Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна
Факультет комп'ютерних наук
Кафедра теоретичної та прикладної системотехніки

«Затверджую»
Зав. кафедри теоретичної та
прикладної системотехніки
_____ д.т.н., проф. С. І. Шматков
«___» _____ 2023 р

Пояснювальна записка

до кваліфікаційної роботи
бакалавра

на тему: «**МОДЕЛЬ СИСТЕМИ КОНТРОЛЮ СТАНУ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯМ MESH-ТЕХНОЛОГІЙ**»

Захищено на засіданні
Атестаційної комісії № 42
протокол № __ від __.06.2023 р.
Оцінка _____ / _____
Голова Атестаційної комісії
_____ **СКОБ Ю. О.**
(підпис) (прізвище та ініціали)

Виконав:
студент 4 курсу, групи КУ– 41
Галузь знань: 15 – Автоматизація та приладобудування
Спеціальність: 151 – «Автоматизація та комп'ютерно-інтегровані технології»
ЧЕРКАСОВ Андрій Іванович_____

Керівник: старший викладач кафедри теоретичної та прикладної системотехніки
АРТЮХ Олексій Анатолійович_____

Рецензент: старший викладач кафедри електроніки і управляючих систем
ОСИПЧУК Андрій Володимирович

Харків – 2023

АНОТАЦІЯ

Пояснювальна записка до кваліфікаційної роботи бакалавра складається зі вступу, трьох розділів, висновків, списку використаних джерел і двох додатків. Загальний обсяг роботи складає 57 сторінок, із яких 41 сторінка основної частини з 24 рисунками, 1 таблицею, 15 найменуваннями списку використаних джерел та трьома додатками.

Метою кваліфікаційної роботи є розробка моделі системи контролю за об'єктом інфраструктури з використанням MESH-мережі.

Об'єкт дослідження – модель системи контролю з використанням MESH - технологій на прикладі умовного об'єкту інфраструктури.

Предмет дослідження – методи та засоби інформаційних технологій для автоматизації дистанційного контролю та управління об'єктами інфраструктури.

Проблема, яка вирішується в кваліфікаційній роботі, полягає в використанні нових технологій та підходів в створенні мереж для моделі контролю стану об'єктів інфраструктури.

Область застосування – модернізація та проектування систем контролю за об'єктами інфраструктури. Розроблена модель може широко використовуватися в сфері сервісів, що надають послуги в обслуговуванні, аналізу і підтримки об'єктів інфраструктури.

Ключові слова: модель, системи контролю стану, UML-модель, Cisco Packet Tracer, реалізація моделі, інтернет речей, MESH-мережа, OSPF.

ABSTRACT

An explanatory note to the master's attestation work is created in the introduction, three sections, conclusion and a list of sources used.

The total volume of work is 57 pages, of which 41 pages of the main part with 24 figures, 1 table, 15 names of the list of used sources and three additions. The purpose of the qualification work is to develop a model of the control system for the infrastructure facility using the MESH network.

The problem that is solved in the qualification work is the use of new technologies and approaches in creating networks for the model of monitoring the state of infrastructure objects.

The field of application is the modernization and design of control systems for infrastructure objects. The developed model can be widely used in the field of services that provide services in maintenance, analysis and support of infrastructure facilities.

Keywords: model, state control systems, UML model, Cisco Packet Tracer, model implementation, Internet of Things, MESH network, OSP

ЗМІСТ

ВСТУП

У зв'язку з постійними аваріями на об’єктах цивільної інфраструктури в наслідок неправомірних атак на них з боку росії, все більш актуальним постає проблема обслуговування об’єктів, аналіз їх стану, підтримки зв’язку з ними та вчасного виявлення проблем в роботі. В нагоді стануть системи, що використовують MESH-технології для збору та передачі інформації. MESH-технології поступово з’являються у всіх сферах життя людей, допомагаючи їм у бізнесі, хатніх справах, догляді за іншими, освіті, безпеці та інше. Серед переваг MESH-технологій відзначають:

- Високу стійкість мережі до збоїв або атак за рахунок самоорганізації та самовідновлення.
- Легку масштабованість покриття мережі за рахунок автоматичного підключення нових пристроїв.
- Зменшене споживання електроенергії та покращення продуктивності та швидкості мережі за рахунок розподілу навантаження між пристроями та оптимізації шляху передачі даних.

Актуальність роботи. Так як, системи контролю, що дозволяють отримувати інформацію і дистанційно керувати об’єктами інфраструктури, є вкрай корисними в мирний час, то і під час військового стану їх користь важко переоцінити. Тому розроблена модель допоможе в створені нових і надійних систем, роботу яких буде важко порушити внаслідок стихійного лиха, бойових дій або виходу з ладу окремих елементів.

Метою дослідження є розробка і створення моделі системи контролю стану інфраструктури з використанням MESH-технологій.

Об’єкт дослідження – модель системи контролю стану об’єктів інфраструктури на основі MESH-мереж.

Предмет дослідження – дослідження принципів роботи MESH-мереж в системах контролю стану різноманітної інфраструктури.

Завдання дослідження

1. Виконати аналіз існуючих систем контролю інфраструктури на предмет їх переваг та недоліків.
2. Виконати аналіз технологій MESH-мереж та порівняти з іншими технологіями створення мереж.
3. Розробити вимоги до системи контролю та створити її модель.
4. Виконати симуляцію роботи мережі системи контролю, та провести аналіз роботи.

РОЗДІЛ 1
СИСТЕМИ КОНТРОЛЮ СТАНУ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ

1.1 Поняття системи контролю стану об'єктів інфраструктури

Система контролю стану інфраструктури - це комплекс технічних засобів та програмного забезпечення, призначений для забезпечення надійності та ефективності роботи різноманітних інженерних систем, таких як енергетичні мережі, транспортні і комунікаційні мережі, водопровідні та каналізаційні системи, будівлі та споруди тощо.

На сьогоднішній день існує багато різних систем контролю стану інфраструктури, до прикладу:

- Системи віддаленого моніторингу. Вони дозволяють віддалено контролювати стан інфраструктури, використовуючи технології Інтернету речей (IoT). За допомогою датчиків, розташованих у різних точках інфраструктури, ці системи можуть зібрати дані про різні параметри, такі як вологість, температура, рівень шуму тощо.
- Системи моніторингу деформацій. Вони використовуються для виявлення деформацій будівель, мостів та інших споруд. Вони включають в себе різні техніки, такі як вібраційний аналіз, акустичну емісію, лазерний сканування тощо.
- Системи візуального моніторингу. Вони використовують камери відеоспостереження для відстеження стану інфраструктури та виявлення можливих проблем.
- Системи геопросторового аналізу. Вони дозволяють аналізувати географічні дані про інфраструктуру та її оточення, що дозволяє виявляти можливі ризики та проблеми.
- Системи управління ресурсами. Вони дозволяють відстежувати споживання ресурсів, таких як енергія та вода, та забезпечують контроль над їх використанням.

Ці системи можуть використовуватися окремо або в комбінації, залежно від потреб інфраструктурного об'єкта та його власника. Важливо вибирати оптимальні системи контролю стану інфраструктури, щоб забезпечити безпеку та ефективну експлуатацію інфраструктури.

1.2 Огляд систем контролю стану інфраструктури в Україні

В Україні можна навести не багато прикладів використання сучасних систем контролю стану інфраструктури, зазвичай, ці системи є застарілими з малою часткою автоматизації процесів контролю та аналізу. Проте впродовж останніх років розробляються та впроваджуються нові технології в галузі контролю стану інфраструктури. На приклад:

Система моніторингу стану та ситуації на дорогах: "Розумна дорога" [1]. Вона включає в себе відеокамери, датчики температури, вологості, опадів, які дозволяють збирати дані про стан доріг та прогнозувати їх ремонт. Також до цієї системи входять WiM-комплекси (Weigh-in-Motion), тобто системи динамічного зважування, що можуть виявляти перевантажені машини на дорогах в реальному часі, та передавати інформацію в диспетчерські пункти за допомогою мережі інтернет. Не слід забувати і про датчики контролю швидкості, системи регулювання трафіку та створення «зелених коридорів». Роботу системи моніторингу проілюстровано на рисунку 1.1.

Переваги системи очевидні – це контроль використання та догляду за станом дорожньої інфраструктури, підвищення безпеки водіїв, завдяки сповіщенню про ситуацію на дорозі: стан дорожнього покриття, погода, можливі ДТП, а також сповіщення органів правопорядку про можливих порушників, та сповіщення працівників швидкої допомоги в режимі реального часу. Проте ми маємо недоліки у вигляді великої розрізненості системи, окремі її елементи не мають звя’зків один з одним та контролюються різними дата центрами, також система має залежність від вже існуючої інфраструктури на місці. Тобто для того щоб окремий датчик або комплекс міг надавати інформацію, нам треба в потрібному місці мати мережеву інфраструктуру або

створити таку, до якої можна під'єднати пристрої, і яка дала б змогу передавати потрібній об'єм даних. Це в свою чергу зменшує кількість можливих місць впровадження такої системи та заважає її масштабуванню.

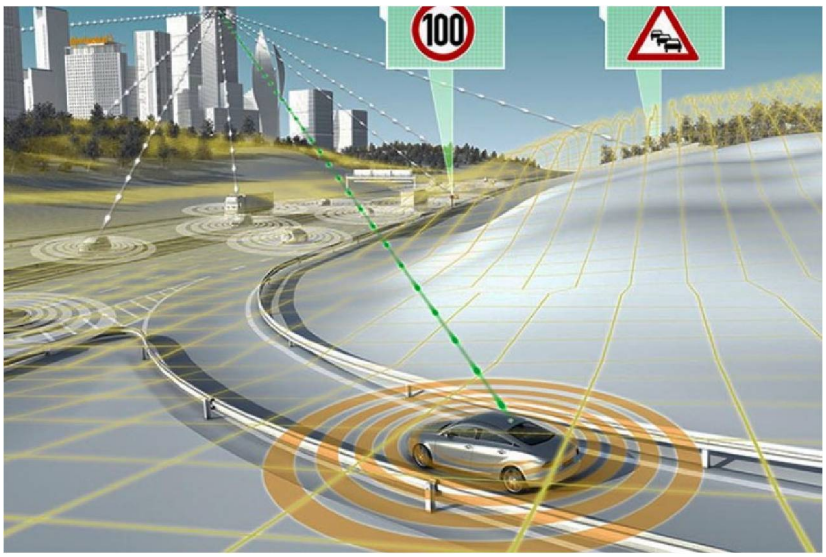

Рисунок 1.1 – Ілюстрація сповіщення клієнта в мережі «розумна дорога»

Система моніторингу стану газопроводів: "Єдина система моніторингу газотранспортної системи" (ЄСМ ГТС) [3]. Газотранспортна система України є однією з найбільших у світі. Вона включає безліч трубопроводів, газовимірювальних станцій, компресорних станцій, газових сховищ, об'єктів видобутку сировини та розподільчих станцій для споживачів. Тому надважливим для країни було створення єдиної системи контролю для газової інфраструктури. До її створення газотранспортною системою керували в телефонному режимі, що займало безліч часу на збір інформації та її обробку. Створення та впровадження ЄСМ ГТС дозволило прискорити процеси збору, обробки інформації, та керування об'єктами. Система базується на базі ITT-PIMS (англ. Pipeline Integrity Management Systems) та включає в себе різноманітні датчики, які дозволяють: вимірювати тиск, об'єми пального, відстежувати стан газопроводів, прогнозувати споживання та виявляти можливі проблеми зі зносом та пошкодженнями, формувати просторові бази даних об'єктів лінійної частини магістральних газопроводів (ЛЧМГ) та їх об'єктів оточення, управління ризиками експлуатації та багато іншого [5].

Датчики поєднуються між собою за допомогою протоколу WirelessHART [6], що використовує часово синхронізовану, самоорганізовану і самозцілювану меш-архітектуру. Протокол підтримує роботу в діапазоні 2,4 ГГц ISM з використанням радіо стандарту IEEE 802.15.4 [8].

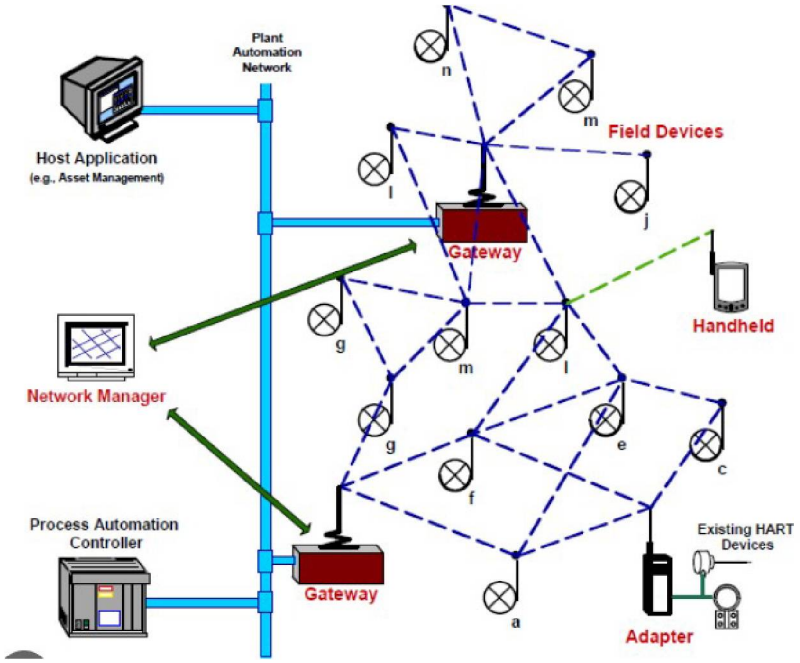

Рисунок 1.2 – Структурна схема організації мережі ЄСМ ГТС

Завдяки меш-архітектурі, вся система є легко поширювальною та може працювати у надскладних умовах, ефективно і безперешкодно надсилаючи дані до центрального диспетчерського департаменту ПАТ "Укртрансгаз", де інформація проходить обробку та аналізується.

Система моніторингу стану залізничної інфраструктури: "Геоінформаційна система залізничної інфраструктури" (ГІС). Ця система знаходиться тільки на стадії впровадження в нашій країні, випробовується на окремих ділянках залізниці та не має об’єднаної мережі. Електронна картографічна модель нашої залізниці, яку можна побудувати з використанням технологій ГІС, буде здатна збирати та зберігати детальну інформацію про стан об’єктів інфраструктури, такі як: залізничні колії, мости, тунелі та інше. В залежності в того, наскільки детальною буде інформація, спеціалісти зможуть швидко діставати дані про об’єкти такі як: технічні

характеристики, прив'язка до загальної бази майна, скільки людей працює на певному підприємстві залізниці, які об'єкти задіяні у виробничому процесі, а які здаються в оренду, тощо. Також ця система може легко поєднуватись з іншими, таким чином створюючи більш повне та реалістичне представлення даних. Країни ЄС та США використовують ГІС як невід'ємну частину транспортної логістики тому, що за допомогою інформації, наданою системою, можна вирішувати будь-які логістичні і транспортні задачі [5].

