудови мереж. [1, 5, 11]

Централізована мережа передбачає наявність єдиного центрального вузла або сервера, через який проходить основна частина процесів збору, обробки та керування даними. У такій архітектурі сенсорні пристрої або периферійні вузли передають інформацію до центрального сервера, де здійснюються її обробка, зберігання та аналіз. Центральний вузол також виконує функції керування мережею та координації взаємодії між пристроями.

Централізований підхід широко використовується у традиційних IoT-системах завдяки простоті реалізації та зручності адміністрування. [1, 12] Основними перевагами централізованих мереж є:

— спрощене керування системою;
— централізоване зберігання даних;
— простота оновлення програмного забезпечення;

— зручність контролю доступу та адміністрування;
— можливість використання потужних серверних ресурсів для обробки інформації.

Попри переваги, централізовані системи мають низку суттєвих недоліків. Основною проблемою є наявність єдиної точки відмови (Single Point of Failure). У випадку виходу з ладу центрального сервера або втрати зв’язку з ним функціонування всієї системи може бути порушене. Для систем моніторингу критичної інфраструктури це створює значні ризики, оскільки затримка або втрата інформації може призвести до аварійних ситуацій. [6, 13]

Іншим недоліком централізованих мереж є складність масштабування. Зі збільшенням кількості підключених пристроїв зростає навантаження на центральний сервер та мережеві канали зв’язку. Це може призводити до збільшення затримок передачі даних, перевантаження системи та зниження її продуктивності.

Крім того, централізовані системи мають підвищені ризики кіберзагроз. [2, 15] Центральний сервер є основною ціллю для атак, а компрометація такого вузла може призвести до втрати або підробки даних усієї системи. Особливо актуальною ця проблема є для систем моніторингу критичної інфраструктури та об’єктів підвищеної небезпеки.

Для усунення зазначених недоліків активно розвиваються децентралізовані мережі. [1, 5] У децентралізованій архітектурі відсутній єдиний центр керування, а функції обробки, зберігання та передачі даних розподіляються між вузлами мережі. Кожен вузол може виконувати частину функцій системи та взаємодіяти з іншими вузлами безпосередньо. [5, 12]

Одним із ключових принципів децентралізованих мереж є розподілена обробка даних. Це дозволяє зменшити навантаження на окремі елементи системи та забезпечити автономну роботу окремих сегментів мережі. У разі пошкодження або відмови одного з вузлів інші елементи можуть продовжувати функціонування без суттєвого впливу на роботу системи в цілому. [1, 11]

Основними перевагами децентралізованих мереж є:

— висока відмовостійкість;
— відсутність єдиної точки відмови;
— масштабованість;
— підвищена надійність передачі даних;
— можливість автономної роботи вузлів;
— гнучкість конфігурації мережі.

Для IoT-систем моніторингу інфраструктури децентралізований підхід має особливе значення, оскільки дозволяє забезпечити безперервний контроль навіть у випадку часткової втрати зв’язку або пошкодження окремих елементів мережі. Це є критично важливим для систем, які функціонують у складних умовах або на великій території.

Однією з поширених форм децентралізованих мереж є mesh-мережі. У таких мережах вузли можуть передавати дані один через одного, формуючи багатохопові маршрути передачі інформації. Це дозволяє забезпечити гнучку маршрутизацію та автоматичне переналаштування мережі у випадку виходу з ладу окремих вузлів. [5, 12]

Для підвищення ефективності децентралізованих IoT-систем використовуються концепції edge computing та fog computing. [5, 7, 11] Частина обчислень виконується безпосередньо на периферійних вузлах мережі або локальних серверах, що дозволяє зменшити затримки передачі даних та скоротити навантаження на мережеву інфраструктуру.

Важливим напрямом розвитку децентралізованих мереж є інтеграція технологій блокчейн та розподіленого реєстру (DLT). [2–4] Такі технології дозволяють забезпечити цілісність даних, автентифікацію вузлів та захист інформації від несанкціонованого втручання. У децентралізованих IoT-системах блокчейн може використовуватись для зберігання журналів подій, підтвердження достовірності даних та організації безпечної взаємодії між вузлами мережі. [2, 3]

Попри значні переваги, децентралізовані мережі також мають певні недоліки. До них належать:

— складність реалізації та адміністрування;
— підвищені вимоги до алгоритмів маршрутизації;
— складність синхронізації даних;
— додаткові обчислювальні витрати;
— необхідність забезпечення узгодженості між вузлами мережі.

Порівняльний аналіз показує, що централізовані мережі є ефективними для невеликих систем із відносно стабільною інфраструктурою та невисокими вимогами до відмовостійкості. У той же час децентралізовані мережі краще підходять для великих розподілених систем моніторингу, де важливими є автономність, масштабованість та стійкість до відмов. [1, 5]

Таким чином, децентралізований підхід є перспективним напрямом розвитку сучасних IoT-систем моніторингу інфраструктури. Використання розподілених архітектур, mesh-мереж, edge/fog computing та технологій блокчейн дозволяє створювати надійні системи з високим рівнем автономності та кіберстійкості, здатні ефективно функціонувати в умовах часткової втрати зв’язку або пошкодження окремих вузлів мережі. [2–5]

1.4. Використання блокчейн і DLT у IoT

Стрімкий розвиток технологій Інтернету речей (IoT) супроводжується збільшенням кількості підключених пристроїв, обсягів переданих даних та складності мережевої взаємодії. Разом із цим зростає актуальність проблем, пов’язаних із безпекою, конфіденційністю, цілісністю інформації та забезпеченням надійності функціонування IoT-систем. Традиційні централізовані архітектури часто не здатні повною мірою забезпечити необхідний рівень захисту даних і стійкості до відмов, особливо у системах моніторингу критичної інфраструктури. Одним із перспективних напрямів вирішення цих проблем є використання технологій блокчейн та розподіленого реєстру (Distributed Ledger Technology, DLT). [2–4]

Технологія блокчейн являє собою розподілену базу даних, у якій інформація зберігається у вигляді послідовності блоків, пов’язаних між собою криптографічними методами. [2, 4] Кожен блок містить набір записів, часову мітку та криптографічний хеш попереднього блоку. Такий підхід забезпечує неможливість непомітної зміни або видалення інформації без порушення цілісності всього ланцюга.

Основною особливістю блокчейн є децентралізований принцип функціонування. Дані зберігаються одночасно на багатьох вузлах мережі, а підтвердження змін виконується за допомогою механізмів консенсусу. Відсутність єдиного центру керування дозволяє зменшити ризики відмови системи та підвищити її стійкість до зовнішніх атак. [2, 3, 4]

У системах IoT технології блокчейн і DLT можуть використовуватися для:

— забезпечення цілісності даних;
— автентифікації пристроїв;
— захисту від несанкціонованого доступу;
— організації безпечного обміну інформацією;
— зберігання журналів подій;
— автоматизації взаємодії між вузлами мережі.

Однією з основних проблем IoT-систем є обмежений рівень безпеки сенсорних пристроїв. Багато IoT-вузлів мають обмежені обчислювальні ресурси та спрощені механізми захисту, що робить їх вразливими до кібератак. [15] Використання централізованих серверів також створює ризик компрометації всієї системи у випадку успішної атаки на центральний вузол.

Технології блокчейн дозволяють підвищити рівень безпеки за рахунок розподіленого зберігання інформації та криптографічного підтвердження транзакцій. [2] Кожен вузол мережі може перевіряти достовірність отриманих даних, що ускладнює можливість підробки інформації або внесення несанкціонованих змін.

Для систем моніторингу інфраструктури це має особливе значення, оскільки достовірність даних безпосередньо впливає на ефективність виявлення пошкоджень та прийняття рішень. [15] Наприклад, підробка або втрата інформації про технічний стан мосту, трубопроводу чи енергетичного об’єкта може призвести до аварійних ситуацій та значних матеріальних збитків. [15]

Одним із важливих напрямів використання блокчейн у IoT є організація децентралізованої взаємодії між вузлами мережі. У традиційних системах IoT передача даних зазвичай здійснюється через центральний сервер або хмарну платформу. У децентралізованих системах вузли можуть взаємодіяти між собою безпосередньо, використовуючи механізми peer-to-peer (P2P). [1, 5] Це дозволяє забезпечити автономність роботи мережі та зменшити залежність від централізованої інфраструктури.

У наукових дослідженнях останніх років значна увага приділяється інтеграції блокчейн із концепціями edge computing та fog computing. У таких системах частина обробки інформації виконується на периферійних вузлах мережі, а блокчейн використовується для координації взаємодії між вузлами та захисту даних. [7, 11]

У роботі Dorri та співавторів розглянуто застосування блокчейн для забезпечення безпеки та конфіденційності IoT-систем на прикладі «розумного будинку». Автори запропонували децентралізовану модель керування пристроями, яка дозволяє зменшити залежність від хмарних сервісів та підвищити рівень захисту даних. Дослідження демонструє перспективність використання блокчейн у системах із великою кількістю взаємодіючих IoT-пристроїв. [2]

Компанія Huawei також досліджує можливості застосування блокчейн у системах управління IoT-мережами. У концепції Decentralized IoT Management on Blockchain пропонується використання розподіленого реєстру для керування пристроями, автентифікації вузлів та захисту інформації. [3] Такий підхід дозволяє створювати більш стійкі та масштабовані IoT-системи.

Важливу роль у розвитку децентралізованих IoT-систем відіграє концепція fog computing, запропонована в межах проєкту OpenFog. Відповідно до OpenFog Reference Architecture, обробка даних виконується на проміжних вузлах між сенсорами та хмарною інфраструктурою. [5] Це дозволяє зменшити затримки передачі даних, скоротити навантаження на мережу та забезпечити автономність функціонування окремих сегментів системи.

Попри значні переваги, використання блокчейн у IoT-системах супроводжується певними труднощами. Основними проблемами є:

— високе енергоспоживання окремих механізмів консенсусу;
— обмежена продуктивність блокчейн-мереж;
— затримки підтвердження транзакцій;
— додаткові вимоги до обчислювальних ресурсів;
— складність інтеграції з малопотужними IoT-пристроями.

Для вирішення цих проблем досліджуються альтернативні механізми консенсусу, адаптовані для IoT-середовищ, зокрема Proof-of-Authority, Delegated Proof-of-Stake та інші енергоефективні алгоритми. [2, 4] Також розробляються гібридні архітектури, у яких блокчейн використовується лише для критично важливих операцій, тоді як основна обробка даних виконується периферійними вузлами мережі. [1, 11]

Таким чином, технології блокчейн та DLT є перспективним напрямом розвитку сучасних IoT-систем моніторингу інфраструктури. Їх використання дозволяє підвищити рівень безпеки, забезпечити цілісність даних, реалізувати децентралізовану взаємодію між вузлами та підвищити стійкість систем до відмов і кіберзагроз. Поєднання IoT, edge/fog computing та технологій розподіленого реєстру створює основу для побудови надійних систем моніторингу критичної інфраструктури нового покоління. [1–5]

1.5. Аналіз сучасних бездротових технологій

Ефективність функціонування IoT-систем моніторингу інфраструктури значною мірою залежить від технологій передачі даних, які використовуються для взаємодії між сенсорними вузлами, периферійними пристроями та центрами обробки інформації. Для систем моніторингу критичної інфраструктури особливе значення мають надійність зв'язку, енергоефективність, дальність передачі даних, масштабованість мережі та здатність функціонувати в умовах часткової втрати зв'язку. [9, 13]

Сучасні IoT-системи використовують різні бездротові технології залежно від вимог до швидкості передачі даних, енергоспоживання, покриття мережі та умов експлуатації. Найбільш поширеними технологіями для побудови систем моніторингу є LoRaWAN, NB-IoT, ZigBee, Wi-Fi, Bluetooth Low Energy (BLE), а також мобільні мережі 4G та 5G. [9, 12]

Однією з найбільш перспективних технологій для систем моніторингу інфраструктури є LoRaWAN (Long Range Wide Area Network). Дана технологія належить до класу LPWAN (Low Power Wide Area Network) та призначена для передачі невеликих обсягів даних на великі відстані при мінімальному енергоспоживанні. [13]

Основними перевагами LoRaWAN є:

— велика дальність передачі даних;
— низьке енергоспоживання;
— можливість автономної роботи сенсорів протягом декількох років;
— підтримка великої кількості пристроїв;
— відносно невисока вартість розгортання мережі.

