Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра мережевих та інтернет технологій

ЗАТВЕРДЖУЮ
завідувач кафедри
мережевих та інтернет технологій
_____ Ю.В. Кравченко
«_____»_____2021 року

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

галузі знань 17 «Електроніка та телекомунікації»
за спеціальністю 172 «Телекомунікації та радіотехніка»

на тему:

Дослідження систем визначення надзвичайних ситуацій на основі сенсорних мереж

Виконала: студентка групи МІТ -41

Покутня Дар'я Олександрівна _____
(прізвище ім'я по-батькові) (підпис)

Керівник: доцент кафедри мережевих та інтернет технологій

к.т.н. **Дуднік А.С.** _____
(посада, прізвище ім'я по-батькові) (підпис)

Київ 2021

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра мережевих та інтернет технологій

ЗАТВЕРДЖУЮ
завідувач кафедри
мережевих та інтернет технологій

_____Ю.В.Кравченко

«_____»_____2021 року

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Здобувачу вищої освіти **Покутня Дар'я Олександрівна**
(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження систем визначення надзвичайних ситуацій на основі сенсорних мереж затверджена на засіданні кафедри МІТ
«___»_____20___р. протокол №____
2. Термін здачі закінченої роботи «30» травня 2021 р.
3. Вихідні дані до проекту (роботи)
Програма моделювання мереж – Cisco Packet Tracer
4. Зміст пояснювальної записки (перелік питань, що їх потрібно розробити, обсяг – 35-40 стор.)
Обґрунтування потреби дослідження систем визначення надзвичайних ситуацій
Дослідити принципи побудови, експлуатації та використання сенсорних мереж
Розробити системи розумних пристроїв на основі сенсорних датчиків
5. Перелік графічного матеріалу, слайдів

Дата видачі завдання _____

Керівник роботи _____ к.т.н., доцент кафедри МІТ
(підпис) (посада, прізвище, ім'я, по батькові)
Дуднік А.С

Завдання прийняла до виконання _____ Покутня Дар'я Олександрівна

КАЛЕНДАРНИЙ ПЛАН ВИКОНАННЯ РОБОТИ

Номер	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Підготовчий	20.01.2021	
2	Розділ 1	01.03.2021	
3	Розділ 2	01.04.2021	
4	Розділ 3	01.05.2021	
5	Доповідь та слайди	27.05.2021	
6	Пояснювальна записка	30.05.2021	

Здобувач вищої освіти Покутня Дар’я Олександрівна

Керівник Дуднік Андрій Сергійович

РЕФЕРАТ

Пояснювальна записка: 75 с., 21 рис., 4 табл., 21 джерело.

Об’єкт дослідження: системи визначення надзвичайних ситуацій на основі сенсорних мереж

Предмет дослідження: процес проектування бездротових сенсорних мереж за допомогою Cisco Packet Tracer

Мета роботи: дослідження бездротових сенсорних мереж, принципи побудови, роботи.

Методи дослідження: системний підхід, порівняльний аналіз, статистичний аналіз, аналітичний аналіз, моделювання сеснорних мереж.

У ході роботи було проведено аналіз основних принципів виявлення раннього виявлення надзвичайних ситуацій.

Обґрунтовано переваги вибору технологій сенсорних мереж у сучасному середовищі.

Був проведений аналіз основних технологічних рис безпроводових сенсорних мереж: протоколи передачі даних, архітектура сенсорних вузлів, структура сенсорної мережі.

В даній роботі представлена взаємодія бездротових сенсорних мереж з мережами зв’язку загального призначення, створеної на базі різних стандартів, протоколів і технологій, таких як: ZigBee, 6loWPAN, DigiMesh стандарту IEEE 802.15.4: Bluetooth стандарту IEEE 802.15.1, WiFi стандарту IEEE 802.11

Дипломна робота включає Проведення досліджень впливу лісової рослиннності, а також полум'я на особливості розповсюдження, в даних середовищах, радіохвиль стандарту IEEE 802.11 в частотному діапазоні 2,4 ГГц.

Практична частина даної роботи розроблена за допомогою програми Cisco Packet Tracer, були змодельовані наступні схеми використання сенсорних датчиків:

- Установка детектора руху та камери спостереження з використанням віддаленого сервера та мережевого комутатора за допомогою безпровідного підключення
- З’єднання детектора диму, сирени та воріт у випадку надзвичайної ситуації, можливість слідкування за ситуацією за допомогою смартфона
- Установка пожежного спринклеру, детектора диму та пожежі за допомогою мікроконтролера, запрограмованого мовою Python
- Розробка IoE проекту з’єднань Інтернет-провайдера, клієнтів для модему та 3G/4G

Результати здійснених у дипломній роботі досліджень можуть бути використані у сфері проектування приватних та корпоративних об’єктів з метою покращення збору інформації про навколишнє середовище, запобігання виникнення надзвичайних ситуацій та усунення їх наслідків.

Ключові слова: БЕЗДРОТОВА СЕНСОРНА МЕРЕЖА,НАДЗВИЧАЙНА СИТУАЦІЯ, IEEE 802.11, IEEE 802.15.1, IEEE 802.15.4, WI-FI, ZIGBEE, BLUETOOTH

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IoT	Internet of Things
MCU	Microcontroller Unit
PC	Personal computer
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol
DNS	Domain Name System
БСМ	Wireless Sensor Network
DSN	Data Sourse Name
NASA	National Aeronautics and Space Administration
Wi-Fi	Wireless Fidelity
MAC	Media Access Control Layer
OSI	Open Systems Interconnection Model
PDR	Packet Delivery Radio
TDMA	Time Division Multiple Access
PHY	Physical Layer
WPAN	Wireless Personal Area Network
LRWPAN	Low-Rate Wireless Personal Area Network
BPSK	Binary Phase Shift Keying
O-QPSK	Offset quadrature phase-shift keying
FFD	Fully Function Device
RFD	Reduced Function Device
PAN	Personal Area Network
FDD	Frequency Division Duplex
AES	Advanced Encryption Standard
EEPROM	Electrically Erasable Programmable Read-Only Memory
CSMA	Carrier Sense Multiple Access
AODV	Ad-hoc On Demand Distance Vector

GPRS General Packet Radio Service

PWRP Predictive Wireless Routing Protocol

DSR Dynamic Source Routing

OLSR Optimized Link State Routing protocol

TORA Temporally-Ordered Routing Algorithm

HSLS Hazy-Sighted Link State

MANET Mobile Ad hoc Network

RPL Recognition of prior learning

DODAG Destination Oriented DirectedAcyclic Graph

MTR Multi-topology routing

USB Universal Serial Bus

QoS Quality of Service

API Application Programming Interface

ERIS

MDT

PDA

ВСТУП

Катастрофи, такі як пожежі, повені, землетруси, громадянська війна або теракти, можуть спричинити надзвичайне становище.

Незалежно від походження, кризові ситуації часто супроводжуються невизначеністю розвитку катастрофи, низькими темпами операцій реагування, серйозними людськими жертвами і матеріальними збитками, якщо не відреагувати належним чином.

Обізнаність та підтримка в прийнятті рішень є важливими чинниками мінімізації збитків і травм, а також своєчасного рятунку людських життів. Задля забезпечення належної ситуативної обізнаності і підтримки прийняття рішень для врегулювання кризових ситуацій, дослідники закликали приділяти увагу розробці заходів реагування, а саме інформаційним системам реагування на надзвичайні ситуації (ERIS).

Вони корисні в першу чергу відповідальним за усунення надзвичайних ситауцій шляхом підвищення їх ситуативної обізнаності, що призведе до кращого прийняття рішень. Стверджується, що людський фактор під час таких інцидентів, як Бхопал, загибель пожежників протягом 9.11 і Трьохмильна Острівна Ядерна Криза були викликані провалом ситуативної обізнаності і відсутністю підтримки в прийнятті рішень.

На відміну від інформаційних систем для офісного використання, інформаційні системи реагування на надзвичайні ситуації можуть працювати в екстремальному і напруженому середовищі, потрібна не тільки статична інформація, така як дорожні карти і плани поверхів будівель, але і динамічна інформація та інформація в реальному часі, наприклад інформація про останню аварію події, нинішнє місцезнаходження персоналу і ресурсів у надзвичайних ситуаціях. По мірі розвинення надзвичайної ситуації, вимоги (як інформаційні, так і логістичні) можуть змінитися, що призведе до обов’язкової зміни робочого процесу. Дослідження миттєвого реагування відповідальних у Голландському

випадку екстреного реагування показало, що більша частина на запит даних під час кризи може розглядатися як динамічна інформація і має бути відображена миттєво.

Крім того, бажана платформа ERIS складається з декількох мобільних терміналів передачі даних (MDT) і багатьох портативних пристроїв, таких як мобільні телефони, iPad, персональні цифрові пристрої (PDA), у співпраці з одним або кількома великомасштабними комп'ютерними серверними системами, розташованими у фіксованому місці. Ці особливості є бажаними для ERIS та повинні бути глобальними і розподіленими інформаційними системами з можливістю збору даних в реальному часі, обробкою, обміном і аналізом інформації.

Наскільки відомо, існує мало великомасштабних ERIS у використанні. Насправді, багато складних питань мають бути розглянуті та вирішені, такі як технічні, організаційні, людські фактори, до того, як бажані ERIS отримають широке визнання. Цей дипломний проект стосується дослідження інфраструктури бажаних ERIS шляхом впровадження технології Інтернет Речей (IoT) в галузі управління надзвичайними ситуаціями і досліджує відповідність вимогам технологічного обладнання.

1 ОБҐРУНТУВАННЯ ПОТРЕБИ ДОСЛІДЖЕННЯ СИСТЕМ ВИЗНАЧЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ

1.1 Важливість та основні принципи раннього виявлення надзвичайних ситуацій

Коли трапляється надзвичайна ситуація, часто виникають розгубленість і паніка, складність в комунікації, затримка реагування та збитки. Перші декілька хвилин надзвичайної ситуації мають вирішальне значення для визначення результатів, тому обов’язково, щоб особи, які реагують як на саме місце надзвичайної ситуації, так і поза ним, знали, що відбувається, де це відбувається і що з цим робити на основі ретельно розроблених планів надзвичайних ситуацій. Правильна інформація повинна надходити до потрібних людей на потрібних пристроях, щоб можна було вжити правильних заходів для захисту безпеки життя. Саме в таких випадках необхідно враховувати ситуативну обізнаність в першу чергу на основі технологічної бази.

Сьогодні ситуативна обізнаність стосується інформації в режимі реального часу того, що відбувається в певному середовищі та навколо нього. Такі знання можливі завдяки інтеграції різних систем сигналізації та зв'язку для централізованого моніторингу, оповіщення та звітування. Будь-яка загроза або відхилення від нормальної роботи вимагає, щоб особи, що реагують як на місце, так і за межами майданчика, мали обізнаність про ситуацію, щойно відбулася ініціююча подія.