Зараз в нашому локомотивному господарстві широко застосовується автоматизована система (АС) «Дельта-СУ» [2], що включає в себе відеокамери, GPS-приймачі, модулі мобільного зв'язку GSM/GPRS та різноманітні датчики, що відстежують місце знаходження локомотиву та контролюють його технічний стан, в режимі реального часу. Також система має змогу об'єднуватись з іншими системами та модифікуватись в залежності від потреб замовника.

В енергетичній інфраструктурі України використовується SCADA (Supervisory Control and Data Acquisition) - це дуже поширена у світі архітектура системи керування, що складається з збірників даних, передавачів даних, мережі зв'язку та центральної системи управління. SCADA забезпечує збір даних з різних датчиків та пристроїв, їх аналіз та відображення у зрозумілій формі для операторів, а також можливість керування процесами у режимі реального часу [11].

Розберемо як працює система в енергетичній інфраструктурі, а саме електромережі. Об'єктами контролю в цій системі є електрогенеруючі об'єкти, передавачі, підстанції, трансформатори, розподільні мережі. Основна мета такої системи полягає в забезпеченні надійності та безпеки роботи інфраструктури, запобігання, вчасного виявлення та усунення будь-яких відхилень, які можуть призвести до аварії. Тому SCADA збирає дані про показники рівня напруги, показники навантаження на обладнання та мережі, дані про роботу електрогенеруючих установок та трансформаторів, дані про

виробництво та споживання електроенергії, дані про режим роботи та стан енергомереж. Збір інформації здійснюється за допомогою датчиків та вимірювальних приладів. А доставка інформації до центру прийняття рішень здійснюється за допомогою мережі передачі даних. Деякі з найпоширеніших мережевих технологій, що використовуються SCADA, є:

- Ethernet/IP - це стандартна технологія IP для промислових мереж, яка дозволяє передавати дані з високою швидкістю та надійністю.
- CWDM (Coarse Wave Division Multiplexing) - це технологія, яка дозволяє передавати кілька сигналів по одному оптоволоконному кабелю, використовуючи різні довжини хвиль світла. CWDM дозволяє збільшити пропускну здатність мережі без необхідності прокладати додатковий кабель.
- MPLS (Multiprotocol Label Switching) - це технологія, яка дозволяє ефективно маршрутизувати пакети даних по мережі на основі спеціальних міток, які додаються до кожного пакета. MPLS покращує продуктивність мережі, зменшує затримки та спрощує управління. MPLS також може підтримувати резервне копіювання та високий рівень безпеки [10].

До недоліків системи можна віднести її високу вартість та складність управління. Також через те, що система є критично важливою для роботи енергомережі, будь-який простій або збій системи може призвести до дорого вартісного ремонту або до зупинки цілого підприємства. Помилка в роботі системи можлива з-за нестачі даних про певний об’єкт, через збій одного з проміжних пристроїв передачі даних.

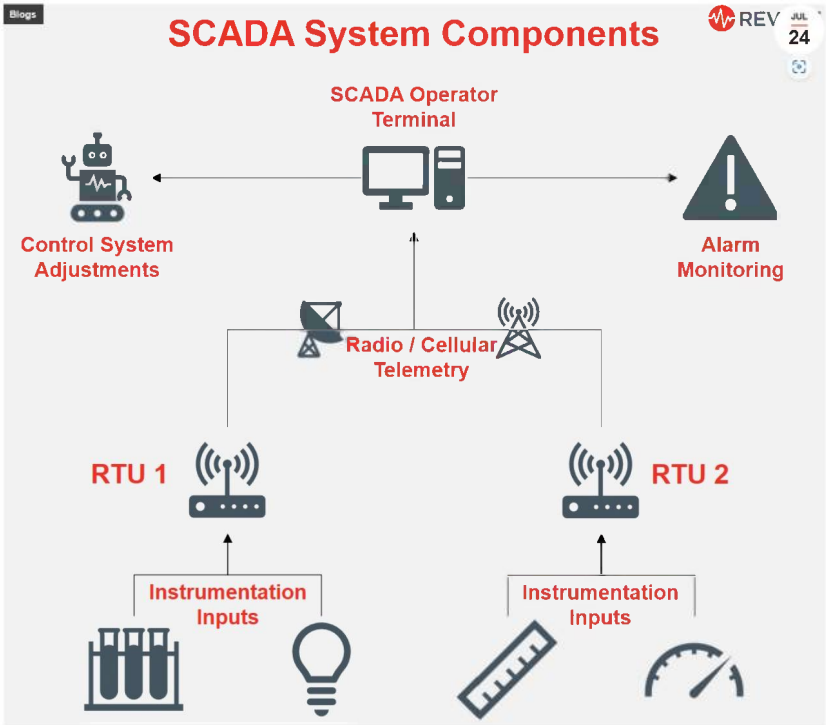

Рисунок 1.3 – Складові системи контролю SCADA

1.3 Аналіз недоліків систем контролю інфраструктури

Однією з найбільш актуальних проблем, з якими стикаються системи контролю стану інфраструктури, є розрізненість між окремими системами та їх невзаємодія. Багато систем контролю стану розробляються та використовуються окремо для кожної інженерної системи, що може призвести до втрати цілісності та недостатньої координації між системами. Це може ускладнювати процес управління та моніторингу.

Також до недоліків можна віднести і те, що всі ці системи використовують для побудови і функціонування технологію Інтернет, що робить їх вразливими до кібератак, та робить їх залежними від обов'язкових обмежень, які викликані застосуванням цієї технології.

Тому для вирішення цих проблем пропонується створювати та об'єднувати системи за допомогою альтернативних технологій побудови мереж.

РОЗДІЛ 2
АЛЬТЕРНАТИВНІ ТЕХНОЛОГІЇ ПОБУДОВИ МЕРЕЖ ДЛЯ СТВОРЕННЯ СИСТЕМ КОНТРОЛЮ

2.1 Поняття MESH-технології

MESH-технологія – це підхід до побудови мережі, в якому вузли з'єднуються між собою, утворюючи мережеву сітку без централізованого керування. MESH-технологія може бути використана як для дротових, так і для бездротових мереж. Вона дозволяє покращити покриття мережі, спростити управління і легко масштабувати мережу за потреби.

MESH-мережа відноситься до типу мереж, які мають надлишкові зв'язки між вузлами. Зазвичай вона складається зі статичних MESH-клієнтів, MESH-маршрутизаторів і шлюзів. Коли вузли часто або регулярно змінюють своє положення, сітці доводиться витрачати багато часу на підтримку актуальних маршрутів, а не на передачу даних.

Ідея MESH-мереж була запропонована ще в 1970-х роках у рамках проекту ARPANET - попередника сучасного Інтернету. Одним з завдань проекту було створення надійної мережі для обміну інформацією між науковими та військовими установами США. Для цього було запропоновано використовувати не традиційну зіркову або кільцеву топологію, а сітчасту, де кожен вузол може підтримувати комунікацію з будь-яким іншим через проміжні вузли. Така топологія дозволяла забезпечити більшу гнучкість, масштабованість і стабільність мережевого з'єднання.

Згодом концепція MESH-мереж була розвинута і застосована для створення бездротових мереж, особливо для задач мобільного зв'язку. Першими прикладами таких мереж були радіомережевий стандарт ALOHA (1971) і радіомережа PRNET (1973), які дозволяли передавати дані між розподіленими станціями без фіксованих каналів. У 1980-х роках були розроблені перші стандарти для бездротових локальних мереж (WLAN), таких

як IEEE 802.11 (Wi-Fi), яким також притаманна MESH-топологія на розподіленому регламентом діапазонах.

Для розробки моделі будемо використовувати технологію Wireless MESH Network (WMN) – це мережа, до складу якої входять радіовузли, організовані за допомогою топології MESH. WMN є різновидом бездротової мережі ad hoc без точки доступу.

2.2 Ad hoc мережа

Бездротова мережа ad hoc (wireless ad hoc network) (WANET) або mobile ad hoc network (MANET) – це децентралізований тип бездротової мережі, яка не схожа на традиційну інфраструктуру, що вже існує у вигляді маршрутизаторів або бездротових точок доступу. Замість цього в мережах ad hoc кожен вузол бере участь у маршрутизації шляхом пересилання даних для інших вузлів. Вузли, які приймають участь у передачі даних, визначаються динамічно на основі мережевого підключення та алгоритму маршрутизації. Встановлюється однорангова взаємодія за типом «точка–точка» [13].

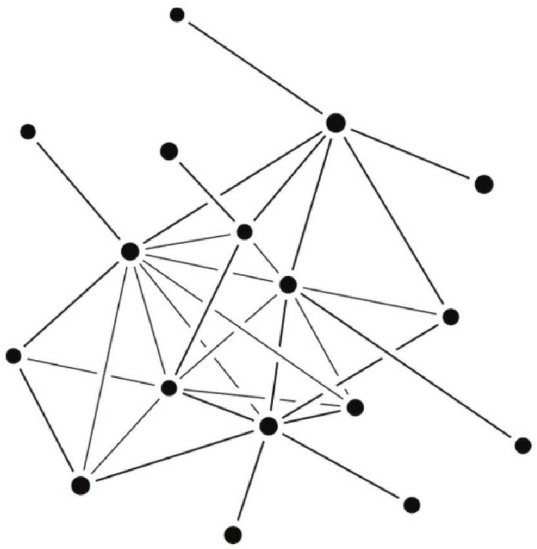

Рисунок 2.1 – Схематичне зображення ad hoc мережі

Така мережа має безліч переваг, а саме у налаштуванні та адмініструванні інфраструктури, що дає змогу пристроям створювати мережі та моментально до них приєднуватись, також:

- Кожен пристрій в WANET має змогу вільно змінювати своє місце знаходження та переміщуватись у будь-якому напрямку, тому постійно буде змінюватись посилання на інші пристрої.
- Містять один або декілька проміжних трансляторів між вузлами, що робить мережу високодинамічною.
- Мають змогу працювати автономно або бути підключеними до глобального інтернету.

До мінусів ad hoc мереж можна віднести те, що кожен вузол повинен перенаправляти трафік не пов'язаний з власним використанням, а значить бути маршрутизатором. Це є основною проблемою при побудові WANET/MANET мереж тому, що:

- Потрібно оснастити кожен вузол пристроями для постійного обслуговування інформації.
- Існує великий відсоток накладного трафіку, необхідного для маршрутизації в реальному часі.
- Кожен вузол має власну пропускну здатність незалежно від того, чи знає він про потреби інших вузлів.
- З попереднього виходить те, що кожен вузол повинен мати однакову пропускну здатність.

2.3 Бездротові MESH-мережі

Коли кожен вузол з'єднаний з кожним іншим вузлом, утворюється «сітка». Бездротові ad hoc мережі можуть мати форму сітки, проте це не завжди так. Фіксованої топології для бездротових ad hoc мереж не існує тому, що зв'язок між вузлами такої мережі повністю залежить від поведінки пристроїв, відстані між ними, їх мобільності або протоколу, що використовується при побудові зв'язків, тощо [14].

У бездротовій сітчастій мережі топологія зазвичай залишається незмінною, тому маршрути обчислюються швидше і дані доходять до місця призначення. Таким чином, це є централізована форма бездротової мережі ad hoc з низькою мобільністю. Крім того, вона інколи використовує статичні вузли як шлюзи, тому це не є повністю бездротова спеціальна мережа.

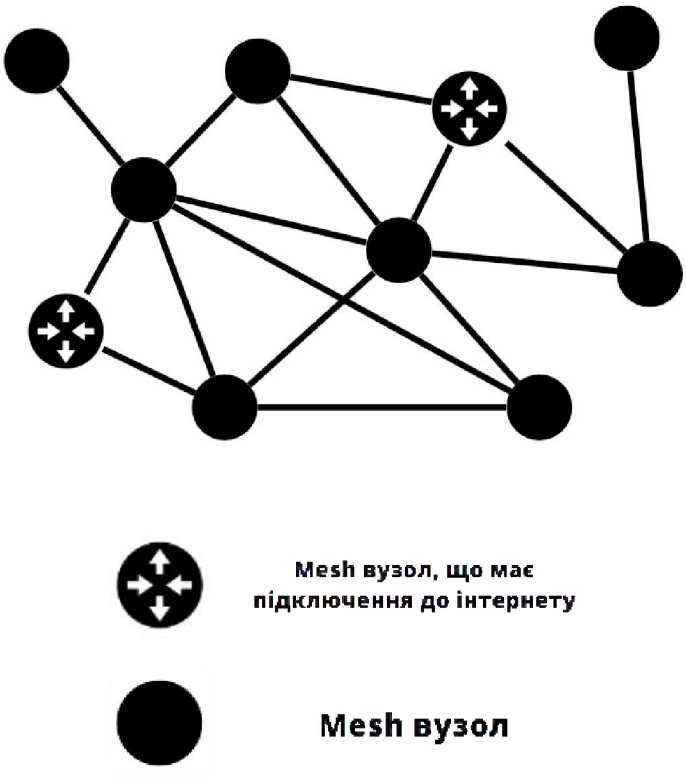

Рисунок 2.2 – Класична схема MESH-мережі

Ноутбуки, мобільні телефони та інші бездротові пристрої часто використовуються як MESH-клієнти. MESH-маршрутизатори дозволяють пересилати трафік між шлюзами, які можуть бути підключені або не підключені до Інтернету. Зона покриття всіх радіовузлів, що працюють як єдина мережа, називається сітчастою хмарою. Доступ до цієї хмари залежить від радіовузлів, що працюють разом над створенням радіомережі. Сітчаста мережа є надійною і забезпечує надмірність, оскільки якщо один вузол припиняє роботу, інші вузли все ще можуть зв'язуватися один з одним через один або кілька проміжних вузлів.

Бездротові MESH-мережі можуть самоформуватися і самовідновлюватися, і вони працюють з різними бездротовими технологіями, такими як 802.11, 802.15, 802.16, та не обмежуються жодною конкретною технологією чи протоколом.