У міських умовах дальність передачі даних у мережах LoRaWAN може досягати 2–5 км, а на відкритій місцевості — понад 10 км. Завдяки цьому технологія ефективно використовується для моніторингу інфраструктурних об'єктів, розташованих на великій території.

Проте LoRaWAN має і певні обмеження:

— невисока швидкість передачі даних;

— обмежений розмір пакетів;
— підвищені затримки передачі;
— залежність від щільності розміщення шлюзів.

Через це LoRaWAN найбільш ефективна для систем, у яких передаються невеликі обсяги телеметричної інформації з невисокою частотою оновлення.

Іншою важливою технологією є NB-IoT (Narrowband Internet of Things), яка базується на інфраструктурі мобільних операторів. NB-IoT також належить до LPWAN-технологій та орієнтована на підключення великої кількості IoT-пристроїв із низьким енергоспоживанням. [9, 13]

До основних переваг NB-IoT належать:

— використання існуючої мобільної інфраструктури;
— висока зона покриття;
— хороша проникність сигналу всередині будівель;
— підтримка великої кількості пристроїв;
— підвищений рівень безпеки.

NB-IoT забезпечує більш стабільний зв’язок у порівнянні з деякими іншими LPWAN-технологіями, особливо в умовах щільної міської забудови. Завдяки використанню ліцензованих частот технологія має менший рівень перешкод та вищу надійність передачі даних.

Недоліками NB-IoT є:

— залежність від мобільних операторів;
— обмежена автономність у разі пошкодження мобільної інфраструктури;
— вища затримка передачі даних порівняно з 4G/5G;
— потреба у використанні SIM-карт або операторських модулів.

Для систем моніторингу, які потребують передачі великих обсягів даних або роботи у режимі реального часу, використовуються мобільні мережі 4G та 5G. Технології четвертого та п’ятого покоління забезпечують високу швидкість передачі інформації, низькі затримки та підтримку великої кількості підключених пристроїв. [6, 9]

Перевагами 4G/5G є:

— висока пропускна здатність;
— підтримка потокової передачі даних;
— мінімальні затримки;
— можливість інтеграції з хмарними сервісами;
— підтримка систем реального часу.

Мережі 5G додатково забезпечують підтримку масових IoT-підключень, мережеву сегментацію (network slicing) та наднизькі затримки передачі даних. Це створює перспективи для використання 5G у системах моніторингу критичної інфраструктури, автономному транспорті та системах швидкого реагування. [6, 9]

Разом із тим використання 4G/5G має певні обмеження:

— високе енергоспоживання;
— залежність від мобільної інфраструктури;
— необхідність щільного покриття базовими станціями;
— вища вартість обладнання та обслуговування.

Для локальних IoT-систем також використовуються технології ZigBee та Bluetooth Low Energy. ZigBee характеризується низьким енергоспоживанням і підтримкою mesh-мереж, що дозволяє вузлам передавати дані один через одного. [12] Це забезпечує гнучкість побудови розподілених мереж та підвищує їх відмовостійкість.

Bluetooth Low Energy використовується переважно для короткодистанційної передачі даних між пристроями з мінімальним енергоспоживанням. Проте обмежена дальність зв’язку не дозволяє ефективно використовувати BLE у великих системах моніторингу інфраструктури. [9]

Окрему увагу слід приділити mesh-мережам, які є одним із ключових елементів децентралізованих IoT-систем. У mesh-мережах кожен вузол може виконувати функції ретранслятора та передавати дані між іншими пристроями. Це дозволяє:

— забезпечити багатохопову передачу інформації;
— підвищити надійність зв’язку;
— автоматично переналаштовувати маршрути передачі даних;
— забезпечити автономність окремих сегментів мережі.

Mesh-архітектура є особливо ефективною у системах моніторингу, де важлива стійкість до пошкодження окремих вузлів або втрати зв’язку з центральним сервером.

Вибір бездротової технології залежить від особливостей конкретної системи моніторингу. Для великомасштабних систем із невеликим обсягом телеметричних даних доцільним є використання LoRaWAN або NB-IoT. Для систем реального часу з високими вимогами до швидкості передачі даних ефективнішими є 4G та 5G. Для локальних децентралізованих мереж перспективним є використання ZigBee та mesh-архітектур.

У сучасних IoT-системах дедалі частіше використовуються комбіновані підходи, коли одночасно застосовуються декілька технологій передачі даних. Наприклад, LoRaWAN може використовуватись для енергоефективного збору телеметрії, а 4G/5G — для передачі агрегованих даних до хмарної інфраструктури або центрів обробки інформації.

Таким чином, сучасні бездротові технології передачі даних створюють основу для побудови ефективних IoT-систем моніторингу інфраструктури. Поєднання LPWAN-технологій, мобільних мереж, mesh-архітектур та децентралізованих підходів дозволяє забезпечити надійний зв’язок, масштабованість, енергоефективність та високу відмовостійкість систем моніторингу пошкоджень інфраструктури

1.6. Постановка задачі дослідження

Сучасний розвиток інформаційно-комунікаційних технологій та поширення концепції Інтернету речей (IoT) створюють нові можливості для побудови систем моніторингу технічного стану інфраструктурних об’єктів. Використання сенсорних мереж, бездротових технологій передачі даних,

edge/fog computing та розподілених обчислень дозволяє забезпечити безперервний контроль стану інженерних споруд, транспортної інфраструктури, енергетичних об’єктів та інших критично важливих систем. [5, 7, 11]

Разом із цим аналіз сучасних IoT-систем показує, що більшість існуючих рішень побудовані за централізованою архітектурою, у якій основна обробка та зберігання даних здійснюються на центральному сервері або у хмарній інфраструктурі. Такий підхід має низку суттєвих недоліків, серед яких:

— наявність єдиної точки відмови;
— залежність від стабільного мережевого з’єднання;
— обмежена відмовостійкість;
— складність масштабування;
— підвищені ризики кіберзагроз;
— значне навантаження на центральні вузли системи.

Для систем моніторингу критичної інфраструктури зазначені недоліки є особливо небезпечними, оскільки втрата зв’язку або пошкодження центрального вузла можуть призвести до втрати важливої інформації та неможливості оперативного реагування на аварійні ситуації.

Додатковою проблемою є необхідність функціонування систем моніторингу в умовах нестабільної мережевої інфраструктури, значної територіальної розподіленості об’єктів та можливих пошкоджень елементів мережі. У таких умовах централізовані підходи не завжди забезпечують необхідний рівень надійності та автономності.

Перспективним напрямом вирішення зазначених проблем є використання децентралізованих IoT-мереж, у яких функції передачі, обробки та зберігання даних розподіляються між вузлами системи. Такий підхід дозволяє забезпечити:

— підвищення відмовостійкості;
— автономність окремих сегментів мережі;

— зменшення навантаження на центральні вузли;
— стійкість до втрати зв’язку;
— покращення масштабованості системи;
— підвищення рівня кібербезпеки. [1, 5]

Важливу роль у побудові децентралізованих IoT-систем відіграють mesh-мережі, edge/fog computing та технології блокчейн і розподіленого реєстру (DLT). [1–5, 11] Їх використання дозволяє реалізувати розподілену взаємодію між вузлами, локальну обробку даних та захист інформації від несанкціонованого втручання.

Аналіз сучасних наукових досліджень показує, що питання інтеграції децентралізованих підходів у системи моніторингу інфраструктури залишаються недостатньо дослідженими. Значна частина існуючих рішень орієнтована на окремі аспекти функціонування IoT-систем, зокрема передачу даних, енергоефективність або безпеку, проте комплексний підхід до побудови відмовостійкої децентралізованої системи моніторингу потребує подальших досліджень. [1, 11, 13]

У зв’язку з цим актуальною є задача розробки архітектури децентралізованої IoT-мережі для моніторингу пошкоджень інфраструктури, яка забезпечуватиме:

— безперервний збір і передачу даних;
— автономне функціонування вузлів;
— стійкість до відмов окремих елементів мережі;
— захист інформації;
— ефективне використання мережевих ресурсів;
— можливість масштабування системи.

Метою даного дослідження є розробка та обґрунтування архітектури децентралізованої IoT-мережі для моніторингу пошкоджень інфраструктури з підвищеним рівнем надійності, відмовостійкості та кіберстійкості.

Для досягнення поставленої мети необхідно вирішити такі основні задачі:

- провести аналіз сучасних IoT-технологій та методів моніторингу інфраструктури;
- дослідити принципи функціонування централізованих і децентралізованих мереж;
- проаналізувати сучасні бездротові технології передачі даних;
- дослідити можливості використання блокчейн і DLT у IoT-системах;
- обґрунтувати вибір архітектури децентралізованої IoT-мережі;
- розробити модель взаємодії вузлів мережі;
- визначити підходи до забезпечення відмовостійкості та захисту інформації;
- оцінити ефективність запропонованих рішень.

Об’єктом дослідження є процеси моніторингу технічного стану об’єктів інфраструктури із використанням децентралізованих IoT-мереж.

Предметом дослідження є методи, архітектури та технології побудови децентралізованих IoT-мереж для збору, передачі та обробки даних під час моніторингу пошкоджень інфраструктури.

Практична цінність роботи полягає у можливості використання запропонованих підходів для створення сучасних систем моніторингу критичної інфраструктури, здатних ефективно функціонувати в умовах нестабільного зв’язку, високого навантаження та часткової втрати елементів мережі. Отримані результати можуть бути використані під час проєктування систем «розумного міста», транспортної, енергетичної та промислової інфраструктури. [10]

Таким чином, дослідження децентралізованих IoT-мереж для моніторингу пошкоджень інфраструктури є актуальним напрямом розвитку сучасних телекомунікаційних систем та має важливе практичне значення для підвищення надійності й безпеки критично важливих об’єктів.

Висновки

У першому розділі дипломної роботи проведено аналіз сучасного стану розвитку технологій Інтернету речей та їх застосування у системах моніторингу інфраструктури. Розглянуто основні принципи функціонування IoT-систем, структуру сенсорних мереж та особливості передачі даних у розподілених середовищах.

Проведено аналіз сучасних методів моніторингу інфраструктурних об’єктів та визначено основні недоліки традиційних централізованих систем, серед яких залежність від центрального вузла, обмежена відмовостійкість та складність масштабування. Встановлено, що для критичної інфраструктури особливо важливими є безперервність функціонування, автономність вузлів та стійкість до пошкодження окремих елементів мережі.