В даний час існує великий асортимент датчиків, які дозволяють отримувати дані з незліченних джерел. Більше того, розгортання бездротових сенсорних мереж (БСМ) дозволяє збирати та передавати дані з датчиків, розташованих на масштабних площах та навіть по всьому світу.

У світі безліч широкодоступних пристроїв транслювання інформації, тому важливо використовувати їх усі для доставки інформації під час надзвичайних ситуацій - особливо на персональні екрани, які більшість із нас постійно використовує або тримає поруч. Сповіщення можна надсилати на будь-який смартфон, але тепер ці пристрої можна перетворити на мобільні командно-адміністративні центри для безперебійного усвідомлення ситуації на ходу. Користувачі можуть швидше реагувати на ситуації, що розгортаються, ефективніше ініціювати попередження та відповідні плани реагування, а також ескалювати/повідомляти інших за потреби - все з одного інтерфейсу користувача. Вони також мають можливість переглядати відео в реальному часі з інтегрованих камер безпеки, а також переглядати попередньо записані відео, плани поверхів та фотографії за допомогою функції, що називається відео-пейджингом. Коли покриття Wi-Fi слабшає, пристрій автоматично перемикається на стільниковий зв’язок для безперебійного попередження як про приміщення, так і за його межі.

Нижче наведено кілька прикладів того, як технологію поінформованості про ситуацію за допомогою сенсорних мереж можна використовувати для інтегрованого управління сигналізацією та автоматичних повідомлень:

- Виклик медичної сестри, розумне ліжко, інтеграція телеметрії;
- Фіксована або мобільна примусова робота в адміністративних офісах, місцях обробки готівки та аптеках;
- Мобільний примус для вчителів, персоналу та студентів з особливими потребами (об'єкти знущання, ті, хто постраждав або має хронічні захворювання, такі як харчова алергія);
- Відстеження активів (наприклад, медичні візки, насоси IV, стрічкові інструменти, комп’ютери тощо);
- Моніторинг/реєстрація температури для медичних холодильників та зберігання продуктів;

- Моніторинг навколишнього середовища на наявність води/вологості, диму, небезпечних речовин тощо, а також датчики для генераторів, котлів, водяних насосів тощо;
- Інтеграція пожежної панелі;
- Сигналізація контактів дверей/вікна та інтеграція з контролем доступу/вторгненням та виявленням руху;
- Інтеграція з внутрішніми та зовнішніми камерами безпеки;
- Детектори розбиття скла та звукові датчики (наприклад, постріли);
- Попередження про погоду;
- Повідомлення про евакуацію та блокування;

Сповіщення повинні надходити в режимі реального часу до кількох груп за кількома каналами - від телефонних дзвінків та текстових повідомлень до електронних листів та повідомлень. Подібне масове сповіщення такого роду забезпечує надмірність, що є критично важливим для безпеки життя.

1.1.2 Класифікація сенсорних мереж відповідно до характеру їх використання

Наразі використовуються різні програми БСМ, як провірені, так і ті, що все ще перебувають на стадії розвитку. Загалом програми БСМ класифікуються відповідно до характеру їх використання на шість основних категорій, як проілюстровано на Рисунку 1.1 , а саме: військові, охорона здоров'я, екологія, флора і фауна, промислові та міські. У кожній категорії розглядаються різні підкатегорії.

Рисунок 1.1 - Огляд найпопулярніших категорій програм БСМ

1.1.3 Підкатегорії застосування бездротових сенсорних мереж та їх огляд

– Наземні БСМ.

Наземні БСМ здатні ефективно зв'язуватися з базовими станціями складаються з сотень або тисяч вузлів бездротових датчиків, розгорнутих неструктурованих (спеціальним) або структурованим (попередньо запланованим) способом. У неструктурованому режимі вузли датчика випадковим чином розподіляються в межах цільової області, яка випадає з фіксованою площиною. Попередньо запланований або структурований режим враховує оптимальне розміщення, розміщення сітки і 2D, 3D моделі розміщення.

У цій БСМ ємність акумулятора обмежена, проте батарея оснащена сонячними елементами як вторинне джерело харчування. Енергозбереження цих БСМ досягається за рахунок використання операцій з низьким робочим циклом, мінімізації затримок, оптимальної маршрутизації і так далі.

– Підземні БСМ.

Підземні бездротові сенсорні мережі дорожче наземних з точки зору розгортання, обслуговування, вартості обладнання та ретельного планування. Мережі БСМ складаються з декількох сенсорних вузлів, які приховані в землі для моніторингу підземних умов. Для передачі інформації від вузлів датчиків до

базової станції додаткові вузли приймача розташовані над землею. Підземні бездротові сенсорні мережі, розгорнуті в землі, важко перезарядити. Акумуляторні вузли датчика, оснащені обмеженим зарядом акумулятора, складно перезарядити. На додаток до цього підземне середовище робить бездротовий зв'язок ненадійним через високий рівень згасання і втрати сигналу.

– Підводні БСМ.

Понад 70% Землі зайнято водою. Ці мережі складаються з ряду сенсорних вузлів і транспортних засобів, розгорнутих під водою. Автономні підводні апарати використовуються для збору даних з цих сенсорних вузлів. Проблемою підводного зв'язку є тривала затримка поширення, а також пропускна здатність і відмова датчиків. Підводні БСМ оснащені обмеженим акумулятором, який не можна заряджати або замінювати. Проблема енергозбереження для підводних мереж БСМ включає розробку методів підводного зв'язку і мереж.

– Мультимедійні БСМ.

Бездротові сенсорні мережі Muttimedia були запропоновані для відстеження та моніторингу подій у вигляді мультимедіа, таких як зображення, відео та аудіо. Ці мережі складаються з недорогих сенсорних вузлів, обладнаних мікрофонами і камерами. Ці вузли пов'язані один з одним по бездротовому з'єднанню для стиснення даних, пошуку та кореляції даних. Проблеми з мультимедійним БСМ включають в себе високе енергоспоживання, високі вимоги до пропускної здатності, методи обробки даних і стиснення. На додаток до цього, мультимедійний контент вимагає високої пропускної здатності, щоб контент доставлявся правильно і швидко.

– Мобільні БСМ.

Ці мережі складаються з набору сенсорних вузлів, які можуть переміщатися самостійно і можуть взаємодіяти з фізичним середовищем.

Мобільні вузли мають можливість обчислювати дан і спілкуватися. Мобільні бездротові сенсорні мережі набагато більш універсальні, ніж статичні сенсорні мережі. Переваги БСМ в порівнянні зі статичними бездротовими сенсорними

мережами включають поліпшене покриття, кращу енергоефективність, чудову пропускну здатність каналу і т.д.

– Навколишнє середовище/Зондування Землі

Існує безліч програм для моніторингу параметрів навколишнього середовища. Вони поділяють додаткові проблеми суворих умов і зниження енергоспоживання.

– Моніторинг забруднення повітря

Бездротові сенсорні мережі були розгорнуті в декількох містах (Стокгольм, Лондоні Брісбен) для моніторингу концентрації небезпечних газів для громадян. Вони можуть використовувати переваги спеціальних бездротових ліній зв'язку, а не дротових установок, що також робить їх більш мобільними для тестування показань в різних областях.

– Виявлення лісових пожеж

Мережа сенсорних вузлів може бути встановлена в лісі, щоб визначати, коли почалася пожежа. Вузли можуть бути оснащені датчиками для вимірювання температури, вологості і газів, які утворюються в результаті пожежі на деревах або в рослинності.

Раннє виявлення має вирішальне значення для успішної дії пожежних завдяки бездротовим сенсорним мереж пожежна команда зможе дізнатися, коли почалася пожежа і як він поширюється.

– Виявлення зсуву

Система виявлення зсувів використовує бездротову сенсорну мережу для виявлення незначних рухів грунту і змін в різних параметрах, які можуть статися до або під час зсуву. Завдяки зібраним даним можна дізнатися про наближення виникнення зсувів задовго до того, як це станеться.

– Запобігання стихійним лихам

Бездротові сенсорні мережі можуть бути ефективними в запобіганні несприятливих наслідків стихійних лих, таких як повені. Бездротові вузли були успішно розгорнуті в річках, де зміни рівня води повинні контролюватися в режимі реального часу.

Метою даної роботи є вивчення характерних прикладів різних існуючих застосувань БСМ, як широко використовуваних, так і нових, а саме сенсорних систем визначення пожежного стану, угарного газу та сенсорних систем несанкціонованого проникнення на приватну територію. Зокрема, у Розділі 2 програми БСМ класифікуються відповідно до їх природи на відповідні категорії, їх специфічні ознаки розглядаються шляхом подання орієнтовних прикладів.

Додатково, через орієнтовне вивчення характерних прикладів кожного з них, пояснюються їхні особливості, переваги та проблеми.

Конкретні приклади розробки прямої дії сенсорних мереж, що виникають внаслідок цього дослідження, представлені в Розділі 3 даної роботи.

1.2 Поняття сенсорних мереж. Сучасні сенсорні мережі

1.1.4 Походження та історія сенсорних мереж

Щоб зрозуміти компроміси в сучасних БСМ, корисно коротко вивчити їх історію. Як безліч розвинутих технологій, походження бездротових сенсорних мереж можна відслідкувати у військових та важких промислових галузях, задовго до того, як вони стали поширені у легких промислових галузях та звичайному повсякденному житті.

Перша бездротова мережа, яка мала хоча б деяку реальну схожість із сучасною мережею БСМ - це система звукового спостереження (SOSUS), розроблена військовими США у 1950-х роках для виявлення та відстеження радянських підводних човнів. Ця мережа використовувала занурені акустичні датчики – гідрофони, розподілені в Атлантиці та Тихому океанах. Така масштабна система звукового спостереження була призначена для виявлення радянських підводних човнів і поряд зі статичними підсистемами включала в себе гідроакустичні сигнальні поплавки, які були скинуті в області пошуку з протичовнових вертольотів НАТО і передавали дані спостережень в центр обробки інформації по радіоканалах. Істотною віхою в історії створення БСМ став 2003 рік, коли вступила в силу перша версія стандарту IEEE 802.15.4. Таким чином історію бездротових сенсорних мереж можна розділити на два великі етапи: перший – до появи першої версії стандарту IEEE 802.15.4; другий – здійснення і модифікація стандарту IEEE 802.15.4 і бездротових систем на його основі. Така технологія зондування використовується і сьогодні, хоча виконує більш мирні функції моніторингу підводної дикої природи та вулканічної діяльності.

Вторячи інвестиції, зроблені в 1960-х і 1970-х роках для розробки обладнання сучасного Інтернету, Агентство перспективних дослідницьких

проектів оборонної галузі США (DARPA) запустило програму розподіленого датчика мережі (DSN) у 1980 р. для формального вивчення проблем впровадження розподіленого/бездротового зв'язку сенсорних мереж. З народженням DSN та його просуванням до наукових кіл через університети-партнери такі як Університет Карнегі Меллона та Массачусетський технологічний інститут Лінкольна, БСМ технологія незабаром знайшла місце в академічних колах та цивільних наукових дослідженнях.