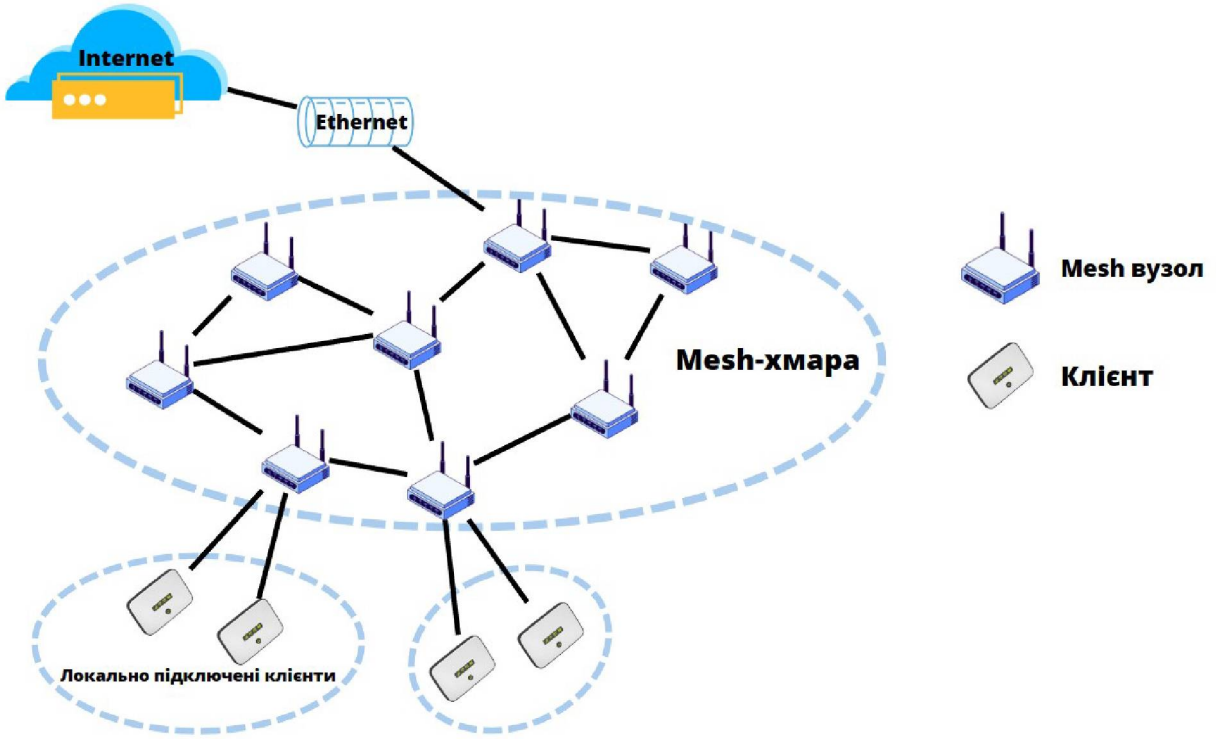

Рисунок 2.3 – Представлення MESH-хмари

2.4 Огляд бездротових технологій для побудови мереж

Як відомо, існує два типи мереж: традиційні дротові і бездротові мережі. У більшості випадків ми маємо справу з дротовими мережами, де дані передаються через кабелі, такі як вита пара, коаксіальний кабель, оптоволокно або телефонні лінії. Основним недоліком таких мереж є необхідність прокладання кабелю і відсутність мобільності. Для вирішення цих проблем були розроблені бездротові мережі, в яких дані передаються по радіоканалу, що забезпечує мобільність користувачам.

Бездротове з'єднання може бути одностороннім або двостороннім, симплексним або дуплексним, одноадресним або багатоадресним. Залежно від цього, бездротова мережа може мати різну структуру і способи координації

передачі даних. Наприклад, у бездротових локальних мережах (WLAN) використовуються протоколи керування доступом до середовища (MAC), які регулюють порядок передачі даних між станціями і точками доступу.

Загалом існує три основні типи бездротовий мереж: WPAC (Wireless Personal Area Connectivity), WWAN (Wireless Wide Area Network), WLAN (Wireles Local Area Network), які розрізняють за територіальною ознакою.

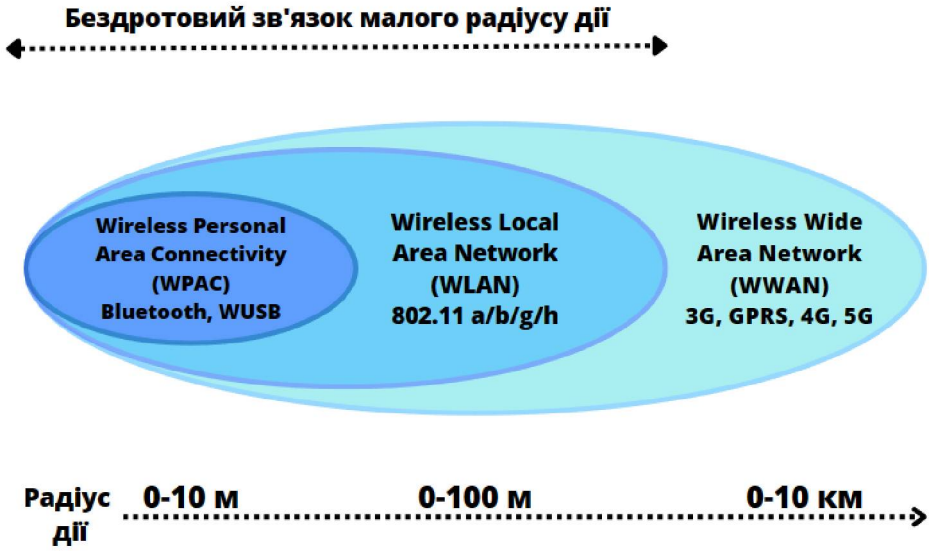

Рисунок 2.4 – Класифікація бездротових мереж за радіусом дії

Головну відмінність між ними складає діапазон робочих частот та радіус дії, що залежить від того ж діапазону частот та характеристик радіо-інтерфейсу. Також мережі WLAN і WPAN функціонують у неліцензованих діапазонах частот 2,4 і 5 ГГц, а це означає, що для їх розгортання не потрібно узгоджувати свої частотні діапазони з іншими радіомережами, які можуть працювати у тому ж діапазоні. З іншого боку, мережі BWA (Broadband Wireless Access) працюють одночасно в ліцензованих і неліцензованих діапазонах частот (від 2 до 66 ГГц).

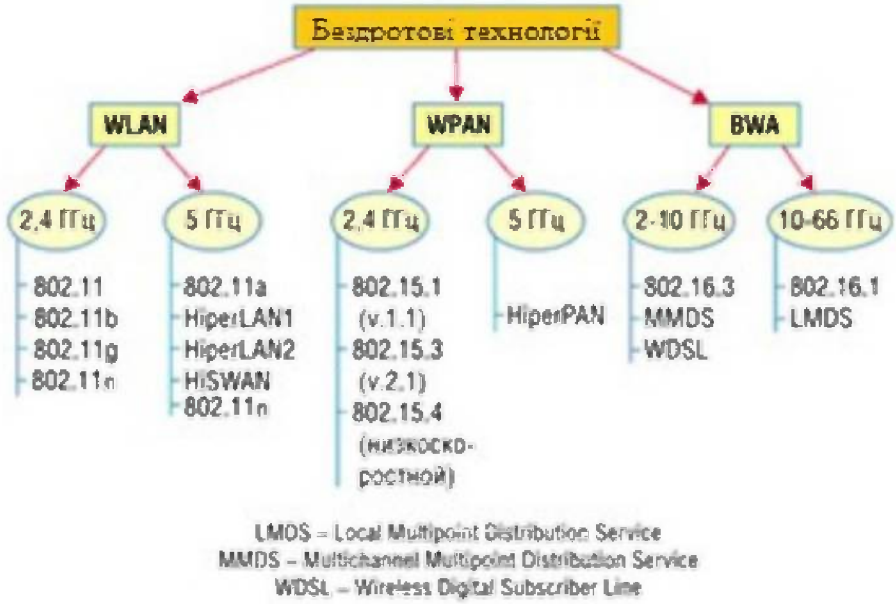

Рисунок 2.5 – Класифікація технологій бездротового зв'язку

2.4.1. Технологія бездротової передачі даних Wi-Fi

Найяскравішим представником бездротової технології є Wi-Fi (Wireless Fidelity), він був розроблений у 1990-х роках як альтернатива дротовим мережам, які були дорогими та складними в установці та обслуговуванні. Перша комерційна версія Wi-Fi була запущена у 1997 році під назвою IEEE 802.11. З того часу Wi-Fi постійно вдосконалюється та покращується, щоб забезпечити більшу швидкість, стабільність та безпеку передачі даних [12]. На сьогодні існує кілька стандартів Wi-Fi, таких як 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac та 802.11ax, кожен з яких має свої переваги та обмеження:

- 802.11a: використовує частотний діапазон 5 ГГц і досягає швидкості передачі даних до 54 Мбіт/с. Має низьку дальність дії та високу ступінь завадостійкості.
- 802.11b: використовує частотний діапазон 2,4 ГГц і досягає швидкості передачі даних до 11 Мбіт/с. Має високу дальність дії та низьку ступінь завадостійкості.

- 802.11g: використовує частотний діапазон 2,4 ГГц і досягає швидкості передачі даних до 54 Мбіт/с. Має високу дальність дії та середню ступінь завадостійкості. Сумісний з 802.11b.
- 802.11n: використовує частотний діапазон 2,4 або 5 ГГц і досягає швидкості передачі даних до 600 Мбіт/с. Використовує технологію MIMO (Multiple Input Multiple Output), яка дозволяє використовувати кілька антен для покращення пропускної здатності та надмежностей сигналу. Сумісний з 802.11a/b/g.
- 802.11ac: використовує частотний діапазон 5 ГГц і досягає швидкості передачі даних до 1,3 Гбіт/с. Використовує технологію MU-MIMO (Multi-User MIMO), яка дозволяє одночасно обслуговувати кілька пристроїв на одному каналі комунікації. Сумісний з 802.11a/n.

В нашому випадку найбільшої уваги заслуговує стандарт 802.11ah, який ще має назву Wi-Fi «HaLow». Його особливість полягає в тому, що він працює в діапазоні 900 МГц, що дозволяє йому підключатись до клієнтів на більшій відстані та при цьому використовувати мінімум енергії.

Новий стандарт майже вдвічі збільшує радіус сигналу, на відміну від вже поширених стандартів, що використовують діапазони 2,5 ГГц та 5 ГГц, також радіохвилі в діапазоні 900МГц спроможні долати більше перешкод, на приклад, стіни, та захищені від впливу мікрохвильових печей і інших побутових приладів. Це полегшує створення бездротових мереж у складних умовах, наприклад, у сільській місцевості або у багатоповерхових будинках.

Wi-Fi HaLow також здатний підтримувати тисячі пристроїв на одну точку доступу, що забезпечує високу щільність покриття. Це особливо актуально для застосувань IoT, які потребують збору та обробки великої кількості даних з розподілених сенсорів.

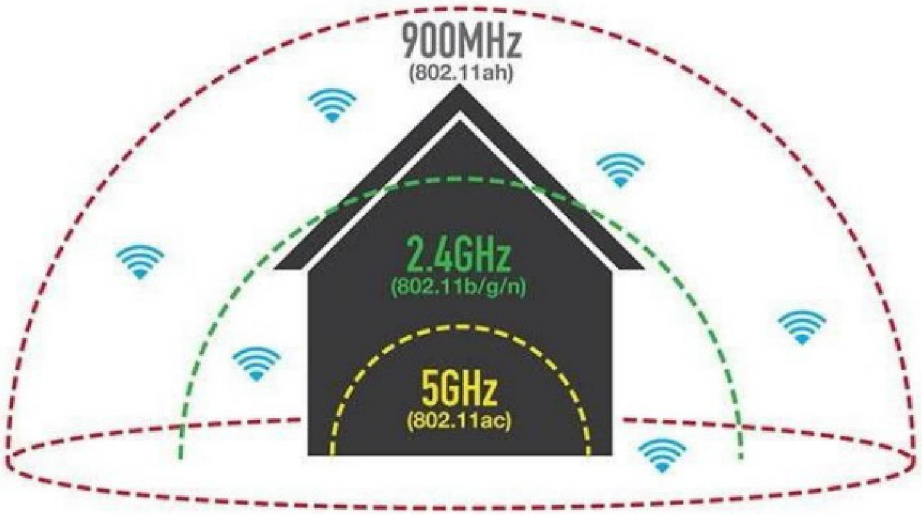

Рисунок 2.6 – Діапазон дії нового стандарту бездротового зв'язку Wi-Fi 802.11ah «HaLow».

Щодо швидкості передачі даних, то Wi-Fi HaLow може досягати до 347 Мбіт/с за рахунок використання модуляції 256-QAM та чотирьох просторових потоків на один 16-МГц канал. Також є можливість використовувати канали шириною 1 МГц або 2 МГц для менш шумних середовищ.

Проте, ця технологія знаходиться ще на стадії сертифікації і випробувань, та все одно потребує дротового підключення до точки доступу та базується на використанні топологій «зірка» або «точка-точка», що не зовсім підходить нам за критерієм стійкості тому, якщо з ладу вийде центральний вузол або один з вузлів топології «точка-точка», то вся мережа перестане функціонувати.

2.4.2. Технологія бездротової передачі даних Bluetooth

Розглянемо стандарт IEEE 802.15 (Bluetooth), це перша технологія, що дозволила організовувати бездротові персональні мережі (WPAN). Вона дає можливість проводити передачу голосу і даних з використанням радіоканалу на короткі відстані (10-100 м) в неліцензійному діапазоні частот 2,4 ГГц, а також з'єднувати мобільні телефони, ПК та інші пристрої в умовах відсутності прямої видимості [9].

Стандарт Bluetooth має більше 10 профілів, тобто наборів функції пристроїв Bluetooth. Основними профілями, затвердженими групою розробників SIG є:

- Advanced Audio Distribution Profile (A2DP) цей профіль призначений для забезпечення передачі музики в бездротові навушники;
- Audio / Video Remote Control Profile (AVRCP) профіль, який дозволяє керувати функціями телевізора;
- File Transfer Profile (FTP_profile) профіль, що забезпечує обмін даними між пристроями;
- Hands-FreeProfile (HFP) профіль призначений для з'єднання бездротових навушників і мобільних пристроїв, оснащений також функцією розмови по телефону;
- LAN Access Profile (LAP) профіль, який забезпечує доступ до мереж LAN, WAN або Internet з використанням засобів іншого Bluetooth пристрою;
- SIM Access Profile (SAP, SIM) профіль, що дозволяє отримати доступ до SIM-картки мобільного пристрою і використовувати одну SIM-карту на декількох пристроях;
- Wireless Application Protocol Bearer (WAPB) профіль який зрівнює протокол для організації (Point-to-Point) з'єднання через Bluetooth.

Як і у випадку з Wi – Fi, Bluetooth також має енергоефективний профіль під назвою Bluetooth Low Energy (BLE), що використовується в галузі охорони здоров'я, безпеки та домашніх розваг. Працює BLE в діапазоні 2,4 ГГц, що може призвести до колізій з іншими мережами, до прикладу того ж Wi – Fi, та негативно позначитись на роботі пристроїв. Тому для подолання перешкод і знаходження чистого шляху передачі, який уникає зіткнення пакетів, Bluetooth використовує технологію AFH (Adaptive Frequency Hopping).