У роботі розглянуто централізовані та децентралізовані архітектури IoT-мереж. Визначено, що децентралізований підхід забезпечує підвищення надійності, масштабованості та кіберстійкості систем моніторингу. Досліджено можливості використання технологій блокчейн і розподіленого реєстру для захисту даних та організації безпечної взаємодії між вузлами мережі.

Також проведено аналіз сучасних бездротових технологій передачі даних, зокрема LoRaWAN, NB-IoT, ZigBee та мобільних мереж 4G/5G. Визначено їх переваги, недоліки та доцільність використання у системах моніторингу пошкоджень інфраструктури.

За результатами аналізу сформульовано постановку задачі дослідження та визначено основні напрями побудови децентралізованої IoT-мережі для моніторингу інфраструктурних об’єктів із підвищеною відмовостійкістю, автономністю та захистом даних.

РОЗДІЛ 2
РОЗРОБКА АРХІТЕКТУРИ ДЕЦЕНТРАЛІЗОВАНОЇ IoT-МЕРЕЖІ ДЛЯ МОНІТОРИНГУ ПОШКОДЖЕНЬ ІНФРАСТРУКТУРИ

2.1. Вимоги до системи моніторингу

У першому розділі було проаналізовано сучасні підходи до побудови IoT-систем моніторингу інфраструктури, визначено основні переваги децентралізованих мереж та розглянуто сучасні технології передачі даних. На основі проведеного аналізу у даному розділі виконується обґрунтування архітектури децентралізованої IoT-мережі для моніторингу пошкоджень інфраструктури.

Основною метою розроблюваної системи є забезпечення безперервного контролю технічного стану інфраструктурних об’єктів, оперативного виявлення пошкоджень та передачі інформації навіть у випадку часткової втрати зв’язку або виходу з ладу окремих вузлів мережі. Для досягнення цієї мети архітектура системи повинна відповідати таким вимогам:

- висока відмовостійкість;
- автономність функціонування вузлів;
- масштабованість;
- енергоефективність;
- можливість роботи у реальному часі;
- захищеність даних;
- підтримка розподіленої обробки інформації.

Традиційні централізовані IoT-системи мають обмеження, пов’язані з використанням центрального сервера для обробки та зберігання даних. У разі перевантаження або пошкодження центрального вузла система може частково або повністю втратити працездатність. Для систем моніторингу критичної інфраструктури така ситуація є неприпустимою, оскільки може призвести до втрати інформації про аварійні або небезпечні стани об’єктів.

З метою усунення зазначених недоліків у роботі пропонується використання децентралізованої архітектури, у якій функції передачі, зберігання та обробки даних розподіляються між вузлами мережі. Такий підхід забезпечує більш високу стійкість системи до відмов та дозволяє окремим сегментам мережі функціонувати автономно.

Запропонована архітектура складається з таких основних рівнів:

— сенсорний рівень;
— рівень периферійної обробки даних (edge/fog);
— мережевий рівень;
— рівень розподіленого зберігання та аналітики;
— прикладний рівень.

Сенсорний рівень включає набір IoT-пристроїв та датчиків, розташованих безпосередньо на об’єктах інфраструктури. Для моніторингу технічного стану можуть використовуватися:

— датчики вібрації;
— датчики деформації;
— температурні сенсори;
— датчики вологості;
— акселерометри;
— сенсори тиску;
— газоаналізатори.

Сенсорні вузли виконують первинний збір інформації та її попередню обробку. Для зменшення навантаження на мережу частина даних може фільтруватися або агрегуватися безпосередньо на рівні сенсорних пристроїв.

Рівень edge/fog computing забезпечує локальну обробку інформації поблизу джерел даних. На цьому рівні виконуються:

— агрегація даних;
— фільтрація шумів;
— виявлення аномалій;
— локальне зберігання інформації;

— передача критично важливих повідомлень.

Використання edge/fog computing дозволяє суттєво зменшити затримки передачі даних та забезпечити автономне функціонування окремих сегментів мережі у випадку втрати зв’язку з центральною інфраструктурою.

Для організації мережевої взаємодії у системі доцільним є використання комбінованого підходу, який поєднує технології LoRaWAN, mesh-мережі та мобільні мережі 4G/5G. [6, 8, 9, 13].

Технологія LoRaWAN використовується для енергоефективної передачі телеметричних даних від сенсорних вузлів на великі відстані. Вона забезпечує низьке енергоспоживання та підтримку великої кількості пристроїв.

Mesh-мережа дозволяє вузлам взаємодіяти між собою безпосередньо та передавати дані багатохоповими маршрутами. Це забезпечує:

— автоматичне переналаштування маршрутів;

— підвищення надійності зв’язку;

— автономність окремих сегментів мережі;

— збереження працездатності системи при пошкодженні вузлів.

Мережі 4G/5G можуть використовуватися для передачі агрегованих даних між локальними вузлами та центрами обробки інформації або хмарними сервісами. Висока швидкість передачі даних дозволяє забезпечити оперативний обмін інформацією між елементами системи.

Для підвищення рівня безпеки та забезпечення цілісності інформації у системі передбачається використання технологій блокчейн та розподіленого реєстру (DLT). [2–4] Блокчейн використовується для:

— реєстрації критичних подій;

— підтвердження достовірності даних;

— автентифікації вузлів;

— захисту журналів подій від змін.

Застосування блокчейн дозволяє забезпечити прозорість взаємодії між вузлами та зменшити ризики несанкціонованого втручання у роботу системи.

У запропонованій архітектурі важливу роль відіграє принцип розподіленої обробки даних. Кожен вузол мережі може виконувати частину функцій системи, що дозволяє зменшити залежність від окремих елементів та забезпечити масштабованість мережі.

Для підвищення енергоефективності системи передбачається використання режимів низького енергоспоживання сенсорних вузлів, адаптивної передачі даних та локальної обробки інформації. Це дозволяє збільшити тривалість автономної роботи пристроїв та зменшити навантаження на канали зв’язку.

Таким чином, запропонована децентралізована архітектура IoT-мережі забезпечує:

- безперервний моніторинг інфраструктури;
- високу відмовостійкість;
- автономність роботи вузлів;
- масштабованість системи;
- захист даних;
- ефективне використання мережевих ресурсів.

Поєднання mesh-мереж, edge/fog computing, LPWAN-технологій та блокчейн створює основу для побудови сучасної системи моніторингу пошкоджень інфраструктури, здатної функціонувати в умовах нестабільного зв’язку, високого навантаження та часткового пошкодження мережевої інфраструктури.

2.2. Загальна архітектура системи

Одним із ключових етапів проєктування децентралізованої IoT-мережі є розробка структури системи та моделі взаємодії між її вузлами. Від організації обміну даними, способу маршрутизації повідомлень та принципів функціонування окремих елементів залежить надійність, масштабованість і відмовостійкість усієї системи моніторингу.

Основною задачею розроблюваної мережі є забезпечення безперервного збору та передачі інформації про технічний стан інфраструктурних об’єктів навіть в умовах часткової втрати зв’язку або пошкодження окремих вузлів. Для цього у роботі пропонується використання багаторівневої децентралізованої архітектури з елементами mesh-взаємодії та розподіленої обробки даних.

Запропонована структура мережі включає такі основні типи вузлів:

— сенсорні вузли;
— маршрутизуючі вузли;
— edge/fog-вузли;
— шлюзи передачі даних;
— сервери аналітики та зберігання інформації.

Сенсорні вузли є базовими елементами системи та встановлюються безпосередньо на об’єктах інфраструктури. [1, 10] Вони здійснюють вимірювання фізичних параметрів та первинний збір інформації. Залежно від типу контрольованого об’єкта сенсорний вузол може містити:

— датчики вібрації;
— акселерометри;
— датчики температури;
— сенсори вологості;
— датчики деформації;
— сенсори тиску;
— модулі геолокації.

Основними функціями сенсорного вузла є:

— збір даних;
— попередня фільтрація інформації;
— локальна обробка;
— передача даних іншим вузлам мережі;
— підтримка енергоефективного режиму роботи.

Оскільки сенсорні пристрої мають обмежені енергетичні та обчислювальні ресурси, у системі використовується принцип адаптивної передачі даних. Передача інформації виконується лише при зміні контрольованих параметрів або виникненні аномальних ситуацій. Це дозволяє суттєво зменшити енергоспоживання та навантаження на мережу.

Маршрутизуючі вузли виконують функції проміжної передачі інформації між сенсорними вузлами та іншими елементами мережі. У mesh-архітектурі кожен вузол може виступати як ретранслятор для інших пристроїв, забезпечуючи багатохопову передачу даних. [5, 12]

Використання mesh-топології дозволяє:

— підвищити надійність передачі інформації;
— автоматично переналаштовувати маршрути;
— забезпечити роботу мережі при пошкодженні окремих вузлів;
— збільшити площу покриття без значного підвищення потужності передавачів.

У запропонованій моделі маршрутизація виконується динамічно залежно від доступності вузлів та якості каналів зв’язку. [5, 12] У разі втрати одного з маршрутів система автоматично обирає альтернативний шлях передачі даних.

Важливим елементом архітектури є edge/fog-вузли, які виконують локальну обробку та агрегацію інформації. [7, 11] Такі вузли мають більші обчислювальні ресурси порівняно із сенсорними пристроями та можуть виконувати:

— аналіз телеметричних даних;
— виявлення аномалій;
— локальне зберігання інформації;
— обробку аварійних повідомлень;
— координацію роботи локального сегмента мережі.

Використання edge/fog computing дозволяє зменшити затримки передачі даних та скоротити навантаження на центральну інфраструктуру. [5]

Крім того, локальні вузли можуть продовжувати функціонування навіть у випадку втрати зв’язку із зовнішніми серверами.

Для передачі інформації між локальними сегментами мережі та центрами обробки даних використовуються шлюзи. [6, 9, 13] Вони забезпечують взаємодію між різними технологіями зв’язку, зокрема:

— LoRaWAN;
— ZigBee;
— Wi-Fi;
— Ethernet;
— 4G/5G.

Шлюзи виконують:

— конвертацію протоколів передачі даних;
— шифрування інформації;
— маршрутизацію повідомлень;
— синхронізацію даних між сегментами мережі.

У роботі передбачається використання комбінованої системи зв’язку. Для передачі телеметричних даних від сенсорів використовується LoRaWAN або mesh-мережа з низьким енергоспоживанням. Для передачі агрегованих даних до зовнішніх серверів можуть використовуватись мережі 4G/5G або дротові канали зв’язку.

З метою забезпечення безпеки інформації у системі використовується багаторівневий механізм захисту даних. Передача інформації між вузлами виконується із використанням криптографічного шифрування та механізмів автентифікації.

Для реєстрації критично важливих подій та перевірки цілісності інформації у системі використовується технологія блокчейн. [2–4] У розподіленому реєстрі можуть зберігатися:

— записи про аварійні ситуації;
— повідомлення про пошкодження;
— журнали взаємодії вузлів;

— дані автентифікації пристроїв.

Використання блокчейн дозволяє забезпечити:

— незмінність критичних даних;

— захист журналів подій;

— прозорість взаємодії між вузлами;

— стійкість до несанкціонованого втручання.

Для оцінки ефективності роботи мережі у роботі враховуються такі основні параметри:

— затримка передачі даних;

— пропускна здатність;

— рівень втрати пакетів;

— енергоспоживання вузлів;

— час автономної роботи;

— відмовостійкість мережі.

