МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія (кафедра) комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

АРХІТЕКТУРА, ПРОТОКОЛИ ТА ЗАСТОСУВАННЯ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

Виконав: студент групи 1К-21
Спеціальності 123 Комп’ютерна інженерія
Дмитро МАКАРЕНКО
Керівник:
Павло РАТАЙЧУК

Черкаси 2025

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ

Кафедра комп'ютерної інженерії та інформаційних технологій

Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувач кафедри КІ та ІТ

_____ Владислав ХОТУНОВ
(підпис)
«_____»_____2025 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Макаренку Дмитру В'ячеславовичу

1. Тема кваліфікаційної роботи Архітектура, протоколи та застосування бездротових сенсорних мереж

Керівник роботи Ратайчук Павло Єгорович, викладач методист _____

затверджені наказом закладу вищої освіти від «07» жовтня 2024 року № 68у.
2. Строк подання студентом кваліфікаційної роботи 02.06.2025
3. Вихідні дані до кваліфікаційної роботи компоненти та типи архітектури WSN, інформація про популярні комунікаційні протоколи, методи маршрутизації та управління енергоспоживанням, сценарії використання WSN у промисловості, сільському господарстві, екологічному моніторингу тощо, методи інтеграції WSN з іншими технологіями (AI, Edge Computing).
4. Зміст кваліфікаційної роботи (перелік питань, які потрібно розробити) Загальні відомості про WSN, архітектура бездротових сенсорних мереж, протоколи передачі даних у WSN, маршрутизація та енергоефективність у WSN, застосування WSN у різних сферах, моделювання роботи WSN у спеціалізованих програмних середовищах.
5. Дата видачі завдання 16.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів	Примітка про виконання з підписами керівника і студента
1	Вступ	14.10.2024	
2	Розділ 1 (Архітектура бездротових сенсорних мереж)	9.12.2024	
3	Розділ 2 (Застосування бездротових сенсорних мереж)	10.03.2025	
4	Розділ 3 (Проблеми та перспективи розвитку бездротових сенсорних мереж)	28.04.2025	
5	Висновки	12.05.2025	
6	Оформлення кваліфікаційної роботи (чистовий варіант)	26.05.2025	
7	Перевірка кваліфікаційної роботи на наявність ознак плагіату (за 10 днів до захисту)	02.06.2025	
8	Подання кваліфікаційної роботи на затвердження завідувачу кафедри (за 7 днів до захисту)	10.06.2025	

Студент _____ Дмитро МАКАРЕНКО
(підпис)

Керівник роботи _____ Павло РАТАЙЧУК
(підпис)

АНОТАЦІЯ

Метою роботи є дослідження архітектури, протоколів та основних напрямків застосування бездротових сенсорних мереж у сучасних технологіях. Основна увага приділяється аналізу архітектури мереж, включаючи компоненти, топології та енергозберігаючі механізми, а також протоколам на різних рівнях взаємодії та їх особливостям для забезпечення високої ефективності.

Галузь застосування охоплює Інтернет речей, промислові системи моніторингу, екологічний моніторинг, "розумне" сільське господарство, медицину та розумні міста. Технологічні та техніко-експлуатаційні характеристики включають низьке енергоспоживання, високу масштабованість і гнучкість конфігурацій, що робить ці системи придатними для роботи в умовах обмеженого енергетичного ресурсу.

У роботі обґрунтовано ступінь впровадження бездротових сенсорних мереж у різних сферах діяльності, реалізовано модель сенсорної мережі, досліджено механізми управління енергоспоживанням, а також розроблено рекомендації щодо вибору протоколів для підвищення ефективності роботи мережі. Окремо розглянуто проблеми безпеки та перспективи розвитку технологій, пов’язаних із сенсорними мережами, з урахуванням сучасних викликів кібербезпеки та інноваційних методів захисту інформації.

Робота має практичну цінність і може бути використана для подальших досліджень та проектування нових рішень у сфері бездротових сенсорних мереж. Ступінь впровадження: розроблені підходи можуть бути застосовані в промислових та екологічних системах моніторингу, а також для створення систем "розумного" управління міською інфраструктурою, що дозволяє оптимізувати використання ресурсів і знижувати витрати на їх експлуатацію.

Ключові слова: БЕЗДРОТОВІ СЕНСОРНІ МЕРЕЖІ, ІНТЕРНЕТ РЕЧЕЙ, ПРОТОКОЛИ ЗВ’ЯЗКУ, ЕНЕРГОЗБЕРЕЖЕННЯ, ТОПОЛОГІЯ МЕРЕЖ, ЗАСТОСУВАННЯ, БЕЗПЕКА ДАНИХ, МОНІТОРИНГ.

ABSTRACT

The aim of the work is to study the architecture, protocols and main areas of application of wireless sensor networks in modern technologies. The main attention is paid to the analysis of network architecture, including components, topologies and energy-saving mechanisms, as well as protocols at different levels of interaction and their features to ensure high efficiency.

The application area covers the Internet of Things, industrial monitoring systems, environmental monitoring, smart agriculture, medicine and smart cities. Technological and technical and operational characteristics include low power consumption, high scalability and flexible configurations, which makes these systems suitable for operation in energy-constrained environments.

The paper substantiates the degree of implementation of wireless sensor networks in various fields of activity, implements a sensor network model, investigates energy consumption management mechanisms, and develops recommendations for the selection of protocols to improve network efficiency. Security issues and prospects for the development of technologies related to sensor networks are separately considered, taking into account modern cybersecurity challenges and innovative methods of information protection.

The work has practical value and can be used for further research and design of new solutions in the field of wireless sensor networks. Degree of implementation: the developed approaches can be applied in industrial and environmental monitoring systems, as well as to create "smart" urban infrastructure management systems, which allows optimizing the use of resources and reducing the costs of their operation.

Keywords: WIRELESS SENSOR NETWORKS, INTERNET OF THINGS, COMMUNICATION PROTOCOLS, ENERGY CONSERVATION, NETWORK TOPOLOGY, APPLICATIONS, DATA SECURITY, MONITORING.

ЗМІСТ

ВСТУП

Актуальність обраної теми. У сучасних умовах розвитку цифрових технологій бездротові сенсорні мережі відіграють ключову роль у формуванні Інтернету речей, кіберфізичних систем та розумних середовищ. Вони складаються з численних автономних сенсорних вузлів, які забезпечують збирання, передавання та обробку даних із фізичного середовища, відкриваючи нові можливості для моніторингу, автоматизації та підтримки прийняття рішень.

Завдяки низькій вартості, енергоефективності й простоті розгортання, бездротових сенсорних мереж широко застосовуються в екологічному моніторингу, медицині, сільському господарстві, “розумних” містах, промисловості та логістиці. Їх ефективне використання потребує глибокого розуміння архітектури, комунікаційних протоколів, енергозберігаючих рішень і засобів захисту.

Особливого значення набуває робота бездротових сенсорних мереж в умовах обмежених ресурсів та зростання ризиків кіберзагроз у межах IoT. Актуальними залишаються питання масштабованості, маршрутизації та стійкості до атак. Інтеграція з технологіями штучного інтелекту та Edge Computing відкриває нові можливості застосування бездротових сенсорних мереж у реальному часі.

Мета дослідження. Метою роботи є всебічне дослідження архітектури, комунікаційних протоколів, топологій, енергозберігаючих алгоритмів та напрямів застосування бездротових сенсорних мереж. Акцент зроблено на аналізі ефективності, масштабованості, безпеки, енергоощадності й потенціалу інтеграції бездротових сенсорних мереж з технологіями IoT, штучного інтелекту та обчислень на периферії.

Завдання дослідження. У відповідності до поставленої мети формулюються такі завдання дослідження:

1. Аналіз теоретичних основ функціонування бездротових сенсорних мереж і визначення їхнього місця в сучасній цифровій інфраструктурі;

2. Дослідження рівневої архітектури бездротових сенсорних мереж та типових топологій побудови мереж;

3. Аналіз основних протоколів взаємодії на різних рівнях моделі OSI: фізичному, канальному, мережевому, транспортному та прикладному;

4. Вивчення сучасних алгоритмів маршрутизації та енергозберігаючих рішень;

5. Оцінка механізмів захисту інформації та криптографічних методів у бездротових сенсорних мережах;

6. Огляд практичних прикладів використання бездротових сенсорних мереж у різних галузях;

7. Проведення експериментального моделювання бездротових сенсорних мереж із використанням актуальних програмних інструментів NS-3, OMNeT++, Cooja;

8. Розробка практичних рекомендацій щодо покращення функціонування бездротових сенсорних мереж на основі отриманих результатів.

Об’єкт дослідження. Об’єктом дослідження є бездротові сенсорні мережі як самоконфігуровані розподілені системи з автономних сенсорних вузлів, здатних до збору, обробки й передавання даних у реальному середовищі. Такі мережі застосовуються в екологічному моніторингу, сільському господарстві, промисловості, медицині, Smart City та кіберфізичних системах.

Предмет дослідження. Предметом дослідження є теоретичні й прикладні основи побудови, функціонування, маршрутизації, моделювання, енергоефективного управління та захисту бездротових сенсорних мереж, а також шляхи їх інтеграції у цифрові інфраструктури. Особлива увага приділяється архітектурним рішенням, протоколам, підтримці QoS та можливостям практичного застосування.

РОЗДІЛ 1
АРХІТЕКТУРА БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

1.1 Основні компоненти бездротових сенсорних мереж (сенсори, вузли, шлюзи)

Бездротова сенсорна мережа — це децентралізована система, що складається з великої кількості датчиків і виконуючих пристроїв, які взаємодіють між собою через радіосигнал. Завдяки можливості ретрансляції даних між вузлами, зона покриття такої мережі може варіюватися від кількох метрів до кількох кілометрів.

Сенсор — це пристрій, який виявляє зміни в навколишньому середовищі та реагує на певний вихід в іншій системі. Сенсор перетворює фізичне явище на вимірну аналогову напругу, що перетворюється на зрозумілий для людини дисплей або передається для зчитування чи подальшої обробки.

Одним із найвідоміших сенсорів є мікрофон, який перетворює звукову енергію на електричний сигнал, який можна посилювати, передавати, записувати та відтворювати.

Існує багато типів сенсорів, які були винайдені для вимірювання фізичних явищ:

1. Термопари, RTD і термістори для вимірювання температури;
2. Тензодатчики для вимірювання напруги на об’єкті, напруга, вага тощо;
3. Тензодатчики для вимірювання ваги та навантаження;
4. Сенсори LVDT використовуються для вимірювання зміщення на відстані;
5. Акселерометри вимірювання вібрації та ударів;
6. Мікрофони для захоплення звукових хвиль;
7. Перетворювачі струму для вимірювання змінного або постійного струму;

8. Трансформатори напруги для вимірювання потенціалів високої напруги;

9. Оптичні сенсори використовуються для виявлення світла, передачі даних і заміни звичайних сенсорів;

10. Сенсори камери використовуються для зйомки окремих і безперервних 2D-зображень;

11. Цифрові сенсори використовуються для дискретного ввімкнення/вимкнення підрахунку, лінійного та ротаційного кодування, вимірювання положення тощо;

12. Сенсори позиціонування (GPS) використовуються для визначення поздовжнього та широтного положення на основі GPS, ГЛОНАСС та інших супутникових систем позиціонування [1, 1].

Бездротові сенсорні мережі складаються з компактних обчислювальних пристроїв, оснащених сенсорами, актуаторами та прийомопередавачами, що працюють у визначеному радіочастотному діапазоні. Такий пристрій називають сенсорним вузлом або просто сенсором. Зазвичай сенсорний вузол має розмір не більше одного кубічного дюйма та містить на платі процесор, флеш- і оперативну пам’ять, цифро-аналогові та аналого-цифрові перетворювачі, радіочастотний приймач, джерело живлення, а також різні датчики та актуатори.

Вузли мережевої інфраструктури Компоненти фізичної та віртуальної інфраструктури, які підтримують з’єднання в мережі, є вузлами. Прикладами цього типу вузлів є маршрутизатори, комутатори, концентратори, шлюзи, балансувальники навантаження та бездротові базові станції. Можливі як фізичні, так і віртуальні екземпляри багатьох із цих типів вузлів. Серверні вузли Розміщують пристрої, які надають послуги в мережі для використання іншими пристроями та вузлами. Приклади включають веб-сервери, файлові сервери, сервери електронної пошти та багато іншого. Вузли, які надають послуги в мережі, також відомі як хости. Вузли сервера можуть бути фізичними або віртуальними примірниками. Вузли кінцевих точок Пристрої кінцевих

користувачів, які люди використовують для доступу до мережі та виконання завдань, є вузлами кінцевих точок. Це стосується настільних комп’ютерів, ноутбуків, смартфонів, планшетів і принтерів. Переважна більшість кінцевих пристроїв все частіше є підключеними до мережі IoT-пристроями та датчиками [2, 1].

Окрім компактних розмірів, вузли бездротових сенсорних мереж мають відповідати й іншим суворим вимогам. Вони повинні:

1. Споживати мінімальну кількість енергії;
2. Ефективно функціонувати у великих мережах на невеликих відстанях;
3. Мати низьку собівартість виробництва;
4. Бути автономними та не потребувати обслуговування;
5. Адаптуватися до змін у навколишньому середовищі.

Для виконання своїх функцій кожен сенсорний вузол працює під керуванням спеціалізованої операційної системи. Однією з найвідоміших ОС для сенсорних вузлів є TinyOS — система з відкритим кодом, розроблена в Університеті Берклі. Вона дозволяє сенсорам автоматично встановлювати з’єднання з сусідніми вузлами та формувати сенсорну мережу заданої топології.

Мережевий шлюз — це апаратний пристрій або програмне рішення, яке з’єднує дві дискретні мережі, які використовують різні протоколи передачі. Шлюз діє як точка входу-виходу з мережі та дозволяє передавати дані з однієї дискретної мережі в іншу шляхом трансляції протоколів зв’язку. Можливості мережевого шлюзу включають покращену безпеку, інтелектуальну маршрутизацію та підтримку IoT із можливістю масштабування для підтримки низки варіантів використання від великих корпоративних кампусів до невеликих віддалених філій [3, 1].

Маршрутизатори є одним із прикладів апаратних мережевих шлюзів, оскільки вони забезпечують маршрутизацію даних між різними мережами, використовуючи різні протоколи для їх з'єднання.

Мережеві шлюзи працюють на всіх відомих операційних системах. Їх основне завдання — конвертувати протоколи між різними мережами. Роутер, у свою чергу, приймає, обробляє та передає пакети тільки між мережами, що використовують однакові протоколи. Мережевий шлюз, на відміну від роутера, може прийняти пакет, сформатований за одним протоколом (наприклад, AppleTalk), і перетворити його в пакет іншого протоколу (наприклад, TCP/IP), перш ніж відправити його в інший сегмент мережі.