Зрештою уряди та університети почали використовувати БСМ в таких додатках, як моніторинг якості повітря, виявлення лісових пожеж, запобігання стихійним лихам, метеостанціях та в структурному моніторингу.

Потім, коли студенти інженерних наук пробивались у корпоративний світ тогочасних гігантів технологій, такі як IBM та Bell Labs, вони почали пропагувати використання БСМ у важких промислових галузях як розподіл електроенергії, очищення стічних вод та спеціалізована автоматизація заводів. Незважаючи на те, що ринковий попит на мережі БСМ був сильним, перехід за межі цих обмежених застосувань був сильним викликом для розробників. Військові, наукові/технологічні та важкі промислові застосування попередніх десятиліть - все це мало будуватися на основі громіздких, дорогих датчиків та власних мережевих протоколів. Ці БСМ надали великого значення на функціональність та продуктивність, тоді як інші фактори, такі як апаратне забезпечення та витрати на розгортання, мережеві стандарти, енергоспоживання та масштабованість впали на другий план. Поєднання високої вартості та низького обсягу перешкоджали широкому розповсюдженню та впровадженню БСМ в більш широкому діапазоні додатків.

Хоча технологій для великих обсягів промислового та споживчого застосування не існувало в 20-му столітті, як наукові кола, так і промисловість визнали потенціал таких мереж і сформували спільні зусилля для вирішення інженерних питань. Приклади цих академічних/промислових ініціатив включають:

– Інтегровані бездротові датчики UCLA (1993)

- програма PicoRadio Каліфорнійського університету в Берклі (1999)
- μ Адаптивна багатодоменна програма енергозберігаючих датчиків на MIT (2000)
- Сенсорні мережі NASA (2001)
- Альянс ZigBee (2002)
- Центр зондування вбудованої мережі (2002).

Метою багатьох із ініціатив цих організацій, що займаються стандартизацією, є забезпечення широкомасштабного розгортання БСМ в легких промислових і споживчих застосуваннях за рахунок зменшення витрат і енергії на датчик, спрощення завдань розробки та обслуговування.

1.1.5 Переваги вибору технологій сенсорних мереж

З точки зору споживача, технології повинні бути недорогими, не повинні накладати обмежень на розташування датчиків, повинні забезпечувати малу затримку сигналу і мати низьке споживання, щоб батарейок вистачало на весь термін служби пристрою. Останні технологічні досягнення дозволяють виконати більшу частину цих вимог.

Для організації мережі бездротових датчиків і систематизованого збору свідчень підходить кілька технологій, в тому числі супутниковий і мобільний зв'язок, Wi-Fi, IEEE 802.15.4. Супутникові та мобільні мережі підходять для великої кількості додатків, однак мають велику витрату енергії в перерахунку на пакет. Їх недоліком є необхідність оплати послуг оператора, хоча це може бути і несуттєвим чинником при адекватній тарифній політиці.

Складнощі можуть виникнути з покриттям. Очевидно, що сигнал від супутника і стільникових мереж погано проникає через перешкоди, а датчики - стаціонарні вузли не можуть змінювати місце розташування в пошуку місця з

прийнятною якістю зв'язку. У той же час для систем, що здійснюють передачу в невеликому обсязі (скажімо, один пакет в день), супутниковий або стільниковий зв'язок - виправданий вибір.

Датчики Wi-Fi (IEEE 802.11b, g) широко поширені. Витрата енергії на пакет Wi-Fi датчика набагато менше, ніж в мережі, при цьому відсутні грошові збори за обсяг даних. Для Wi-Fi-датчиків актуальні проблеми з покриттям і зв’язністю, оскільки щільність точок доступу, необхідна для надійного зв'язку з фіксованими датчиками, як правило, вище, ніж потрібно для мобільних користувачів.

Стандарт 802.15.4 визначає фізичний і канальний (MAC) рівні моделі OSI. Він забезпечує зв'язок на невеликій відстані при порівняно малому споживанні і підходить для мереж бездротових датчиків. Швидкість передачі даних досягає 250 кбіт/с, довжина пакета не перевищує 128 байт. На пересилку декількох байтів показань датчиків з даними про маршрут, криптографічним захистом і заголовком йде менше 1 мс. При цьому витрачається менше 30 мкДж, як показано на рисунку 1.2. Датчики можуть пересилати пакети від рівноправних пристроїв, розширюючи зону дії мережі далеко за рамки доступу одного радіоприймача. При цьому забезпечується збереження функціонування мережі при відмові окремих радіоприймачів.

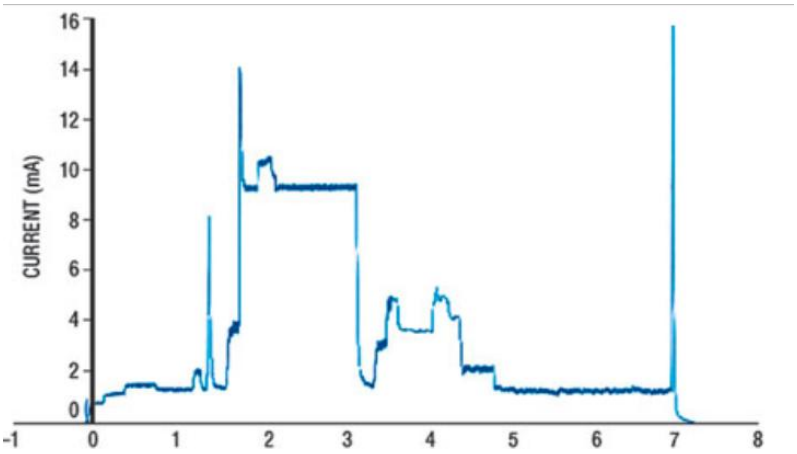

Рисунок 1.2 - Енергозатрати на передачу та підтвердження приймати пакети 802.15.4. time - час; current – струм

1.1.6 Критерії вибору сенсорних мереж

При порівнянні декількох БСМ необхідно оцінити, наскільки швидко передаються дані, і які витрати. Мережа повинна бути розрахована на роботу в середовищі з часткою переданих пакетів (PDR), що становить приблизно 50%.

При розробці бездротових систем збору даних необхідно витримати відповідність кільком критеріям. По-перше, система повинна відповідати мінімальним вимогам по надійності. У промислових додатках необхідно отримувати 99,9% показань, а втрата даних може привести до небажаних наслідків.

По-друге, система повинна забезпечувати задану смугу пропускання, тобто здійснювати успішну передачу певної кількості пакетів в одиницю часу.

По-третє, пакети необхідно передати за вказаний проміжок часу, інакше у них інформація може застаріти.

По-четверте, мережа повинна бути розрахована на роботу в жорстких середовищах, наприклад, при сильних коливаннях температури або при дотриманні обмежень, пов'язаних з питаннями безпеки. Нижче будуть розглянуті рішення, що відповідають всім чотирьом вимогам. Ключовим критерієм вибору того чи іншого рішення є вартість володіння і гнучкість.

Вартість володіння має на увазі витрати на розробку продукту, його установку, вартість апаратної частини, і витрачається протягом усього терміну служби енергії. Бездротові технології дозволяють істотно знизити вартість установки, однак при харчуванні від батареї потрібно періодична заміна елементів живлення. Доводиться вибирати метод отримання енергії. З одного боку, можна обійтися кількома потужними джерелами живлення (при цьому скорочується вартість апаратної частини), або використовувати велику кількість малопотужних

пристроїв. У пристроях, що живляться від екологічно чистих джерел (сонячні або термоелектричні елементи), ємність конденсатора сильно впливає на вартість. Послабити цю залежність можна за допомогою введення детермінованого планування, наприклад, за рахунок тимчасового поділу доступу (TDMA), коли ресурсомісткі події не відбуваються одночасно.

Оскільки неможливо передбачити кінцеві умови експлуатації, мережі повинні забезпечувати гнучкість і масштабованість залежно від кількості датчиків і щільності їх розміщення. Для забезпечення надійності рівень інтерференції повинен бути невисоким, і система повинна зберігати функціонування в разі відмови окремих вузлів. Підвищити надійність і зменшити затримку передачі можна за допомогою додаткових ресурсів, наприклад, за рахунок збільшення кількості бездротових каналів, збільшення кількості сусідніх пристроїв для кожного вузла, збільшення коефіцієнта посилення сигналу. При цьому зростає споживання, тому рекомендується проводити динамічний розподіл ресурсів.

Стандартні рішення забезпечують нечутливість до збоїв в ланцюзі постачань одного з постачальників, а також відповідають керівним принципам роботи, таким як безпека архітектури.

2. ПРИНЦИПИ ПОБУДОВИ, ЕКСПЛУАТАЦІЇ ТА ВИКОРИСТАННЯ СЕНСОРНИХ МЕРЕЖ

2.1 Характерні технологічні риси безпроводових сенсорних мереж

2.1.1 Основи побудови бездротових сенсорних мереж

Бездротова сенсорна мережа або бездротова персональна мережа WPAN (Wireless Personal Area Networks) - це розподілена мережа необслуговуваних мініатюрних електронних пристроїв (сенсорних вузлів), які здійснюють збір даних про параметри зовнішнього середовища і їх передачу в центр обробки за допомогою ретрансляції від вузла до вузла. Широке використання таких мереж можливо в області автоматизації процесів збору інформації, моніторингу та контролю характеристик різноманітних технічних і природних об'єктів. Сенсорні вузли можуть встановлюватися стаціонарно або мати можливість довільно переміщатися в деякому просторі, не порушуючи логічної зв'язаності мережі, в цьому випадку сенсорна мережа не має фіксованої топології і володіє самоорганізовуваною структурою. Під самоорганізацією (SelfOrganizing) розуміється автоматичний вибір топології мережі, автоматичне підключення нових пристроїв до мережі, автоматичний вибір маршрутів передачі пакетів в мережі без участі людини.

Стандарт IEEE 802.15.4 визначає два нижніх рівні моделі: фізичний рівень (PHY) і рівень управління доступом до радіоканалу (MAC) для діапазонів частот 868, 915 МГц і 2,4 ГГц. Рівень управління орієнтований на організацію WPAN з невеликими швидкостями передачі даних (LowRate WPANs, LRWPAN), радіусом дії мережевих пристроїв від 10 до 75 м. Всі інші функції реалізуються

протоколами верхніх рівнів. Стек протоколів найбільш відомих стандартів сенсорних мереж (ZigBee, 6loWPAN) наведено на рисунку 2.1.