Одним із важливих критеріїв ефективності є здатність системи функціонувати при частковому пошкодженні мережевої інфраструктури. У децентралізованій архітектурі відмова окремих вузлів не повинна призводити до повної втрати працездатності системи. Для цього реалізуються механізми резервування маршрутів та автоматичного переналаштування мережі.

Таким чином, розроблена структура децентралізованої IoT-мережі забезпечує ефективний збір, передачу та обробку інформації для моніторингу пошкоджень інфраструктури. Поєднання mesh-топології, edge/fog computing, LPWAN-технологій та блокчейн дозволяє створити надійну систему з високим рівнем автономності, масштабованості та стійкості до відмов.

2.3. Вибір технологій передачі даних

Ефективність функціонування децентралізованої IoT-мережі значною мірою залежить від правильного вибору технологій та протоколів передачі даних. Для систем моніторингу пошкоджень інфраструктури важливими є такі характеристики мережі, як надійність зв’язку, енергоефективність,

затримка передачі інформації, масштабованість та можливість функціонування в умовах нестабільної інфраструктури зв’язку.

У процесі проєктування системи необхідно враховувати специфіку роботи IoT-пристроїв. Сенсорні вузли зазвичай мають обмежені енергетичні ресурси, невисоку обчислювальну потужність та працюють у складних умовах експлуатації. Тому обрані технології повинні забезпечувати мінімальне енергоспоживання при достатньому рівні надійності передачі даних.

Для запропонованої системи моніторингу використовується комбінований підхід, який передбачає застосування декількох технологій зв’язку залежно від рівня мережі та типу переданої інформації.

Основною технологією для взаємодії сенсорних вузлів обрано LoRaWAN. Дана технологія належить до класу LPWAN та забезпечує передачу невеликих обсягів даних на великі відстані при низькому енергоспоживанні.

Основними причинами вибору LoRaWAN є:

— велика зона покриття;
— підтримка великої кількості пристроїв;
— низьке енергоспоживання;
— можливість автономної роботи сенсорів протягом тривалого часу;
— ефективність для передачі телеметричних даних.

У системах моніторингу інфраструктури більшість сенсорних даних має невеликий обсяг та передається періодично або при виникненні аномалій. За таких умов LoRaWAN є доцільним рішенням, оскільки дозволяє мінімізувати навантаження на батареї сенсорних вузлів та забезпечити покриття значної території. [9, 13]

Разом із тим використання лише LoRaWAN не дозволяє повністю реалізувати децентралізований принцип функціонування мережі, оскільки класична архітектура LoRaWAN передбачає наявність шлюзів та мережевих

серверів. Тому в роботі додатково використовується mesh-взаємодія між локальними вузлами.

Mesh-архітектура дозволяє вузлам мережі передавати дані один через одного, формуючи багатохопові маршрути. Це забезпечує:

— автоматичне переналаштування маршрутів передачі даних;
— підвищення відмовостійкості мережі;
— можливість функціонування при пошкодженні окремих вузлів;
— зменшення залежності від центральної інфраструктури.

Для локальної mesh-взаємодії можуть використовуватися технології ZigBee або Wi-Fi Mesh. ZigBee є більш енергоефективною технологією та підходить для взаємодії великої кількості IoT-пристроїв із невеликим обсягом переданих даних. Wi-Fi Mesh забезпечує вищу швидкість передачі інформації, проте має більше енергоспоживання.

У роботі доцільним є використання ZigBee для взаємодії сенсорних вузлів у локальних сегментах мережі, де важливо забезпечити енергоефективність та підтримку mesh-топології.

Для передачі агрегованих даних між edge/fog-вузлами та центрами обробки інформації використовуються мобільні мережі 4G/5G. Основними перевагами цих технологій є:

— висока швидкість передачі даних;
— низькі затримки;
— підтримка віддаленого доступу;
— інтеграція з хмарними сервісами;
— підтримка систем реального часу.

Мережі 5G додатково забезпечують підтримку масових IoT-підключень та можливість мережевої сегментації, що є перспективним для побудови масштабованих систем моніторингу критичної інфраструктури. [6, 13]

Важливим аспектом функціонування IoT-мережі є вибір протоколів передачі даних. Для взаємодії між вузлами мережі використовуються протоколи MQTT та CoAP. [14]

MQTT (Message Queuing Telemetry Transport) є одним із найбільш поширених протоколів у IoT-системах. Він працює за моделлю publish/subscribe та забезпечує:

— мінімальний службовий трафік;
— ефективну передачу телеметричних даних;
— підтримку великої кількості клієнтів;
— надійний механізм доставки повідомлень.

MQTT особливо ефективний у мережах із нестабільним зв’язком або обмеженою пропускною здатністю. У запропонованій системі цей протокол використовується для обміну даними між сенсорними вузлами, edge/fog-вузлами та серверною інфраструктурою. [14]

Для пристроїв із мінімальними обчислювальними ресурсами може використовуватись CoAP (Constrained Application Protocol). Даний протокол оптимізований для IoT-пристроїв із низьким енергоспоживанням та дозволяє ефективно працювати у мережах із невеликою пропускною здатністю. [14]

Для забезпечення захисту інформації використовується шифрування даних та механізми автентифікації вузлів. [15] У мережі передбачається застосування:

— TLS/SSL для захищеної передачі інформації;
— криптографічних ключів автентифікації;
— цифрових сертифікатів;
— механізмів контролю доступу.

Додатково для забезпечення цілісності критичних даних використовується технологія блокчейн. [2–4] Розподілений реєстр дозволяє зберігати журнали подій, інформацію про пошкодження та записи взаємодії між вузлами мережі. Це підвищує рівень довіри до системи та ускладнює можливість несанкціонованого втручання. [14]

У процесі вибору технологій також враховуються такі критерії:

— енергоспоживання;
— дальність передачі даних;

— пропускна здатність;
— затримка передачі;
— вартість розгортання;
— масштабованість;
— стійкість до відмов.

Порівняльний аналіз показує, що використання комбінованої архітектури дозволяє поєднати переваги різних технологій передачі даних. LoRaWAN забезпечує енергоефективний збір телеметрії на великій території, mesh-мережі підвищують автономність та відмовостійкість локальних сегментів, а 4G/5G дозволяють організувати швидкісний обмін агрегованою інформацією між вузлами системи.

Таким чином, обрані технології та протоколи передачі даних забезпечують ефективне функціонування децентралізованої IoT-мережі для моніторингу пошкоджень інфраструктури. Запропонований підхід дозволяє досягти високої надійності, енергоефективності, масштабованості та стійкості системи до пошкодження окремих елементів мережі.

2.4. Організація децентралізованої взаємодії вузлів

Для систем моніторингу критичної інфраструктури одними з найважливіших вимог є надійність функціонування, безперервність передачі даних та захист інформації від зовнішніх і внутрішніх загроз. У випадку пошкодження окремих вузлів, втрати зв’язку або кібератак система повинна зберігати працездатність та забезпечувати передачу критично важливих повідомлень.

Особливістю IoT-систем є велика кількість розподілених пристроїв, які можуть працювати у складних умовах експлуатації та мати обмежені обчислювальні ресурси. Це створює додаткові проблеми щодо забезпечення відмовостійкості та кібербезпеки мережі.

У запропонованій децентралізованій IoT-мережі забезпечення надійності роботи системи реалізується за рахунок:

— використання mesh-архітектури;
— резервування маршрутів передачі даних;
— розподіленої обробки інформації;
— локального зберігання даних;
— автономного функціонування вузлів;
— багаторівневого захисту інформації.

Однією з основних переваг децентралізованої архітектури є відсутність єдиної точки відмови. У централізованих системах пошкодження центрального сервера або каналу зв’язку може призвести до повної втрати працездатності мережі. У децентралізованій системі функції передачі та обробки інформації розподіляються між вузлами, що значно підвищує стійкість мережі до відмов.

Використання mesh-топології дозволяє вузлам взаємодіяти між собою безпосередньо та формувати альтернативні маршрути передачі даних. [8,12] Якщо один із вузлів виходить з ладу або стає недоступним, система автоматично перенаправляє трафік через інші доступні маршрути.

Основними перевагами mesh-мережі є:
— автоматичне переналаштування маршрутів;
— підтримка багатохопової передачі даних; [8, 13]
— збереження працездатності мережі при частковому пошкодженні;
— підвищення надійності зв’язку.

Для забезпечення безперервності функціонування системи використовується принцип локальної автономності вузлів. Edge/fog-вузли здатні виконувати частину обчислень без необхідності постійного підключення до центральної інфраструктури. У випадку втрати зовнішнього зв’язку локальний сегмент мережі продовжує:
— збір даних;
— аналіз інформації;
— реєстрацію подій;
— передачу аварійних повідомлень між локальними вузлами.

Після відновлення зв’язку накопичені дані синхронізуються з іншими сегментами мережі або серверною інфраструктурою.

Для підвищення відмовостійкості системи передбачається резервування критично важливих елементів мережі. Це включає:

— дублювання маршрутів передачі даних;
— резервування джерел живлення;
— використання декількох каналів зв’язку;
— збереження копій журналів подій на різних вузлах мережі.

Важливим аспектом функціонування IoT-систем є забезпечення кібербезпеки. Велика кількість підключених пристроїв створює потенційні точки для несанкціонованого доступу або атак на систему. Основними загрозами для IoT-мереж є:

— перехоплення даних;
— підробка повідомлень;
— несанкціонований доступ до вузлів;
— DDoS-атаки;
— компрометація сенсорних пристроїв;
— модифікація або видалення інформації.

Для захисту мережі у роботі використовується багаторівнева система безпеки.

На рівні передачі даних застосовується криптографічне шифрування інформації. Для захищеного обміну даними використовуються протоколи TLS/SSL, які забезпечують:

— конфіденційність інформації;
— захист від перехоплення трафіку;
— автентифікацію вузлів;
— контроль цілісності повідомлень. [15]

Для ідентифікації вузлів мережі використовуються механізми автентифікації на основі криптографічних ключів та цифрових сертифікатів.

Кожен вузол отримує унікальний ідентифікатор та набір ключів, що дозволяє перевіряти достовірність пристроїв під час обміну інформацією.

Додатковий рівень безпеки забезпечується використанням технологій блокчейн та розподіленого реєстру (DLT). [2–4] У системі блокчейн використовується для:

— реєстрації критичних подій;
— фіксації змін стану системи;
— підтвердження достовірності даних;
— захисту журналів подій від модифікації.

Оскільки записи у блокчейн неможливо змінити без порушення цілісності ланцюга, це дозволяє забезпечити високий рівень довіри до інформації, що надходить із сенсорних вузлів.

Для зменшення навантаження на IoT-пристрої у системі використовується гібридний підхід до роботи з блокчейн. Безпосередньо на сенсорних вузлах не виконується повноцінна обробка блокчейн-транзакцій. Основні функції реєстрації та перевірки записів виконуються edge/fog-вузлами, які мають більші обчислювальні ресурси.

Важливим напрямом забезпечення надійності є контроль стану вузлів мережі. У системі реалізується механізм моніторингу активності пристроїв, який дозволяє:

— визначати недоступні вузли;
— оцінювати якість каналів зв’язку;
— контролювати рівень заряду батарей;
— автоматично змінювати маршрути передачі даних.