У великих мережах сервер, який виконує функцію мережевого шлюзу, зазвичай інтегрується з проксі-сервером та міжмережевим екраном. Часто мережевий шлюз об'єднується з роутером, який керує розподілом і конвертацією пакетів між мережами.

Мережевий шлюз може бути спеціальним апаратним роутером або програмним забезпеченням, встановленим на звичайний сервер або персональний комп'ютер.

Функція маршрутизації пакетів через різні неоднорідні мережеві інтерфейси полягає в забезпеченні ефективного перенаправлення даних між мережами, що використовують різні протоколи або фізичні середовища. Локалізація всього оброблюваного трафіку є важливою функцією шлюзу, яка зазвичай реалізується в межах міжмережевого екрану, який забезпечує безпеку та контроль доступу до мережі, фільтруючи непотрібний або небажаний трафік.

Друга функція шлюзу зазвичай реалізується за допомогою спеціального програмного забезпечення (операційної системи), а в деяких випадках може бути вбудованою частиною програмного модуля інтернет-браузера.

Шлюз за умовчанням або шлюз останньої надії — це адреса маршрутизатора, на який направляється трафік, для якого неможливо визначити маршрут за допомогою таблиць маршрутизації. Такий шлюз застосовується в мережах з вираженими центральними маршрутизаторами, малих мережах і клієнтських сегментах. Шлюз за умовчанням задається відповідним записом у

таблиці маршрутизації, який має вигляд «мережа 0.0.0.0 з маскою мережі 0.0.0.0».

1.2 Топології мереж (деревоподібна, зірка, комірчаста тощо)

Топологія комп'ютерної мережі зазвичай визначає логічне взаєморозташування комп'ютерів у мережі та спосіб їх з'єднання лініями зв'язку. Важливо, що це поняття переважно застосовується до локальних мереж, де структура зв’язків добре простежується. У глобальних мережах структура зв’язків часто прихована від користувачів і не є настільки критичною, оскільки кожен сеанс зв'язку може проходити своїм окремим шляхом.

У топології шини комп'ютери з'єднуються коаксіальним кабелем за схемою «монтажного АБО». Інформація, що передається від одного комп'ютера до іншого, поширюється в обидва напрямки. Основні переваги цієї топології — низька вартість і простота прокладання кабелів, а також можливість швидко надіслати повідомлення всім пристроям мережі одночасно. Однак головний недолік — низька надійність.

У мережах з кільцевою топологією дані передаються по кільцю від одного комп'ютера до іншого, зазвичай в одному напрямку. Кожна станція в такій мережі має два з'єднання з іншими станціями. Коли комп'ютер отримує дані, що відповідають його адресі, він копіює їх у свій внутрішній буфер.

Топологія дерева є різновидом топології зірки. Ця топологія має ієрархічний потік даних. У топології дерева використовуються такі протоколи, як DHCP і SAC. У деревовидній топології різноманітні вторинні концентратори з’єднані з центральним концентратором, який містить повторювач. Ці дані перетікають зверху вниз, тобто від центрального концентратора до вторинного, а потім до пристроїв, або знизу вгору, тобто пристроїв, до вторинного концентратора, а потім до центрального концентратора. Це багатоточкове з’єднання та ненадійна топологія, тому що якщо магістраль виходить з ладу, топологія виходить з ладу [4, 1].

У сітчастій топології кожен пристрій підключається до іншого пристрою через певний канал. Кожен пристрій підключається до іншого через виділені канали. Ці канали називаються посиланнями. У сітчастій топології використовуються такі протоколи: AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol) тощо.

Змішана (гібридна) топологія - це комбінація двох або більше різних мережевих топологій. Однак не кожне об'єднання вважається гібридним — якщо поєднання не змінює загальну структуру мережі, то мережа залишається в межах однієї топології [4, 1].

Топологія подвійного кільця використовується в мережах FDDI та забезпечує підвищену надійність завдяки вбудованій надлишковості. В такій мережі є два кільця: основне, призначене для передавання даних, і допоміжне, яке використовується для передавання керуючих сигналів. У нормальному режимі мережа може здійснювати передавання даних в обох напрямках.

У лінійній топології кожен комп'ютер з'єднаний із сусідніми вузлами — попереднім і наступним, утворюючи послідовний ланцюг. Вона є похідною від кільцевої топології, яка виникає після видалення одного з'єднання, що розриває кільце.

Зіркова топологія є єдиною мережею з чітко визначеним центром, до якого підключаються всі інші вузли. Обмін даними здійснюється виключно через центральний вузол, який несе основне навантаження, тому зазвичай використовується лише для керування мережею.

З точки зору стійкості до відмов, зіркова топологія має як переваги, так і недоліки. Вихід з ладу периферійного пристрою або його мережевого обладнання не впливає на загальну роботу мережі – інші вузли продовжують функціонувати без змін.

Комірчаста топологія є однією з основних комп'ютерних мережевих структур. Вона передбачає розташування вузлів у вигляді комірок, які

найчастіше мають гексагональну або квадратну форму. Ця топологія може використовуватися як у провідних, так і в бездротових мережах.

Основні характеристики комірчастої топології:

1. Кожен комп’ютер чи пристрій розташовується в окремій "клітині" або "комірці", що може бути представлена геометричною фігурою, наприклад, гексагоном або квадратом. Кожна клітина зазвичай містить один або кілька вузлів;

2. Клітини зазвичай з’єднані зі своїми сусідніми клітинами через зв’язки, які можуть бути як провідними, так і бездротовими, залежно від конкретної реалізації мережі;

3. У комірчастій топології маршрутизація даних здійснюється через сусідні клітини. Кожен вузол може передавати дані безпосередньо своїм сусідам або маршрутувати їх через кілька клітин до досягнення кінцевої точки призначення;

4. Комірчаста топологія є дуже масштабованою, оскільки її легко розширювати шляхом додавання нових клітин або вузлів.

1.3 Енергозалежність і енергозберігаючі механізми

Найбільш енерговитратною операцією для сенсорних вузлів є передача даних у бездротовому середовищі. Тому використання енергозберігаючих методів передачі даних є важливим аспектом для продовження терміну служби сенсорів, оскільки їх робота значною мірою залежить від ресурсу батарей.

Враховуючи різні варіанти використання мережевих ресурсів, бездротові сенсорні мережі можна поділити на класи, виходячи з їх функціональних особливостей та типу застосування:

1. Проактивні мережі — це мережі, в яких вузли періодично активують свої сенсори та передавачі, здійснюють зняття показань і передають їх на базову станцію;

2. Реактивні мережі — це мережі, в яких вузли з певною періодичністю знімають показання, але передають їх лише у випадку, коли отримані дані виходять за межі визначеного діапазону нормальних значення;

3. Гібридні мережі поєднують характеристики проактивних і реактивних мереж. В таких мережах сенсорні вузли не лише періодично передають зібрані дані, але й реагують на різкі зміни в показниках, негайно передаючи інформацію на базову станцію у разі виявлення аномалій.

При практичній реалізації бездротових сенсорних мереж виникає низка проблем, серед яких:

1. Обмеження енергоспоживання виникає через те, що сенсори працюють на батареях, які мають обмежений ресурс. Чим рідше потрібно замінювати або заряджати ці батареї, тим дешевше буде обслуговування мережі;

2. Сенсорні мережі зазвичай працюють у віддалених місцях та в складних умовах, де неможливо забезпечити їх обслуговування чи ремонт;

3. Використання бездротових з'єднань створює певні обмеження при розгортанні сенсорних мереж. Одним із таких обмежень є загасання сигналу, яке зменшує відстань, на яку можна передавати інформацію;

4. В таких мережах сенсорні вузли повинні самостійно обмінюватися інформацією з сусідніми вузлами для прийняття рішень про комутацію без глобальної карти мережі;

5. Основною метою бездротових сенсорних мереж є створення малих, дешевих та ефективних пристроїв;

6. Віддалене розташування сенсорів і їх автономна робота підвищують вразливість до зовнішніх вторгнень і атак. Завдяки бездротовому з'єднанню зловмисникам легше перехоплювати пакети.

Однією з основних вимог до вузлів сенсорної мережі є забезпечення тривалого часу їх автономної роботи. Задача зменшення енергоспоживання може вирішуватися через оптимізацію конструкції та режимів роботи аналогових і

цифрових схем вузлів, а також за рахунок отримання енергії з навколишнього середовища.

У навколишньому середовищі існують чотири основні джерела енергії: механічна енергія (вібрації, деформації), теплова енергія (температурні перепади або зміни), енергія випромінювання (сонячне світло, інфрачервоні промені, радіочастоти) та хімічна енергія (хімічні і біохімічні процеси). Кожне з цих джерел має різну щільність потужності, що визначає їх потенціал для використання в якості джерела енергії для сенсорних мереж.

У сенсорних мережах можна виділити три типових рівні споживаної потужності:

1. 1-5 мкВт - споживання енергії в "сплячому" режимі, коли сенсорні вузли не виконують активних операцій і перебувають у стані очікування;
2. 500 мкВт - 1 мВт - споживання енергії в активному режимі, коли сенсори знімають показання або виконують інші функції обробки даних;
3. 50 мВт - пік передачі енергії, коли вузол передає дані через бездротове з'єднання, що є найвищим енергоспоживанням.

1.4 Протоколи фізичного та канального рівня (IEEE 802.15.4, Zigbee, Bluetooth Low Energy)

IEEE 802.15.4 — це недорога технологія бездротового доступу з низькою швидкістю передачі даних для пристроїв, які працюють або працюють від батарейок. Це описує, як функціонують низькошвидкісні бездротові персональні мережі (LR-WPAN).

Для чого потрібна IEEE 802.15.4e:

1. 802.15.4e для промислових застосувань і 802.15.4g для інтелектуальних комунальних мереж;
2. 802.15.4e покращує старий стандарт, запроваджуючи такі механізми, як доступ із інтервалами часу, багатоканальний зв’язок і перемикання каналів.

IEEE 802.15.4e містить наступні загальні функціональні вдосконалення:

1. Low Energy призначений для додатків, які можуть обмінювати затримку на енергоефективність. Це дозволяє вузлу працювати з дуже низьким робочим циклом;

2. Інформаційні елементи - це розширюваний механізм для обміну інформацією на підрівні MAC;

3. Покращені маяки є розширенням кадрів маяків 802.15.4 і забезпечують більшу гнучкість. Вони дозволяють створювати фрейми для конкретної програми;

4. Багатоцільовий кадр забезпечує гнучкий формат кадру, який може адресувати низку операцій MAC. Він заснований на IE;

5. Метрика продуктивності MAC - це механізм для надання належного зворотного зв'язку щодо якості каналу мережевим і верхнім рівням;

6. Швидка асоціація (FastA) – це процедура асоціації 802.15.4 передбачає значну затримку з метою економії енергії [5, 1].

ZigBee — це бездротовий стандарт передачі даних, який підтримується та розвивається альянсом ZigBeeTM. Цей альянс був заснований у 2002 році для координації зусиль із розробки ефективних протоколів зв'язку та забезпечення сумісності пристроїв різних виробників.

Меш-топологія Zigbee дозволяє підключати кілька пристроїв, забезпечуючи резервування та надійність у мережі. Mesh-мережі децентралізовані, тобто кожен вузол здатний самостійно виявляти в мережі. Коли вузли залишають мережу, вузли переналаштовують шляхи маршрутизації на основі нової структури мережі. Топологія сітки та спеціальна маршрутизація створюють кращу стабільність у змінних хвильових умовах або у разі збою на окремих вузлах [6, 1].

ZigBee має високу швидкість активації: пристрій може перейти з режиму сну в активний стан всього за 30 мілісекунд або навіть швидше. Завдяки тому, що пристрої ZigBee більшу частину часу знаходяться в сплячому режимі, вони споживають мінімальну кількість енергії, що дозволяє значно продовжити

термін роботи від батарей. Перший випуск протоколу отримав назву ZigBee 2004. Наступна версія, ZigBee 2006, замінила застарілу структуру MSG/KVP новою «бібліотекою кластерів». Актуальною на даний момент є реалізація ZigBee 2007, яка містить два основних профілі: стековий профіль №1, відомий просто як ZigBee, орієнтований на домашнє та мале комерційне застосування, і стековий профіль №2, який називають ZigBee Pro, призначений для більш складних мережевих рішень.

Bluetooth Low Energy, також відомий як Bluetooth Smart, — це технологія цифрової бездротової передачі даних, що відзначається наднизьким енергоспоживанням та малим радіусом дії (близько 10 м). Вона використовує недорогі мікросхеми у передавальних пристроях і потенційно може стати відкритим стандартом для бездротового зв'язку. Спочатку ця технологія була відома як Wibree, а в червні 2007 року її перейменували на Bluetooth Ultra Low Power. У 2008 році вона отримала свою сучасну назву — Bluetooth Low Energy.

Інтернет речей — це мережа мільярдів пристроїв — «речей», які підключені бездротовим способом для обміну даними через Інтернет. Технологія IoT допомагає підключати такі речі, як термостати, розумні світильники, людей із вбудованими медичними пристроями, тварин із імплантованими трекерами та автомобілі з датчиками допомоги водієві.

Щоб зробити всі ці з'єднання можливими, IoT покладається на бездротові технології. ZigBee, Bluetooth Classic і Wi-Fi можна використовувати для бездротового підключення пристроїв. Однак BLE часто розглядається як найбільш оптимальна технологія для додатків Інтернету речей через дві основні причини:

1. Низьке енергоспоживання. Багато пристроїв IoT живляться від батареї і повинні працювати в польових умовах дуже довго.

2. Тип даних, якими обмінюються. BLE оптимізовано для передачі невеликої кількості даних. Це чудово працює для пристроїв Інтернету речей, таких як датчики, яким просто потрібно передавати дані про стан [7, 1].

Wibree була розроблена для роботи поряд із Bluetooth, забезпечуючи енергоефективну передачу даних. Вона функціонує в частотному діапазоні 2,4 ГГц і підтримує фізичну швидкість передачі до 1 Мбіт/с.

1.5 Протоколи мережевого рівня (Routing Protocols, LEACH)

Протокол маршрутизації – це мережевий протокол, який використовується маршрутизаторами для вибору оптимальних шляхів передачі даних у комп'ютерній мережі. Його застосування усуває необхідність ручного налаштування всіх можливих маршрутів, що зменшує ризик помилок, забезпечує узгоджену роботу всіх маршрутизаторів у мережі та спрощує завдання адміністраторів.

Протоколи маршрутизації поділяються на два типи залежно від алгоритмів, що лежать в їх основі:

1. Дистанційно-векторні протоколи, що базуються на алгоритмі Distance Vector Algorithm (DVA);
2. Протоколи стану каналу зв'язку, що використовують алгоритм Link State Algorithm (LSA).

Протоколи маршрутизації класифікуються за сферою застосування на два типи:

1. Міждоменна маршрутизація;
2. Внутрішньодоменна маршрутизація.