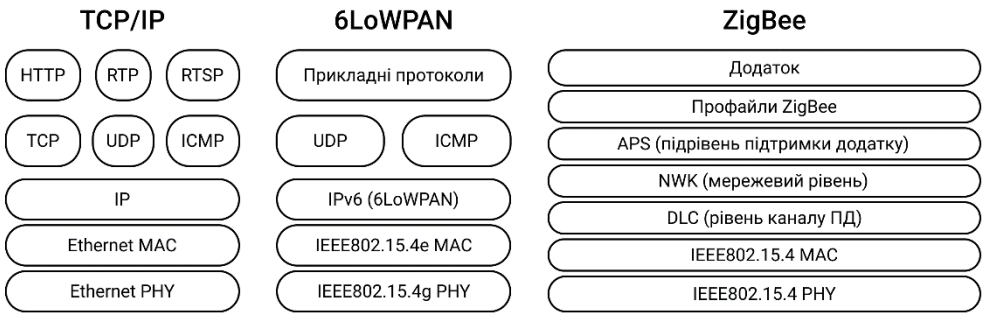

Рисунок 2.1 – стек протоклів сенсорної мережі

У стандарті IEEE 802.15.4 (2006) виділяється чотири режими PHY:

- 868/915-МГц широкосмуговий спектр прямої послідовності (DSSS) PHY, що використовує двопозиційну фазову маніпуляцію (BPSK);

- 868/915-МГц DSSS PHY використовує квадратурну фазову маніпуляцію із зсувом (O-QPSK);

- 868/915-МГц широкосмуговий спектр зворотньої послідовності (PSSS) PH, який використовує двопозиційний фазову маніпуляцію (BPSK) і амплітудну маніпуляцію (ASK);

- 2450-МГц DSSS PHY, що використовує квадратурну фазову маніпуляцію із зсувом (O-QPSK).

Типовий вузол може бути представлений двома типами пристроїв:

- мережевий координатор FFD (Fully Function Device), що здійснює глобальну координацію, організацію та установку параметрів мережі, потребує найбільшого обсягу пам'яті і ємного джерела живлення, підтримує всі типи топологій («лінійна», «зірка», «дерево», «коміркова мережа»);

- RFD (Reduced Function Device) підтримує обмежений набір функцій стандарту 802.15.4 (топології «точка - точка», «зірка»), не може здійснювати зв'язок з іншим RFD.

Повнофункціональний мережевий пристрій FFD здатний здійснювати зв'язок як з декількома FDD, так і кількома RFD і може працювати в трьох режимах: майстер-координатор PAN, координатор і простий пристрій.

Функцією майстер-координатора володіє одне FFD в мережі, воно ініціює процес самоорганізації, в його функцію входить сканування частотних каналів для знаходження вільного каналу і створення мережі. Після виявлення вільного каналу FDD формує 16-розрядну адресу PAN (PAN identifier), який інтерпретується як корінь дерева адресного простору мережі. Після цього координатор PAN періодично передає в мережу сигнали маяка (Beacons). Мережеві пристрої виявляють цей сигнал (функція Energy Detection) і використовують для подальшого приєднання до існуючого PAN. В адресному просторі PAN, що має ємність 264, типи пристроїв (FFD або RFD) відрізняються спеціальним бітом в поле MAC-адреси. Для приєднання до мережі віддалених від координатора PAN нових мережевих пристроїв можуть використовуватися вже приєднані до мережі FFD в режимі координатора. З пристроїв, які «чують» свого координатора, формуються кластери або мультикластери мережі. Функція координатора зводиться до випромінювання кадрів синхронізації доступу до радіоканалу, які передаються між сигналами маяків, тимчасові інтервали між ними називаються «кадрами маяків» (Beacon Frame). Передача даних по мережі може бути організована і без синхронізації доступу.

При передачі пакета даних (Data Frame) по мережі мережевий пристрій перетворює його в кадр даних, що включає адресу призначення, преамбулу для синхронізації, два перевірочних байта циклічного коду (CRC) для виявлення помилок і т. д. Кадр даних з максимальним розміром 127 байт може бути зашифрований 128-бітовим ключем стандарту AES (Advanced Encryption Standard). Спеціалізований стек протоколів передбачає функції самоорганізації і само-відновлення мережі, забезпечує багаторівневу систему динамічної аутентифікації.

Вузол мережі містить: датчик або безліч датчиків (власне сенсорів), які приймають дані від зовнішнього середовища, мікроконтролер, запам'ятовуючий пристрій, приймач, автономне джерело живлення, виконавчі механізми для передачі керуючих впливів від вузлів мережі до зовнішнього середовища. Велике значення мають способи інтеграції датчиків, що вимірюють значення первинних

електричних величин, функціонально залежних від контрольованих параметрів. Відмова від датчиків з цифровими проміжними інтерфейсами дозволяє не тільки економити апаратні засоби, а й перетворювати сигнали зі всіх датчиків в коди в одному багатоканальному АЦП.

Бездротовий сенсор являє собою плату, на якій розташовуються цифрові і аналого-цифрові перетворювачі, мікропроцесор, оперативна і флеш-пам'ять, блок інтерфейсів, приймач (радіомодем), джерело електроживлення, а також датчик (датчики).

Блок інтерфейсів містить інші порти введення/виводу, наприклад програмування або підключення зовнішнього датчика.

Радіомодем включає в себе низькопотужний приймач і мікроконтролер, який, в свою чергу, має в своєму складі процесор, ОЗУ, FlashROM, ПЗУ, EEPROM, АЦП, блок обробки переривань, певну номенклатуру інтерфейсів і інші периферійні вузли.

У джерелі електроживлення реалізований захист від перенапруги. Харчування сенсора здійснюється від батареї потужністю в кілька ват. Можлива додаткова схема подачі живлення від зовнішнього джерела.

В якості опції до складу сенсора може входити блок візуалізації для відображення поточного стану пристрою і блок введення для зміни режимів роботи, перезавантаження і т.д.

Основна обробка даних, отриманих сенсором і включають в себе інформацію датчиків, а також інформацію про стан сенсорів і результати процесу передачі даних, проведені вузлом або шлюзом мережі.

В рамках протоколу 6LoWPAN виділяються наступні типи мереж: ad-hoc, проста 6LoWPAN-мережа і розширена 6LoWPAN-мережа.

Ad-hoc-мережа не має граничного маршрутизатора і підключення до зовнішньої IP-мережі. Проста 6LoWPAN-мережа має один граничний маршрутизатор, підключений до зовнішньої IP-мережі безпосередньо (наприклад, GPRS / 3G / 4G модем), або може входити до складу іншої підмережі. Розширена 6LoWPAN-мережа складається з однієї або декількох підмереж, підключених до

зовнішньої IP-мережі через кілька граничних маршрутизаторів. При цьому граничні маршрутизатори в розширеній мережі поділяють один і той же мережевий префікс. Вузли розширеної мережі можуть вільно переміщатися в межах мережі та здійснювати обмін із зовнішньою мережею через будь-який граничний маршрутизатор (вибирається маршрут з найкращими показниками якості сигналу - рівень помилок, рівень сигналу).

На даний момент існує безліч алгоритмів маршрутизації, призначених для використання в самоорганізованих мережах зі змінною топологією, таких як AODV (Ad-hoc On Demand Distance Vector), PWRP (Predictive Wireless Routing Protocol), DSR (Dynamic Source Routing), OLSR (Optimized Link State Routing protocol), TORA (Temporally-Ordered Routing Algorithm), HSLS (Hazy-Sighted Link State).

Протокол DSR здійснює динамічну маршрутизацію від джерела і призначений для mesh-мереж MANET (Mobile Ad hoc Network). Так само, як і протокол AODV, він формує маршрут на вимогу за допомогою передачі широкомовного (broadcast) запиту, при цьому використовується явна маршрутизація без прямого обліку таблиць маршрутизації на кожному проміжному пристрої. Існує ще версія комбінованого протоколу DSR-Flow, що поєднує в собі явну маршрутизацію і маршрутизацію за таблицями.

Протокол AODV є дистанційно-векторно реактивним протоколом, він призначений для динамічної маршрутизації в мережах MANET та інших радіомережах.

Однак ефективність роботи відомих алгоритмів різко знижується в разі, коли швидкість зміни топології мережі зростає, що і характерно для сенсорних мереж, особливо в області спеціального призначення. Зниження ефективності роботи реактивних алгоритмів в цій ситуації пояснюється тим, що кешування маршрутів транспортування пакетів будуть швидко «старіти» через руйнування складових їх зв'язків, тому при відправці пакета доведеться будувати новий маршрут, що призведе до великих затримок в доставці даних.

Проактивні алгоритми, засновані на постійній підтримці в актуальному стані таблиць маршрутизації в вузлах мережі, також малозастосовні через обмежену місткість запам'ятовуючих пристроїв сенсорних вузлів і високу динаміку зміни топології.

В силу вищевказаних технічних і архітектурних особливостей сенсорних мереж дані рішення неприйнятні, тому необхідно вживати заходів для забезпечення ефективної маршрутизації. Зокрема, для цього був розроблений протокол RPL (Routing Protocol for Low power and Lossy Networks), що відноситься до сімейства протоколів Distant Vector. Він використовує принципи побудови спрямованих ациклічних графів DODAG (Destination Oriented DirectedAcyclic Graph) і підтримує маршрутизацію множинної топології MTR (Multi-topology routing), мобільність вузлів і всі механізми для відновлення графів в разі переміщення вузла.

2.1.2 Аналіз протоколів передачі даних у БСМ

Побудова класичних мереж характеризується великою кількістю етапів від ідеї до готової функціональної системи.

Спрощено, ці етапи можна розділити на:

1) проектування:

- з'ясування початкових умов - числа вузлів, умов середовища; критеріїв вибору і т.д .;
- вибір технологій, специфікацій, протоколів і алгоритмів;
- моделювання;
- перевірка і усунення недоліків;

2) реалізація:

- монтаж згідно з проектом;
- тестова експлуатація;

- усунення недоліків;
- експлуатація.

Побудова БСМ проходить аналогічні етапи. Розглянемо детальніше етап вибору технологій, специфікацій, протоколів і алгоритмів.

Для кожного рівня є велика кількість протоколів. Розглянемо основні, які найбільш часто використовуються. Дана класифікація має поділ протоколів за рівнями моделі OSI. Базовий принцип моделі OSI - технології, що використовуються на кожному з рівнів, які не залежать від технологій, що використовуються на інших рівнях, що спрощує вибір протоколів.

Розглянемо особливості кожного рівня і протоколів, що відносяться до них.

Фізичний рівень - найнижчий рівень моделі призначений безпосередньо для передачі потоку даних. Він здійснює передачу електричних або оптичних сигналів в кабель або в радіоефір і, відповідно, їх прийом і перетворення в біти даних відповідно до методів кодування цифрових сигналів. У БСМ на фізичному рівні широко використовується стандарт IEEE 802.15.4.

Він забезпечує достатню швидкість передачі і економію енергоспоживання за рахунок розбиття мережі на пікомережі - це так звана ad-hoc (децентралізована система, в якій кілька незалежних пристроїв можуть безпосередньо взаємодіяти один з одним. Розміри пікомережі, як правило, не перевищують 10 м. Основні вимоги до неї - висока швидкість передачі даних, проста інфраструктура, легкість встановлення з'єднання і входження в мережу, наявність засобів захисту даних і надання для певних типів даних гарантованих параметрів передачі (гарантія якості обслуговування, QoS -Quality of Service).