Для мінімізації ризику втрати інформації використовується локальне кешування даних. У випадку тимчасової втрати зв’язку інформація зберігається на локальних вузлах і передається після відновлення мережевого з’єднання.

У системі також враховуються питання енергоефективності, оскільки значна частина сенсорних вузлів працює автономно. Для зменшення енергоспоживання використовуються:

— режими сну (sleep mode);
— адаптивна передача даних;
— локальна обробка інформації;
— мінімізація службового трафіку.

Таким чином, запропонований комплекс заходів забезпечує високу відмовостійкість та безпеку функціонування децентралізованої IoT-мережі. Поєднання mesh-архітектури, edge/fog computing, резервування маршрутів, криптографічного захисту та технологій блокчейн дозволяє створити надійну систему моніторингу інфраструктури, здатну ефективно функціонувати навіть у складних умовах експлуатації та часткового пошкодження мережевої інфраструктури.

2.5. Методи збору та обробки даних

Ефективність функціонування децентралізованої IoT-мережі значною мірою залежить від організації процесів збору, передачі та обробки інформації. У системах моніторингу пошкоджень інфраструктури сенсорні вузли постійно генерують великі обсяги телеметричних даних, які необхідно оперативно аналізувати для виявлення аварійних ситуацій та потенційних дефектів. Тому важливими складовими системи є механізми агрегації, фільтрації, локальної обробки та аналітики даних.

У запропонованій системі збір інформації здійснюється за допомогою сенсорних вузлів, обладнаних датчиками температури, деформації, вібрації, тиску та вологості. Дані передаються через бездротові канали зв’язку до edge/fog-вузлів, де виконується первинна обробка інформації.

Агрегація даних

У процесі функціонування IoT-мережі велика кількість сенсорів генерує значний обсяг службової та телеметричної інформації. Без

попередньої агрегації це може призвести до перевантаження каналів зв’язку та підвищення енергоспоживання пристроїв.

Агрегація даних передбачає об’єднання інформації від декількох сенсорних вузлів у компактні пакети перед передачею до інших сегментів мережі. [1] Основними задачами агрегації є:

— зменшення обсягу переданих даних;
— зниження навантаження на канали зв’язку;
— оптимізація використання енергетичних ресурсів;
— скорочення кількості дубльованої інформації.

Edge/fog-вузли виконують попереднє групування інформації, формують узагальнені пакети телеметрії та передають лише критично важливі або змінені параметри.

Фільтрація даних

Сенсорні пристрої можуть генерувати шумові або помилкові значення, пов’язані з нестабільністю середовища, перешкодами або похибками вимірювання. Для підвищення достовірності інформації використовується фільтрація даних.

У системі застосовуються:

— порогова фільтрація;
— усереднення значень;
— видалення аномальних показників;
— фільтрація дубльованих повідомлень. [10]

Порогова фільтрація дозволяє передавати дані лише при перевищенні встановлених критичних значень. Це суттєво зменшує навантаження на мережу та скорочує кількість службового трафіку. [8, 10]

Edge Computing

Одним із ключових елементів запропонованої архітектури є використання технології edge computing. Даний підхід передбачає виконання частини обчислень безпосередньо поблизу джерела даних, а не у віддалених дата-центрах. [5, 7, 11]

Edge-вузли виконують:

— первинну обробку телеметрії;
— локальний аналіз даних;
— виявлення аномалій;
— формування аварійних повідомлень;
— кешування інформації.

Використання edge computing дозволяє:

— зменшити затримки передачі інформації;
— скоротити навантаження на центральні сервери;
— підвищити автономність системи;
— забезпечити функціонування при частковій втраті зв’язку.

Локальна аналітика

Для оперативного виявлення пошкоджень у системі використовується локальна аналітика даних. Edge/fog-вузли виконують аналіз телеметрії без необхідності постійної передачі інформації до хмарної інфраструктури.

Локальна аналітика включає:

— аналіз трендів зміни параметрів;
— виявлення різких змін показників;
— визначення аномальних режимів роботи;
— прогнозування потенційних пошкоджень. [11]

У випадку виявлення критичних відхилень система автоматично формує тривожне повідомлення та передає його іншим вузлам мережі або оператору системи.

Таким чином, використання агрегації, фільтрації, edge computing та локальної аналітики дозволяє підвищити ефективність функціонування децентралізованої IoT-мережі, зменшити затримки передачі інформації та забезпечити оперативне реагування на пошкодження інфраструктури. [1, 11]

2.6. Забезпечення безпеки системи

Однією з основних вимог до систем моніторингу критичної інфраструктури є забезпечення високого рівня інформаційної безпеки. Децентралізовані IoT-мережі функціонують у середовищі з великою кількістю підключених пристроїв, що створює потенційні ризики несанкціонованого доступу, втрати даних або кібератак.

У запропонованій системі безпека реалізується шляхом використання криптографічного захисту, механізмів автентифікації та технологій blockchain.

Blockchain

Для забезпечення цілісності даних та захисту журналів подій використовується технологія blockchain. [2–4] Розподілений реєстр дозволяє зберігати записи про події мережі у незмінному вигляді.

Blockchain забезпечує:

— захист від модифікації даних;
— контроль цілісності інформації;
— прозорість обміну повідомленнями;
— підвищення рівня довіри між вузлами мережі.

У системі blockchain використовується для реєстрації:

— аварійних подій;
— змін стану вузлів;
— критичних повідомлень;
— журналів взаємодії між пристроями.

Шифрування

Для захисту інформації під час передачі даних використовується криптографічне шифрування. [15] Передача інформації між вузлами мережі здійснюється через захищені канали зв’язку.

У системі застосовуються:

— TLS/SSL;

— симетричне шифрування;
— криптографічні ключі доступу.

Шифрування дозволяє запобігти:

— перехопленню інформації;
— зміні даних під час передачі;
— несанкціонованому доступу до мережі.

Автентифікація

Для контролю доступу до мережі використовується механізм автентифікації вузлів. [2, 15] Кожен пристрій отримує унікальний ідентифікатор та набір криптографічних ключів.

Автентифікація забезпечує:

— перевірку справжності вузлів;
— контроль підключення нових пристроїв;
— захист від підроблених повідомлень;
— обмеження доступу до критичних ресурсів системи.

Захист від втрати даних

Для забезпечення надійності функціонування мережі використовується система резервування та локального зберігання інформації. [5,11]

У системі реалізовано:

— локальне кешування даних;
— дублювання маршрутів передачі;
— резервне копіювання журналів подій;
— повторну передачу пакетів при втраті зв’язку.

У випадку тимчасової недоступності мережі дані зберігаються на edge/fog-вузлах та передаються після відновлення з’єднання.

Таким чином, комплексне використання blockchain, криптографічного захисту, механізмів автентифікації та резервування даних дозволяє забезпечити високий рівень безпеки децентралізованої IoT-мережі.

2.7. Опис алгоритму роботи системи

Алгоритм роботи запропонованої системи моніторингу пошкоджень інфраструктури базується на безперервному зборі, аналізі та передачі телеметричних даних між вузлами децентралізованої IoT-мережі.

На першому етапі сенсорні вузли здійснюють вимірювання параметрів стану інфраструктурного об’єкта. Датчики контролюють температуру, рівень вібрації, деформації, вологість та інші показники.

Після збору інформації дані проходять локальну фільтрацію та первинну обробку. Некритичні або дубльовані повідомлення відсіюються, а агрегована інформація передається до edge/fog-вузлів.

Для забезпечення безперервності функціонування мережі використовується багатохопова маршрутизація. [8,12] Якщо один із вузлів стає недоступним, система автоматично перенаправляє трафік альтернативним маршрутом.

Для візуалізації роботи системи:

На рисунку 2.1 наведено структурну блок-схему запропонованої децентралізованої IoT-мережі для моніторингу пошкоджень інфраструктурних об’єктів. Основними елементами системи є сенсорні вузли, mesh-мережа, edge/fog-вузли, блокчейн-мережа та сервер моніторингу.

Сенсорні вузли здійснюють безперервний збір інформації про стан об’єкта інфраструктури за допомогою датчиків вібрації, температури, деформації, вологості та інших параметрів. Зібрані дані передаються через бездротові канали зв’язку до сусідніх вузлів мережі.

Обмін інформацією між вузлами реалізується за допомогою mesh-топології, у якій кожен вузол може виступати не лише джерелом інформації, а й ретранслятором для інших пристроїв. Такий підхід дозволяє забезпечити багатохопову передачу даних і підтримувати працездатність мережі навіть у випадку втрати окремих вузлів або каналів зв’язку.

Edge/fog-вузли виконують функції локальної обробки, агрегації та фільтрації інформації. Це дозволяє зменшити обсяг переданих даних,

скоротити затримки та підвищити швидкість реагування системи на аварійні ситуації.

Для забезпечення цілісності та захисту інформації використовується блокчейн-рівень, який забезпечує розподілене зберігання журналів подій та підтвердження достовірності отриманих даних. Центральний сервер використовується переважно для довготривалого зберігання інформації, візуалізації результатів моніторингу та формування повідомлень для операторів системи.

Таким чином, запропонована архітектура поєднує переваги децентралізованих мереж, edge/fog computing та технологій блокчейн, що дозволяє підвищити надійність, масштабованість та кіберстійкість системи моніторингу.

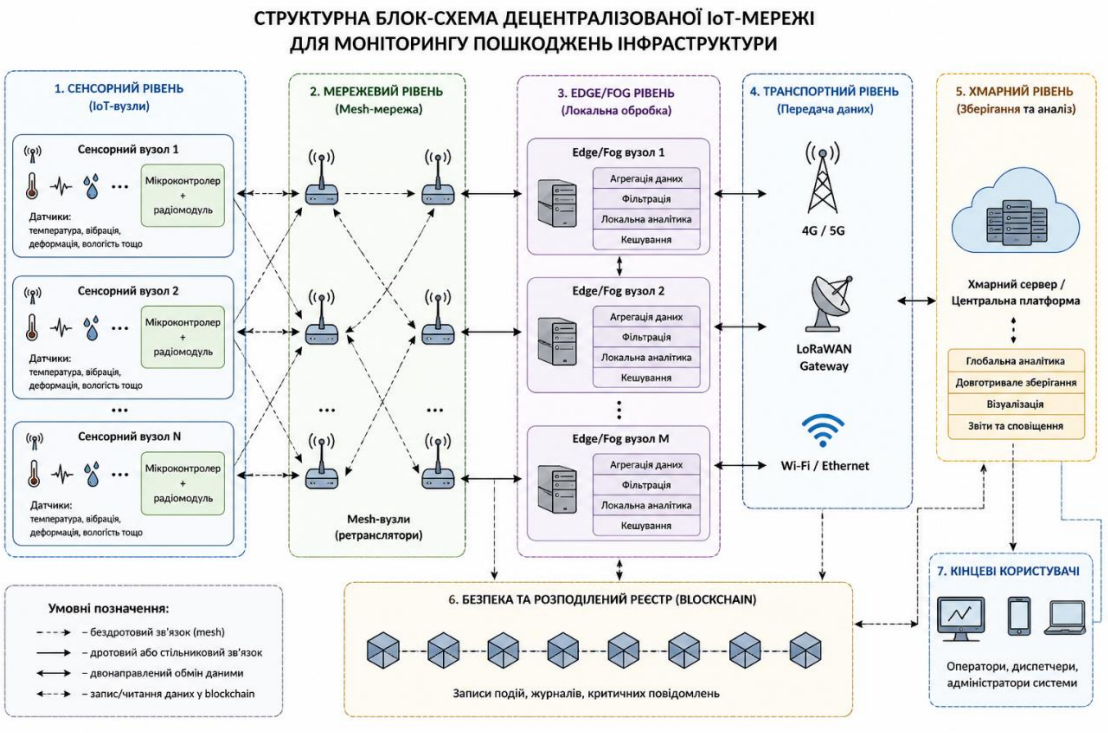

Рис. 2. 1. Структурна блок-схема мережі

На рисунку 2.2 представлено UML-діаграму взаємодії основних компонентів системи моніторингу пошкоджень інфраструктури.