AFH є формою спектру розсіювання частоти (FHSS), яка застосовується на рівні апаратного забезпечення (фізичного). Bluetooth ділить смугу частот на

менші канали (наприклад, 40 каналів у випадку BLE) і швидко перемикається між цими каналами під час передачі пакетів. Для подальшого зниження ймовірності перешкод Bluetooth адаптує свою послідовність перемикання частот. Канали, які є шумними та зайнятими, динамічно відстежуються і уникаються при надсиланні пакетів.

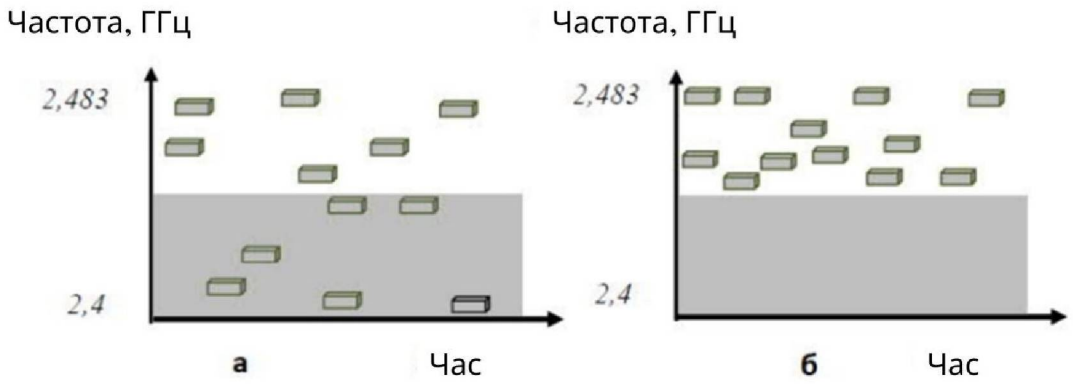

Рисунок 2.7 – Принцип роботи технології AFH: а - колізії; б - перехід від колізій за допомогою адаптивної перебудови частоти.

Підсумовуючи, можна зробити висновки, що перевагами технології Bluetooth є: мобільність і малі розміри; простота використання готових модулів; значна швидкість передачі даних; безпеку передачі даних; доступність; необхідність авторизації пристрою; низький поріг чутливості до перешкод (залежить від товщини і матеріалу перешкоди); високий рівень стандартизації.

Однак, слід зазначити, що дана технологія не позбавлена і недоліків. Якщо, наприклад, два користувача хочуть обмінятися даними, то в процесі пошуку пристроїв один одного будуть знайдені всі пристрої, які включені в радіусі 10-15 метрів, що знижує швидкість ініціалізації пристроїв. Крім того, слід зазначити неможливість побудови мереж складної топології і великі (у порівнянні з мережами ZigBee) обсяги енергоспоживання.

2.4.3 Технологія бездротової передачі даних ZigBee

ZigBee – це стандарт, який визначає набір протоколів зв'язку для бездротових мереж з низькою швидкістю передачі даних (англ. Low rate

wireless personal area network, LR-WPAN). Також стандарт ZigBee спеціально розроблений для того, щоб задовольнити потребу в дуже низькій вартості впровадження мереж WPAN та із наднизьким споживанням енергії. Бездротові пристрої на основі ZigBee працюють у діапазонах частот 868 МГц, 915 МГц та 2,4 ГГц. Максимальна швидкість передачі даних – 250 кбіт/с.

ZigBee орієнтований головним чином на пристрої, що мають акумуляторне живлення, для яких основні вимоги – низька швидкість передачі даних, низька вартість та тривалий час роботи акумулятора. У багатьох застосуваннях ZigBee загальний час, коли пристрій з бездротовим зв'язком зайнятий виконанням своїх основних функцій, дуже обмежений; пристрій проводить більшу частину свого часу в сплячому режимі (тобто у режимі енергозбереження). Завдяки цьому пристрої ZigBee здатні працювати кілька років, перш ніж їх батареї потрібно буде замінити [15].

Стандарт ZigBee розроблений Альянсом ZigBee, який налічує сотні компаній-членів, від напівпровідникової індустрії та розробників програмного забезпечення до виробників обладнання. Альянс ZigBee був утворений у 2002 році як некомерційна організація, відкрита для всіх, хто хоче приєднатися. Фізичний рівень (англ. Physical layer, PHY) та рівень керування доступом до середовища (англ. Media access control, MAC) ZigBee керуються стандартом IEEE 802.15.4.

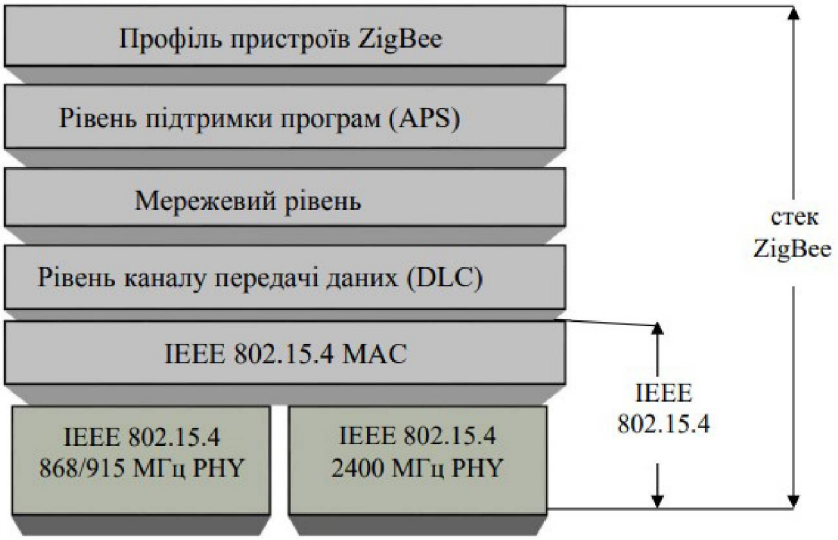

Рисунок 2.8 - Зв'язок стека ZigBee зі стандартом IEEE 802.15.4

Характеристики ZigBee:

- Частотний діапазон - 2,4 ГГц, 16 частот з шириною 5 МГц;
- DS-SS - пряме розширення спектра сигналу;
- O-QPSK - квадратурна фазова маніпуляція зі зміщенням;
- Автоматичне регулювання виходить потужності в широких межах для забезпечення енергоефективності;
- Дозволена потужність - 100 мВт;
- Оцінка рівня потужності сигналу в ефірі - RSSI і підтвердження про успішну доставку для кожного пакету даних;
- MESH-мережева технологія, яка забезпечує самовідновлення і самоорганізацію, надійність і гнучкість маршрутизації;
- До 65536 вузлів (модемів) в мережі;
- Механізм множинного доступу в ефір з контролем несучої і запобіганням колізій - CSMA (Carrier Sense, Multiple Access);
- 128-бітове шифрування даних за алгоритмом AES;
- Швидкість передачі даних, включаючи службову інформацію - до 250 кбіт / с.

Одне з найперших застосувань ZigBee – це спостереження за здоров'ям пацієнтів вдома. Наприклад, лікарю постійно треба відстежувати стан пацієнта, для цього він дає йому переносний датчик, що здатен взаємодіяти з пристроєм ZigBee. Датчик час від часу вимірює кров'яний тиск і серцебиття пацієнта. Інформація, завдяки пристрою ZigBee, потрапляє бездротовим шляхом до локального серверу, до прикладу, персонального комп'ютера пацієнта. Далі інформація проходить попередню обробку, і, в залежності від її результатів, приймається рішення про надсилання даних до лікарні, щоб допомогти пацієнту або ж попередити його про погіршення стану здоров'я.

Ще один з найяскравіших прикладів використання приладів, що працюють за стандартом ZigBee – моніторинг стану конструкцій великих будівель. В цей раз мережа бездротових датчиків із підтримкою ZigBee

складається з десятків або сотень вимірювальних приладів (наприклад, акселерометри). Вони створюють єдину мережу для збору даних про стан будівлі, що скорочує час та зменшує витрати на перевірку під час обслуговування споруди.

Стандарт ZigBee використовують для того, щоб знизити складність та вартість реалізації мережі, шляхом скорочення швидкості передачі та спрощення протоколів зв'язку. Тому мінімальні вимоги згідно заявленим специфікаціям ZigBee та IEEE 802.15.4 є відносно простими у дотриманні, ніж вимоги до того ж Wi-Fi стандарту IEEE 802.11.

2.5 Порівняння мережевих технологій Wi – Fi, Bluetooth та ZigBee

Порівняльні характеристики технологій Bluetooth, Wi-Fi і ZigBee наведені в Таблиці 1. Ця таблиця зможе надати повний обсяг інформації в зручному для розуміння вигляді та допоможе прийняти правильне рішення при виборі технології бездротової передачі даних для побудов систем контролю стану об'єктів.

Таблиця 1

Порівняння мережевих технологій Wi – Fi, Bluetooth та ZigBee

Стандарти	Технології						
	ZigBee 802.15.4			Bluetooth	Wi-Fi		
					802.1i1b	802.11g	802.11n
Частота ГГц	0,868	0,915	2,4	2,4	2,4	2,4	2,4 (5)
Швидкість	20 кб/с	40 кб/с	250 кб/с	1 Мб/с	11 Мб/с	54 Мб/с	600 (300) Мб/с
Вихідна потужність	0 дБм			0-20 дБм	20 дБм	20 дБм	20 дБм
Радіус дії, м	10-100			10-100	100	100	150-300
Розмір стека Кбайт	4-32			>250	>1000	>1000	>1000
Розмір мережі	216, 264			7 + 1	64	64	64
Час роботи від батареї, г.	2400-24000			24-240	12-120		

Продовження таблиці 1

Максимальна кількість елементів мережі	65536	7	100
Безпека	+	Аутентифікація, кодування	68/124 бітове шифрування
Енергоспоживання	Низьке	Низьке	Високе
Ціна	Низька	Низька	Висока
Реалізовані стандарти	IEEE 802.14.5	IEEE 802.15.1 IEEE 802.11	IEEE 802.11 a, b, n, g, ah
Сфера застосування	Сенсорні системи	Мобільні пристрої	Локальні мережі

Одне з популярних застосування Bluetooth – бездротові гарнітури, фітнес браслети, смарт годинники та навушники. ZigBee має найнижчу швидкість передачі даних і складність серед цих трьох стандартів і забезпечує значно довший термін служби акумулятора. Технологія Wi-Fi потребує дотримання складніших стандартів, ніж у конкурентів, проте забезпечує найбільшу швидкість передачі даних. Це робить його доцільним у випадках, якщо система потребує якісного зображення з камер відеоспостереження або дуже швидкої передачі інформації з датчиків (до прикладу тиску).

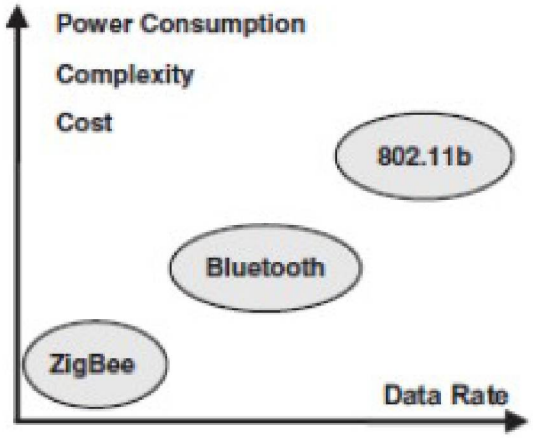

Рисунок 2.9 – Ілюстративне порівняння ZigBee, Bluetooth та IEEE 802.11b

Низька швидкість передачі даних ZigBee робить його непридатним для здійснення бездротового підключення до Інтернету або безпровідної

гарнітури, де бажана швидкість передачі більше 1 Мбіт/с. Однак, якщо ми потребуємо передачі та отримання простих команд і збирання інформації від датчиків, таких як датчики температури чи вологості, ZigBee має найкраще співвідношення за швидкістю передачі та ціною у порівнянні з Bluetooth та IEEE 802.11b.

РОЗДІЛ 3
МОДЕЛЬ СИСТЕМИ КОНТРОЛЮ СТАНУ ІНФРАСТРУКТУРИ

3.1 Обґрунтування вимог до моделі

Отже, аналізуючи інформацію про альтернативні технології побудови мережі, можемо дійти до висновку, що для забезпечення надійності функціонування, масштабованості, адаптації та стійкості до впливу чинників руйнації розроблюваної системи контролю, використаємо технології побудови MESH-мереж.

Для розробки моделі висунемо і обґрунтуємо вимоги до мережі, яким вона має відповідати:

1. Надійність і відмовостійкість. Це саме те, що може нам забезпечити MESH-мережа. При виході з ладу одного вузла, всі інші повинні залишатись функціонуючими, тому мережа в загалом не має втрачати своєї здатності передавати інформацію. Навіть у випадку якщо з ладу вийде група вузлів, то мережа може втратити зв'язок з конкретною зоною об'єкта, проте в загальному має продовжити своє функціонування.

2. Надлишковість зв'язків. Саме MESH-мережа може забезпечити виконання цього критерію. Також не тільки вузли повинні мати таку надлишковість, а ще й зони покриття цих вузлів. Тобто, припустимо, що ми маємо розрізненні групи сенсорів та датчиків на об'єкті інфраструктури, вони є кінцевими користувачами нашої мережі, та мають підключення до своїх точок доступу, якими виступають вузли MESH-мережі. Якщо з невідомих причин, один вузлів вийде з ладу, то інші вузли, суміжні з ним, повинні мати достатній радіус покриття для забезпечення підключення цієї групи датчиків. Таким чином збільшиться навантаження на сусідні вузли мережі, проте втрата інформації буде мінімальною.

3. Легке розгортання. Це одна з головних вимог для нашої моделі. Впровадження подібної системи має бути максимально дешевим та простим

для широкого розгортання мережі. Але це також не проблема для MESH-мереж тому, що в принцип дії цих мереж закладено самоорганізація та самовідновлення. Також в моделі має бути передбачене широке використання бездротових технологій зв'язку, для полегшення розгортання мережі в важкодоступних місцях, або в місцях, де не має відповідної інфраструктури.

4. Гнучкість і масштабованість. Впровадити MESH-мережу одночасно на всіх об'єктах не вийде, так само як і на окремо взятих об'єктах також. На нових об'єктах це не було б проблемою, так як на етапі проектування можна закласти впровадження подібної системи, проте якщо розглядати вже існуючі об'єкти, які при цьому активно використовуються, треба мати на увазі те, що ми не можемо переривати їх роботу для встановлення відповідного обладнання. Також система повинна бути здатною працювати з різними типами датчиків та забезпечувати масштабованість як на одному об'єкті так і на великій кількості інших об'єктів. Вона повинна впоратися зі зростаючим обсягом даних та забезпечувати їх транспортування.