БСМ розраховані на тривалий термін експлуатації (до 10 років). При таких термінах великий вплив надає зміна фізичного середовища (в основному на канали зв'язку) - це і поява перешкод, що веде за собою зміну умов поширення радіохвиль (поява додатково мудьтипотоку, затухання або зовсім неможливість подолати перешкоду), і зміна температури, вологості, іонізації, потужності шуму, і виникнення нових джерел перешкод, і т.п. Все це передбачає наявність гнучкості

параметрів вузлів і алгоритмів мережі, тобто можливість контролювати зміни навколишнього середовища і реагувати на них.

Канальний рівень - призначений для забезпечення взаємодії мереж на фізичному рівні і контролю виникнення помилок. Отримані з фізичного рівня дані він упаковує в кадри, перевіряє на цілісність, якщо потрібно, виправляє помилки (формує повторний запит пошкодженого кадру) і відправляє на мережевий рівень.

Канальний рівень може взаємодіяти з одним або декількома фізичними рівнями, контролюючи і керуючи цією взаємодією.

Специфікація IEEE 802 розділяє цей рівень на два підрівні - MAC (Media Access Control) регулює доступ до поділюваного фізичного середовища, LLC (Logical Link Control) забезпечує обслуговування мережевого рівня.

У БСМ для управління доступом до середовища передачі (MAC-рівень) найчастіше використовуються розподілені протоколи: «за розкладом» і засновані на конкуренції. Прикладом протоколу за розкладом (гарантованого доступу) є TDMA (Time Division Multiple Access - Множинний доступ з тимчасовим поділом), а конкурентного (випадкового) - CSMA (Carrier Sense Multiple Access - Множинний доступ з контролем несучої).

Вибір протоколів канального рівня проектувальником проводиться виходячи з початкових умов з урахуванням критеріїв вибору для ефективного функціонування мережі. Гібридні протоколи являють собою комбінування основних переваг протоколів «з розкладом» (TDMA) і «конкурентних» протоколів (CSMA).

Мережевий рівень - призначений для визначення шляхів передачі даних. Він відповідає за трансляцію логічних адрес і імен у фізичні, визначення найкоротших (ефективних) маршрутів, комутацію і маршрутизацію, відстеження неполадок і колізій в мережі. Протоколи мережевого рівня маршрутизують дані від джерела до одержувача.

Незважаючи на те, що наведені оцінки мобільності, споживаної потужності, узгодженості агрегації даних, локалізації, якості послуг, складності структури,

масштабованості і збільшення шляхів носять невизначений характер (низька, хороша, обмежена і т.п.) і не оперують конкретними числовими значеннями, дані оцінки дозволяють на етапі ескізного проектування мережі здійснити вибір одного з протоколів (або їх відповідні комбінації) в якості першого наближення.

Таким чином можна стверджувати, що аналіз протоколів передачі даних, що використовуються в БСМ, орієнтований на вибір одного з протоколів (або їх комбінацій) з метою ефективного вирішення завдання мережі моніторингу і контролю з причини відсутності загального алгоритму побудови сенсорних мереж.

На жаль, при переході до мережі конкретного застосування загальних оцінок (низька, хороша, обмежена і т.п.) недостатньо і висновки по конкретній ситуації можуть з'явитися визначальними (на що розробники мереж часто звертали свою увагу). Маршрутизація в БСМ є новою областю досліджень, з обмеженим, але швидко зростаючим набором результатів досліджень. Вони націлені на спробу продовжити термін служби сенсорної мережі без збитку доставки даних.

2.1.3 Архітектура сенсорних вузлів. Основні принципи реагування сенсорних бездротових датчиків при виникненні надзвичайної ситуації.

Мережа бездротових датчиків (БСМ) - це група просторово розсіяних вузлів датчиків, які взаємопов’язані за допомогою бездротового зв'язку. Як видно на Рисунку 2.2, вузол датчика, який також називають мотами, є електронним пристроєм, який складається з процесора разом з блоком зберігання, модулем приймача, одного датчика або кількох датчиків, а також аналого-цифрового перетворювача (АЦП) та джерела живлення, що зазвичай є акумулятором. Він може додатково включати блок позиціонування та / або блок мобілізації. Вузол датчика використовує датчик(и) для вимірювання коливань поточних умов у його

сусідньому середовищі. Ці вимірювання перетворюються через блок АЦП у відносні електричні сигнали, які обробляються через процесор вузла. Через свій трансивер вузол може бездротово передавати дані, вироблені його ж процесором, до інших вузлів або / та до вибраної точки зливу, про яку йдеться в якості базової станції.

Як проілюстровано на Рисунку 2.3, базова станція, використовуючи дані, які передає сама собі, здатна як здійснювати наглядовий контроль за БСМ, якому він належить, так і передавати відповідну інформацію людині, користувачам або / та іншим мережам.

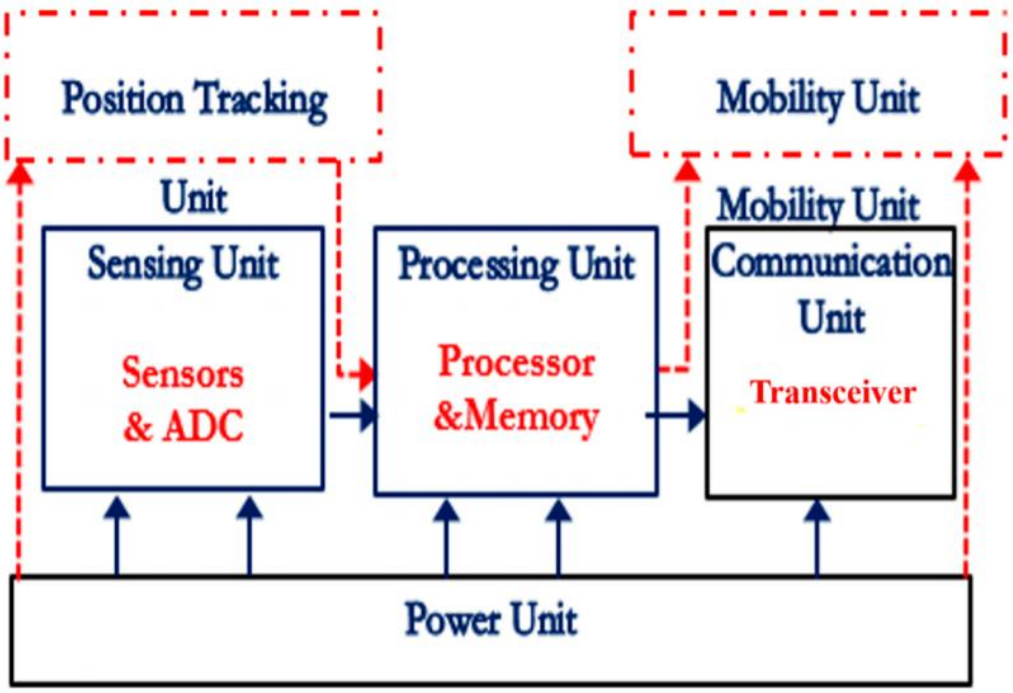

Рисунок 2.2 – Типова архітектура сенсорного вузла, що використовується в бездротових сенсорних мережах (БСМ)

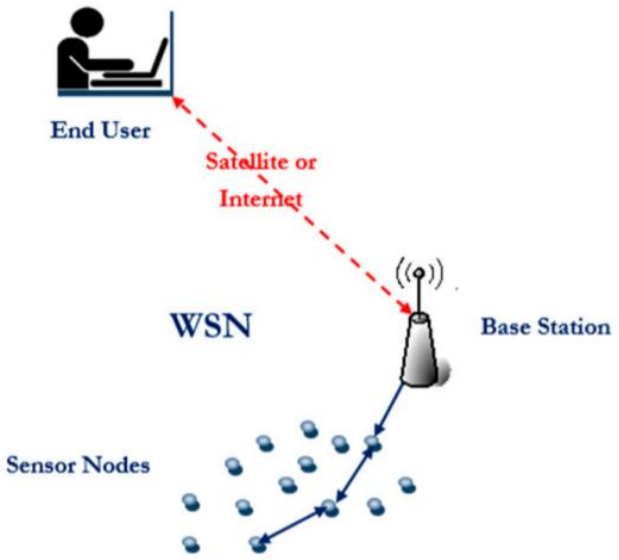

Рисунок 2.3 – Типова архітектура сенсорної мережі (БСМ)

Спільне використання достатньої кількості таких вузлів датчика дозволяє виконувати БСМ одночасне отримання даних навколишньої інформації в декількох точках, розташованих на широких площах. Стандартами в області програмного забезпечення бездротових сенсорних мереж залишаються стек протоколів ZigBee, який базується на технології IEEE 802.15.4, і операційна система реального часу TinyOS. Ця ОС функціонує на мікропроцесорах з розрядною сіткою від 8 до 32 біт і оперативною пам'яттю 2 Кбайт і вище. У складі TinyOS є набір функцій API, що дозволяє організувати попередню обробку даних безпосередньо на моті. Більшість компаній-розробників випускає і обладнання (моти, сенсори, шлюзи), і програмне забезпечення, що відповідають даним стандартам. Мабуть, найбільшого успіху домоглися кілька компаній, серед яких глибиною і закінченістю своїх розробок виділяються Crossbow і Sentilla.

2.1.4 Структура сенсорної мережі. Mesh-мережа. Датчики, мережевий шлюз, клієнтсерверна частина.

Бездротові сенсорні мережі складаються з мініатюрних обчислювальних пристроїв - мотів, забезпечених сенсорами (температури, тиску, освітленості, рівня вібрації, розташування і т.п.) і прийомопередавачами сигналів, які працюють в радіодіапазоні. Оскільки розмір моту повинен бути невеликим, його харчування здійснюється від малопотужної батареї. Моти використовуються тільки для збору і первинної обробки сенсорних даних, які вони пересилають по ланцюжку один одному, а в кінцевому рахунку спеціального пристрою - шлюзу, що має з'єднання з корпоративною мережею. Основний обробіток сенсорних даних здійснюється одними додатками корпоративної мережі.

Стандартами в області програмного забезпечення бездротових сенсорних мереж залишаються стек протоколів ZigBee, який базується на технології IEEE 802.15.4, і операційна система реального часу TinyOS. Більшість компаній-розробників випускає і обладнання (моти, сенсори, шлюзи), і програмне забезпечення, що відповідають даним стандартам. Найбільшого успіху домоглися кілька компаній, серед яких глибиною і закінченістю своїх розробок виділяються Crossbow і Sentilla.

Основною є Mesh-мережа (приклад мережі з комірчастою топологією наведено на Рисунку 2.4), де всі моти мають функції маршрутизації. Можливості самовідновлення мереж комірчастої топології в разі виходу з ладу деяких мотів дозволяють досить швидко формувати мережу з новою конфігурацією. Вся інформація, яку збирають мережею, передається на шлюз, який по суті є таким же мотом, як і всі інші, але з розширеною функціональністю. Відмінностей шлюзу від звичайного мота три: шлюз пов'язаний з корпоративною мережею (наприклад, з сервером) за допомогою дротового або бездротового зв'язку; він не має в своєму складі сенсорів; шлюз виконує ряд координуючих функцій, пов'язаних з організацією роботи бездротової мережі. У найпростішому випадку шлюз має

відповідний інтерфейс (USB-порт, послідовний порт або Ethernet-порт) і підключається до комп'ютера, що виконує функції сервера бездротової мережі.