Процес роботи системи починається із сенсорного вузла, який виконує вимірювання контрольованих параметрів об’єкта інфраструктури. Після отримання нових даних сенсорний вузол формує пакет інформації та передає його до мережі.

Отримані дані надходять до edge-вузла, де здійснюється їх попередня обробка. На цьому етапі виконується фільтрація шумів, агрегація вимірювань та перевірка наявності аномальних значень. У разі відсутності критичних відхилень інформація передається до серверної частини для подальшого аналізу та зберігання.

Якщо виявлено аномальні показники або ознаки пошкодження інфраструктурного об’єкта, edge-вузол формує тривожне повідомлення та передає його до блокчейн-мережі для фіксації події. Після цього інформація надходить до сервера моніторингу, який генерує сповіщення для оператора.

Оператор отримує повідомлення про потенційну аварійну ситуацію та може оперативно прийняти рішення щодо подальших дій. UML-діаграма демонструє послідовність обміну повідомленнями між вузлами системи та підтверджує можливість локального прийняття рішень без необхідності постійного звернення до центрального сервера.

Рис. 2. 2. UML-діаграма взаємодії вузлів

На рисунку 2.3 наведено алгоритм передачі тривожного повідомлення у випадку виявлення пошкодження інфраструктурного об’єкта.

Процес починається з безперервного моніторингу параметрів об’єкта сенсорним вузлом. У разі перевищення встановленого порогового значення система виконує перевірку достовірності отриманих даних для виключення помилкових спрацювань.

Після підтвердження аномалії формується тривожне повідомлення, яке передається через mesh-мережу до найближчого edge-вузла. Використання mesh-маршрутизації дозволяє автоматично обирати доступний маршрут передачі даних навіть за умови пошкодження окремих вузлів або каналів зв’язку.

Edge-вузол здійснює додаткову перевірку отриманої інформації та формує запис у блокчейн-системі для забезпечення цілісності та незмінності даних. [2-4, 5, 11] Після успішної реєстрації події інформація надходить до сервера моніторингу.

Сервер виконує обробку отриманих даних, оновлює базу подій та генерує повідомлення для оператора або відповідних служб реагування. У результаті забезпечується оперативне інформування про можливі пошкодження інфраструктури та скорочується час реагування на аварійні ситуації.

Запропонована схема дозволяє забезпечити надійну передачу критично важливих повідомлень навіть в умовах часткової втрати зв’язку, пошкодження вузлів мережі або зовнішніх кіберзагроз.

Рис. 2. 3. Схема передачі тривожного повідомлення

Алгоритм маршрутизації даних у mesh-мережі включає такі етапи:

— Сенсорний вузол формує пакет даних після вимірювання параметрів об’єкта інфраструктури.

— Вузол перевіряє наявність прямого маршруту до edge/fog-вузла або шлюзу мережі.

— Якщо прямий маршрут доступний, пакет передається безпосередньо до вузла призначення.

— Якщо прямий зв’язок відсутній, виконується пошук сусідніх вузлів mesh-мережі.

— Система визначає оптимальний маршрут передачі на основі:

1) рівня сигналу;
2) кількості переходів;
3) навантаження вузлів;
4) стабільності з’єднання;
5) енергетичного стану вузлів.

— Пакет передається через проміжні вузли мережі.
— Кожен проміжний вузол:
    1) перевіряє цілісність пакета;
    2) записує інформацію про маршрут;
    3) перенаправляє пакет наступному вузлу.
— У випадку втрати зв’язку:
    1) виконується автоматичний пошук альтернативного маршруту;
    2) дані тимчасово кешуються;
    3) повторна передача здійснюється після відновлення мережі.
— Після доставки пакета edge/fog-вузол надсилає підтвердження отримання (ACK).
— Інформація про критичні події додатково реєструється у blockchain для забезпечення цілісності журналів подій.

Для підвищення надійності передачі даних у системі використовується адаптивна маршрутизація, яка дозволяє динамічно змінювати маршрути залежно від стану мережі.

Основними перевагами запропонованого алгоритму є:

— відмовостійкість;
— автономність функціонування;
— відсутність єдиної точки відмови;
— підтримка багатохопової передачі;
— масштабованість мережі;
— стійкість до втрати окремих вузлів.

Для візуалізації алгоритму маршрутизації даних розроблено блок-схему алгоритму (Рис. 2.4).

Рис. 2. 4. Алгоритм маршрутизації даних у mesh-мережі

Таким чином, запропонований алгоритм забезпечує автоматизований моніторинг інфраструктури, оперативне виявлення пошкоджень та надійну передачу критично важливої інформації в умовах децентралізованої мережевої архітектури.

Висновки

У другому розділі дипломної роботи виконано розробку та обґрунтування архітектури децентралізованої IoT-мережі для моніторингу пошкоджень інфраструктури. На основі аналізу сучасних підходів до побудови IoT-систем визначено основні вимоги до мережі, серед яких ключовими є відмовостійкість, автономність функціонування, масштабованість, енергоефективність та захищеність інформації.

У роботі запропоновано багаторівневу архітектуру системи, що включає сенсорний рівень, edge/fog-рівень, мережевий сегмент передачі

даних та систему розподіленого зберігання інформації. Встановлено, що використання децентралізованої структури дозволяє усунути проблему єдиної точки відмови та забезпечити безперервне функціонування системи навіть у випадку пошкодження окремих вузлів або сегментів мережі.

Проведено аналіз сучасних бездротових технологій передачі даних, зокрема LoRaWAN, ZigBee, NB-IoT та мобільних мереж 4G/5G. Визначено, що комбіноване використання LPWAN-технологій та mesh-мереж дозволяє забезпечити ефективний обмін інформацією між вузлами системи при мінімальному енергоспоживанні.

Розглянуто методи збору та обробки даних у децентралізованій IoT-мережі. Встановлено, що застосування агрегації, фільтрації, edge computing та локальної аналітики дозволяє зменшити навантаження на канали зв’язку, скоротити затримки передачі інформації та підвищити швидкість реагування системи на аварійні події.

Окрему увагу приділено питанням інформаційної безпеки. У роботі досліджено можливості використання blockchain-технологій, криптографічного шифрування та механізмів автентифікації вузлів для забезпечення цілісності, конфіденційності та достовірності даних. Встановлено, що використання розподіленого реєстру дозволяє підвищити рівень кіберстійкості системи та унеможливити несанкціоновану зміну критичних повідомлень.

Також у розділі розроблено алгоритм роботи системи та алгоритм маршрутизації даних у mesh-мережі. Визначено принципи багатохопової передачі інформації, автоматичного пошуку альтернативних маршрутів та відновлення передачі даних у випадку втрати зв’язку. Це дозволяє забезпечити високу надійність функціонування мережі в умовах нестабільного середовища або пошкодження окремих вузлів.

Отримані результати свідчать про доцільність використання децентралізованих IoT-мереж для моніторингу критичної інфраструктури та створюють основу для подальшого дослідження ефективності роботи

системи, оцінки її продуктивності, надійності та кіберстійкості, що буде розглянуто у наступному розділі дипломної роботи.

РОЗДІЛ 3
ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ТА ОЦІНКА РОБОТИ СИСТЕМИ

У попередньому розділі було розроблено архітектуру децентралізованої IoT-мережі для моніторингу пошкоджень інфраструктури, визначено принципи взаємодії вузлів, методи збору та обробки даних, а також підходи до забезпечення інформаційної безпеки системи. Наступним етапом є оцінка ефективності запропонованої архітектури в умовах реальної експлуатації.

У даному розділі проводиться моделювання роботи мережі, аналіз її надійності, відмовостійкості, продуктивності та кіберстійкості. Також виконується техніко-економічне обґрунтування системи та розглядаються питання охорони праці й безпеки експлуатації IoT-обладнання.

3.1. Моделювання роботи мережі

Для оцінки ефективності запропонованої децентралізованої IoT-мережі проведено моделювання роботи системи в умовах різних сценаріїв функціонування. Основною метою моделювання є визначення здатності мережі забезпечувати безперервний моніторинг інфраструктури, своєчасну передачу даних та стійкість до відмов окремих вузлів. [14]

У моделі мережа складається із сенсорних вузлів, mesh-маршрутизаторів, edge/fog-вузлів та шлюзів доступу до хмарної інфраструктури. Сенсорні вузли здійснюють постійний контроль параметрів об’єктів інфраструктури та передають інформацію через mesh-мережу до edge/fog-вузлів для локальної обробки. [5, 11, 12]

Під час моделювання враховуються:

- кількість вузлів мережі;
- відстань між вузлами;
- інтенсивність передачі даних;
- рівень втрати пакетів;
- затримки передачі інформації;

— енергоспоживання вузлів;

— можливість виходу вузлів з ладу.

Сценарії пошкодження

Для оцінки працездатності системи розглянуто декілька типових сценаріїв пошкодження інфраструктури:

— локальне пошкодження мостових конструкцій;

— деформація будівельних елементів;

— аварійні вібрації конструкцій;

— перевищення допустимих температурних показників;

— часткове руйнування сегментів мережі.

У кожному сценарії сенсорні вузли фіксують зміну контрольованих параметрів та передають інформацію до edge/fog-вузлів. Після локального аналізу система формує тривожне повідомлення та виконує передачу інформації оператору.

Відмова вузлів

Одним із ключових етапів моделювання є аналіз роботи мережі при відмові окремих вузлів. У централізованих системах відмова центрального вузла може призвести до повної втрати працездатності системи. У запропонованій mesh-архітектурі використовується багатохопова маршрутизація, що дозволяє автоматично перенаправляти трафік альтернативними маршрутами. [8, 12, 13]

Під час моделювання досліджується:

— відмова сенсорного вузла;

— відмова mesh-маршрутизатора;

— відключення edge/fog-вузла;

— втрата зв’язку з gateway.

Результати показують, що навіть при виході з ладу декількох вузлів система продовжує функціонувати завдяки автоматичному пошуку нових маршрутів передачі інформації.

Втрата зв’язку

У реальних умовах експлуатації можливе тимчасове порушення зв’язку між сегментами мережі. Для перевірки стійкості системи змодельовано ситуації часткової та повної втрати зв’язку.

У випадку втрати з’єднання edge/fog-вузли виконують:

— локальне кешування даних;

— повторну передачу пакетів;

— використання резервних маршрутів;

— автономну обробку критичних повідомлень.

Використання децентралізованої архітектури дозволяє забезпечити безперервність функціонування системи навіть у складних умовах експлуатації. [5, 11, 13]

3.2. Аналіз надійності та відмовостійкості

Однією з основних вимог до систем моніторингу критичної інфраструктури є забезпечення високого рівня надійності та відмовостійкості. Для оцінки ефективності запропонованої архітектури виконано порівняльний аналіз централізованої та децентралізованої моделей побудови IoT-мереж.