5. Сумісність з існуючими системами контролю за об'єктами інфраструктури. Це теж є не менш вирішальним пунктом у нашому списку вимог. Якщо ми будемо поєднувати різні системи та мережі, нам не вдасться привести все до одного стандарту або однієї технології мережі. Тому вирішальним рішенням для створення моделі системи контролю буде використання змішаних технологій зв'язку. Для цього можна використовувати стикові мережеві протоколи.

Система контролю повинна включати в свій склад:

1. Датчики та сенсори.
2. Мережу передачі інформації.
3. Пристрої реагування.
4. Центр збору інформації, її обробки та прийняття рішень.

Мережу збору і передачі інформації будуватимемо як змішану, з використанням різних технологій. Це дозволить побудувати гнучку мережу,

здатну адаптуватися до виникаючих умов з одного боку, з другого боку використання різних підходів залежно від умов дозволить вибрати найбільш доречний підхід з точки зору умов передачі інформації, забезпечення надійності функціонування і забезпечення економічного підходу до застосування обладнання і витрат матеріальних і фінансових ресурсів.

Склад датчиків, пристроїв контролю і збору інформації, пристроїв реагування обумовлюється типом системи, її складом, глибиною необхідного контролю, вимогами до швидкості і обсягу реагування на ситуації. В якості такого обладнання можуть виступати аналогові чи цифрові датчики для збору різноманітних даних (тиск, температура, вологість, рівень радіації, рівень шуму, його характер, освітленість), газоаналізатори, просторові датчики положення об'єктів контролю, камери відеоспостереження та інше. Всі вони будуть продукувати різноманітну інформацію, яку потрібно надійно доставляти до центу контролю, а також за необхідності, до інших систем. Тому відповідно в мережі будуть використовуватися різні протоколи і технології.

Враховуючи вище викладене розробимо модель системи контролю системи об'єктів інфраструктури.

3.2 Модель системи контролю системи об'єктів інфраструктури

Для опису кращого опису зв'язків між елементами моделі під час розробки застосуємо сервіс будування UML-діаграм. UML (Unified Modeling Language) – це стандартизована мова моделювання, що складається з інтегрованого набору діаграм, розроблених для допомоги розробникам систем і програмного забезпечення у визначенні, візуалізації, побудові та документуванні артефактів програмних систем, а також для бізнес-моделювання та інших не програмних систем.

UML-модель складається з наступних класів: ControlStation, Sensor, MehCloud, DataCollectoinNode, Gateway та DataCenter.

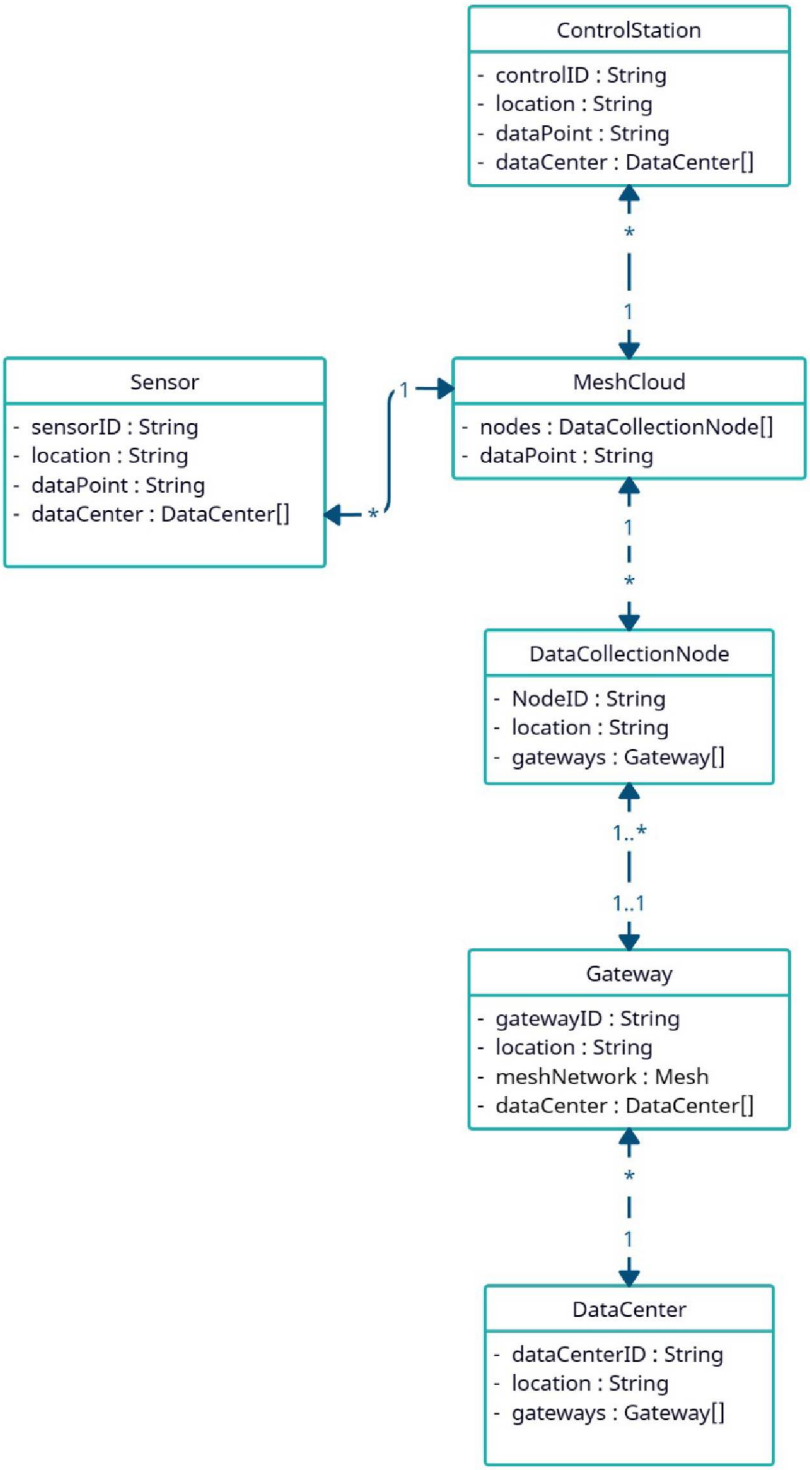

Рисунок 3.1 – UML-модель системи контролю стану об’єкту інфраструктури

Розглянемо елементи цієї моделі. Клас MESHCloud представляє собою MESH-мережу, що складає основу цієї моделі. Як і було зазначено у Розділі

2, MESH-хмара – це велика кількість пристроїв MESH, що створюють зв'язки один з одним. MESHCloud відповідає за передачу інформації від сенсорів до шлюзу, та від шлюзу до пристроїв реагування. Також в MESHCloud є два типи вузлів:

1. Вузли, що приймають інформацію від датчиків і є для них точками доступу. Для цього в класі є відповідний параметр datapoint.

2. Вузли, що мають зв'язки тільки всередині MESH-хмари, тобто вони не приймають дані з датчиків, та слугують тільки для концентрування інформації, щоб передати її до шлюзу. Ці вузли виділені в окремий клас DataCollectionNode. Тому клас MESHCloud містить в собі посилання на ці вузли.

Клас DataCollectionNode представляє собою вузол MESH-мережі та належить до класу MESHCloud. Так, як єдина функція цього вузла – концентрувати інформацію для подальшої передачі до шлюзу, його можна назвати вузол «концентратор». Клас містить: ID вузла, що означає, кожен вузол має свій ідентифікаційний номер для розпізнавання себе в мережі; вказане місце свого розташування на об'єкті; посилання на шлюз, якому потрібно надати дані.

Клас Gateway представляє собою шлюз, він може бути у вигляді порту маршрутизатору, або окремого пристрою, що моє доступ до Інтернету. Його мета – отримати дані від вузлів «концентраторів» і надсилати їх до дата-цетру. Також шлюз має змогу надсилати інформацію з дата-центру до пристроїв керування за допомогою зворотного зв'язку з вузлами «концетраторами». Клас містить: ID шлюзу, для ідентифікації себе в мережі; вказане місце свого розташування; посилання на MESH-мережу, з якої він отримує дані та куди надсилає команди; посилання на дата-центр.

Клас DataCenter представляє собою дата-центр, який збирає дані від декількох шлюзів, обробляє їх та аналізує. Після обробки інформації, або оператор, або автоматизована система має змогу надіслати вказівки на пункти

керування, або пристрої реагування на об'єкті. На приклад: відповідні перемикачі, трансформатори, системи сповіщення персоналу. Клас містить: ID дата-центру, для ідентифікації себе в мережі; вказане місце свого розташування; масив шлюзів, що належать дата-центру. Завдяки такому компонуванню ми маємо змогу отримувати інформацію одразу з декількох віддалених точок одного об'єкта інфраструктури або декількох, за потреби розширення мережі.

Клас Sensor представляє собою звичайний сенсор або датчик, що здатен збирати дані, він є кінцевим користувачем мережі, та має можливість обмінюватись інформацією з сервером. Клас містить: ID сенсора для ідентифікації себе в мережі; вказане місце свого розташування; інформацію про точку доступу, до якої він підключений; та інформацію про сервер, якому треба надіслати дані.

Клас ControlStation, останній в запропонованій моделі, представляє собою пристрій реагування, який за вказівками з дата-центру має виконувати певні дії на об'єкті інфраструктури. Клас містить: ID пристрою, для ідентифікації себе в мережі; вказане місце свого розташування; інформацію про точку доступу, до якої підключений; інформацію про дата-центр, з якого має отримувати команди.

Також розглянемо зв'язки між класами моделі:

- Клас Sensor має асоціацію з класом MESHCloud, і так як датчики і сенсори мають змогу обмінюватись інформацією з сервером, то клас має двосторонні зв'язки з класом MESHCloud.
- Клас MESHCloud, окрім асоціації до класу Sensor, має асоціацію до класу ControlStation. Пристрої реагування також мають змогу обмінюватись даними з сервером, тому клас має двобічні зв'язки з класом ControlStation. Також MESHCloud має агрегацію до класу DataCollectionNode тому, що DataCollectionNode представляє собою такі самі MESH-вузол, як і в цілій

хмарі, проте вони відіграють іншу роль в системі, тому і відокремлені в свій клас.

- Клас DataCollectionNode, окрім агрегації з класом MESHCloud, також має асоціацію з класом Gateway тому, що дані, які збирають вузли «концентратори», надсилаються до шлюзу, щоб потрапити до дата-центру.
- Клас Gateway має асоціацію з класом DataCenter, оскільки шлюзи передають дані до дата-центрів для подальшої обробки, і навпаки, команди до пристроїв класу ControlStation, надсилаються через шлюзи, тому клас Gateway має асоціацію до класу MESHCloud.

3.3 Симуляція роботи моделі

Модель створена за допомогою програми симуляції роботи комп'ютерних мереж Cisco Packet Tracer враховуючи вимоги та обмеження, які має засіб моделювання.

Cisco Packet Tracer - це інструмент моделювання мережі, який дозволяє на практиці засвоювати навички створення мереж, налаштування сервісів IoT та кібербезпеки в віртуальній лабораторії без потреби в апаратному забезпеченні. Крім того, він дозволяє своїм користувачам ознайомитися з командним інтерфейсом, властивим пристроям бренду Cisco. Він схожий на GN3 (теж симулятор проектування мереж), але більш інтуїтивний та простий у використанні.

Для створення моделі комп'ютерної мережі в програмі Cisco Packet Tracer необхідно:

- Проаналізувати вимоги до мережі.
- Розробити схему мережі.
- До кожного сегменту мережі призначити свою мережеву адресу.
- З'єднати пристрої між собою.
- Налаштувати зв'язок між пристроями.
- Налаштувати зв'язок кінцевих користувачів з сервером.
- Протестувати роботу мережі.

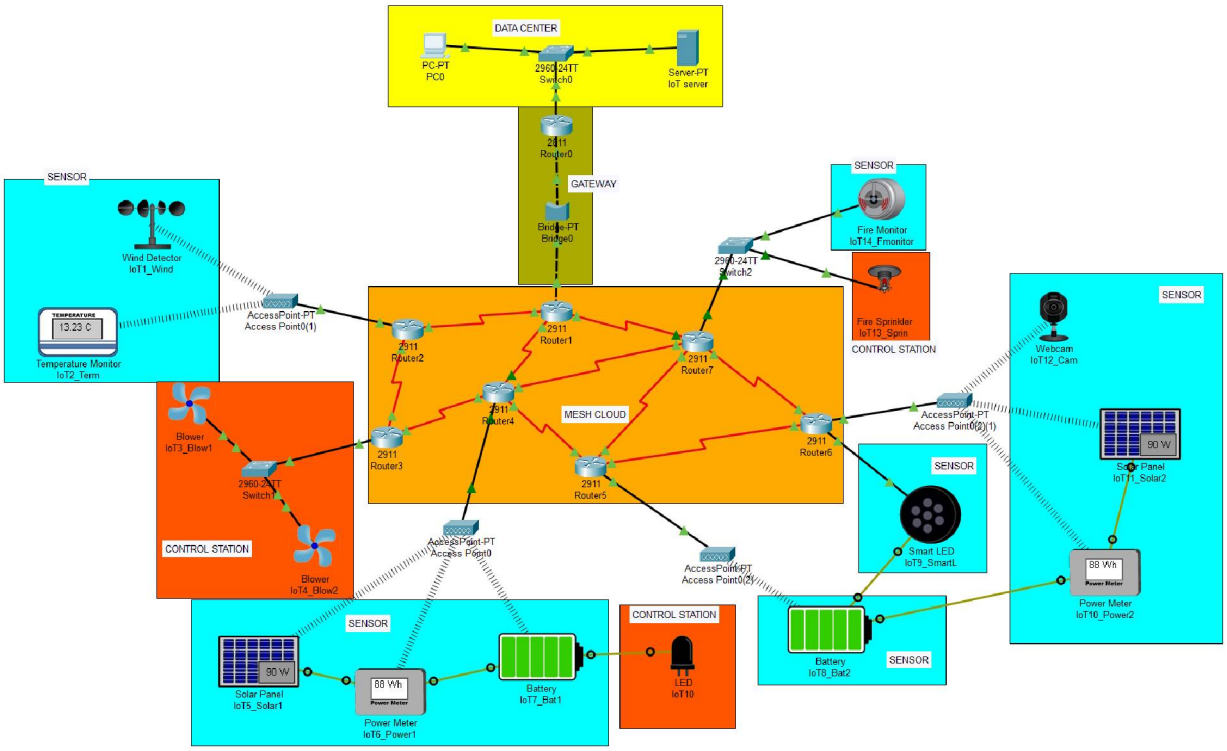

Рисунок 3.2 – Модель мережі системи контролю стану об’єктів інфраструктури

3.3.1 Огляд компонентів мережі

Під час створення мережі в програмі Cisco Packet Tracer було використано наступні пристрої:

- Комутатор для підключення серверу до мережі в блоці Data Center та комутатори для підключення різних датчиків, що потребують дротового з’єднання.
- Міст для симуляції шлюзу та віддаленого підключення до мережі системи контролю стану об’єкту.
- Роутери, що слугують вузлами в MESH-мережі.
- Бездротові точки доступу для під’єднання датчиків до мережі.
- Датчики в блоці Sensor, пристрої реагування в блоці Control Station та сервер, які належать до «Інтернету речей» і є зручними для модуляції потрібної нам системи.