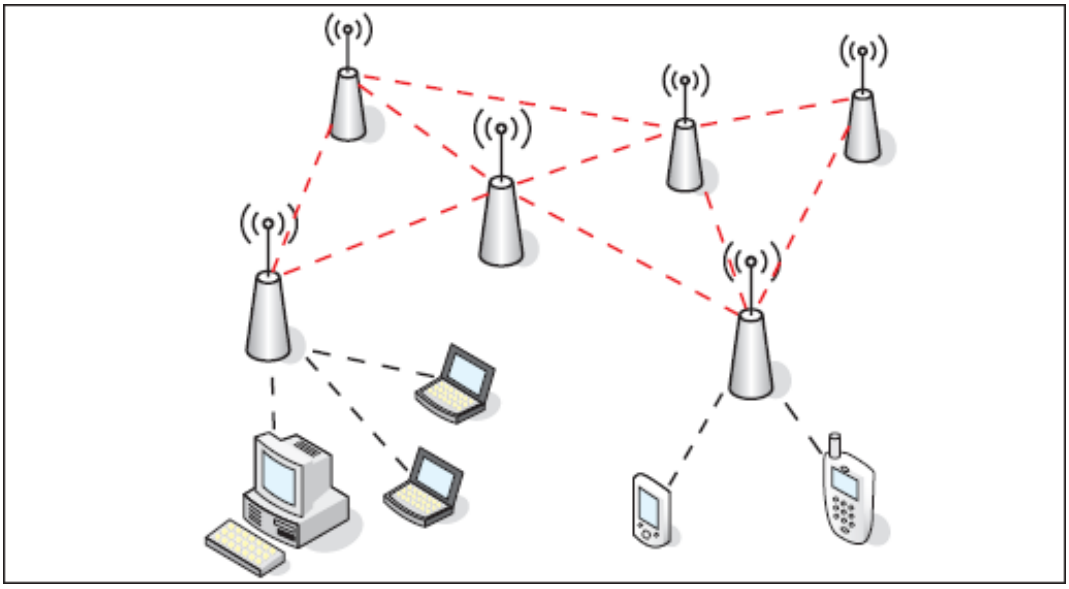

Рисунок 2.4 – Вигляд Mesh-мережі

Бездротова мережа разом із засобами контролю і управління її роботою може бути розділена на три рівні. Відповідно до термінології Crossbow вони носять такі назви: рівень мотів, серверний рівень і клієнтський рівень. Кожному рівню відповідають свої апаратні і програмні засоби. Апаратні засоби першого рівня - це власне моти і шлюз. На другому, серверному рівні, знаходиться комп'ютер, що виконує функції сервера бездротової мережі. Саме йому шлюз передає дані сенсорів, які зберігаються в базі даних сервера. Обчислювальне навантаження на нього невелика, тому в якості нього може використовуватися не повнофункціональний сервер, а звичайний ПК. І нарешті, на клієнтському рівні знаходиться термінал (ПК або ноутбук), оснащений програмними засобами візуалізації і аналізу функціонування сенсорної мережі, який підключений до сервера (по локальній мережі або через Інтернет).

2.2 Взаємодія бездротових сенсорних мереж з мережами зв'язку загального призначення

БСМ відносяться до класу бездротових персональних обчислювальних мереж (WPAN) за розмірами фізичної зони розміщення і можуть бути створені на базі різних стандартів, протоколів і технологій, таких як: ZigBee, 6loWPAN, DigiMesh стандарту IEEE 802.15.4: Bluetooth стандарту IEEE 802.15.1, WiFi стандарту IEEE 802.11. У даному підрозділі розглянемо два класи бездротових сенсорних мереж: зі збільшеним радіусом дії (ZigBee, WiFi) і з укороченим радіусом дії (Bluetooth).

Протокол ZigBee є найбільш відомим протоколом БСМ. Основою для створення протоколу став стандарт IEEE 802.15.4, який описує фізичний рівень і рівень доступу до середовища. Протоколи альянсу ZigBee дозволяють створювати самоорганізовучі мережі і самовідтворювані сенсорні мережі. Відстань між робочими станціями мережі ZigBee становить десятки метрів всередині приміщень і сотні метрів на відкритому просторі. Мережа в будь-який момент може бути розподілена, шляхом додавання нових елементів, або розбита на кілька зон, це буває корисно для зниження навантаження і підвищення швидкості передачі даних.

Всі пристрої стандарту ZigBee поділяються на три класи: координатор (в мережі, як правило використовується тільки один) - містить в собі дані про топологію мережі, служить шлюзом для передачі даних, які він збирає від усіх сенсорів БСМ для подальшої обробки, керує процесом формування мережі, встановлює політику безпеки, володіє ключами безпеки і зазвичай має зв'язок із зовнішньою IP-мережею, маршрутизатор здійснює динамічну маршрутизацію, підтримує якість топології мережі, може координувати вузли, ретранслювати сенсорні дані від вузлів, передаючи їх координатору. Маршрутизатори працюють в безперервному режимі, мають стаціонарне харчування, і можуть обслуговувати «сплячі» пристрої, термінал передає дані найближчого маршрутизатора. Схема взаємодії ZigBee с ССОП приведена на Рисунку 2.5.

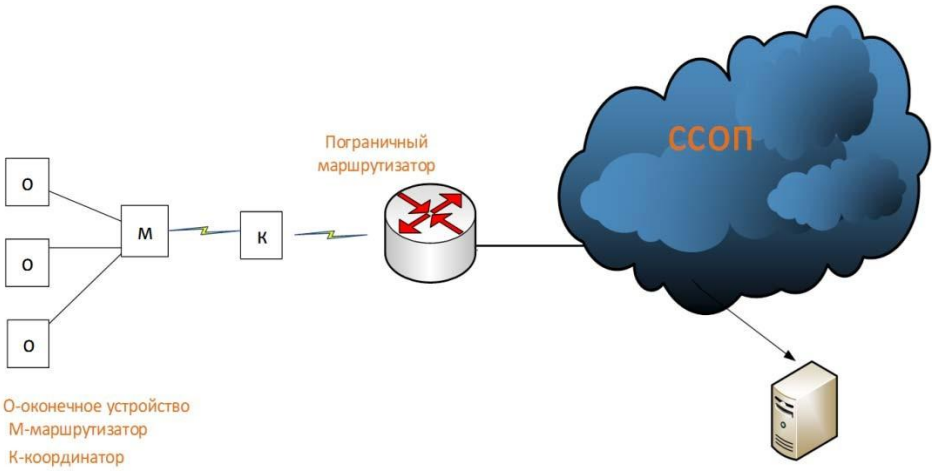

Рисунок 2.5 - Схема взаємодії ZigBee с ССОП

Технологія WiFi забезпечує відносно високу швидкість передачі даних і передбачає застосування в самоорганізованих сенсорних мережах, в яких необхідно передавати великі обсяги інформації в реальному часі. У традиційних мережах WiFi використовується два типи пристроїв «точка доступу» і «термінал». В даний час технологія WiFi включає в себе ряд стандартів IEEE 802.11a, 802.11b, 802.11g, 802.11n і 802.11ac, 802.11p, 802.11ad, 802.11s і т.д. Діяльність WiFi пристроїв залежить від потужності встановленого в них передавача, а також від типу використовуваної антени. Технологія WiFi є достатньо надійною, але дуже схильна до впливу різних електромагнітних перешкод, які випромінюються різною технікою, що стоїть в зоні покриття мережі. Вони впливають, перш за все, на швидкість з'єднання. Вона може суттєво впасти при потраплянні радіопотоку в зону перешкод. Схема взаємодії WiFi с ССОП приведена на Рисунку 2.6.

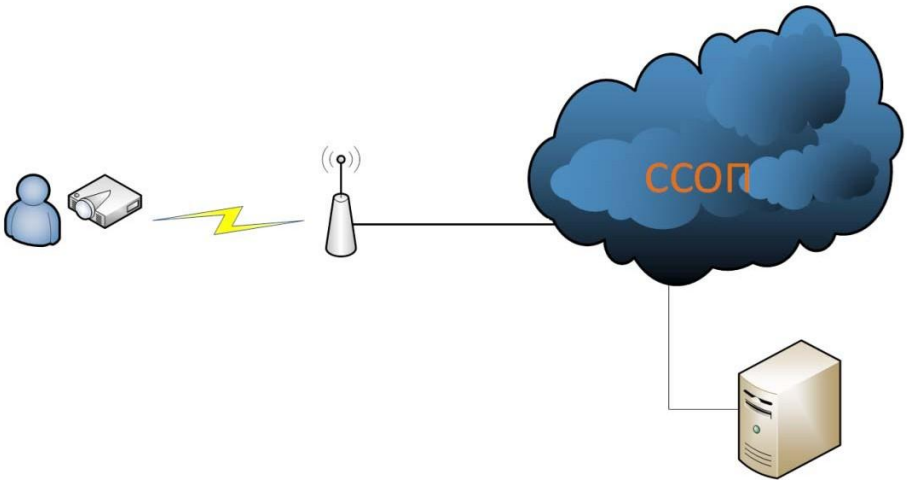

Рисунок 2.6 - Схема взаємодії WiFi с ССОП

2.3 Особливості поширення радіохвиль стандарту IEEE 802.11 у частотному діапазоні 2,4 ГГц в лісовому масиві при ліквідації надзвичайнох ситуації

2.2.1 Актуальність використання стандарту IEEE 802.11 у зоні надзвичайної ситуації

У 2012 році на території України протягом пожежонебезпечного періоду з квітня по жовтень сталось 1990 лісових пожеж на загальній площі 3500 га, а в 2013 році - 806 лісових пожеж на площею 220 га. Застосування технології IEEE 802.11 дає можливість швидкої передачі інформації в реальному режимі часу таких, як відео, фото, біометричні дані співробітників аварійно рятувальних підрозділів, їх місцезнаходження в зоні ліквідації надзвичайної ситуації.

Суттєвий вплив на умови поширення радіохвиль і на роботу всього радіозв'язку в лісі в цілому надає наявність рослинності і ґрунтового настилу. Радіохвилі, проходячи через лісові масиви, мають властивість розсіюватися і поглинатися. Так як при цьому рівень випромінювання зменшується, то даний спосіб поширення ефективний на невеликих дистанціях. Дослідження ослаблення радіохвиль лісними покривами є предметом інтенсивного вивчення фахівцями з різних країн.

Ці дослідження допоможуть проаналізувати вплив лісів на якість радіозв'язку в цілому.

2.2.2 Проведення досліджень впливу лісової рослиннності, а також полум'я на особливості розповсюдження, в даних середовищах, радіохвиль стандарту IEEE 802.11 в частотному діапазоні 2,4 ГГц.