Порівняння централізованої та децентралізованої моделей

У централізованих IoT-системах обробка та зберігання інформації здійснюється через центральний сервер. Такий підхід має низку недоліків:

— наявність єдиної точки відмови;

— високе навантаження на центральний вузол;

— складність масштабування;

— залежність від стабільності мережевого з’єднання. [6, 12, 13]

У децентралізованій системі функції передачі та обробки даних розподіляються між edge/fog-вузлами. Це забезпечує:

— автономність сегментів мережі;

— підвищення відмовостійкості;

— скорочення затримок передачі даних;

— можливість роботи при частковій втраті зв’язку. [5, 11, 12]

Порівняльний аналіз показує, що децентралізована архітектура є більш стійкою до відмов та краще адаптована до роботи в умовах нестабільного середовища. [5, 8, 12]

Час доставки даних

Одним із ключових показників ефективності системи є затримка передачі інформації. У системах моніторингу критичної інфраструктури важливо забезпечити оперативну передачу аварійних повідомлень.

Використання edge/fog computing дозволяє:

— виконувати локальну обробку інформації;

— скоротити обсяг трафіку;

— зменшити затримки передачі даних.

Під час моделювання встановлено, що локальна обробка інформації дозволяє зменшити середній час реагування системи у порівнянні з централізованими моделями. [5, 7, 11].

Втрати пакетів

Для оцінки надійності передачі даних проведено аналіз рівня втрати пакетів у мережі.

У mesh-мережі використовується:

— багатохопова маршрутизація;

— резервування маршрутів;

— повторна передача пакетів;

— ACK-підтвердження доставки.

Результати дослідження свідчать про зменшення кількості втрат пакетів у порівнянні з класичними централізованими системами. [8, 12, 13]

3.3 Розрахунок автономної роботи LoRaWAN-вузлів

Для забезпечення безперервного моніторингу інфраструктурних об’єктів важливим параметром IoT-вузлів є тривалість автономної роботи від джерела живлення. У системах моніторингу, побудованих на базі технології

LoRaWAN, сенсорні вузли переважно працюють у режимі низького енергоспоживання та більшу частину часу перебувають у режимі сну (sleep mode) [9, 13].

Для оцінки автономності роботи вузла проведемо розрахунок енергоспоживання типового LoRaWAN-пристрою.

Нехай використовується:

— акумулятор ємністю:

$$C = 2400 \text{ мА\год} \quad (3.1)$$

— середній струм споживання вузла:

$$I_{avg} = 0.12 \text{ мА} \quad (3.2).$$

Термін автономної роботи визначається за формулою:

$$T = \frac{C}{I_{avg}} \quad (3.3)$$

де:

— T— час автономної роботи, год;

— C— ємність батареї, мА·год;

— I_{avg}— середній струм споживання, мА.

Підставивши значення, отримаємо:

$$T = \frac{2400}{0.12} = 20000 \text{ год} \quad (3.4)$$

Переведемо отримане значення у роки:

$$T = \frac{20000}{24 \cdot 365} \approx 2.28 \text{ роки} \quad (3.5)$$

Отже, за умови оптимізованого режиму передачі даних та використання режимів енергозбереження автономний LoRaWAN-вузол може працювати понад 2 роки без заміни батареї. Це підтверджує доцільність використання LoRaWAN для побудови розподілених систем моніторингу інфраструктури з великою кількістю сенсорних вузлів [9, 13].

3.4. Оцінка продуктивності системи

Продуктивність децентралізованої IoT-мережі визначається швидкістю передачі інформації, стабільністю роботи вузлів та ефективністю використання ресурсів системи. [14]

Затримки передачі даних

Під час функціонування мережі затримки можуть виникати через:

— перевантаження каналів зв’язку;
— велику кількість вузлів;
— багатохопову передачу;
— обробку даних на edge/fog-рівні.

Використання локальної аналітики та edge computing дозволяє мінімізувати затримки шляхом обробки інформації безпосередньо поблизу джерела даних. [5, 7, 11]

Навантаження на мережу

Для зменшення навантаження у системі використовуються:

— агрегація даних;
— фільтрація службового трафіку;
— адаптивна передача пакетів;
— локальна обробка телеметрії.

Передача лише критично важливої інформації дозволяє знизити навантаження на канали зв’язку та оптимізувати використання мережевих ресурсів. [5, 11]

Енергоспоживання

Оскільки значна частина IoT-вузлів працює автономно, важливим параметром є енергоефективність системи.

Для зменшення енергоспоживання використовуються:

— LPWAN-технології;

— sleep-режими;

— адаптивна частота передачі даних;

— локальна обробка інформації. [9, 11, 13]

Для оцінки ефективності різних бездротових технологій у системах моніторингу інфраструктури проведено їх порівняльний аналіз за основними параметрами (Таблиця 3.1) [9, 12, 13].

Таблиця 3.1

Порівняльний аналіз бездротових технологій

Параметр	**LoRaWAN**	**NB-IoT**	**ZigBee**
Дальність зв’язку	5–15 км	1–10 км	10–100 м
Швидкість передачі	Низька	Середня	Середня
Енергоспоживання	Дуже низьке	Низьке	Низьке
Топологія	Star / Mesh	Star	Mesh
Підтримка mesh	Частково	Ні	Так
Робота без оператора	Так	Ні	Так
Вартість обслуговування	Низька	Середня	Низька
Стійкість до втрати вузлів	Висока	Середня	Висока
Підтримка великих територій	Так	Так	Обмежено
Типове застосування	LPWAN IoT	Операторські IoT-системи	Локальні мережі

Аналіз показує, що LoRaWAN є найбільш ефективною технологією для побудови великомасштабних систем моніторингу інфраструктури завдяки великій дальності зв’язку та низькому енергоспоживанню. ZigBee є доцільним для локальних mesh-мереж, а NB-IoT забезпечує стабільний зв’язок за наявності мобільної інфраструктури (Таблиця 3.1)[9, 12, 13].

3.5. Аналіз безпеки та кіберстійкості

Системи моніторингу критичної інфраструктури повинні забезпечувати високий рівень захисту інформації та стійкість до кібератак.

Захист від атак

У системі використовуються:

— криптографічне шифрування;

— TLS/SSL-з’єднання;

— цифрові підписи;

— автентифікація вузлів.

Такі механізми дозволяють захистити мережу від:

— перехоплення даних;

— підміни пакетів;

— несанкціонованого доступу;

— атак типу spoofing. [2, 15]

Стійкість до втрати вузлів

Децентралізована архітектура забезпечує можливість функціонування системи навіть при частковій втраті вузлів.

Mesh-маршрутизація дозволяє:

— автоматично знаходити альтернативні маршрути;

— зберігати працездатність системи;

— мінімізувати ризик повної відмови мережі. [8, 12, 13]

Цілісність даних

Для забезпечення цілісності інформації використовується blockchain-технологія.

Розподілений реєстр дозволяє:

— фіксувати критичні події;

— унеможливити зміну журналів;

— підтверджувати достовірність повідомлень;

— підвищити рівень довіри між вузлами мережі. [2, 3, 4]

У сучасних IoT-системах значну небезпеку становлять кібератаки, спрямовані на порушення роботи мережі, втрату даних або несанкціонований доступ до вузлів системи [2, 15].

DDoS-атака

Одним із найпоширеніших типів загроз є DDoS-атака (Distributed Denial of Service), під час якої велика кількість фальшивих запитів перевантажує мережу або окремі вузли системи.

У централізованих IoT-системах DDoS-атака на центральний сервер може повністю вивести систему з ладу. У запропонованій децентралізованій архітектурі навантаження розподіляється між edge/fog-вузлами, що зменшує ризик повної відмови системи. [1, 5]

Для протидії DDoS-атакам у системі застосовуються:

— розподілена обробка даних;
— обмеження кількості запитів;
— фільтрація підозрілих пакетів;
— резервні маршрути mesh-мережі;
— локальна автономна робота вузлів.

Sybil attack

Іншим небезпечним типом загроз є Sybil attack, за якої зловмисник створює велику кількість фальшивих вузлів для порушення роботи мережі або підміни даних. [2,4]

У mesh-мережах така атака може призвести до:

— спотворення маршрутів передачі;
— перехоплення пакетів;
— перевантаження мережі;
— втрати достовірності інформації.

Для протидії Sybil attack у запропонованій системі використовуються:

— автентифікація вузлів;
— криптографічні ключі;
— blockchain для перевірки цілісності даних;
— контроль довіри між вузлами;
— перевірка цифрових підписів повідомлень.

Забезпечення кіберстійкості системи

Використання децентралізованої архітектури, mesh-взаємодії та blockchain-технологій дозволяє підвищити рівень кіберстійкості системи моніторингу інфраструктури. [2–5]

Основними перевагами запропонованої архітектури є:

— відсутність єдиної точки відмови;
— можливість локальної автономної роботи;
— резервування маршрутів передачі;
— розподілене зберігання інформації;
— підвищена стійкість до атак на окремі вузли мережі.

Отримані результати підтверджують доцільність використання децентралізованих IoT-мереж для побудови захищених систем моніторингу критичної інфраструктури.

3.6. Техніко-економічне обґрунтування

Важливим етапом оцінки системи є визначення економічної доцільності її впровадження.

Для оцінки практичної доцільності впровадження децентралізованої IoT-мережі проведено орієнтовний розрахунок вартості обладнання для невеликої системи моніторингу інфраструктурного об’єкта (таблиця 3.2).

До складу системи входять:

— 10 сенсорних LoRaWAN-вузлів;
— 1 edge-шлюз;
— 1 сервер моніторингу;
— мережеве обладнання;
— джерела живлення.

Таблиця 3.2

Орієнтовна вартість обладнання

Обладнання	**Кількість**	**Орієнтовна вартість за одиницю**	**Загальна вартість**
LoRaWAN-вузол	10	45 USD	450 USD
Edge/Fog шлюз	1	180 USD	180 USD
Сервер моніторингу	1	400 USD	400 USD
Джерела живлення	10	12 USD	120 USD
Мережеве обладнання	1 комплект	150 USD	150 USD

Загальні капітальні витрати (CAPEX) становлять:

$$CAPEX = 450 + 180 + 400 + 120 + 150 = 1300\ USD \quad (3.6)$$

Таким чином, орієнтовна вартість впровадження базової системи моніторингу складає близько 1300 USD без урахування витрат на монтаж та технічне обслуговування. [6, 9]

Використання децентралізованої архітектури дозволяє:

— знизити витрати на прокладання кабельної інфраструктури;

— мінімізувати ризики повної відмови системи;

— зменшити навантаження на центральний сервер;

— скоротити витрати на обслуговування мережі.

Крім того, використання LoRaWAN забезпечує низьке енергоспоживання та тривалий термін автономної роботи сенсорних вузлів, що дозволяє зменшити експлуатаційні витрати системи. [9, 13]

Економічна ефективність системи також проявляється у можливості раннього виявлення пошкоджень інфраструктури. Оперативне виявлення аварійних ситуацій дозволяє знизити витрати на ремонтні роботи та мінімізувати ризики виникнення масштабних аварій. [6, 8]

Ефективність системи

Запропонована система дозволяє:

— зменшити час виявлення пошкоджень;

— скоротити витрати на технічне обслуговування;

— підвищити рівень безпеки інфраструктури;
— знизити ризики аварійних ситуацій.