3.3.2 Вибір протоколу комунікації між компонентами мережі

Для комунікації між пристроями в MESH-мережі використано дротове з'єднання, проте симулятор передбачає також використання бездротового з'єднання. Процес налаштування та створення мережі в обох випадках не має суттєвої різниці, тому модель відповідає вимогам надійності, легкості встановлення та масштабування.

Щоб забезпечити маршрутизацію пакетів між пристроями використовують протоколи, які встановлюють правила обміну повідомленнями. Саме протоколи відповідають за відправку, прийняття повідомлень, пошук маршруту між вузлами. Також вони присутні на різних рівнях моделі OSI. Набір протоколів, що дозволяє організувати взаємодію між вузлами в мережі, називається стеком протоколів.

Під час створення моделі для зв'язку між вузлами було обрано протокол OSPF. OSPF (Open Shortest Path First) – протокол динамічної маршрутизації, що використовує алгоритм Дейкстри для пошуку найкоротшого шляху між вузлами. Переваги, якими володіє цей протокол:

- Висока швидкість збіжності при змінах в топології мережі.
- Він не є запатентованим, а значить може використовуватись на різних платформах і обладнанні.
- Оптимальне використання пропускної здатності мережі.
- Оптимальний вибір шляху і розподіл навантаження.
- Підтримка масок змінної довжини (VLSM).