Дистанційно-векторні протоколи:

1. RIP (Routing Information Protocol);
2. IGRP (Interior Gateway Routing Protocol);
3. BGP (Border Gateway Protocol);
4. EIGRP (Enhanced Interior Gateway Routing Protocol);
5. AODV (Ad hoc On-Demand Distance Vector).

Протоколи стану каналу зв'язку:

1. IS-IS (Intermediate System to Intermediate System);

2. OSPF (Open Shortest Path First);
3. NLSP (NetWare Link-Services Protocol);
4. HSRP і CARP;
5. OLSR (Optimized Link State Routing);
6. TBRPF (Topology Broadcast based on Reverse-Path Forwarding).

Протокол інформації про маршрутизацію (RIP) покладається на кількість переходів для визначення найкоротшого шляху між мережами. RIP — це застарілий протокол, який сьогодні ніхто не використовує.

Протокол Open Shortest Path First (OSPF) збирає інформацію з усіх інших маршрутизаторів в автономній системі, щоб визначити найкоротший і найшвидший маршрут до місця призначення пакета даних.

BGP визначає зв'язок через Інтернет. Інтернет — це велика сукупність автономних систем, які з’єднані разом. Кожна автономна система має номер автономної системи (ASN), який вона отримує, зареєструвавшись в Управлінні з присвоєння номерів Інтернету.

BGP працює шляхом відстеження найближчих ASN і зіставлення адрес призначення з відповідними ASN [8, 1].

Low-energy adaptive clustering hierarchy (LEACH) — це кластерний протокол, який мінімізує розсіювання енергії в сенсорних мережах. Метою LEACH є випадковий вибір вузлів датчиків як головок кластера, щоб високе розсіювання енергії під час зв’язку з базовою станцією поширювалося на всі вузли датчиків у мережі [9, 1].

Протокол LEACH працює у дві фази: формування кластерів та передача даних спочатку cluster head’у, а потім – на базову станцію. Вибір cluster head’а відбувається поетапно. Спочатку кожен вузол має шанс стати головним вузлом з певною ймовірністю. Якщо вузол не був обраний, він може отримати цю роль пізніше. Процес вибору залежить від заданої щільності cluster head’ів у мережі. Щоб рівномірно розподіляти енергетичне навантаження, cluster head’и періодично змінюються. Новопризначений cluster head повідомляє про свій

статус усім вузлам мережі. Кожен вузол обирає, до якого кластера приєднатися, орієнтуючись на енергетичну ефективність. Після формування кластерів cluster head створює розклад для передачі даних кожним вузлом.

На етапі самоорганізації відбувається формування кластерів. Кожен cluster head надсилає ADV-повідомлення за допомогою протоколу CSMA/CA. Це повідомлення містить ідентифікатор вузла та заголовок, який вказує, що це саме ADV-повідомлення. Вузли аналізують силу сигналу від кожного cluster head'а і вибирають найбільш оптимальний кластер для приєднання. Потім вони надсилають своєму вибраному cluster head'у join-request–повідомлення (також через CSMA/CA), яке містить ідентифікатор як вузла, так і головного вузла кластера. Після цього cluster head створює TDMA-розклад, що дозволяє уникнути колізій під час передачі даних та сприяє збереженню енергії вузлів.

Після формування кластерів починається фаза передачі даних, яка складається з кількох етапів. Кожен вузол надсилає свої дані у визначений для нього часовий інтервал. Отримавши інформацію від усіх вузлів свого кластера, cluster head обробляє та формує власне повідомлення. Далі cluster head передає ці дані на базову станцію.

Переваги протоколу LEACH:

1. Адаптивний самоорганізувальний протокол дозволяє рівномірно розподіляти енергетичне навантаження серед усіх вузлів мережі;
2. Обробка даних на cluster head'і дозволяє знизити обсяг переданих даних, що оптимізує використання мережі;
3. Кількість кластерів можна визначити наперед, виходячи з топології мережі та балансу між затратами на обробку та передачу даних;
4. Перше відключення вузла відбувається вісім разів пізніше, ніж у випадку використання прямої передачі чи статичних кластерних протоколів.

1.6 Протоколи транспортного рівня, протоколи для керування живленням і передачі даних

Транспортний рівень (Transport layer) — це 4-й рівень моделі OSI, який забезпечує доставку даних без помилок, втрат і дублювання, а також гарантує їхнє правильне впорядкування відповідно до початкової послідовності передачі. Цей рівень не залежить від типу даних, їхнього джерела або призначення, оскільки він відповідає лише за механізм передачі. Транспортний рівень розбиває блоки даних на фрагменти, розмір яких визначається конкретним протоколом: короткі фрагменти об'єднуються в один, а довгі — розділяються на частини [10, 1].

Приклади протоколів транспортного рівня:

1. CUDP, Cyclic UDP;
2. SCTP, Stream Control Transmission Protocol;
3. TCP, Transmission Control Protocol.

Протокол UDP (User Datagram Protocol) — це протокол зв’язку для чутливих до часу програм, як-от ігор, відтворення відео або пошуку в системі доменних імен (DNS).

Протокол UDP використовується такими сервісами та протоколами вищого рівня:

1. TFTP (Trivial File Transfer Protocol) — найпростіший протокол передачі файлів;
2. SNMP (Simple Network Management Protocol) — простий протокол управління мережею;
3. DHCP (Dynamic Host Configuration Protocol) — протокол динамічної конфігурації вузла;
4. DNS (Domain Name System) — служба доменних імен.

Stream Control Transmission Protocol (SCTP) — це мережевий протокол, орієнтований на з’єднання, для одночасної передачі кількох потоків даних між двома кінцевими точками, які встановили з’єднання в комп’ютерній мережі.

Іноді відомий як протокол керування передачею нового покоління або TCPng, SCTP дозволяє легко підтримувати телефонне з'єднання через інтернет [11, 1].

Переваги використання SCTP включають:

1. Множинні інтерфейси (Multihoming). Два хости мають хоча б один з яких має кілька мережевих інтерфейсів і, відповідно, кілька IP-адрес;
2. Пошук шляху з моніторингом. Протокол обирає первинний маршрут для передачі даних та здійснює перевірку і моніторинг зв'язності цього шляху;
3. Механізми перевірки дійсності. Захист від flood-атак за допомогою технології 4-way handshake, а також повідомлення про втрачені пакети і порушені ланцюжки;
4. Покращена система контролю помилок, яка оптимально підходить для jumbo-пакетів в Ethernet.

Протокол керування передачею (TCP) — це стандарт зв'язку, який дозволяє прикладним програмам і комп'ютерним пристроям обмінюватися повідомленнями через мережу. Він призначений для надсилання пакетів через інтернет і забезпечення успішної доставки даних і повідомлень через мережі.

TCP є одним із основних стандартів, які визначають правила Інтернету, і входить до стандартів, визначених інженерною робочою групою Інтернету (IETF). Це один із найбільш часто використовуваних протоколів у цифровій мережі зв'язку, який забезпечує наскрізну доставку даних [12, 1].

TCP отримує потоки даних від протоколів вищих рівнів моделі OSI, початковим джерелом яких є протоколи прикладного рівня, такі як HTTP, FTP та інші. Кожен протокол верхнього рівня має свій специфічний TCP-порт.

TCP розбиває потік даних на частини і додає до кожної з них заголовок з номером послідовності. Ці частини даних, відомі як TCP-сегменти, після цього інкапсулюються в IP-пакет і передаються через IP-протокол до хоста-отримувача.

Після того як IP-пакет надходить до хоста-отримувача, перевіряється коректність даних у TCP-сегменті за допомогою контрольної суми, а також підтверджується, що попередні сегменти були успішно отримані. Потім хост-отримувач надсилає запит до хоста-відправника на повторне або нове передавання порції даних, що однозначно підтверджує успішне отримання всіх сегментів з номерами послідовності, меншими за номер нового запиту.

Power over Ethernet (PoE) — це технологія, яка дозволяє передавати електроенергію та дані через один кабель "звитої пари". Завдяки цьому можна використовувати один кабель для передачі як даних, так і живлення для периферійних пристроїв, які є частинами мережі Ethernet, таких як пристрої VoIP, бездротові мережеві адаптери і точки доступу, вебкамери тощо.

Існує дві специфікації стандартних реалізацій PoE, IEEE 802.3af (2003) та IEEE 802.3at (2009), які враховують різні рівні потужності.

Перший стандарт IEEE 802.3af PoE забезпечує до 15,4 Вт живлення постійного струму на інтерфейс комутатора (сторона PSE). Через розсіювану потужність у кабелі лише 12,95 Вт гарантовано буде доступним для кінцевого клієнта. Оскільки технологія стала популярною та широко розповсюдженою, потреба кінцевих клієнтів у потужності зросла. Це призвело до впровадження стандарту IEEE 802.3at, відомого як PoE+. Він забезпечує до 30 Вт живлення постійного струму на інтерфейс комутатора, забезпечуючи 25,5 Вт потужності на кінцевому пристрої.

Обидва стандарти забезпечують електричне живлення через дві з чотирьох пар кабелю UTP, cat5e або краще [13, 1].

Технологія USB Power Delivery дозволяє передавати енергію потужністю до 100 Вт, що достатньо для живлення та зарядки будь-яких смартфонів, планшетів та інших гаджетів. Завдяки цій технології, стало можливим живлення та заряджання електронних пристроїв за допомогою звичайного USB-кабелю.

HTTP — це протокол передачі даних, що використовується в комп'ютерних мережах. Абревіатура походить від Hypertext Transfer Protocol, і

він є частиною 7-го прикладного рівня моделі OSI, що відповідає за передачу гіпертекстових документів.

Основне призначення протоколу HTTP — це передача вебсторінок. Однак завдяки своїй універсальності, HTTP також ефективно використовується для передачі інших файлів, що дозволяє йому конкурувати з більш складним FTP-протоколом.

HTTP передбачає, що клієнтська програма, як-от веббраузер, має можливість коректно відображати гіпертекстові вебсторінки та файли інших форматів у зручному для користувача вигляді. Для забезпечення правильного відображення HTTP надає клієнтові можливість визначити мову та кодування символів вебсторінки.

Типовий HTTP-запит містить:

1. Тип версії HTTP;
2. URL;
3. Метод HTTP;
4. Заголовки запитів HTTP;
5. Додаткове тіло HTTP.

Метод HTTP, який іноді називають дієсловом HTTP, вказує на дію, яку HTTP-запит очікує від запитуваного сервера. Наприклад, двома найпоширенішими методами HTTP є «GET» і «POST»; запит «GET» очікує повернення інформації, тоді як запит «POST» зазвичай вказує на те, що клієнт надсилає інформацію на веб-сервер [14, 1].

FTP (англ. File Transfer Protocol, укр. протокол передавання файлів) — це загальноприйнятий мережевий протокол прикладного рівня, який використовується для обміну файлами між клієнтом і сервером у комп'ютерних мережах.

Для забезпечення захисту даних і процесу автентифікації застосовують FTPS — варіант FTP, що використовує SSL/TLS, або SFTP — розширення протоколу SSH, призначене для безпечного передавання файлів.

Перші FTP-клієнти з’явилися ще до впровадження графічного інтерфейсу в операційних системах, тому мали вигляд командного рядка.

Типова передача по FTP працює таким чином:

1. Користувачеві зазвичай потрібно ввійти на FTP-сервер, хоча деякі сервери роблять частину або весь вміст доступним без входу в систему, модель, відома як анонімний FTP;

2. Клієнт ініціює розмову з сервером, коли користувач просить завантажити файл;

3. За допомогою FTP клієнт може завантажувати, завантажувати, видаляти, перейменовувати, переміщувати та копіювати файли на сервері [15, 1].

Simple Mail Transfer Protocol (SMTP) є комунікаційним протоколом, що використовується для надсилання електронних листів.

SMTP був затверджений як Інтернет-стандарт у 1982 році в RFC 821, а у 2008 році оновлений до ESMTP (Extended SMTP, або Розширений SMTP) у RFC 5321, який залишається актуальним і сьогодні. Цей протокол застосовується поштовими серверами та іншими системами передачі повідомлень для відправлення та отримання електронної пошти.

Приватні системи, такі як Microsoft Exchange Server і HCL Domino, а також вебпоштові сервіси, зокрема Outlook.com, Gmail і Yahoo! Mail, можуть застосовувати нестандартні протоколи всередині своєї інфраструктури. Однак для надсилання та отримання електронної пошти за межами цих систем використовується SMTP. Як правило, SMTP-сервери працюють через TCP.

Компоненти SMTP:

1. Mail User Agent (MUA) - це комп’ютерна програма, яка допомагає вам надсилати та отримувати пошту. Він відповідає за створення повідомлень електронної пошти для передачі агенту передачі пошти (MTA);

2. Mail Submission Agent (MSA) - це комп’ютерна програма, яка отримує пошту від Mail User Agent (MUA) і взаємодіє з Mail Transfer Agent (MTA) для передачі пошти;

3. Агент передачі пошти (MTA) - це програмне забезпечення, яке виконує роботу з передачі пошти з однієї системи в іншу за допомогою SMTP;

4. Агент доставки пошти (MDA) - це агент доставки пошти або локальний агент доставки — це, по суті, система, яка допомагає доставляти пошту в локальну систему [16, 1].

РОЗДІЛ 2
ЗАСТОСУВАННЯ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

2.1 Інтернет речей (IoT) та роль сенсорних мереж у цій технології

Інтернет речей — це концепція мережі, що об'єднує фізичні пристрої з вбудованими давачами та програмним забезпеченням, яке забезпечує передачу й обмін даними між реальним світом і комп'ютерними системами в автоматичному режимі через стандартні комунікаційні протоколи. Окрім давачів, така мережа може включати виконавчі пристрої, інтегровані у фізичні об'єкти та з'єднані між собою дротовими або бездротовими технологіями. Ці пристрої здатні зчитувати інформацію, виконувати дії, програмуватися та ідентифікуватися, що дозволяє мінімізувати необхідність людського втручання завдяки використанню інтелектуальних інтерфейсів.

Також набуває популярності термін Internet of Everything (IoE) — всеохопний або всеосяжний інтернет. Розвиток цього явища викликав занепокоєння щодо конфіденційності даних та сприяв появі нового поняття — безпека Інтернету речей.

Термін «Інтернет речей» вперше запровадив Кевін Ештон у 1999 році під час роботи в компанії Procter & Gamble. Він використовував його для опису системи, в якій фізичні об’єкти могли підключатися до мережі Інтернет за допомогою давачів. Ештон ввів цей термін, щоб продемонструвати можливості радіочастотної ідентифікації (RFID), що застосовується в корпоративних системах постачання для автоматичного підрахунку та відстеження товарів без залучення людини. Сьогодні Інтернет речей є загальновживаним терміном для позначення сценаріїв, у яких інтернет-з’єднання та обчислювальні потужності поширюються на різноманітні пристрої, давачі та повсякденні об’єкти.