Переваги впровадження

Основними перевагами системи є:

— відмовостійкість;
— масштабованість;
— автономність;
— зменшення експлуатаційних витрат;
— можливість інтеграції у smart city-системи.

3.7. Охорона праці та безпека

Під час проєктування та експлуатації IoT-систем необхідно враховувати вимоги охорони праці та техніки безпеки. [15]

Електробезпека

Під час роботи з IoT-обладнанням необхідно:

— використовувати стабілізовані джерела живлення;
— забезпечувати заземлення обладнання;
— застосовувати захист від короткого замикання;
— дотримуватись правил експлуатації електронних пристроїв.

Безпека роботи з IoT-обладнанням

Для безпечної експлуатації обладнання необхідно:

— контролювати температурний режим пристроїв;
— забезпечувати захист обладнання від вологи;
— виконувати регулярне технічне обслуговування;
— використовувати сертифіковані компоненти.

Кібербезпека

Для забезпечення безпеки мережі необхідно:

— використовувати шифрування даних;
— регулярно оновлювати програмне забезпечення;
— контролювати доступ до системи;

— застосовувати механізми автентифікації вузлів. [2, 15]

Комплексне використання заходів електробезпеки та кіберзахисту дозволяє забезпечити стабільне та безпечне функціонування системи. [2, 15]

Висновки

У третьому розділі дипломної роботи проведено дослідження ефективності та оцінку роботи децентралізованої IoT-мережі для моніторингу пошкоджень інфраструктури.

Виконано моделювання роботи системи в умовах різних сценаріїв функціонування, включаючи пошкодження інфраструктурних об’єктів, втрату зв’язку та відмову окремих вузлів. Встановлено, що використання mesh-архітектури та багатохопової маршрутизації дозволяє забезпечити безперервне функціонування мережі навіть при пошкодженні окремих сегментів системи.

Проведено аналіз надійності та відмовостійкості системи. Визначено, що децентралізована архітектура має суттєві переваги над централізованими моделями завдяки відсутності єдиної точки відмови, можливості автономної роботи вузлів та використанню резервних маршрутів передачі даних.

У роботі досліджено продуктивність системи та оцінено затримки передачі інформації, навантаження на мережу та енергоспоживання IoT-вузлів. Встановлено, що застосування edge computing, агрегації даних та LPWAN-технологій дозволяє зменшити затримки передачі інформації та підвищити енергоефективність системи.

Також проведено аналіз безпеки та кіберстійкості системи. Визначено, що використання blockchain-технологій, криптографічного захисту та механізмів автентифікації дозволяє забезпечити цілісність інформації та підвищити рівень захищеності системи від кібератак.

Крім того, у процесі дослідження встановлено, що використання децентралізованої архітектури дозволяє значно підвищити стійкість системи до зовнішніх впливів, зокрема до пошкодження каналів зв’язку,

перевантаження окремих вузлів та кібератак. Завдяки використанню mesh-маршрутизації система здатна автоматично перебудовувати маршрути передачі даних, що забезпечує безперервність функціонування навіть у випадку часткової втрати елементів мережі.

Проведене дослідження показало, що застосування edge/fog computing дозволяє виконувати локальну обробку даних без необхідності постійної передачі всієї інформації до центрального сервера. Це сприяє скороченню затримок передачі даних, зниженню навантаження на мережеву інфраструктуру та підвищенню швидкості реагування системи на аварійні ситуації.

У ході аналізу безпеки встановлено, що використання blockchain-технологій забезпечує додатковий рівень захисту інформації та дозволяє гарантувати цілісність журналів подій і достовірність переданих повідомлень. Застосування криптографічного шифрування та механізмів автентифікації вузлів дозволяє мінімізувати ризики несанкціонованого доступу до системи та підвищити рівень кіберстійкості мережі.

Результати техніко-економічного аналізу свідчать про доцільність впровадження запропонованої системи у сферах моніторингу транспортної, енергетичної, промислової та міської інфраструктури. Використання автоматизованого моніторингу дозволяє скоротити витрати на технічне обслуговування об’єктів, зменшити ризики аварійних ситуацій та підвищити рівень безпеки експлуатації критично важливих систем.

Таким чином, результати проведеного дослідження підтверджують ефективність використання децентралізованих IoT-мереж для моніторингу пошкоджень інфраструктури та демонструють перспективність подальшого розвитку таких систем із використанням сучасних технологій штучного інтелекту, машинного навчання та розподілених обчислень.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

1. У дипломній роботі проведено аналіз сучасного стану розвитку технологій Інтернету речей, децентралізованих мереж, blockchain, edge/fog computing та бездротових технологій передачі даних у системах моніторингу критичної інфраструктури. Встановлено, що централізовані IoT-системи мають низку суттєвих недоліків, серед яких наявність єдиної точки відмови, залежність від стабільного мережевого з'єднання, обмежена масштабованість та підвищені ризики кіберзагроз.

2. У роботі досліджено принципи побудови децентралізованих IoT-мереж та визначено основні переваги mesh-архітектури, зокрема можливість багатохопової передачі даних, автоматичного переналаштування маршрутів, автономності окремих сегментів мережі та підвищеної відмовостійкості системи.

3. Виконано аналіз сучасних бездротових технологій LoRaWAN, NB-IoT, ZigBee, 4G/5G та Bluetooth Low Energy. Встановлено, що для систем моніторингу пошкоджень інфраструктури найбільш ефективним є комбіноване використання LPWAN-технологій, mesh-мереж та мобільного зв'язку для забезпечення оптимального співвідношення між енергоефективністю, дальністю передачі даних та надійністю зв'язку.

4. Розроблено архітектуру децентралізованої IoT-мережі для моніторингу пошкоджень інфраструктури, яка включає сенсорні вузли, mesh-маршрутизатори, edge/fog-вузли, шлюзи передачі даних та систему розподіленого зберігання інформації. Запропонована архітектура забезпечує безперервний збір, передачу та локальну обробку даних навіть у випадку часткової втрати зв'язку або пошкодження окремих вузлів.

5. У роботі обґрунтовано доцільність використання edge computing та fog computing для локальної обробки інформації. Встановлено, що перенесення частини обчислень на периферійні вузли дозволяє скоротити затримки передачі даних, зменшити навантаження на мережу та підвищити швидкість реагування системи на аварійні події.

6. Запропоновано методи збору та обробки даних, що включають агрегацію, фільтрацію, локальну аналітику та edge processing. Використання зазначених методів дозволяє оптимізувати використання мережевих ресурсів, знизити обсяг службового трафіку та забезпечити ефективну роботу системи в умовах великої кількості IoT-пристроїв.

7. У роботі досліджено можливості використання blockchain та технологій розподіленого реєстру для забезпечення безпеки IoT-систем. Встановлено, що застосування blockchain дозволяє гарантувати цілісність даних, забезпечити автентифікацію вузлів, захистити систему від несанкціонованого втручання та підвищити рівень кіберстійкості мережі.

8. Розроблено алгоритм функціонування системи та алгоритм маршрутизації даних у mesh-мережі. Визначено принципи автоматичного пошуку альтернативних маршрутів передачі інформації та механізми відновлення роботи системи у випадку втрати окремих вузлів або каналів зв’язку.

9. Проведено моделювання роботи мережі в умовах різних сценаріїв функціонування, включаючи пошкодження інфраструктури, втрату зв’язку та відмову окремих вузлів. Результати моделювання показали, що запропонована система забезпечує високий рівень надійності, відмовостійкості та автономності функціонування.

10. Виконано аналіз продуктивності системи та оцінено затримки передачі інформації, навантаження на мережу та енергоспоживання IoT-вузлів. Встановлено, що використання LPWAN-технологій та edge/fog computing дозволяє підвищити енергоефективність системи та забезпечити тривалий автономний режим роботи сенсорних пристроїв.

11. Проведений аналіз безпеки підтвердив, що використання криптографічного шифрування, механізмів автентифікації та blockchain-технологій дозволяє забезпечити захист системи від кібератак, несанкціонованого доступу та підробки даних.

12. Виконано техніко-економічне обґрунтування запропонованої системи. Встановлено, що впровадження децентралізованих IoT-мереж дозволяє скоротити витрати на технічне обслуговування інфраструктурних об’єктів, підвищити ефективність виявлення пошкоджень та зменшити ризики виникнення аварійних ситуацій.

13. Результати дипломної роботи можуть бути використані у системах моніторингу транспортної, енергетичної, промислової та міської інфраструктури, а також у проєктах створення smart city-систем і розподілених систем моніторингу критично важливих об’єктів.

14. Перспективами подальших досліджень є інтеграція методів машинного навчання та штучного інтелекту для прогнозування пошкоджень інфраструктури, вдосконалення алгоритмів маршрутизації в mesh-мережах, а також підвищення автономності IoT-вузлів і розвитку гібридних децентралізованих архітектур.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Yasser Z., Hammoud A., Mourad A., Otrok H., Dziong Z., Guizani M. Federated Learning and Evolutionary Game Model for Fog Federation Formation // arXiv. – 2024.

2. Dorri A., Steger M., Kanhere S. S., Jurdak R. Blockchain for IoT security and privacy: The case study of a smart home // 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). – 2017. – P. 618–623.

3. Huawei. Decentralized IoT Management on Blockchain. – 2022.

4. Колбасін Г. О. Технології блокчейн в Інтернеті речей : навчальний посібник. – Київ : НТУУ «КПІ ім. Ігоря Сікорського», 2020. – 156 с.

5. OpenFog Consortium. OpenFog Reference Architecture. – 2017.

6. Cisco Systems. IoT Reference Model and Architecture. – Cisco White Paper, 2021.

7. IBM Corporation. Edge Computing for Industrial IoT Systems. – IBM Research Report, 2022.

8. Minoli D., Sohraby K., Occhiogrosso B. IoT Considerations, Requirements, and Architectures for Smart Buildings // IEEE Internet of Things Journal. – 2017. – Vol. 4, No. 1. – P. 269–283.

9. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols and Applications // IEEE Communications Surveys & Tutorials. – 2015. – Vol. 17, No. 4. – P. 2347–2376.

10. Zanella A., Bui N., Castellani A., Vangelista L., Zorzi M. Internet of Things for Smart Cities // IEEE Internet of Things Journal. – 2014. – Vol. 1, No. 1. – P. 22–32.

11. Gupta H., Vahid Dastjerdi A., Ghosh S. K., Buyya R. iFogSim: A toolkit for modeling and simulation of resource management techniques in Internet of Things, Edge and Fog computing environments // Software: Practice and Experience. – 2017. – Vol. 47, No. 9. – P. 1275–1296.

12. Ray P. P. A survey on Internet of Things architectures // Journal of King Saud University – Computer and Information Sciences. – 2018. – Vol. 30, No. 3. – P. 291–319.

13. Lin J., Yu W., Zhang N., Yang X., Zhang H., Zhao W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications // IEEE Internet of Things Journal. – 2017. – Vol. 4, No. 5. – P. 1125–1142.

14. Borgia E. The Internet of Things vision: Key features, applications and open issues // Computer Communications. – 2014. – Vol. 54. – P. 1–31.

15. Sicari S., Rizzardi A., Grieco L. A., Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead // Computer Networks. – 2015. – Vol. 76. – P. 146–164.