Також до переваг протоколу OSPF варто додати швидкість рекалькуляції таблиці маршрутизації при зміні топології або розташування вузлів в мережі, також немає обмеження на довжину шляху в 15 стрибків (до прикладу, як в RIP), а головним чинником при виборі маршруту є пропускна здатність мережі. Все це робить OSPF потужним і легко масштабованим протоколом маршрутизації. На рисунку 3.3 зображено налаштування проколу на одному з вузлів мережі.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.18.1 255.255.255.0
Router(config-if)#ip address 192.168.18.1 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 192.168.19.1 255.255.255.0
Router(config-if)#ip address 192.168.19.1 255.255.255.0
Router(config-if)#ip help
Router(config-if)#ip helper-address 192.168.1.1
Router(config-if)#ex
Router(config)#router ospf 1
Router(config-router)#network 192.168.18.0 0.0.0.255 area 0
Router(config-router)#network 192.168.19.0 0.0.0.255 area 0
Router(config-router)#
```

Рисунок 3.3 – Призначення IP-адрес на портах та налаштування протоколу маршрутизації OSPF

3.3.3 Опис роботи моделі під керівництвом протоколу OSPF

Роботу моделі під керівництвом протоколу маршрутизації OSPF можна поділити на шість етапів:

1. Маршрутизатори обмінюються hello-пакетами, щоб скласти таблицю маршрутизації. Коли маршрутизатори досягають домовленості про певні параметри, зазначені в їх hello-пакетах, тоді вони стають сусідами на загальному каналі передачі даних.

2. Маршрутизатори намагаються увійти в стан суміжності зі своїми сусідами. Перехід до стану суміжності залежить від типу маршрутизаторів і типу мережі. OSPF має змогу визначати кілька типів мереж і кілька типів маршрутизаторів. Пара маршрутизаторів, що знаходиться в стані суміжності, синхронізує свої бази даних стану каналів.

3. Кожен маршрутизатор надсилає оголошення про стан каналу сусіднім маршрутизаторам, з якими він перебуває у стані суміжності. Маршрутизатор, який отримує повідомлення від сусіднього маршрутизатора,

записує отриману інформацію до своєї бази даних стану каналів і розсилає копію повідомлення всім іншим сусіднім маршрутизаторам.

4. При розсиланні повідомлень всередині однієї OSPF-зони, всі маршрутизатори будують ідентичну базу даних стану каналів.

5. Після побудови бази даних, кожен маршрутизатор використовує алгоритм "найкоротший шлях першим" для обчислення графа без циклів, який відображає найкоротший шлях до кожного відомого пункту призначення, використовуючи себе як корінь. Цей граф є деревом найкоротших шляхів.

6. Кожен маршрутизатор будує таблицю маршрутизації на основі свого дерева найкоротших шляхів.

3.3.4 Налаштування зв'язків між елементам мережі

Почнемо з налаштування серверу в блоці Data Center тому, що він допоможе нам здійснювати керування пристроями реагування та збирати інформацію з датчиків на об'єкті інфраструктури. На рисунку 3.4 показане налаштування IP-адреси серверу та шлюзу для виходу в мережу.

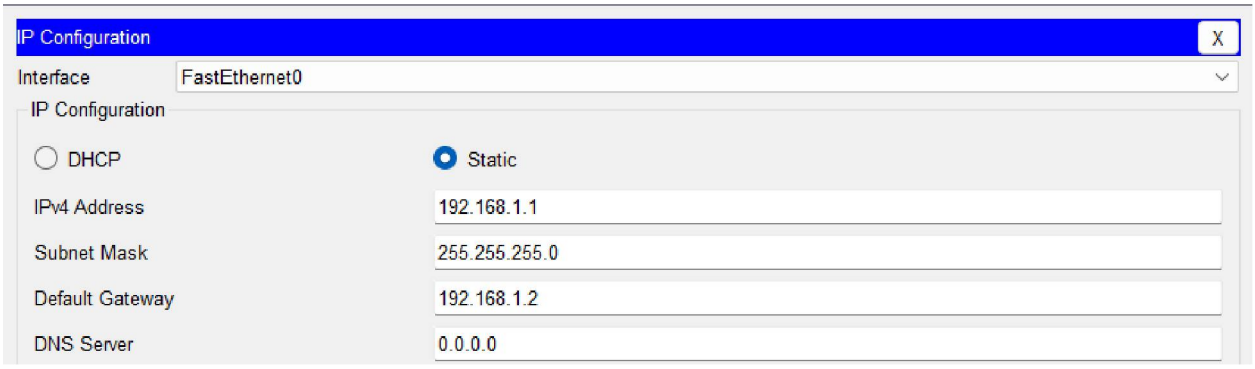

Рисунок 3.4 – Налаштування маски, IP-адреси серверу та шлюзу

Також, для зручної подальшої роботи з пристроями «інтернету речей», налаштуємо DHCP-сервіс, тобто для кожної групи датчиків і пристроїв реагування створимо свій пул адрес, які буде видавати сервер. Налаштування DHCP показано на рисунку 3.5.

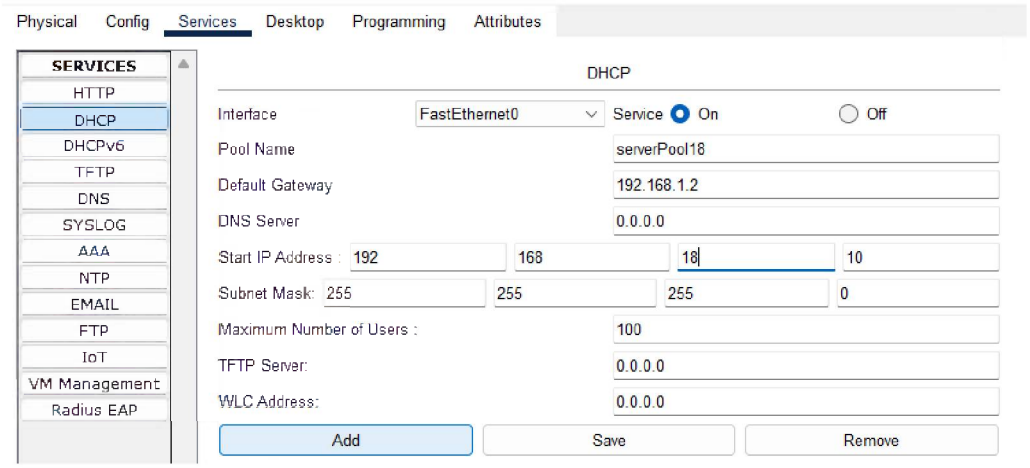

Рисунок 3.5 – Створення пулу адрес для групи датчиків з IP-адресою мережі 192.168.18.0/24.

Для того, щоб сервіс DHCP стабільно функціонував, треба, під час налаштування вузлів мережі, вказати IP-адресу серверу, з використанням команди «ip helper-address», як показано на рисунку 3.3. Після цього сервіс стабільно працює, та має змогу надавати адреси користувачам.

Останнім приготуванням серверу до роботи є увімкнення IoT серверу та створення профілю у ньому.

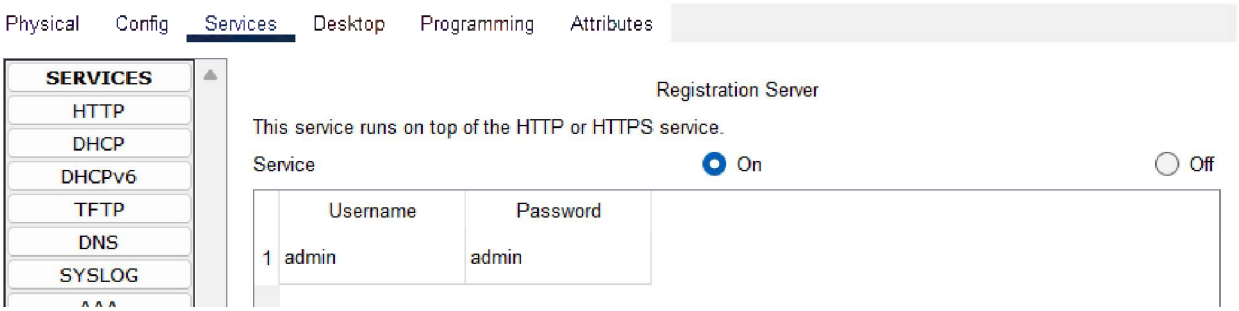

Рисунок 3.6 – Увімкнення серверу «інтернету речей»

Наступним кроком буде підключення датчиків та пристроїв реагування до мережі, це можна зробити (в залежності від датчика) за допомогою комутаторів або бездротових точок доступу. Після чого їх треба підключити до серверу та ввести дані від свого профілю, як це вказано на рисунку 3.7.

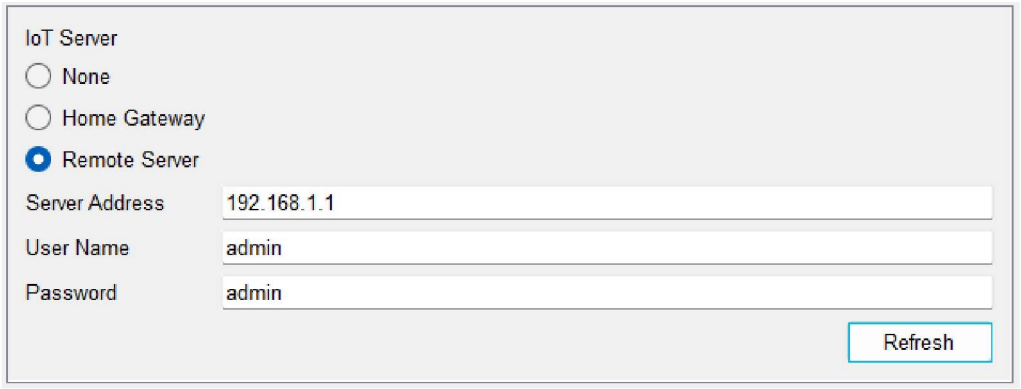

Рисунок 3.7 – Підключення датчику до серверу

Кінцевим етапом є підключення клієнту до серверу та перевірка роботи системи. Для цього через персональний комп'ютер увійдемо в браузер та перейдемо за IP-адресою серверу, де нас зустріне вікно входу до сервісу, як зображено на рисунку 3.8.

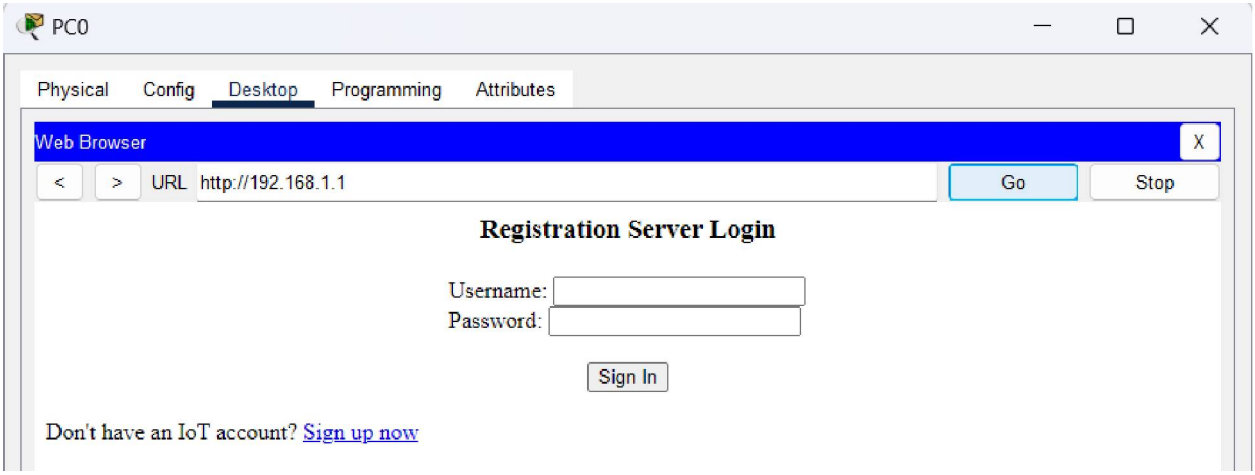

Рисунок 3.8 – Вікно входу на сервер

Достатньо ввести ті дані, які ми застосовували для реєстрації під час створення сервісу та підключення датчиків до мережі.

Після входу до свого профілю, ми можемо побачити усі пристрої, що під'єднанні до нашої мережі. Також сервіс надає нам змогу відслідковувати стан об'єкту інфраструктури за допомогою інформації, наданої датчиками, та роботі відповідних пристроїв реагування. До прикладу, на рисунку 3.9 видно, стан датчику, що може вказувати на наявність протягів, або вітру на об'єкті,

також можна дізнатись температуру, напругу, контролювати роботу вентиляції та інше.

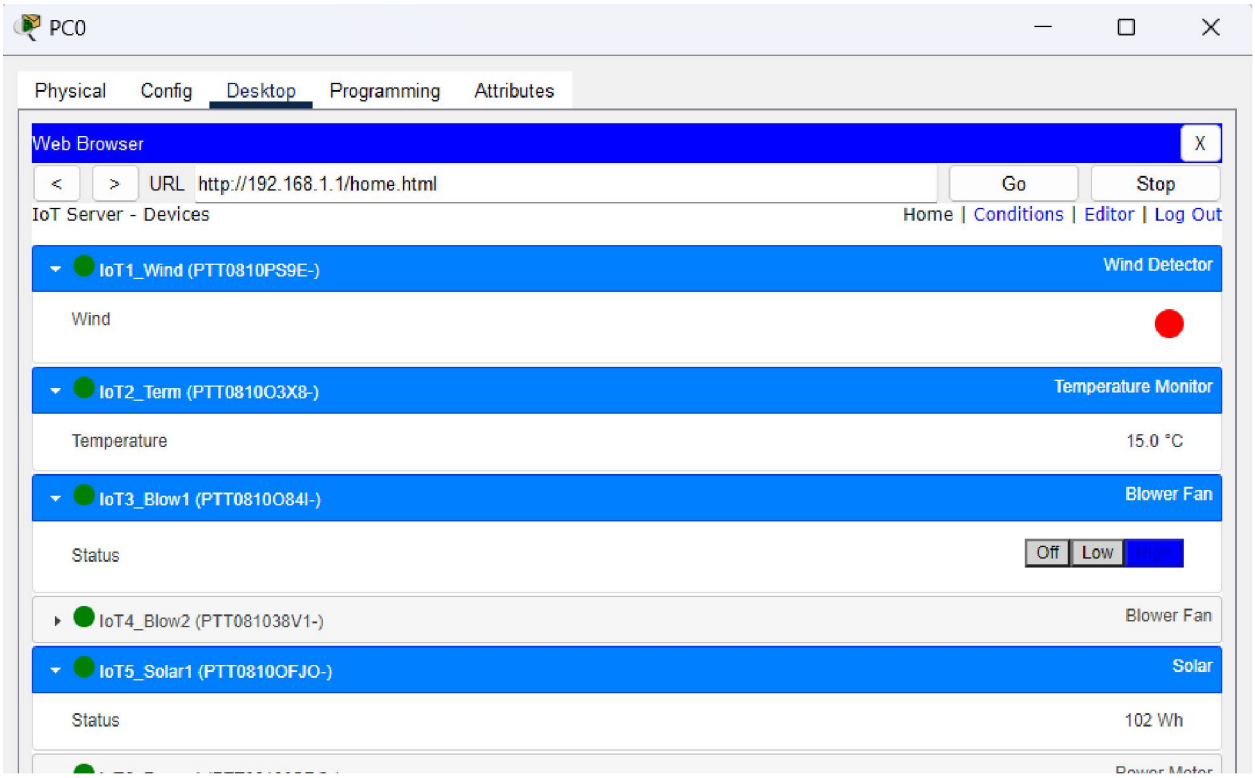

Рисунок 3.9 – Інтерфейс системи контролю стану об’єкту інфраструктури

3.4 Тестування та аналіз роботи моделі

В розділі 3.3 було продемонстровано налаштування та роботу мережі в реальному часі, проте програма Cisco Packet Tracer, для дослідження і тестування роботи окремих елементів мережі, дозволяє нам користуватися режимом симуляції. В цьому режимі ми маємо можливість побачити маршрут кожного окремого пакету, побачити його зміст, та надсилати ICMP-пакети. Таким чином, на рисунку 3.10 можна побачити крокування пакетів в мережі від серверу, до датчиків. В цих пакетах знаходяться команди для датчиків, які містять в собі вимогу надіслати свій поточний стан, для оновлення інформації.

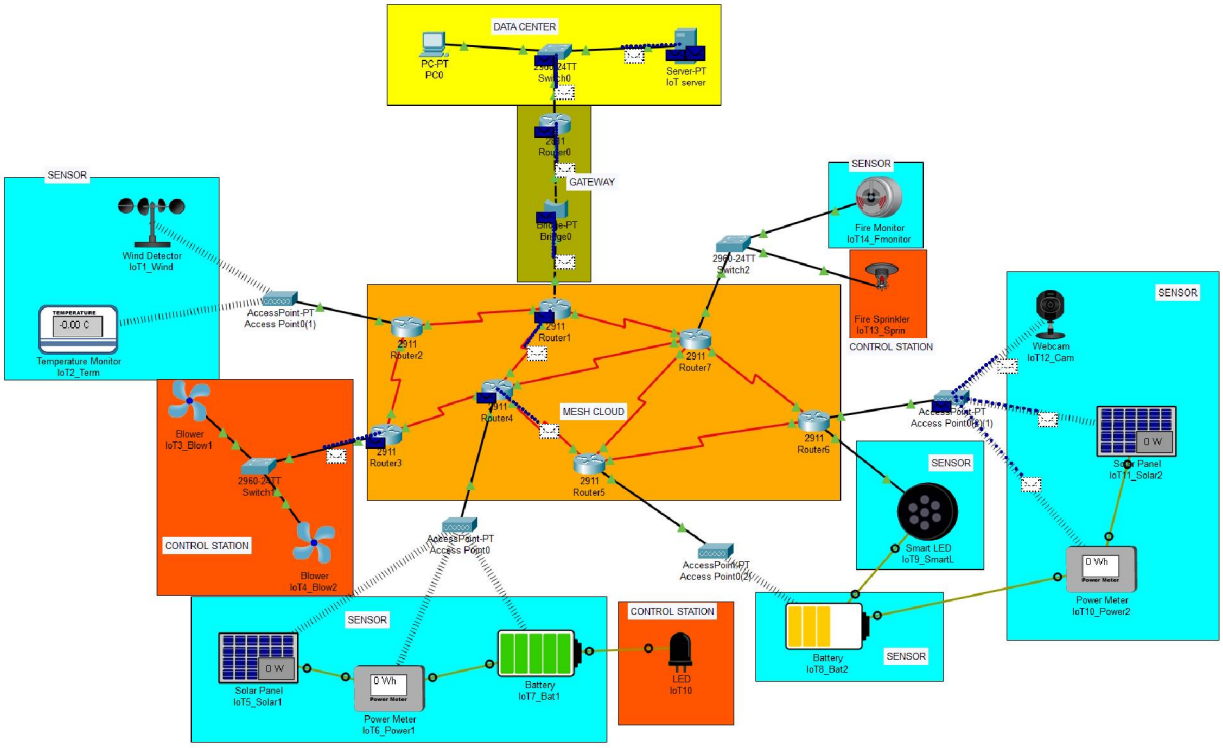

Рисунок 3.10 – Маршрутизація пакетів по мережі

До прикладу, під час подібного оновлення даних, на сервер надійшла інформація про низьку температуру від датчика IoT2_Term на певній ділянці об’єкту, що є замалим показником для правильної роботи устаткування. Тому для запобігання поломки в таких випадках, оператор за допомогою PC0 надсилає команду на промисловий вентилятор IoT3_Blow1 про перехід в режим роботи High. На рисунку 3.11 продемонстровано останній перехід пакету команд від серверу до розумного пристрою.

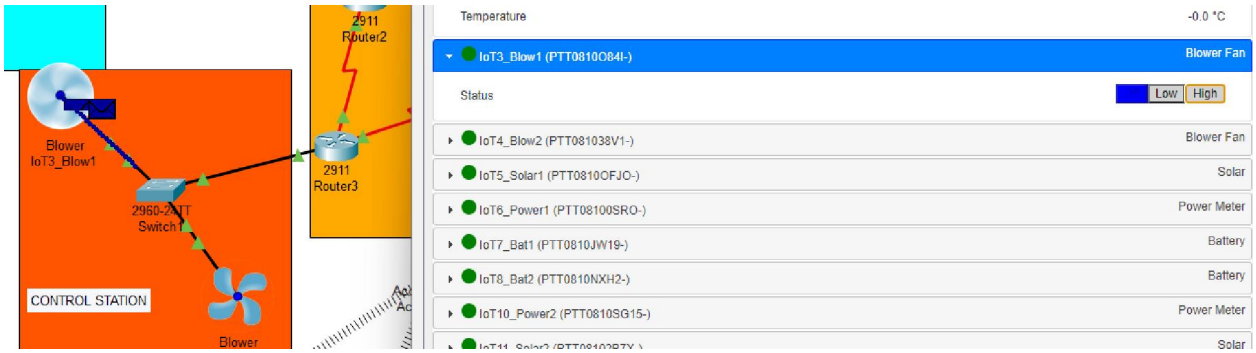

Рисунок 3.11 – Надходження команди від серверу пристрою реагування

Таким чином, було проведено тестування роботи цілої мережі. Також для цього було застосовано тестування ICMP-пакетами. Результати

продемонстровано на рисунку 3.12. Тестування пройдено успішно, модель працює.

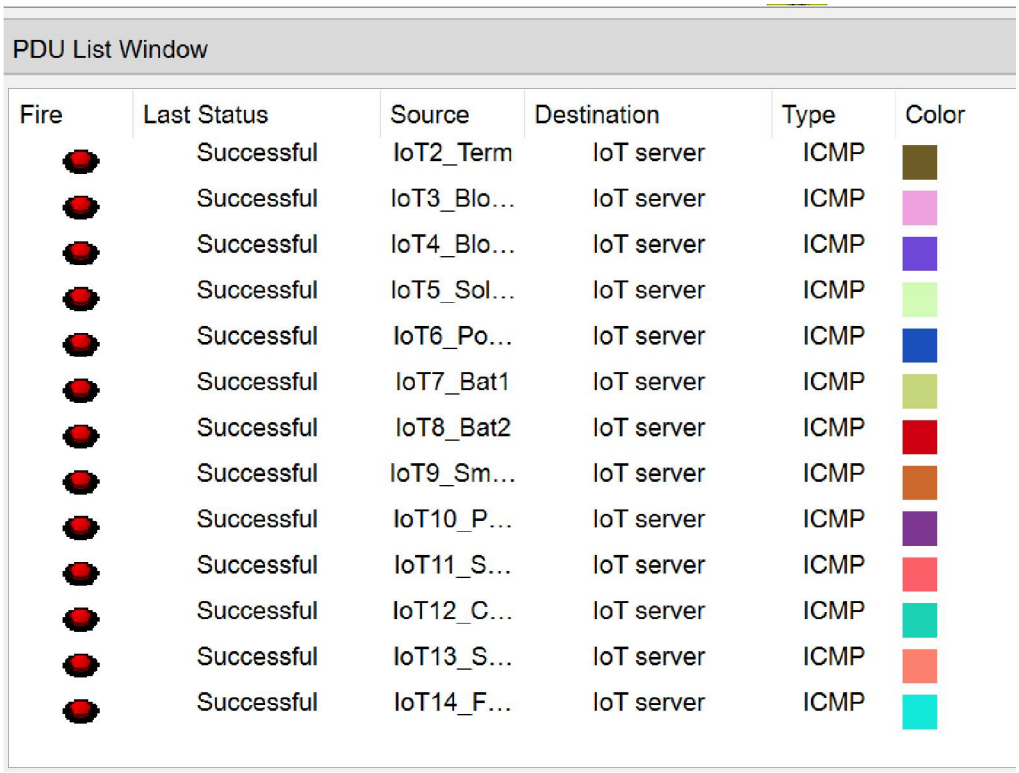

Рисунок 3.12 – Результати проходження ICMP-пакетів

ВИСНОВКИ

У даній дипломній роботі була розроблена модель системи контролю об'єктів інфраструктури з використанням MESH-технологій. Ця модель спроектована для ефективного контролю та управління розподіленою інфраструктурою, в якій використовуються мережі MESH.

Досліджено принципи роботи MESH-технологій та їх переваги у контексті систем контролю об'єктів інфраструктури. MESH-мережі забезпечують високу надійність, автономність та гнучкість, що робить їх ідеальними для застосування в розподілених системах контролю.

У роботі було проведено аналіз вимог до системи контролю об'єктів інфраструктури та розроблено архітектуру моделі. Реалізовано прототип системи контролю на основі запропонованої моделі. Прототип включає в себе MESH-вузли, які забезпечують збір та передачу даних, а також центральну систему контролю для аналізу та керування об'єктом інфраструктури.

Проведено експериментальне дослідження прототипу системи контролю та оцінено його ефективність. Експерименти показали, що використання MESH-технологій у системі контролю об'єктів інфраструктури дозволяє забезпечити стабільний зв'язок та високу швидкість передачі даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. В Україні з'явиться перша «розумна дорога»: стартував пілотний проект. Федерація роботодавців автомобільної галузі [Електронний ресурс]. – режим доступу: URL: https://fra.org.ua/uk/an/publikatsii/novosti/v-ukrayini-z-iavit-sia-piersha-rozumna-dorogha-startuvav-pilotnii-proiekt (дата звернення – 12.05.2023).
2. Дельта для тепловозів – НВО "Дніпротехтранс". НВО "Дніпротехтранс [Електронний ресурс]. – режим доступу: URL: http://dneproteh.com/?page_id=8293 (дата звернення – 05.05.2023).
3. Економічна правда. На “трубі”: репортаж з диспетчерської української ГТС. Економічна правда [Електронний ресурс]. – режим доступу: URL: https://www.epravda.com.ua/publications/2018/03/7/634729/ (дата звернення – 02.05.2023).
4. Застосування технологій геоінформаційних систем для побудови картографічних моделей залізничних сполучень. Open Journal Systems [Електронний ресурс]. – режим доступу: URL: http://journals.nupp.edu.ua/sunz/article/view/2200/1689 (дата звернення – 05.05.2023).
5. Оператор ГТС України впроваджує цифрову систему управління цілісністю магістральних газопроводів. Оператор ГТС України [Електронний ресурс]. – режим доступу: URL: https://tsoua.com/news/ogtsu-vprovadzhue-cyfrovu-systemu-upravlinnya-tsilisnistu-magistralnyh-gazoprovodiv/ (дата звернення – 03.05.2023).
6. Basics of wirelessHART network protocol. Instrumentation and Control Engineering [Електронний ресурс]. – режим доступу: URL: https://automationforum.co/basics-wirelesshart-network/ (дата звернення – 04.05.2023).

7. Hildenbrand J. How Wi-Fi mesh networks work. Android Central [Електронний ресурс]. – режим доступу: URL: https://web.archive.org/web/20180912204710/https://www.androidcentral.com/how-wifi-mesh-networks-work?_ga=2.118951497.1982325821.1494489061-1333092243.1494489050 (дата звернення – 10.05.2023).
8. IEC 62591:2016. IEC Webstore [Електронний ресурс]. – режим доступу: URL: https://webstore.iec.ch/publication/24433 (дата звернення – 03.05.2023).
9. Networking A to Z. Google Books [Електронний ресурс]. – режим доступу: URL: https://books.google.pl/books?id=0qv4KbasX7wC&q=bluetooth&pg=PA45&redir_esc=y#v=snippet&q=bluetooth&f=false (дата звернення – 10.05.2023).
10. Understanding fiber-optic network technology for SCADA. Control Engineering [Електронний ресурс]. – режим доступу: URL: https://www.controleng.com/articles/understanding-fiber-optic-network-technology-for-scada/ (дата звернення – 06.05.2023).
11. What Is SCADA and SCADA System? Fortinet [Електронний ресурс]. – режим доступу: URL: https://www.fortinet.com/resources/cyberglossary/scada-and-scada-systems (дата звернення – 06.05.2023).