Пристрої Інтернету речей, також відомі як «розумні об’єкти», можуть варіюватися від простих пристроїв «розумного дому», таких як розумні термостати, до переносних пристроїв, таких як розумні годинники та одяг із підтримкою RFID, до складного промислового обладнання та транспортних

систем. Технологи навіть уявляють собі цілі «розумні міста», засновані на технологіях IoT.

IoT дозволяє цим розумним пристроям спілкуватися один з одним та з іншими пристроями з підтримкою Інтернету. Як смартфони та шлюзи, створюючи величезну мережу взаємопов’язаних пристроїв, які можуть обмінюватися даними та виконувати різні завдання автономно [17, 1].

Основні технології Інтернету речей:

1. Для інтеграції повсякденних речей у мережу необхідне використання кількох технологій;
2. Для ідентифікації кожного об'єкта необхідна проста та компактна технологія;
3. Для моніторингу змін у стані елементів або навколишнього середовища об'єкти мають бути оснащені датчиками;
4. Обробка та збереження даних, отриманих від датчиків, повинні здійснюватися за допомогою вбудованого комп'ютера;
5. Для обміну даними між пристроями можуть застосовуватися технології бездротового зв’язку, такі як Wi-Fi, Bluetooth, ZigBee, 6LoWPAN;
6. Для передачі даних застосовуються ефективні та малоресурсні протоколи, такі як MQTT. Вони працюють за принципом публікації та підписки.

2.2 Застосування в промисловості (промисловий IoT, моніторинг обладнання)

Промисловий Інтернет Речей — це комплекс взаємопов’язаних комп’ютерних мереж та підключених до них виробничих об'єктів, оснащених вбудованими датчиками та програмним забезпеченням. Він забезпечує збір і обмін даними, а також віддалений контроль та управління у автоматизованому режимі без прямої участі людини.

На початковому етапі впровадження IIoT промислове обладнання оснащується датчиками, виконавчими механізмами, контролерами та людино-

машинними інтерфейсами. Це дає змогу збирати дані, що забезпечують керівництво об’єктивною та точною інформацією про стан виробництва. Оброблені дані стають доступними для всіх підрозділів підприємства, сприяючи ефективній взаємодії між співробітниками та прийняттю обґрунтованих рішень.

Отримані дані можуть використовуватися для запобігання непередбаченим простоям, поломкам обладнання, скорочення кількості незапланованих технічних обслуговувань та збоїв в управлінні ланцюгами постачання. Це сприяє підвищенню ефективності роботи підприємства.

Підключені датчики та виконавчі механізми дозволяють компаніям швидше виявляти неефективність і проблеми, заощаджуючи час і гроші, а також підтримуючи зусилля бізнес-аналітики. Зокрема, у виробництві IIoT має потенціал для забезпечення контролю якості, стійких і екологічних практик, відстеження ланцюга постачання та загальної ефективності ланцюга постачання. У промисловому середовищі IIoT є ключовим для таких процесів, як прогнозне технічне обслуговування, покращене обслуговування на місцях, управління енергією та відстеження активів [18, 1].

Яскравим прикладом використання Промислового Інтернету Речей є проєкт компанії Harley Davidson, відомої своїми легендарними мотоциклами. Основним викликом для компанії стала низька швидкість реагування на запити клієнтів в умовах зростаючої конкуренції, а також обмежена можливість дилерів налаштовувати п’ять доступних моделей.

Види технічного обслуговування:

1. Експлуатація до відмови виконується лише після виходу з ладу певної деталі машини. Цей підхід передбачає періодичну заміну незалежно від їх поточного стану, заміни не тільки зношених, але і працездатних деталей;

2. Технічне обслуговування за фактичним станом передбачає моніторинг і аналіз стану обладнання під час його роботи.

Діагностичні інструменти:

1. Термометри – використовуються для виявлення зон з підвищеною температурою, що може свідчити про перегрів або несправності обладнання;

2. Тахометр – прилад для вимірювання швидкості обертання, який допомагає контролювати роботу механізмів, запобігати несправностям і підвищувати безпеку експлуатації;

3. Детектор стану масла – важливий інструмент для обслуговування механізмів, призначений для контролю рівня та якості мастила в системі.

2.3 Екологічний моніторинг та "розумне" сільське господарство

Бездротові сенсорні мережі відіграють ключову роль у сучасному екологічному моніторингу, забезпечуючи автоматизований збір та обробку даних про стан довкілля. Ці системи складаються з великої кількості мініатюрних датчиків, які розміщуються на територіях, що потребують постійного спостереження. Вони здатні працювати автономно, передаючи інформацію у реальному часі через бездротові канали зв’язку, такі як Wi-Fi, LoRa, ZigBee або мобільні мережі.

Сенсори можуть визначати концентрацію таких забруднювальних речовин, як діоксид вуглецю, оксиди азоту, сірчаний газ, тверді частинки PM2.5 і PM10, які є основними показниками стану атмосфери у містах та промислових зонах. Особливо важливим є використання таких систем у мегаполісах, де рівень забруднення може змінюватися впродовж дня залежно від трафіку, роботи підприємств та погодних умов. Завдяки бездротовим сенсорним мережам можна не лише оперативно виявляти підвищення рівня шкідливих речовин, а й прогнозувати розвиток ситуації, що дозволяє вживати відповідних заходів, наприклад, обмежувати рух транспорту або знижувати інтенсивність роботи промислових об'єктів у певні періоди.

Також сенсори, встановлені у річках, озерах, водосховищах і навіть у ґрунтових водах, здатні визначати рівень забруднення, температуру, кислотність, концентрацію розчиненого кисню та наявність небезпечних

хімічних сполук. Така технологія є незамінною для запобігання екологічним катастрофам, особливо в регіонах із високим рівнем промислового забруднення або інтенсивним сільськогосподарським використанням земель.

Ґрунтовий моніторинг також є важливим аспектом екологічного контролю, оскільки стан землі безпосередньо впливає на продуктивність сільського господарства та здоров'я екосистем. Бездротові сенсорні мережі дозволяють вимірювати рівень вологості, температуру, концентрацію мінеральних речовин і виявляти можливу присутність важких металів або пестицидів.

Важливим аспектом використання бездротових сенсорних мереж є спостереження за рівнем радіації, що особливо актуально для територій, які зазнали впливу техногенних катастроф або знаходяться в зоні потенційного ризику. Радіаційні сенсори можуть оперативно виявляти зміни у рівнях випромінювання та попереджати відповідні служби про небезпеку.

Багато сенсорів працюють на сонячних батареях або мають наднизьке енергоспоживання, що дозволяє їм функціонувати роками без необхідності заміни елементів живлення.

Швидкість реагування на екологічні загрози значно підвищується завдяки можливості обробки отриманих даних за допомогою хмарних технологій та штучного інтелекту. Інформація, зібрана численними сенсорами, може бути миттєво проаналізована, а алгоритми машинного навчання допомагають знаходити закономірності та прогнозувати потенційні ризики.

Сучасне сільське господарство активно рухається в напрямку автоматизації, намагаючись зменшити або повністю усунути участь людини в виробничих процесах. У аграрному секторі широко застосовується технологія Інтернету речей (IoT), яка передбачає створення мереж для обміну даними між фізичними об'єктами, оснащеними вбудованими технологіями для взаємодії між собою чи з іншими системами.

Термін «розумне сільське господарство» означає використання таких технологій, як Інтернет речей, датчики, системи визначення місцезнаходження,

роботи та штучний інтелект на вашій фермі. Кінцевою метою є підвищення якості та кількості врожаю при оптимізації людської праці [19, 1].

Інтернет речей у сільському господарстві має широкий спектр застосувань, зокрема для оптимізації і автоматизації таких процесів, як вирощування сільськогосподарських рослин, управління технікою та догляд за тваринами. Окрім цього, IoT технології активно використовуються для моніторингу зовнішніх факторів, таких як погодні умови або шкідники, що допомагає приймати більш обґрунтовані рішення щодо ведення господарства.

Датчики IoT допомагають оптимізувати управління сільським господарством та виробничими процесами, здійснюючи вимірювання таких параметрів, як вологість ґрунту та атмосфери, температура, кількість опадів та рівень поживних речовин у ґрунті.

Працівники можуть використовувати цю інформацію для вдосконалення методів ведення сільського господарства, таких як вибір оптимальних гібридів рослин, створення карт живлення та захисту рослин, сезонне планування аграрних робіт, а також для визначення найбільш сприятливого часу для збирання врожаю.

Дрони стали важливою складовою точного землеробства, і їх інтеграція в загальну мережу Інтернету речей (IoT) відкриває нові можливості для сільськогосподарського сектору. Вони використовуються не лише для моніторингу стану посівів, погодних умов тощо, а й активно застосовуються для обробки посівів або насаджень пестицидами. Дрони дозволяють отримувати високоякісні зображення полів, що є перевагою в порівнянні з супутниковими знімками, оскільки вони можуть працювати в поганих погодних умовах або за складного освітлення, чого супутники часто не здатні зафіксувати.

Також важливо враховувати аспект технічного обслуговування, оскільки довговічність і ремонтопридатність пристроїв стають вирішальними факторами для ефективної роботи в складних і непередбачуваних умовах сільськогосподарського виробництва на відкритому повітрі. Нові системи та

датчики потребуватимуть залучення кваліфікованих інженерів для їхнього встановлення та ремонту, що додає складності у процес обслуговування.

2.4 Застосування у медицині (моніторинг стану пацієнтів)

Сучасна медицина стрімко розвивається завдяки впровадженню новітніх технологій, зокрема бездротових сенсорних мереж. Такі мережі складаються з безлічі компактних біосенсорів, які здатні вимірювати фізіологічні параметри пацієнта та передавати дані на центральний сервер або мобільний пристрій лікаря в режимі реального часу. Це значно покращує точність діагностики, дозволяє швидко реагувати на зміни в стані пацієнта та сприяє розвитку телемедицини.

Бездротові сенсорні мережі складаються з датчиків, які фіксують певні медичні показники, таких як температура тіла, серцевий ритм, рівень кисню в крові, артеріальний тиск, рівень глюкози тощо. Зібрані дані передаються на хмарні сервери або спеціальні приймачі в лікарнях, де вони обробляються та аналізуються. В разі критичних змін система може автоматично сповіщати медичний персонал або самих пацієнтів, що дозволяє оперативно реагувати на потенційно небезпечні ситуації.

Бездротові сенсорні мережі дозволяють безперервно контролювати життєво важливі ознаки та фізіологічні параметри, такі як частота серцевих скорочень, артеріальний тиск, температура та рівень кисню, без необхідності безпосередньої взаємодії з пацієнтом. Цей дистанційний моніторинг сприяє ранньому виявленню аномалій, своєчасному втручанню та покращенню лікування хронічних захворювань [20, 1].

Наприклад, кардіологічні бездротові сенсорні мережі відстежують ритм серця та ЕКГ, передаючи результати лікарям у віддаленому режимі. Це дозволяє запобігти раптовим серцевим нападам або іншим серцево-судинним ускладненням. Монітори Холтера, що використовуються для тривалого

контролю серцевої діяльності, також можуть бути вдосконалені завдяки інтеграції у бездротових сенсорних мережах.

Бездротові сенсорні мережі відіграють ключову роль у розвитку телемедицини. Вони дозволяють дистанційно контролювати стан пацієнта, передаючи дані через Інтернет лікарям або спеціалізованим центрам моніторингу. Це особливо важливо для людей, які проживають у віддалених районах, де доступ до медичних закладів обмежений.

Наприклад, носимі пристрої, оснащені бездротові сенсорні мережі, можуть виявляти ознаки погіршення стану пацієнта та автоматично надсилати сигнал тривоги лікарю. Такі системи активно застосовуються у догляді за людьми похилого віку та пацієнтами з хронічними захворюваннями, наприклад, діабетом або гіпертонією.

Бездротові сенсорні мережі також використовуються у створенні розумних лікарняних палат. Вони контролюють не лише стан пацієнта, а й параметри навколишнього середовища – температуру, вологість, якість повітря. Це особливо важливо у відділеннях інтенсивної терапії та для пацієнтів з ослабленим імунітетом. Сенсори можуть автоматично регулювати рівень кисню або включати додаткову вентиляцію в разі потреби.

Під час хірургічних втручань бездротові сенсорні мережі забезпечують безперервний моніторинг життєво важливих параметрів пацієнта. Також вони застосовуються для контролю процесу загоєння ран після операцій. Наприклад, спеціальні сенсори можуть виявляти зміни температури або рівня вологості навколо рани, що допомагає визначити розвиток інфекції на ранній стадії.

Бездротові сенсорні мережі також сприяють розвитку біомедичних досліджень. Вони допомагають у зборі великої кількості даних про фізіологічні процеси людини, що використовується для вдосконалення методів лікування та діагностики. Наприклад, в експериментальній медицині сенсори застосовуються для вивчення впливу нових ліків на організм у реальному часі.

Незважаючи на численні переваги, впровадження бездротових сенсорних мереж у медичну практику супроводжується певними викликами. Основні проблеми включають:

1. Забезпечення надійності передачі даних – медична інформація має бути точною і доступною без затримок;
2. Конфіденційність і безпека – важливо гарантувати захист персональних даних пацієнтів;
3. Довговічність сенсорів – пристрої повинні мати тривалий термін служби та бути енергоефективними;
4. Сумісність з існуючими медичними системами – необхідність інтеграції бездротових сенсорних мереж з іншими електронними медичними записами та лікарняними інформаційними системами.

Майбутнє бездротових сенсорних мереж у медицині виглядає багатообіцяючим. З розвитком технологій, зокрема штучного інтелекту та Інтернету речей (IoT), бездротові сенсорні мережі будуть ставати ще більш автономними та ефективними. Очікується, що в найближчі роки вони стануть стандартом у медичній практиці, значно покращуючи якість догляду за пацієнтами та підвищуючи ефективність роботи медичних закладів.

2.5 Розумні міста та інфраструктура

Розумне місто — це ефективна інтеграція фізичних, цифрових та людських систем у штучному середовищі з метою забезпечення сталого розвитку, благополуччя та всебічного майбутнього для громадян. Таке визначення було надано Британським інститутом стандартів.

Розумне місто — це цілісна система, у якій міські комунікації, інформаційні технології для передачі даних та пристрої IoT (Інтернет речей) органічно взаємодіють між собою.

Метою створення «розумного міста» є поліпшення та спрощення управління міськими процесами, покращення міського середовища, забезпечення безпеки та підвищення якості життя мешканців.

У «розумному місті» сучасні інформаційні технології виконують три основні функції:

1. Надають швидкі канали для передачі інформації;
2. Забезпечують збір та передачу необхідних даних до органів управління міським господарством;
3. Служать засобом зворотного зв'язку між міською адміністрацією та жителями.

Використання камер відеоспостереження, фотофіксації, систем відеоаналізу, засобів зв'язку та комп'ютерних технологій дозволяє створити безпечне і комфортне міське середовище для мешканців.

Система «розумного міста» працює завдяки постійній обробці та оновленню даних, які надходять через інформаційні канали.