З огляду на вищесказане, завданням безпосереднього наукового дослідження є експериментальне і практичне виявлення ослаблення потужності сигналу та передачі даних на відкритій місцевості, а також у лісовому масиві на різних відстанях. Експериментальна оцінка ослаблення сигналу проводилася в три етапи.

Перша частина експерименту полягала в вимірі потужності сигналу і пропускної здатності каналу на відкритій місцевості на стадіоні, при цьому будь-які перешкоди для проходження сигналу були відсутні, як показано на рисунку 2.7. Заміри проводилися зі зміною дистанції кожних п'ять метрів.

Рисунок 2.7 - вимір потужності сигналу і пропускної здатності каналу на відкритій місцевості на стадіоні.

Друга частина експерименту проводилася в листяному (дубовому) лісі, середньої щільності, при рівному рельєфі з густою рослинністю. Висота дерев у середньому дорівнювала 15 м, середній діаметр стовбурів - 0,3 м, чагарники висотою 2 м, як показано на рисунку 2.8. Заміри проводились через кожні десять метрів. Передавач і приймач перебували на висоті 1,2 м від поверхні землі і були оптимально спрямовані один на одного.

Рисунок 2.8 - Друга частина експерименту в листяному (дубовому) лісі

Третя частина експерименту проводилася при впливі на сигнал полум'ям вогню, при цьому відстань між приймальним і передавальним пристроєм дорівнювала 6 м. У цій частині експерименту, зображеній на Рисунку 2.9 моделювалася лісова пожежа підстильної поверхні

Рисунок 2.9 – моделювання лісової пожежі підстильної поверхні

Передача даних проводилася по бзспроводовому каналу зв'язку Wi-Fi IEEE 802.11 в частотному діапазоні 2,4 ГГц і потужністю сигналу 100 мВт при коефіцієнті посилення антени не більше 6 дБ. Вимірювання потужності сигналу проводилося за допомогою персонального комп'ютера, програмним забезпеченням Houmedale версії 1.40. Інтенсивність сигналу вимірювалася в dBm і відображалсь на осцилограмі, зображеній на рисунку 2.10, яка представляє собою графік залежності потужності приходить сигналу на приймач від часу його приходу

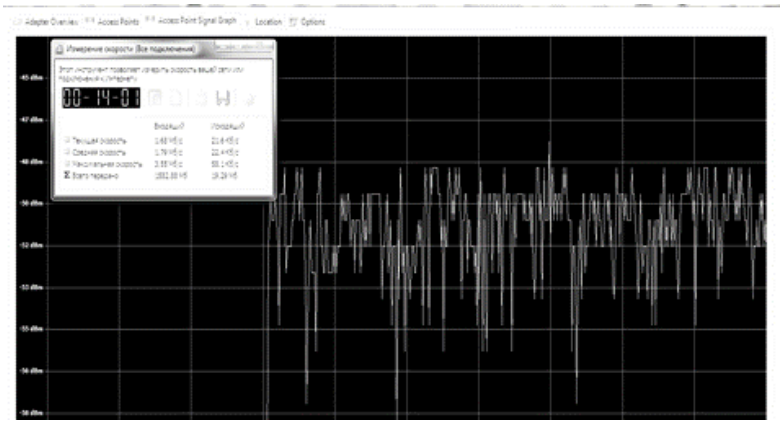

Рисунок 2.10 - Інтенсивність сигналу

На осциллограмі помітні пікові значення потужності сигналу. Сигнал фіксувався, в середньому, 14 хвилин на кожній ділянці дистанції. Отримання таким чином результатів згодом усереднювалися.

Аналіз даних графіків, представлених на Рисунку 2.11, дозволяє зробити наступні висновки.

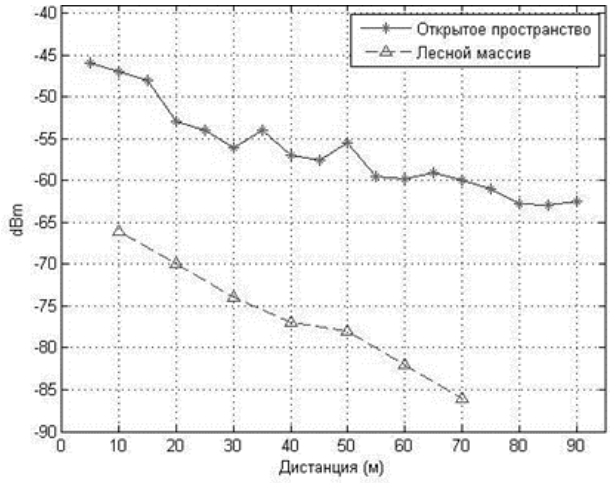

Рисунок 2.11 - Аналіз даних графіків

Потужність сигналу при збільшенні відстані між передавачем і приймачем падає. На від критої місцевості на відстані 90 метрів сигнал зменшився на 15 dBm. Обсяг передачі інформації ції коливався в діапазоні від 1,85 Мб/С до 1,65 Мб /С, і при збільшенні відстані обсягу зменшувався відповідно. У лісовому масиві сигнал істотно ослаблений, це пов'язано з прохожденням сигналу через густий чагарник на перших десяти метрах експерименту (рис. 2) і вже на 70 метрах сигнал стає значно низьким, підходячи до порогової чутливості. При впливі полум'ям на сигнал спостерігалося зменшення потужності сигналу з - 46,7 dBm до - 47,6 dBm.

Це, перш за все, пов'язано з тим, що в полум'ї, в результаті хімічної реакції, утворюються рухливі позитивні іони і негативні частинки - електрони.

Так, концентрація заряджених частинок в плазмі полум'я становить 1012 іонів/см3. Дані частинки в свою чергу впливають на розповюдження і потужності сигналу.

3 РОЗРОБКА СИСТЕМ РОЗУМНИХ ПРИСТРОЇВ НА ОСНОВІ СЕНСОРНИХ ДАТЧИКІВ

3.1 Установка детектора руху та камери спостереження з використанням віддаленого сервера та мережевого комутатора за допомогою безпровідного підключення

1) Перш за все запустимо програму Cisco Packet Tracer та виберемо необхідні елементи: детектор руху, веб-камера, сервер та Home Gateway на панелі Devices. З’єднаємо сервер та мережевий шлюз за допомогою прямого кабелю (FastEthernet0 та Ethernet1)

Рисунок 3.1 – Панель знаків

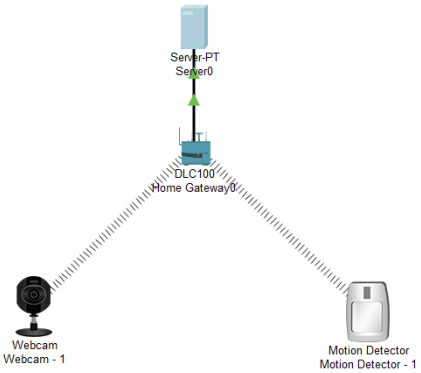

Рисунок 3.2 – Зображення мережі з безпровідним підключенням

2) Присвоюємо серверу статичну IP-адресу - 1.1.1.1, для цього у вкладці Desktop обираємо Static та вводимо IP – адресу, веб камері присвоїмо IP-адресу 1.1.1.3, детектору руху присвоїмо IP-адресу 1.1.1.2

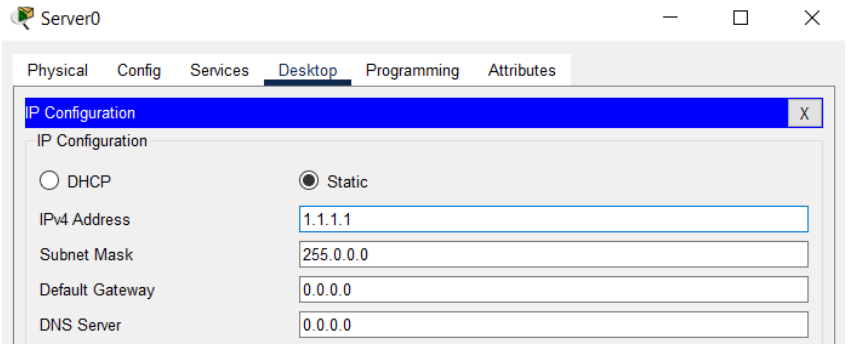

Рисунок 3.3 – Присвоєння статичної IP адреси

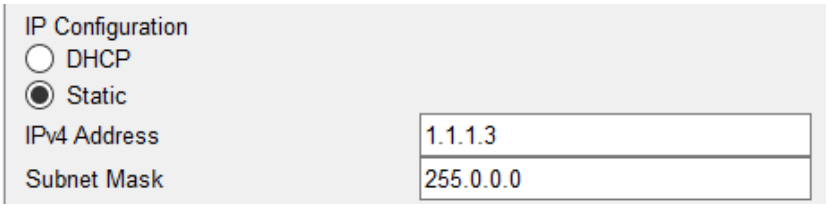

Рисунок 3.4 – присвоєння IP адреси веб камері

3) Налаштовуємо сервер на реєстрацію інформації від пристроїв у вкладці Services

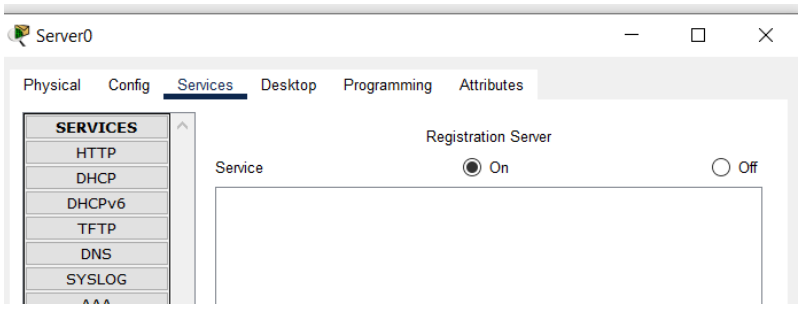

Рисунок 3.5 – налаштування серверу

4) Перевіряємо правильність підключення пристроїв (Webcam – 1 та Motion Detector), підключення має бути бездротовим, тому у вкладці IO/Config, Network Adapter обираємо підключення PT-IOT-NM-1W

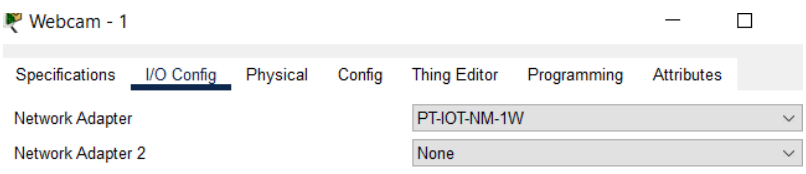

Рисунок 3.6 – Перевірка правильності підключення

5) Заходимо у веб-браузер сервера

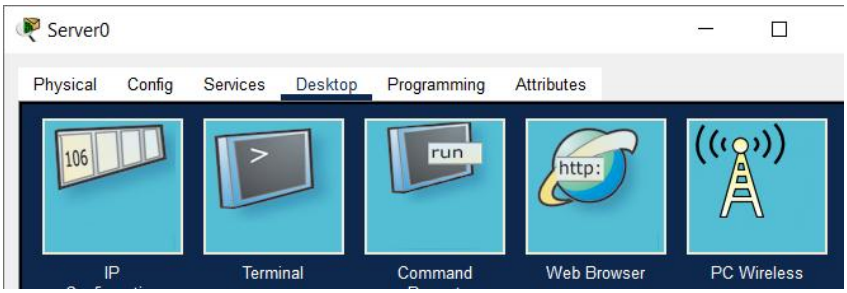

Рисунок 3.7 – Вкладка Desktop

6) Для першої реєстрації вводимо ім'я користувача та пароль, ім’я користувача – admin, пароль – cisco