12. Wi-Fi Generation Numbering. Electronics Notes: reference site for electronics, radio & wireless [Електронний ресурс]. – режим доступу: URL: https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/wifi-alliance-generations-designations-numbers.php (дата звернення – 11.05.2023).
13. Wireless ATM and Ad-Hoc Networks. Google Books [Електронний ресурс]. – режим доступу: URL: https://books.google.pl/books?id=0hMfAQAAIAAJ&redir_esc=y (дата звернення – 07.05.2023).

14. Wireless mesh networks: Everything you need to know. PCWorld [Електронний ресурс]. – режим доступу: URL: https://www.pcworld.com/article/407165/mesh-network-explained.html (дата звернення – 10.05.2023).
15. ZigBee Smart Energy Overview. Wayback Machine [Електронний ресурс]. – режим доступу: URL: https://web.archive.org/web/20110315083259/http://zigbee.org/Standards/ZigBeeSmartEnergy/Overview.aspx (дата звернення – 10.05.2023).

ДОДАТКИ

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В. Н. Каразіна

Факультет комп'ютерних наук
Кафедра теоретичної та прикладної системотехніки
Рівень вищої освіти (освітньо-кваліфікаційний рівень) бакалавр
Галузь знань: 15 – Автоматизація та приладобудування
Спеціальність: 151 «Автоматизація та комп'ютерно-інтегровані технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри теоретичної
та прикладної системотехніки
_____ д.т.н., проф. Шматков С. І.

«17»листопада 2022 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Черкасова Андрія Івановича

1. Тема роботи «**Модель системи контролю стану об'єктів інфраструктури з використанням MESH-технологій**»,
керівник роботи Артюх Олексій Анатолійович, старший викладач кафедри теоретичної та прикладної системотехніки

затверджені наказом по університету від «23» травня 2023 року № 4101-5/895

2. Строк подання студентом роботи 26 травня 2023

3. Перелік питань, які потрібно розробити
1. Аналіз існуючих систем контролю стану інфраструктури.
2. Аналіз популярних технологій побудови мереж.
3. Вивчення технологій побудови mesh-мереж.
4. Вибір програмного забезпечення для симуляції мережі.
5. Аналоги додатку.
6. Розробка моделі з застосуванням UML-діаграм.
7. Розробка mesh-мережі в середовищі симуляції мережі.

4. План роботи

№ з/п	Назви етапів роботи	Термін виконання етапів роботи
1	Аналіз та пошук методичної літератури	Листопад - Грудень 2022
2	Вивчення технологій MESH	Січень – Лютий 2023
3	Аналіз та розробка моделі	Березень 2023
4	Пошук засобів симуляції мережі	Березень 2023
5	Побудова мережі	Квітень 2023
6	Налагодження роботи мережі	Квітень 2023
7	Оформлення пояснювальної записки	Квітень 2023- Травень 2023
8	Перед захист кваліфікаційної роботи	Травень 2023
9	Представлення кваліфікаційної роботи керівнику та рецензенту	Червень 2023

5. Дата видачі завдання 19 жовтня 2022

Студент Черкасов А. І.
ініціали, прізвище
підпис

Керівник роботи Артюх О. А.
ініціали, прізвище
підпис

Додаток Б

Затверджую

_____

«_____»_____2023 р.

Технічне завдання
на розробку програмного виробу «МОДЕЛЬ СИСТЕМИ КОНТРОЛЮ СТАНУ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯМ MESH-ТЕХНОЛОГІЇ»

1.	Введення	1.1. Назва: Модель системи контролю стану об'єктів інфраструктури з використанням MESH-технології. 1.2. Галузь застосування: системи контролю.
2.	Підстава для розробки	2.1. Навчальний план за спеціальністю 151 – Автоматизація та комп'ютерно-інтегровані технології 2.2. Завдання на кваліфікаційну роботу бакалавра № _4101-5/895_ від «_23_» ___травня__2023 (представити як Додаток А до пояснювальної записки до кваліфікаційної роботи).
3.	Призначення розробки	3.1. Мета розробки: розробка моделі системи контролю за об'єктом інфраструктури з використанням MESH-мережі. 3.2. Призначення розробки надає можливість визначати найбільш інформативні параметри стану керованих чи діагностованих систем з метою підвищення швидкості прийняття рішень, зменшення комплекту датчиків для моніторингу стану та підвищення точності діагностування. 3.3. Вихідні дані розробки: статистичні експериментальні дані (з галузі систем контролю).
4.	Технічні вимоги до програмного виробу	4.1. Вимоги до функціональних характеристик: немає. 4.2. Вимоги до надійності: стійкий зв'язок між пристроями, постійний обмін інформацією, надійність передачі даних. 4.3.Вимоги до умов експлуатації: немає. 4.4. Вимоги до складу і параметрів технічних засобів: роутери, маршрутизатори з підтримкою MESH-технологій. 4.5. Вимоги до інформаційної та програмної сумісності: немає. 4.6. Вимоги до маркування та упаковки: немає. 4.7. Вимоги до транспортування і зберігання: немає. 4.8. Спеціальні вимоги: немає.

<table>
<tr><td>5.</td><td>Вимоги до програмної документації</td><td colspan="2">Програмною документацією до виробу «МОДЕЛЬ СІСТЕМІ КОНТРОЛЮ СТАНУ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ З ВІКОРИСТАННЯМ MESH-ТЕХНОЛОГІЇ» вважати:
1) Справжнє Технічне завдання на розробку виробу (представити у вигляді Додатку Б до пояснювальної записки до кваліфікаційної роботи).
2) Методику проектування та налаштування мереж (у вигляді глав 3.3 та 3.4 пояснювальної записки до кваліфікаційної роботи).
3) Опис виробу (представити в розділі 3 пояснювальної записки до кваліфікаційної роботи).</td></tr>
<tr><td>6.</td><td>Вимоги до техніко-економічних показників</td><td colspan="2">Програмною документацією до виробу «МОДЕЛЬ СІСТЕМІ КОНТРОЛЮ СТАНУ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ З ВІКОРИСТАННЯМ MESH-ТЕХНОЛОГІЇ» вважати:
1) Справжнє Технічне завдання на розробку виробу (представити у вигляді Додатку Б до пояснювальної записки до кваліфікаційної роботи).
2) Методику розрахунку інформативності змінних стану (у вигляді глав 3.3 та 3.4 пояснювальної записки до кваліфікаційної роботи).
3) Опис виробу (представити в розділі 3 пояснювальної записки до кваліфікаційної роботи).</td></tr>
<tr><td rowspan="4">7.</td><td rowspan="4">Стадії і етапи розробки</td><td>Дата</td><td>Назва етапу</td></tr>
<tr><td>від 15 лютого 2023
до 15 березня 2023</td><td>Аналіз практики предметної області.</td></tr>
<tr><td>від 16 березня 2023
до 16 квітня 2022</td><td>Аналіз існуючого науково-методичного апарату систем контролю за об'єктами інфраструктури.</td></tr>
<tr><td>від 15 березня 2023
до 2 квітня 2023</td><td>Аналіз існуючого програмного забезпечення симуляції мереж.</td></tr>
<tr><td></td><td></td><td>від 3 січня 2023
до 30 березня 2023</td><td>Розробка (доопрацювання) моделі системи контролю стану об'єктів інфраструктури в середовищі симуляції мереж</td></tr>
</table>

		від 11 лютого 2023 до 27 травня 2023 від 31 березня 2023 до 27 квітня 2023 від 1 травня 2023 до 28 травня 2023 30 травня 2023	Розробка (доопрацювання) моделі системи контролю стану об'єкта або об'єктів інфраструктури. Налагодження роботи мережі в програмі симуляції. Оформлення результатів. Написання пояснювальної записки. Представлення кваліфікаційного проєкту керівнику кваліфікаційної роботи та рецензенту.
8.	Порядок контролю і приймання програмного продукту (моделі)	1. Перевірку ходу розробки програми виконувати раз в 3 тижні. 2. Захист розробленої моделі провести на засіданні Атестаційної комісії. 3. Пояснювальну записку подати в електронному вигляді в 1 примірнику.	

Виконавець
студент групи КУ- 41
ЧЕРКАСОВ А. І.

Замовник
старший викладач
АРТЮХ О. А

Додаток В

Програма і методика випробувань програмного виробу

МОДЕЛЬ СИСТЕМИ КОНТРОЛЮ СТАНУ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯМ MESH-ТЕХНОЛОГІЙ

1 Об'єкт випробувань

1. Назва програмного виробу : «Модель мережі системи контролю стану об'єктів інфраструктури»
2. Галузь застосування : модернізація/створення систем контролю
3. Перераховані відомості запозичуються з відповідних розділів Технічного завдання.

2. Мета випробувань

Перевірка відповідності функціональності моделі системи заявленим функціональним можливостям в технічному завданні (Додаток Б до пояснювальної записки до кваліфікаційної роботи).

3. Загальні положення

1. Підстави для проведення випробувань

Підставою для проведення випробувань є наказ про призначення атестаційної комісії.

2. Місце і тривалість випробувань

Приймальні (приймально-здавальні) випробування проводяться на базі комп'ютерного класу кафедри в період роботи атестаційної комісії.

3. Обсяг випробувань

Приймальні випробування програмного виробу проводяться в обсязі відповідному цієї програми і методики випробувань.

4. Організації, які беруть участь у випробуваннях

Приймальні випробування проводяться атестаційною комісією напередодні засідання (або в процесі засідання) за участю Замовника, Виконавця та інших осіб, присутніх на засіданні.

4. Вимоги до програми або програмного виробу

Модель повинна задовольняти наступним вимогам:

1. вимоги до надійності;
2. сумісність з іншими системами контролю;
3. легкість масштабування мережі;
4. вимоги до складу і параметрів технічних засобів:

Система контролю повинна включати в свій склад:

1. Датчики та сенсори.
2. Мережу передачі інформації.
3. Пристрої реагування.
4. Центр збору інформації, її обробки та прийняття рішень.

5. вимоги до маркування та упаковки (не висуваються);
6. вимоги до транспортування і зберігання (не висуваються).

Спеціальні вимоги (не пред'являються).

5. Вимоги до програмної документації

Програмною документацією щодо розроблюваної моделі системи контролю вважати:

1. справжнє технічне завдання на розробку моделі (представити як Додаток Б до пояснювальної записки до кваліфікаційної роботи);
2. Програму і методику випробувань розробленої моделі (представити як Додаток В до пояснювальної записки до кваліфікаційної роботи);
3. рекомендацій щодо застосування створеної моделі у проєктах (представити в Розділі 3 пояснювальної записки до кваліфікаційної роботи).

6. Засоби і порядок випробувань

6.1 Засоби випробувань

Для проведення випробувань необхідне програмне забезпечення для симуляції роботи мереж Cisco Paket Tracer останньої версії.

6.2 Порядок проведення випробувань

Як правило, випробування проводяться в два етапи:
-ознайомчий (1-й етап);
-випробування моделі мережі (2-й етап).
Перелік перевірок, що проводяться на 1 етапі випробувань, включає в себе:

1. Перевірку цілісності файлу
2. Перевірка відповідності мережі до описаної в роботі.

Перелік перевірок, що проводяться на 2 етапі випробувань, включає в себе:

1. Запуск проекту в режимі симуляції
2. Перевірка з'єднання між елементами мережі за допомогою вбудованого інтерфейсу симулятора роботи серверу.
3. Надсилання пакетів ICMP

Для проведення випробувань пропонується тест 1, тест 2 та тест 3.

Тест 1

1. Перевірка функціонування мережі;
2. Отримання відповіді серверу про успішне з'єднання з пристроями.

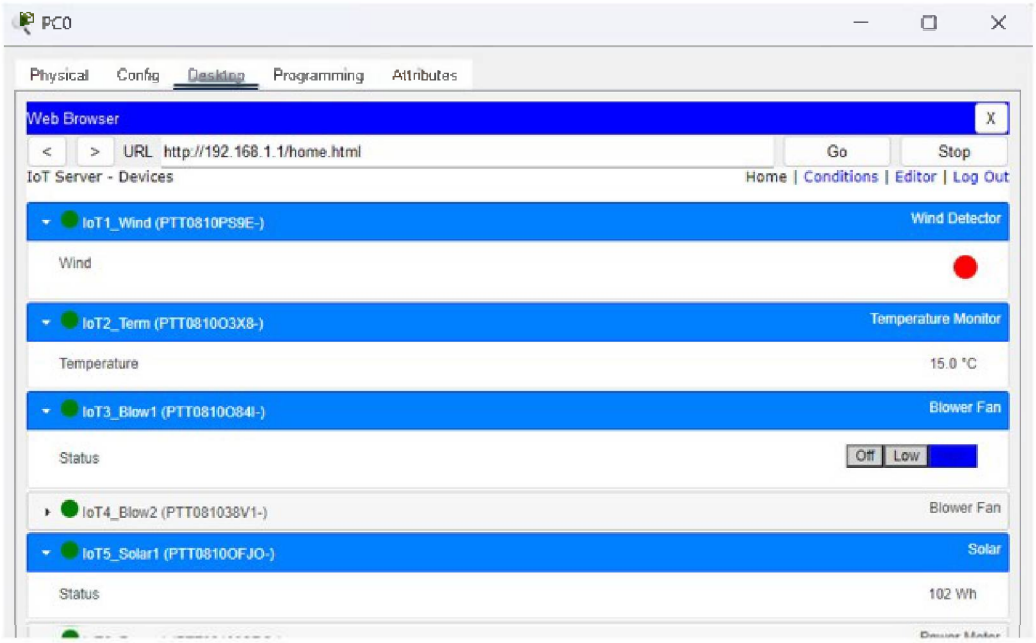

Рис. В.1 Тест 1

Тест 2

1. Перевірка надсилання даних на пристрої реагування на об'єкті

Рис. В.2 Тест 2

Висновки: тест 1 успішно пройшов випробування, тест 2 успішно пройшов випробування. Випробування пройшло успішно.

Виконавець: студент групи КУ-41, Черкасов А. І.