З точки зору безпеки, «розумне місто» має забезпечувати автоматичний контроль не лише за громадськими просторами та транспортом, а й за електромережами, газо- та водопостачанням, станом тепломереж і водостоків тощо.

Експерт у сфері урбаністики Білл Хатчінсон запропонував зрозумілу класифікацію «розумних міст», поділивши їх на три версії:

1. Версія 1.0 — автоматизація впроваджується лише в окремих, не пов’язаних між собою сферах, без загальної стратегії розвитку;
2. Версія 2.0 — раніше незалежні ініціативи об’єднуються, створюючи єдину систему з інтеграцією великої кількості інформаційних джерел;
3. Версія 3.0 — усі компоненти повністю взаємопов’язані, а міська інфраструктура функціонує на основі розвинених інтелектуальних технологій.

LoRaWAN — це бездротовий протокол зв’язку, який використовується для IoT-додатків, забезпечуючи підключення пристроїв до інтернету та дистанційне

керування ними. Датчики або пристрої з автономним живленням передають радіосигнали до базової станції (шлюзу), яка надсилає отримані дані на сервер, доступний через інтернет.

LoRaWAN застосовується для підключення пристроїв із низькою швидкістю передавання даних. Завдяки можливості сигналів проникати крізь стіни та перешкоди, датчики можна встановлювати в підвальних приміщеннях, багатоповерхових будівлях.

Ключові переваги LoRaWAN для IoT-інфраструктури:

1. Висока здатність сигналу проникати крізь перешкоди;
2. Двосторонній обмін даними;
3. Низькі витрати на впровадження та технічне обслуговування;
4. Великий радіус дії сигналу;
5. Енергоефективність і тривалий термін експлуатації;
6. Простота впровадження без потреби у вузькопрофільних спеціалістах;
7. Мінімальне енергоспоживання;
8. Надійне шифрування та захист переданих даних.

Завдяки своїм характеристикам ця технологія є ідеальним рішенням для управління IoT-даними в розумних містах, сприяючи підвищенню комфорту та безпеки мешканців. Її застосовують у різних сферах, зокрема:

1. Енергоменеджмент. Завдяки інтелектуальним пристроям LoRaWAN компанії можуть ефективно управляти освітленням, системами опалення та кондиціонування, а також здійснювати автоматизований облік енергоресурсів;
2. Безпека громадськості. Завдяки датчикам, встановленим на виробництвах та в офісах, можна своєчасно виявляти загрози;
3. Моніторинг водопостачання та виявлення витоків. Комунальні служби та постачальники ресурсів можуть оперативно виявляти аварії у водопровідних мережах, своєчасно реагувати на витоки;

4. Розумне керування будівлями. Інтелектуальні системи в торговельних центрах, офісах та адміністративних будівлях дозволяють автоматично створювати комфортні умови;

5. Екологічний моніторинг. Інтелектуальні сенсори дозволяють фіксувати показники температури та вологості, зокрема в теплицях;

6. Оптимізація збору відходів. Інтелектуальні сміттєві контейнери, оснащені датчиками заповненості та пресувальними механізмами, дозволяють зменшити обсяг відходів і покращити ефективність роботи комунальних служб;

7. Інтелектуальні паркувальні системи. Оснащення стоянок датчиками вільних місць і виведення інформації на електронні табло дозволяє водіям швидко знаходити місця для паркування;

8. Розумне освітлення вулиць. Система адаптивного управління освітленням дозволяє автоматично змінювати яскравість ліхтарів залежно від рівня природного світла, руху пішоходів та транспорту;

9. Розумний громадський транспорт. Системи моніторингу транспорту дозволяють пасажирам у реальному часі відстежувати місцезнаходження автобусів і трамваїв, оптимізувати маршрути та зменшувати затори на дорогах.

Розвиток розумного міста неможливо уявити без використання великої кількості розумних пристроїв, таких як датчики руху чи детектори диму. Хоча ці пристрої можна підключити безпосередньо до Інтернету, це не найпрактичніше чи економічно ефективне рішення.

Тому рішення LPWAN — технології, які не потребують великого енергоспоживання — стають все більш популярними у великих містах. Протоколи LPWAN призначені для передачі невеликих пакетів даних на неліцензованих частотах. Розгортання цих мереж простіше та дешевше, ніж використання бездротового Інтернету [21, 1].

РОЗДІЛ 3
ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

3.1 Проблеми безпеки та захисту даних

Бездротові сенсорні мережі є особливим видом мережі, що має значні обмеження порівняно з традиційними комп'ютерними мережами. Тому, перед впровадженням ефективних механізмів безпеки на основі сучасних технологій, важливо спочатку вивчити та усвідомити ці обмеження:

1. Датчики є компактними пристроями з обмеженим обсягом пам'яті та сховища для коду. Для створення ефективного механізму безпеки необхідно мінімізувати розмір коду алгоритму;

2. Нестабільність зв'язку є однією з ключових загроз для безпеки датчиків. Надійність мережі значною мірою визначається використовуваним протоколом, який, у свою чергу, залежить від якості зв'язку.

Безпека бездротової сенсорної мережі включає кілька ключових аспектів, які можна класифікувати наступним чином:

1. Під час прийняття рішень вузли-одержувачі мають бути впевнені, що отримані дані надходять із достовірного джерела. Автентифікація необхідна для безпечного обміну керуючою інформацією в мережі;

2. Передані дані можуть зазнавати змін як внаслідок атак зловмисників, так і через несприятливі умови зв'язку. Забезпечення цілісності гарантує, що дані залишаються незмінними під час передачі, незалежно від випадкових або навмисних спроб їх модифікації;

3. У сферах, як моніторинг, захист промислових секретів, розповсюдження ключів, збереження конфіденційності є критично важливим. Стандартним методом її забезпечення є шифрування. Основна загроза в тому, що радіочастотний спектр доступний для всіх, хто має відповідне обладнання;

4. Вимога гарантує, що отримана інформація є актуальною і не була повторно відтворена зловмисниками;

5. Сенсорні вузли можуть втратити працездатність через виснаження заряду батареї, викликане надмірними обчисленнями або активним обміном даними. Крім того, зловмисник може навмисно заблокувати зв’язок, спричинивши недоступність датчика;

6. У бездротових сенсорних мережах кожен вузол працює автономно та має бути достатньо гнучким для самоорганізації та самовідновлення в умовах змінного середовища;

7. Для збереження енергії окремі сенсорні вузли можуть періодично вимикатися. Тому будь-який механізм безпеки у бездротових сенсорних мережах повинен бути синхронізованим за часом;

8. Для багатьох сенсорних мереж важливо мати точну й автоматизовану інформацію про місцезнаходження вузлів. Однак незахищені дані про місцезнаходження можуть бути легко скомпрометовані зловмисниками.

Щоб усунути загрози конфіденційності, з якими стикаються бездротові сенсорні мережі, було розроблено декілька ефективних методів збереження конфіденційності:

1. Шифрування є основним методом захисту даних у бездротових сенсорних мережах. Він перетворює вихідні дані в нечитабельний формат, забезпечуючи доступ до інформації лише авторизованим особам із правильним ключем дешифрування;

2. Агрегація даних передбачає об’єднання даних із кількох вузлів і передачу лише агрегованих результатів. Цей підхід мінімізує кількість даних, які піддаються потенційному перехопленню, зменшуючи ризики конфіденційності та зберігаючи мережеві ресурси за рахунок зменшення обсягу переданих даних.

3. Захищені протоколи маршрутизації є важливими для захисту конфіденційності в бездротових сенсорних мережах. Ці протоколи забезпечують передачу пакетів даних уздовж надійних шляхів, зменшуючи ризик перехоплення зловмисниками [22, 1].

3.2 Обмеження енергії та автономної роботи

Бездротові сенсорні мережі є важливою складовою сучасних технологій Інтернету речей (IoT) та відіграють важливу роль у моніторингових системах, екологічних спостереженнях, сільському господарстві, медицині та розумних містах. Їх головна особливість полягає у здатності функціонувати в автономному режимі без необхідності постійного втручання людини.

Основним джерелом живлення для сенсорів є акумуляторні або одноразові батареї. Зазвичай використовуються літій-іонні, літій-полімерні або літій-тіонілхлоридні батареї, які мають високу щільність енергії. Проте навіть ці батареї мають обмежену тривалість роботи — від кількох місяців до кількох років залежно від типу застосування та частоти обміну даними. У віддалених або важкодоступних місцях заміна батарей є дуже складною, а іноді й взагалі неможливою.

Альтернативою батареям можуть бути системи енергетичного збирання, що використовують енергію сонця, вітру, вібрацій або теплових градієнтів. Хоча такі рішення продовжують автономність роботи, вони залежать від зовнішніх умов та не завжди можуть забезпечити стабільне живлення. Наприклад, у закритих приміщеннях або під землею можливості енергетичного збирання різко обмежені, що змушує шукати комбіновані підходи до живлення.

SCP-MAC — це новий протокол MAC для бездротових сенсорних мереж, який забезпечує наднизькі робочі цикли. Існуючі протоколи MAC, такі як S-MAC і B-MAC, зазвичай працюють із робочими циклами 1-10%, коли немає трафіку даних. SCP-MAC прагне знизити обмеження до 0,1% і нижче, що забезпечує більшу економію енергії, ніж існуючі протоколи.

Випущене програмне забезпечення SCP-MAC — це комунікаційний стек, який включає MAC, фізичний рівень (PHY) і компоненти підтримки системи, такі як таймер, локальний системний час, програми для тестування та засоби налагодження. На даний момент програмне забезпечення працює лише на шматочках Mica2.

На що поділяється випущене програмне забезпечення SCP-MAC:

1. Рівень MAC - рівень MAC включає SCP-MAC і два інших MAC, на яких було побудовано SCP-MAC: множинний доступ із визначенням несучої (CSMA) і прослуховування з низьким енергоспоживанням (LPL). CSMA або LPL можна використовувати як окремий MAC;

2. Фізичний рівень - PHY обробляє передачу та прийом на рівні пакетів, контроль стану радіостанції, підтримку відмітки часу та фізичне визначення несучої, включаючи вимірювання рівня шуму та потужності отриманого сигналу;

3. Таймер і місцевий час - реалізується новий таймер, який підтримує режим сну ЦП (розширений режим очікування або енергозбереження) між подіями таймера. Цей таймер забезпечує асинхронний інтерфейс, який запускається з дуже низьким джиттером [23, 1].

Кожен сенсорний вузол складається з кількох основних компонентів: сенсора, мікроконтролера, радіомодуля та джерела живлення. Найбільше енергії витрачається на бездротову передачу даних, особливо якщо зв'язок відбувається на значні відстані або в складних умовах, таких як густі лісові масиви чи міські забудови.

Щоб знизити енергоспоживання, розробляються спеціальні протоколи зв'язку, які мінімізують кількість передач і використовують ефективні методи стиснення даних. Крім того, сенсорні вузли можуть працювати в режимі періодичного сну, коли більшу частину часу вони перебувають у неактивному стані й лише зрідка прокидаються для вимірювання параметрів і передачі інформації.

Важливою складовою енергоефективності є оптимізація програмного забезпечення сенсорних вузлів. Алгоритми збору даних, обробки та передачі повинні бути максимально простими та швидкими, щоб знижувати час активної роботи вузла. Впровадження методів локальної обробки даних також знижує обсяги переданих даних, що позитивно позначається на енергетичному балансі.

Постійний моніторинг з високою частотою вимірювань значно знижує термін служби батареї, тому в багатьох випадках застосовуються адаптивні алгоритми, які динамічно змінюють частоту вимірювань залежно від змінюваних умов навколишнього середовища.

Енергетична ефективність багато в чому залежить від обраної топології мережі. Мережі з багатоступеневою передачею дозволяють рівномірно розподіляти енергетичне навантаження, але при цьому виникають додаткові втрати на кожному проміжному вузлі.

Для бездротових сенсорних мереж розроблено низку енергоефективних протоколів зв'язку, серед яких найбільш популярними є ZigBee, LoRa, Bluetooth Low Energy та NB-IoT. Вибір технології залежить від відстані, обсягу даних та необхідного часу автономної роботи.

3.3 Виклики масштабування та стабільності роботи

Бездротові сенсорні мережі є однією з ключових технологій у сфері Інтернету речей (IoT), автоматизованих систем моніторингу, промислової автоматизації та екологічних досліджень. Вони складаються з великої кількості сенсорних вузлів, які збирають, передають та обробляють дані. Проте збільшення масштабу мережі та забезпечення її стабільної роботи супроводжуються численними викликами, пов’язаними з ресурсними обмеженнями, ефективністю передачі даних, збереженням енергії та безпекою.

При розширенні бездротових сенсорних мереж виникає низка технічних і організаційних проблем, які впливають на ефективність її роботи.

Сенсорні вузли зазвичай мають обмежені обчислювальні можливості, малий обсяг пам’яті та обмежений запас енергії. Це створює труднощі при виконанні складних алгоритмів обробки даних, маршрутизації та безпеки. Зі збільшенням розміру мережі необхідно розробляти ефективні методи оптимізації ресурсів, які забезпечать баланс між продуктивністю та енергоспоживанням.

Чим більше вузлів у мережі, тим більше навантаження на бездротовий канал зв’язку. Це може призводити до перевантаження мережі, зростання затримок у передачі пакетів і збільшення втрат даних. Оскільки сенсори зазвичай використовують низькошвидкісні канали зв’язку, необхідно впроваджувати ефективні алгоритми маршрутизації, що зменшують перевантаження мережі та мінімізують використання енергетичних ресурсів.

У великих бездротових сенсорних мережах структура мережі постійно змінюється через вихід із ладу окремих вузлів, зміну місцезнаходження мобільних вузлів або зовнішні умови. Це ускладнює підтримку стабільної комунікації між вузлами. Для ефективного масштабування необхідні алгоритми самоналаштування, що дозволяють мережі адаптуватися до змін без втрати продуктивності.

Для підтримки надійної роботи бездротових сенсорних мереж важливо враховувати такі аспекти, як енергетична ефективність, перешкоди у зв’язку, надійність програмного забезпечення та захист від кібератак.

Більшість сенсорних вузлів живляться від батарей або використовують енергію навколишнього середовища, наприклад сонячну або кінетичну. Витрати енергії на передачу даних є значними, тому необхідно використовувати енергоефективні методи маршрутизації та механізми стиснення даних, щоб зменшити навантаження на вузли. Впровадження протоколів з низьким споживанням енергії, таких як IEEE 802.15.4, допомагає збільшити час роботи сенсорних мереж.

Зовнішні умови, такі як електромагнітні завади, погодні фактори, фізичні перешкоди та радіочастотне перевантаження, можуть призводити до погіршення якості зв’язку або повної втрати даних. Для мінімізації впливу цих факторів застосовують методи адаптивного керування потужністю сигналу, використання альтернативних частотних діапазонів і корекцію помилок у переданих даних.

Стабільність роботи бездротових сенсорних мереж значною мірою залежить від програмного забезпечення, яке керує вузлами. Помилки в

алгоритмах збору, обробки та передачі даних можуть призвести до нестабільної роботи мережі.

Бездротові сенсорні мережі є вразливими до атак зловмисників, зокрема перехоплення даних, атак типу «відмова в обслуговуванні» (DoS) та компрометації вузлів. Захист від загроз вимагає впровадження механізмів автентифікації, шифрування переданих даних та алгоритмів виявлення аномальної активності.

У бездротових сенсорних мережах існує постійний конфлікт між збереженням енергії та продуктивністю системи. Наприклад, часті передачі даних збільшують навантаження на мережу та витрати енергії, але рідкісні передачі можуть знизити точність та актуальність отриманих даних. Для подолання цієї проблеми застосовують адаптивні протоколи зв'язку, які змінюють частоту передачі залежно від критичності отриманої інформації.

Керування пристроєм є критично важливим аспектом будь-якої системи IoT і може значно вплинути на масштабованість рішення в цілому. Пристрої IoT потрібно активувати, контролювати, підтримувати, оновлювати, налаштовувати та ефективно виводити з експлуатації, особливо у великомасштабних розгортаннях.

Ефективна система керування пристроями IoT має бути здатна обробляти величезну кількість пристроїв , включаючи маршрутизатори, датчики та контролери, у різних місцях. Оновлення мікропрограми по повітрю (FOTA) є обов'язковою функцією, що дозволяє дистанційно оновлювати мікропрограму, щоб забезпечити безпеку та оновлення пристроїв.

Хоча системи керування пристроями Інтернету речей можуть бути високоавтоматизованими, для безперебійної роботи системи та вирішення будь-яких проблем, які можуть виникнути, необхідна людська підтримка. Масштабовані стратегії розгортання , такі як підключення «plug and play» і попередньо налаштовані пристрої , можуть спростити процес встановлення та зменшити потребу в спеціалізованих технічних експертах [24, 1].

Було виконано моделювання бездротової сенсорної мережі в Cooja, що складається з двох логічних частин: клієнтської (позначеної фіолетовим кольором) та серверної (позначеної жовтим кольором).

Клієнтська частина включає в себе мобільні вузли, бездротові хости та стаціонарні комп’ютери. Ці вузли імітують кінцевих користувачів або пристрої, які збирають дані з навколишнього середовища чи надсилають запити на сервер. Вони розміщені по колу, імітуючи розподілену інфраструктуру з різною функціональністю: деякі пристрої стаціонарні, інші мають можливість руху. Усі вони взаємодіють з мережею через точки доступу або безпосередньо передають дані в бездротовому середовищі.

Серверна частина представлена мережею з фіксованими вузлами: комутатором (ethernetSwitch), маршрутизатором (myRouter), головним вузлом (myHost) і точками доступу (accessPoint0–3). Саме тут відбувається основна обробка даних, прийом запитів від клієнтів, їх аналіз і відповіді. Серверна частина працює як центр управління, координуючи взаємодію всієї мережі.

У моделі використано протоколи бездротового зв’язку (наприклад, Rime або UDP), а також передбачено маршрутизацію даних між клієнтами і сервером на рис. 3.1. Кожен вузол має свою IP-адресу і здатний передавати або приймати повідомлення. Під час роботи програми в Cooja проводиться аналіз затримки доставки повідомлень, стабільності з'єднання, маршрутизації та загальної продуктивності мережі.

Це моделювання дозволяє дослідити поведінку мережі в умовах динамічного трафіку, перевірити стійкість архітектури, а також оцінити ефективність обраного протоколу в умовах бездротового середовища.

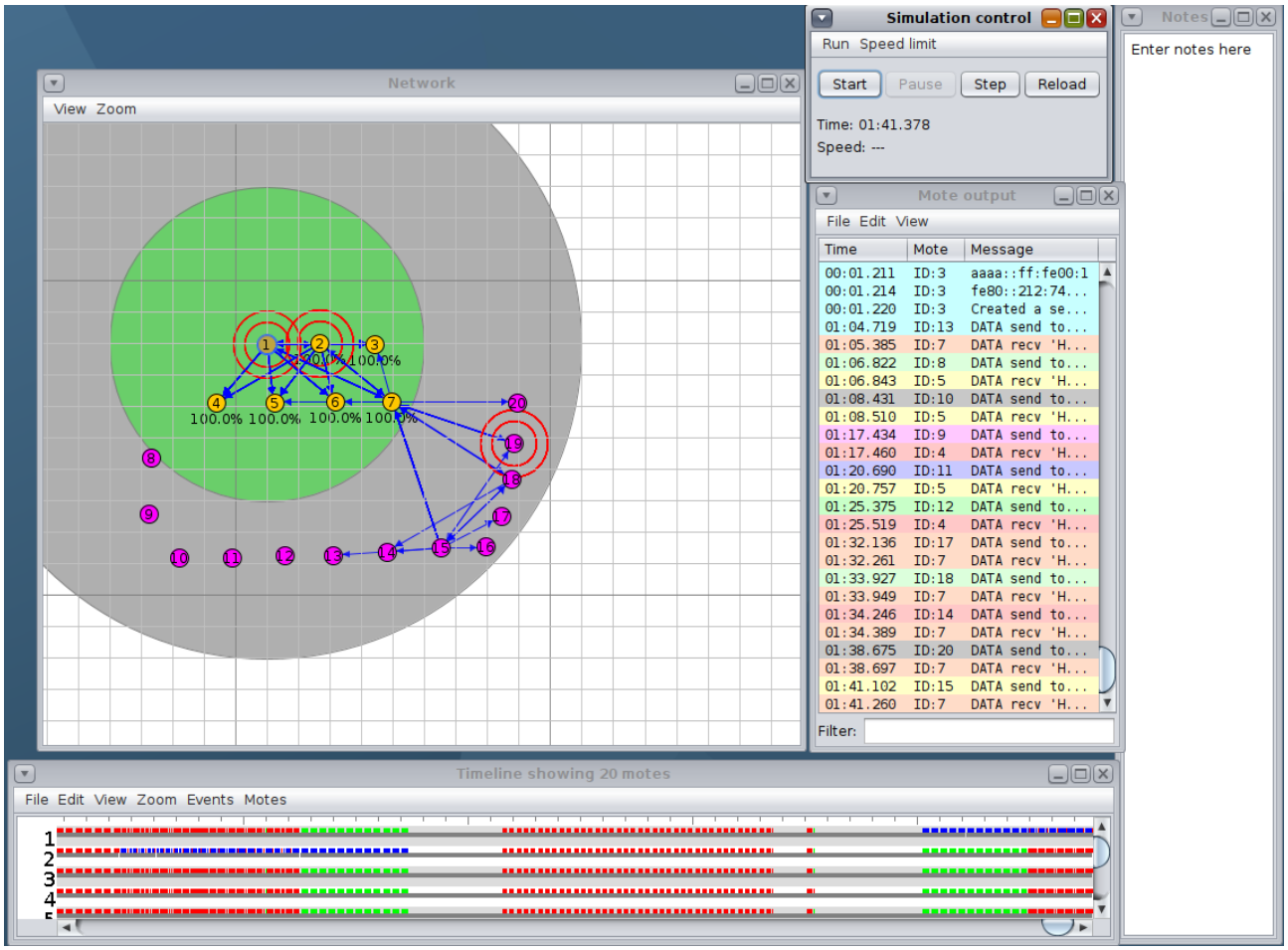

Рисунок 3.1 - Передача даних між клієнтами і сервером

3.4 Тенденції розвитку технологій у цій сфері

Бездротові сенсорні мережі є важливою складовою сучасних інформаційних систем, що використовуються в екологічному моніторингу, розумних містах, промисловій автоматизації, медицині та військовій сфері. З розвитком технологій удосконалюються їхні можливості, що сприяє підвищенню ефективності, стабільності та масштабованості мереж. Основні тенденції розвитку бездротових сенсорних мереж спрямовані на розширення функціональності, покращення енергозбереження, підвищення безпеки та інтеграцію з іншими інноваційними рішеннями.

Однією з ключових проблем бездротових сенсорних мереж є обмежене живлення сенсорних вузлів, що працюють на батареях або енергії з навколишнього середовища. Нові розробки спрямовані на зменшення

енергоспоживання за допомогою оптимізованих протоколів зв’язку, енергоефективних процесорів і алгоритмів стиснення даних.

Зростання вимог до швидкості, надійності та дальності передачі даних стимулює впровадження нових стандартів зв’язку. Протоколи, такі як 5G, Wi-Fi 6 та LPWAN (Low Power Wide Area Network), дозволяють значно покращити продуктивність бездротових сенсорних мереж. Технологія 5G забезпечує низьку затримку та високу пропускну здатність, що особливо важливо для критично важливих застосувань. LPWAN-технології, такі як LoRaWAN та NB-IoT, спрямовані на зменшення енергоспоживання та збільшення дальності зв’язку.

Бездротові сенсорні мережі часто використовуються в чутливих сферах, де безпека даних є критично важливою. Розвиток технологій шифрування, автентифікації та захисту від кібератак дозволяє запобігти втручанню зловмисників.

Сучасні бездротові сенсорні мережі активно розвиваються у напрямку автономності та самоналаштування. Інтелектуальні алгоритми дозволяють мережам самостійно оптимізувати маршрутизацію, розподіл навантаження та управління енергоресурсами.

Зростання Інтернету речей (IoT) сприяє тіснішій інтеграції бездротових сенсорних мереж з хмарними платформами для обробки та зберігання даних. Хмарні обчислення дозволяють централізовано аналізувати великі обсяги інформації, забезпечуючи гнучке масштабування та високу доступність. Граничні обчислення (Edge Computing) також відіграють важливу роль, зменшуючи затримки та дозволяючи обробляти дані безпосередньо на сенсорних вузлах або локальних серверах. Інтеграція WSN з технологіями штучного інтелекту (AI) та обчисленнями на периферії (Edge Computing) відкриває нові можливості для аналізу даних у реальному часі. Використання штучного інтелекту дозволяє сенсорним мережам ефективніше обробляти великі обсяги інформації, прогнозувати події та оптимізувати роботу мережі. Завдяки Edge Computing обробка даних відбувається ближче до джерела їхнього виникнення,

що зменшує затримки передачі, розвантажує центральні сервери та підвищує швидкість реагування системи.

Поєднання різних типів бездротових мереж у межах однієї інфраструктури дозволяє підвищити ефективність роботи бездротових сенсорних мереж. Гібридні мережі можуть використовувати одночасно кілька протоколів зв'язку, наприклад комбінацію LPWAN для віддалених вузлів та Wi-Fi або 5G для високошвидкісної передачі даних.

Завдяки розвитку мікроелектроніки сучасні сенсори стають більш компактними, точними та багатофункціональними. Використання нових матеріалів і технологій дозволяє створювати сенсори, що працюють у жорстких умовах або мають додаткові можливості, такі як самовідновлення.

Одним із перспективних напрямків є розробка біосенсорних мереж, що використовуються в медицині та екології. Такі мережі можуть контролювати фізіологічні параметри пацієнтів у режимі реального часу або відстежувати забруднення навколишнього середовища. Використання біосенсорів дозволяє створювати персоналізовані системи моніторингу здоров'я.

Оскільки розгортання бездротових сенсорних мереж зростає, зростає й турбота про безпеку даних. Впровадження надійних заходів безпеки є критичною тенденцією на ринку. Це включає використання протоколів шифрування, захищених каналів зв'язку та систем виявлення вторгнень для захисту цілісності та конфіденційності даних, зібраних сенсорними мережами [25, 1].

Прикладом сучасного інструментарію для дослідження бездротових сенсорних мереж є використання середовища OMNeT++ з фреймворком INET. Реалізовано бездротову сенсорну мережу на основі симулятора OMNeT++ з використанням фреймворку INET. Мережа складається з різних типів вузлів, включаючи провідні та бездротові хости, мобільні вузли, точки доступу, маршрутизатори, комутатори та спеціалізовані сенсорні вузли. Основною метою даної моделі є дослідження взаємодії між вузлами через бездротове середовище,

передача даних протоколом UDP, а також моделювання сенсорної активності в мережі.

Для створення бездротового середовища використано модуль Ieee80211ScalarRadioMedium, який дозволяє моделювати передачу радіосигналів з урахуванням відстані та чутливості приймача. Усі бездротові вузли мають радіус дії 250 метрів та чутливість приймача -85 dBm, що дозволяє забезпечити стабільне з'єднання в межах заданої топології.

Мережева конфігурація здійснюється за допомогою модуля Ipv4NetworkConfigurator, який автоматично призначає IP-адреси та створює статичні маршрути. Для комутації Ethernet-з'єднань застосовується шестипортовий комутатор (EthernetSwitch), до якого підключено провідні вузли та точки доступу.

У мережі реалізовано три мобільні вузли, розташовані в різних координатах, з модулем MovingMobilityBase, що дозволяє задати початкові позиції та, за потреби, змоделювати рух. Таким чином, мережа поєднує стаціонарні та мобільні сенсорні елементи.

AccessPoint (0-3) виконує роль як джерела (див. на рис. 3.2), так і приймача трафіку (див. на рис. 3.3). Інші вузли також виконують роль як джерела, так і приймача трафіку. Для генерації трафіку використано додатки UdpBasicApp (для передачі повідомлень розміром 1000 байт з інтервалом 1 секунда) та UdpSink (для прийому повідомлень). Вузли надсилають трафік один одному, утворюючи інтенсивний обмін даними в мережі. Один з вузлів додатково використовує PingApp для оцінки доступності інших вузлів. Передаються між accesPoint(0-3) і бездротовими вузлами пакети Beacon, WlanAck, ProbeReq (див. на рис. 3.4), ProbeResp (див. на рис. 3.5).

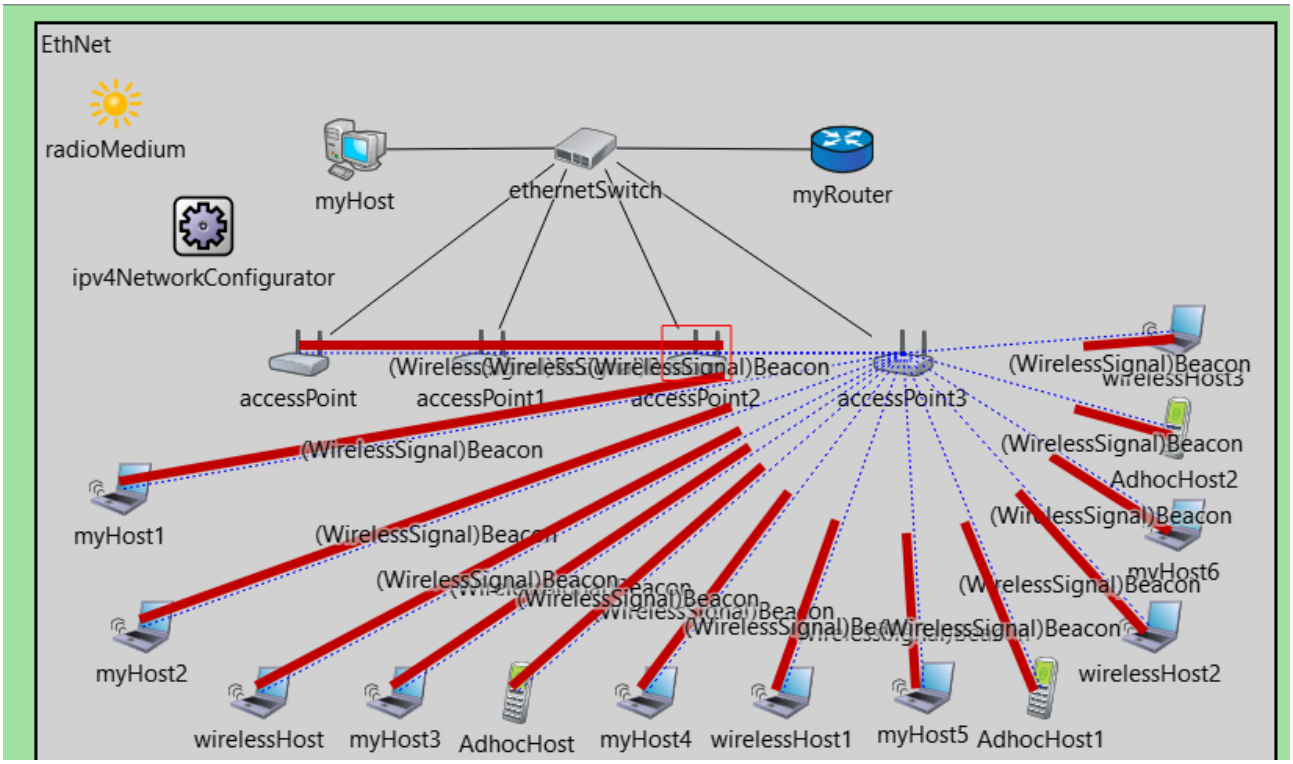

Рисунок 3.2 - AccessPoint3 передає Beacon-пакети усім клієнтам

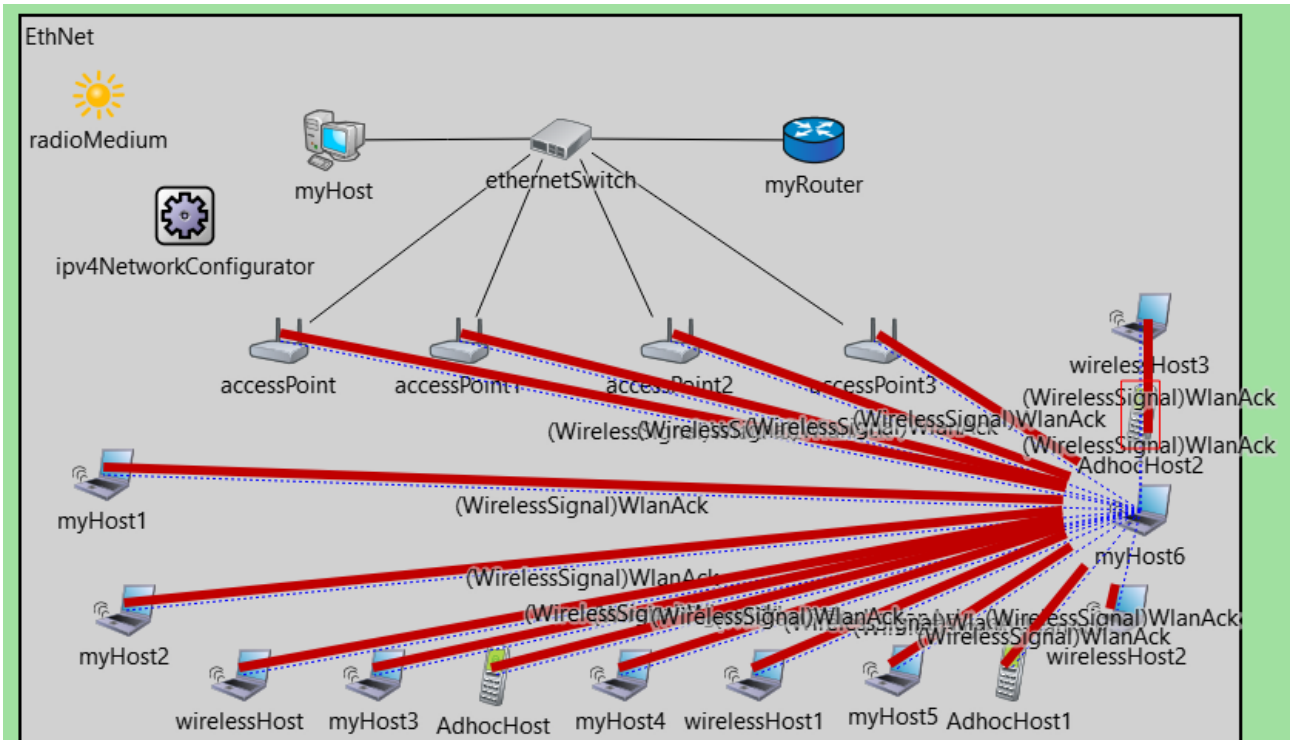

Рисунок 3.3 - AccessPoint приймає WlanAck-пакети від клієнта

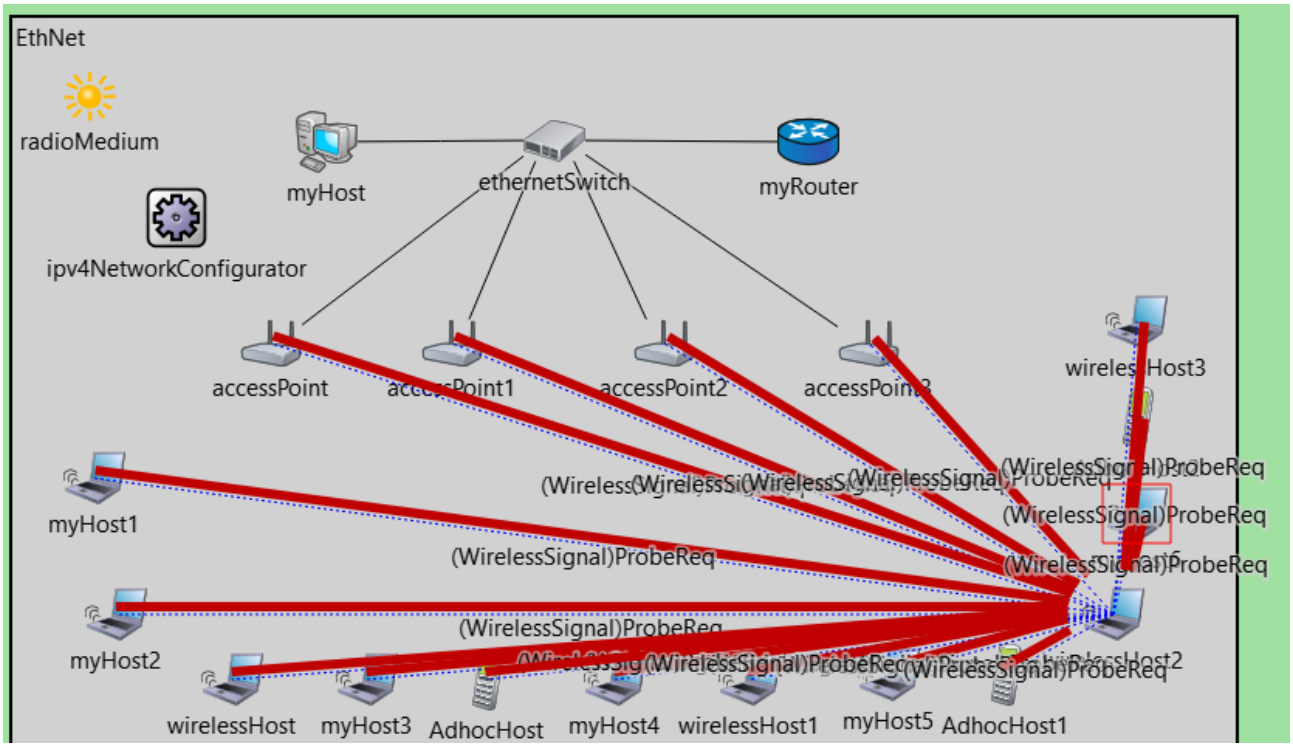

Рисунок 3.4 - WirelessHost3 надсилає ProbeReq-пакети до accessPoint і клієнтів

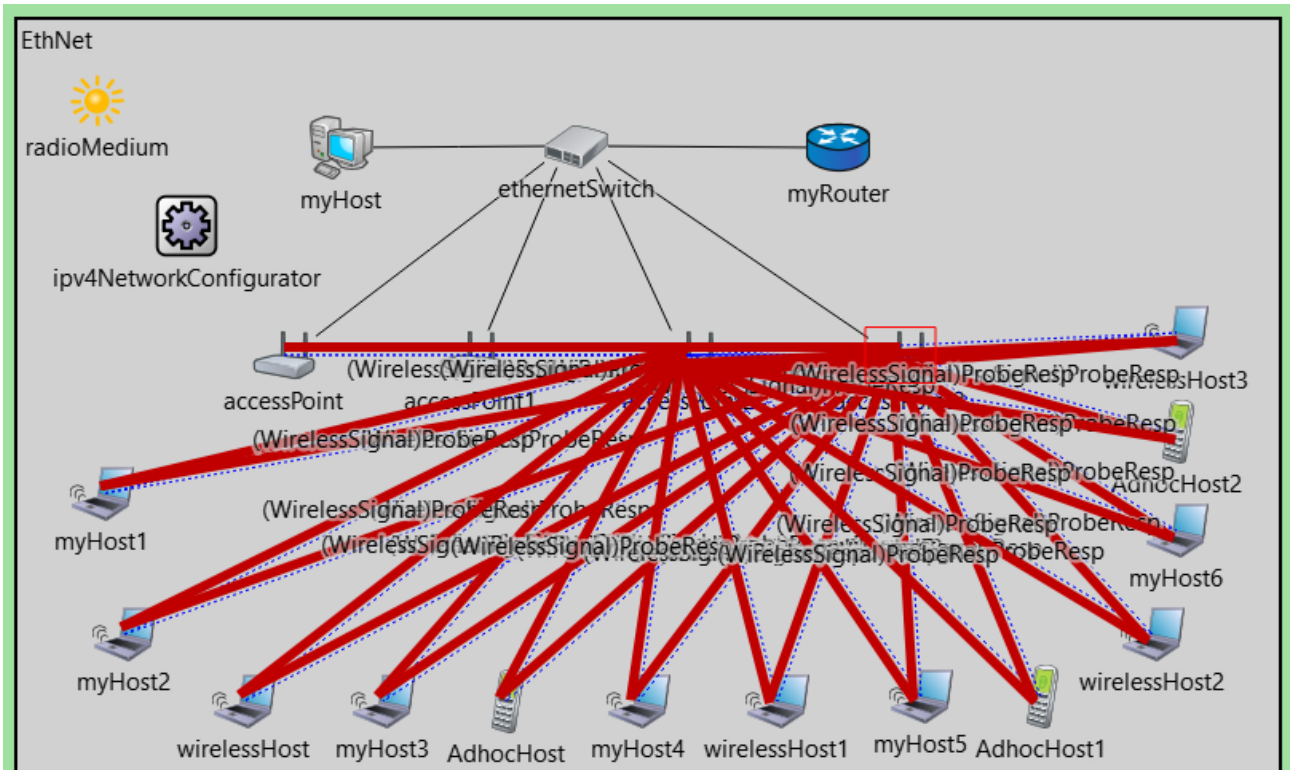

Рисунок 3.5 - AccessPoint надсилає ProbeResp-пакети у відповідь бездротовим вузлам

Уся топологія моделює типову сенсорну мережу, яка може застосовуватись для моніторингу навколишнього середовища, збору даних з численних сенсорних точок та передавання цієї інформації на центральний сервер або хмарне сховище. Завдяки широкому використанню бездротових інтерфейсів, система демонструє високу гнучкість та масштабованість.

Ця модель дозволяє досліджувати такі важливі аспекти роботи бездротових сенсорних мереж, як передача даних у реальному часі, вплив щільності вузлів на затримки, ефективність протоколів маршрутизації, та вплив мобільності на якість зв’язку.

Також у NS-3 змодельована бездротова сенсорна мережа з 20 вузлів, об’єднаних у єдину дротову Ethernet-мережу. Кожен вузол віртуально створюється за допомогою симулятора NS-3, а для зв’язку між ними використовується CSMA (Carrier Sense Multiple Access) — це модель дротової мережі, яка імітує типову локальну мережу (LAN), аналогічну Ethernet. Така мережа передбачає, що всі вузли фізично підключені до одного середовища передачі і звертаються по доступ до нього.

Спочатку створюється 20 вузлів (маршрутизаторів, точок доступу, ноутбуків, смартфонів). Усі вони підключаються до одного Ethernet-сегменту. Швидкість передавання даних між вузлами задається як 100 мегабіт на секунду, а затримка каналу — 6560 наносекунд.

На кожному вузлі встановлюється мережевий стек TCP/IP, що забезпечує обробку IP-пакетів і підтримку інтернет-протоколів, таких як UDP. Після цього вузлам автоматично призначаються IP-адреси з підмережі 10.1.1.0/24, де перший вузол отримає адресу 10.1.1.1, другий — 10.1.1.2, і так далі.

Для демонстрації роботи мережі один вузол грає роль сервера, а інший — клієнта:

1. UDP-сервер запускається на вузлі 0, який слухає на порту 9. Він починає роботу на першій секунді симуляції (див. на рис. 3.6);

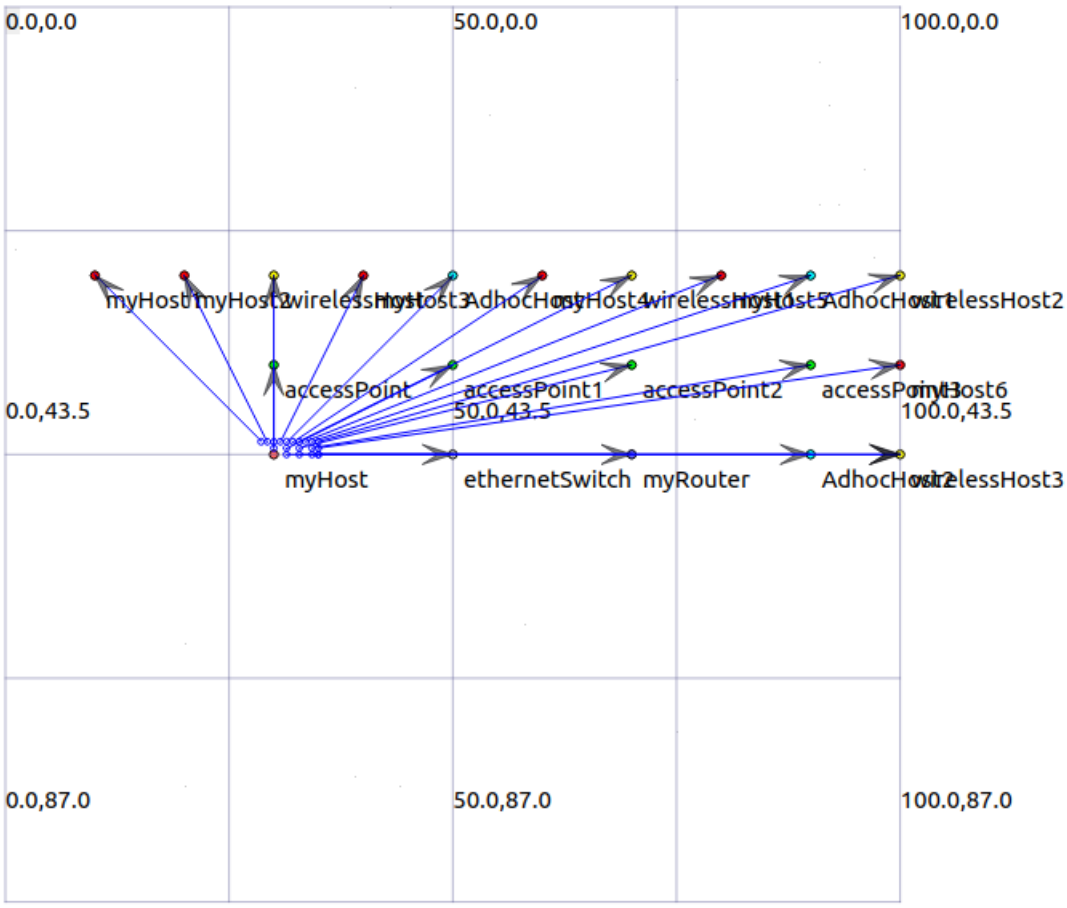

Рисунок 3.6 - MyHost надсилає трафік до клієнтів

2. UDP-клієнт розміщується на вузлі 19, називається wirelessHost3 і налаштований на надсилання 5 повідомлень до сервера розміром 1024 байти кожне, з інтервалом 1 секунда між надсиланнями. Клієнт починає передавання з другої секунди, щоб сервер уже був готовий приймати пакети (див. на рис. 3.7).

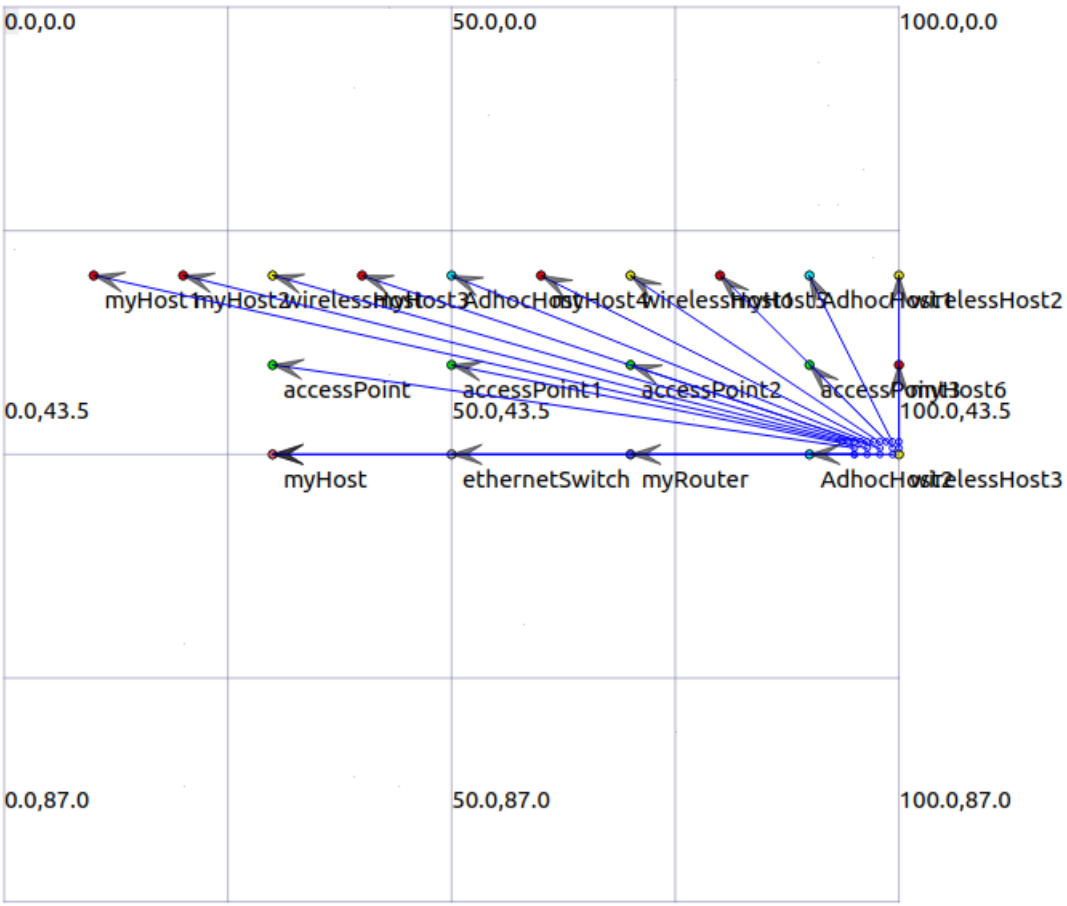

Рисунок 3.7 - UDP-клієнти надсилають дані серверу

Таким чином, у мережі моделюється типовий сценарій: ініціація зв’язку клієнтом, передача даних, і прийом сервером — усе через реалістичну Ethernet-мережу з IP-адресацією.

У файлі визначаються координати кожного вузла у двовимірному просторі, щоб розташування візуально нагадувало топологію локальної мережі.

Наприклад:

1. Вузол 0 має назву myHost;
2. Вузол 1 називається ethernetSwitch, тобто комутатор;
3. Вузол 2 — myRouter, він імітує маршрутизатор;
4. Вузли 3–6 іменуються як accessPoint, accessPoint1, тощо — це точки доступу, які могли б у реальному житті працювати з бездротовими вузлами;
5. Інші вузли мають імена, як-от wirelessHost, wirelessHost1, wirelessHost2, wirelessHost3, AdhocHost, AdhocHost1, AdhocHost2, myHost1, myHost2, myHost3,

myHost4, myHost5, myHost6. Назви натякають на можливу роль вузлів — мобільні пристрої, звичайні хости або бездротові клієнти.

Крім цього, для кожного вузла задається певний колір у анімації, що допомагає візуально ідентифікувати тип пристрою:

1. MyHost — червоний;
2. Маршрутизатор — синій;
3. Точки доступу — зелений;
4. Мобільні вузли — блакитний;
5. Бездротові вузли — жовтий.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було проведено комплексне дослідження архітектурних, протокольних, енергетичних і прикладних аспектів функціонування бездротових сенсорних мереж. У вступі роботи було поставлено низку завдань, на які в процесі дослідження отримано аргументовані відповіді.

Перш за все, здійснено загальний огляд сучасного стану розвитку бездротових сенсорних мереж. Встановлено, що бездротові сенсорні мережі є важливою складовою сучасної цифрової інфраструктури. Вони лежать в основі функціонування Інтернету речей (IoT), розумних міст (Smart Cities), кіберфізичних систем (CPS), систем екологічного моніторингу, охорони здоров'я, військових застосувань, транспортної інфраструктури, сільського господарства та промисловості. Їх популярність пояснюється автономністю, гнучкістю в розгортанні, енергоефективністю та здатністю до масштабування.

Проведено глибокий аналіз архітектурних принципів побудови бездротових сенсорних мереж. Розглянуто структуру сенсорного вузла, включаючи сенсор, мікроконтролер, радіомодуль та блок живлення. Вивчено рівнево-орієнтовану архітектуру бездротових сенсорних мереж і типові топології: зіркоподібну, деревоподібну, сітчасту та кластерну. Показано, що вибір топології залежить від середовища, вимог до QoS, рівня енергоспоживання й потреб у надійності передавання даних.

Ретельно проаналізовано комунікаційні протоколи на всіх рівнях моделі OSI. На фізичному рівні досліджено стандарти IEEE 802.15.4 та Bluetooth Low Energy; на канальному — ZigBee. На мережевому рівні вивчено ефективність застосування протоколів маршрутизації LEACH, AODV, RPL. На транспортному та прикладному рівнях проаналізовано протоколи, що підтримують надійну передачу даних із урахуванням обмеженої пропускної здатності та енергоспоживання. Відзначено роль кластерних протоколів у зниженні навантаження на мережу та продовженні терміну роботи вузлів.

Окрему увагу приділено безпеці бездротових сенсорних мереж. Досліджено актуальні загрози, такі як атаки типу «людина посередині», підміну вузлів, підробку маршрутів, перехоплення трафіку та DoS-атаки. Проаналізовано існуючі підходи до захисту з урахуванням обмежених обчислювальних ресурсів вузлів. Обґрунтовано доцільність використання полегшених криптографічних алгоритмів, таких як ECC, а також впровадження механізмів аномалійного виявлення та автентифікації.

У практичній частині дослідження проведено моделювання бездротових сенсорних мереж у програмних середовищах NS-3, OMNeT++, Cooja. Виконано серію симуляцій з різними топологіями, типами вузлів, сценаріями навантаження та протоколами маршрутизації. У Cooja здійснено аналіз енергоспоживання залежно від щільності розміщення вузлів. В NS-3 змодельовано затримки, втрати пакетів і швидкість передавання. В OMNeT++ протестовано масштабованість мережі при зростанні кількості вузлів і зміні топологій.

На основі отриманих результатів сформовано практичні рекомендації щодо покращення ефективності бездротових сенсорних мереж. Зокрема, рекомендовано впроваджувати кластерні маршрутизатори, використовувати адаптивні протоколи, застосовувати Edge Computing для зменшення навантаження на центральні вузли, а також інтегрувати бездротових сенсорних мереж із хмарними або гібридними інфраструктурами. Вказано на перспективність розвитку самонавчальних бездротових сенсорних мереж, які використовують штучний інтелект, машинне навчання та енергоавтономні джерела живлення.

Узагальнюючи, результати дослідження мають як наукову, так і практичну цінність, сприяючи створенню ефективних, безпечних та енергоощадних бездротових сенсорних мереж наступного покоління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What Is A Sensor and What Does it Do? URL: https://dewesoft.com/blog/what-is-a-sensor (дата звернення: 13.03.2025).

2. Network Node – Glossary – Kemp. URL: https://kemptechnologies.com/resources/glossary/network-node (дата звернення: 13.03.2025).

3. What is a network gateway? URL: https://www.hpe.com/asia_pac/en/what-is/network-gateway.html (дата звернення: 13.03.2025).

4. Types of Network Topology – GeeksforGeeks. URL: https://www.geeksforgeeks.org/types-of-network-topology/ (дата звернення: 13.03.2025).

5. Introduction of IEEE 802.15.4 Technology – GeeksofGeeks. URL: https://www.geeksforgeeks.org/introduction-of-ieee-802-15-4-technology/ (дата звернення: 18.03.2025).

6. What is Zigbee? About Zigbee Wireless Mesh Technology. URL: https://www.digi.com/solutions/by-technology/zigbee-wireless-standard (дата звернення: 18.03.2025).

7. Bluetooth Low Energy (BLE): A Complete Guide. URL: https://novelbits.io/bluetooth-low-energy-ble-complete-guide/ (дата звернення: 18.03.2025).

8. What is Routing? – Network Routing Explained – AWS. URL: https://aws.amazon.com/what-is/routing/ (дата звернення: 19.03.2025).

9. Low-Energy Adaptive Clustering Hierarchy – Knowledge and References | Taylor & Francis. URL: https://taylorandfrancis.com/knowledge/Engineering_and_technology/Computer_science/Low-Energy_Adaptive_Clustering_Hierarchy/ (дата звернення: 20.03.2025).

10. What Is User Datagram Protocol (UDP)? | Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/user-datagram-protocol-udp (дата звернення: 20.03.2025).

11. Stream Control Transmission Protocol (SCTP). URL: https://www.techtarget.com/searchnetworking/definition/SCTP (дата звернення: 20.03.2025).

12. What is TCP/IP in Networking? | Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/tcp-ip (дата звернення: 23.03.2025).

13. Power over Ethernet (PoE, PoE+, UPOE, UPOE+) | NetworkAcademy.io. URL: https://www.networkacademy.io/ccna/ethernet/power-over-ethernet (дата звернення: 23.03.2025).

14. What is HTTP? | Cloudflare. URL: https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/ (дата звернення: 23.03.2025).

15. FTP (File Transfer Protocol). URL: https://www.techtarget.com/searchnetworking/definition/File-Transfer-Protocol-FTP (дата звернення: 23.03.2025).

16. Simple Mail Transfer Protocol (SMTP) – GeeksforGeeks. URL: https://www.geeksforgeeks.org/simple-mail-transfer-protocol-smtp/ (дата звернення: 23.03.2025).

17. What is the Internet of Things (IoT)? | IBM. URL: https://www.ibm.com/think/topics/internet-of-things (дата звернення: 26.03.2025).

18. Industrial Internet of Things (IIoT). URL: https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT (дата звернення: 26.03.2025).

19. What is smart agriculture and why smart agriculture is the future? | ONDO. URL: https://ondo.io/what_is_smart_agriculture/ (дата звернення: 28.03.2025).

20. Беной С. Бездротові сенсорні мережі для моніторингу охорони здоров'я: проблеми та можливості // Журнал біомедичних систем та нових технологій. – 2023. – № 2. – С. 1.

21. LoRaWaN: benefits of wireless sensor networks for smart cities – Jooby. URL: https://jooby.eu/blog/lorawan-benefits-of-wireless-sensor-networks/ (дата звернення: 30.03.2025).

22. Understanding Privaty Issues in Wireless Sensor Networks. URL: https://www.azosensors.com/article.aspx?ArticleID=3111 (дата звернення: 31.03.2025).

23. SCP-MAC: Information and Source Code. URL: https://www.isi.edu/websites/ilense/software/scpmac/ (дата звернення: 02.04.2025).

24. Sensor Network Scalability: Overcoming Challenges in Large-Scale IoT Deployments – Wireless Sensor Networks Research. URL: https://sensor-networks.org/sensor-network-scalability-overcoming-challenges-in-large-scale-iot-deployments/ (дата звернення: 05.04.2025).

25. Top 7 Trends in the Wireless Sensor Network Market – Verified Market Reports. URL: https://www.verifiedmarketreports.com/blog/top-7-trends-in-the-wireless-sensor-network-market/ (дата звернення: 05.04.2025).