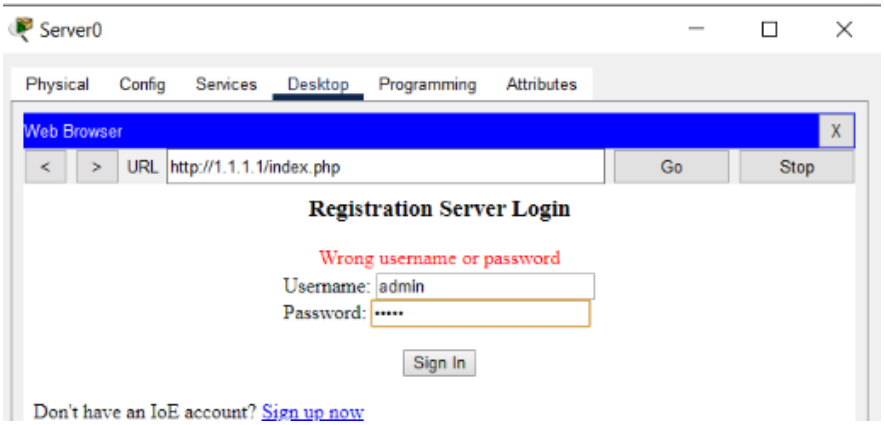

Рисунок 3.8 – Реєстрація

7) Налаштуємо роботу веб-камери та детектора руху з сервером. Для цього зайдемо у вкладку Config в налаштуваннях пристроїв, оберемо підключення Remote Server, укажемо його адресу, ім’я користувача та пароль, натиснемо клавішу Connect для з’єднання з сервером

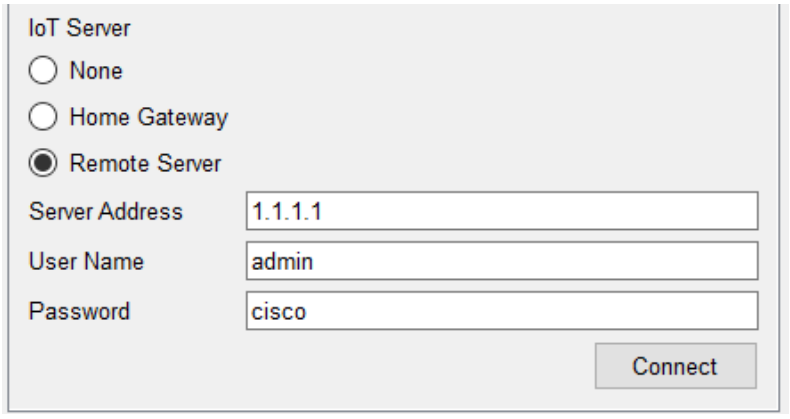

Рисунок 3.9 – Налаштування веб-камери для роботи з сервером

8) Знову заходимо у веб-браузер сервера через вкладку Desktop, вводимо ім'я користувача та пароль, перевіряємо підключення пристроїв

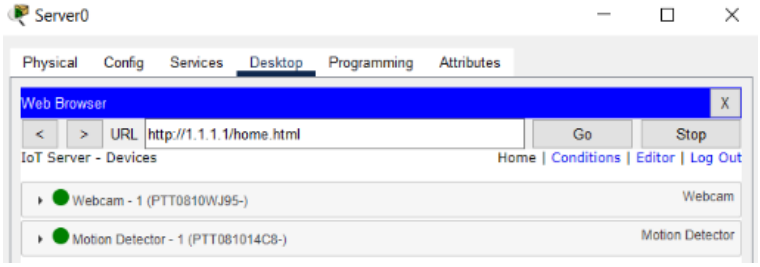

Рисунок 3.10 – Перевірка підключення пристроїв

9) Встановимо правила роботи пристроїв у вкладці Conditions. Веб-камера вмикатиметься автоматично, якщо датчик руху спрацює та навпаки.

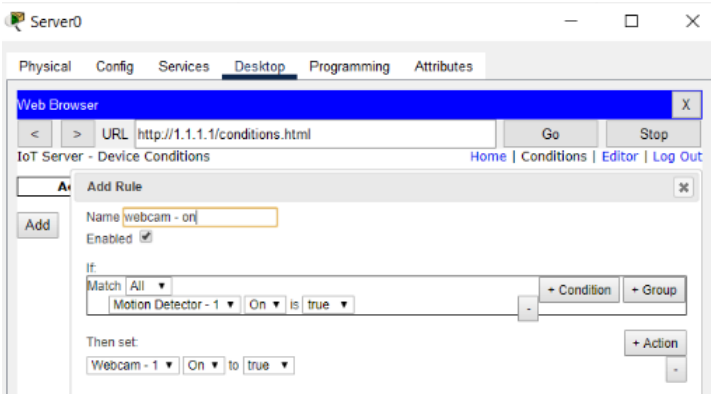

Рисунок 3.11 – Встановлення правил роботи пристроїв при увімкненій камері

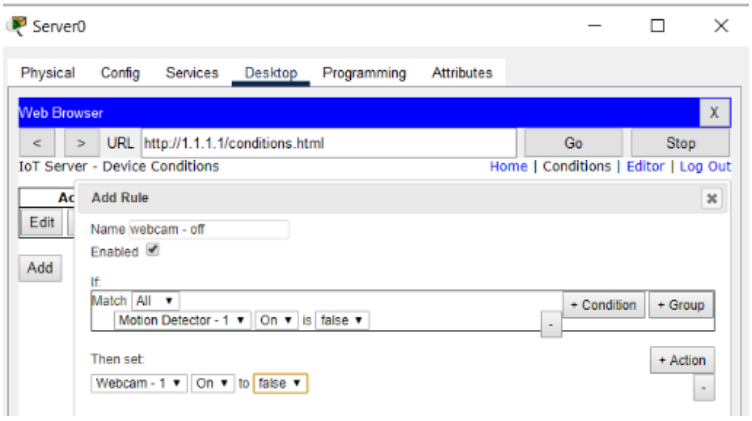

Рисунок 3.12 – Встановлення правил роботи пристроїв при вимкненій камері

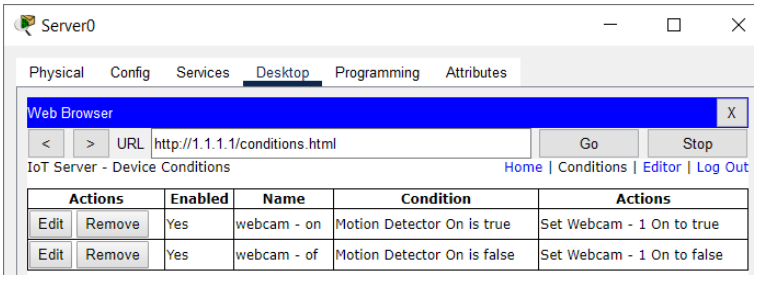

Рисунок 3.13 – Встановлені правила

10) Перевірка правильності роботи. Переходимо у вкладку Home. Розміщуємо на екрані монітора модель і налаштування сервера так щоб їх було видно одночасно. Натискаємо та утримуємо клавішу ALT, одночасно проводимо курсором миші перед датчиком руху у полі моделювання. Він повинен спрацювати, а камера повинна фіксувати зображення.

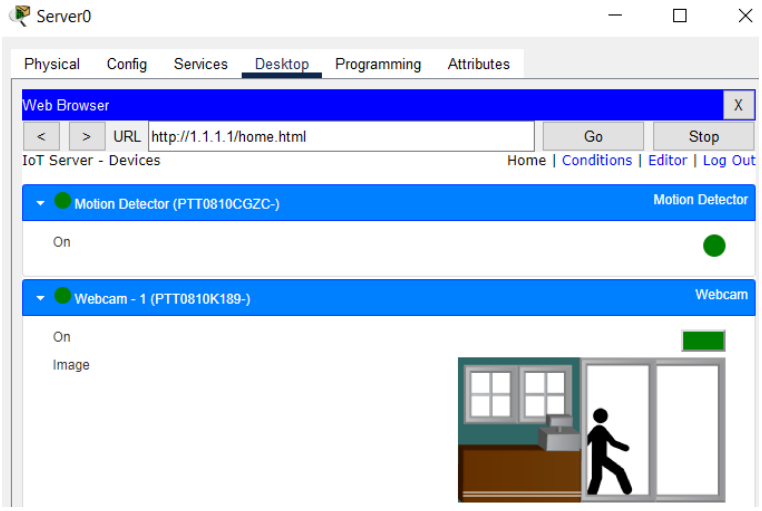

Рисунок 3.14 – Перевірка синхронізації вб-камери та детектора руху

Рисунок 3.15 – Вигляд пристроїв у робочому стані

3.2 З’єднання детектора диму, сирени та воріт у випадку надзвичайної ситуації, можливість слідкування за ситуацією за допомогою смартфона

1) Знайдемо усі необхідні елементи для проектування моделі. Для цього необхідні детектор диму, ворота, сирена, Home Gateway, смартфон.

З’єднаємо детектор диму, сирену, ворота до мережевого шлюзу прямим кабелем (fa0/1 – 01, fa0 – 0/3, fa0 – 0/2)

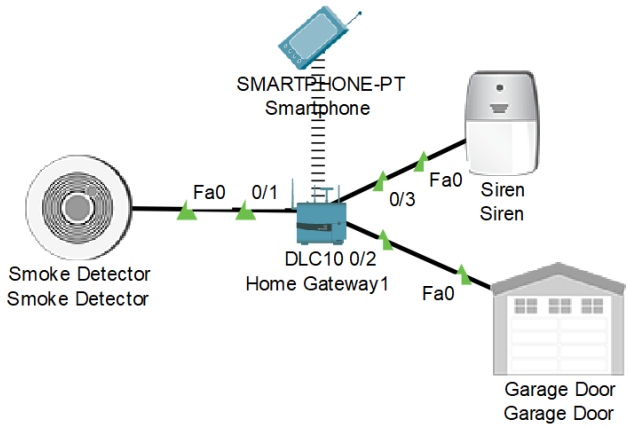

Рисунок 3.16 – Проектована модель

2) Зайдемо у налаштування смартфона, оберемо вкладку Wireless0 (бездротове з’єднання), призначаємо SSID (унікальне найменування бездротової мережі) HomeGateway

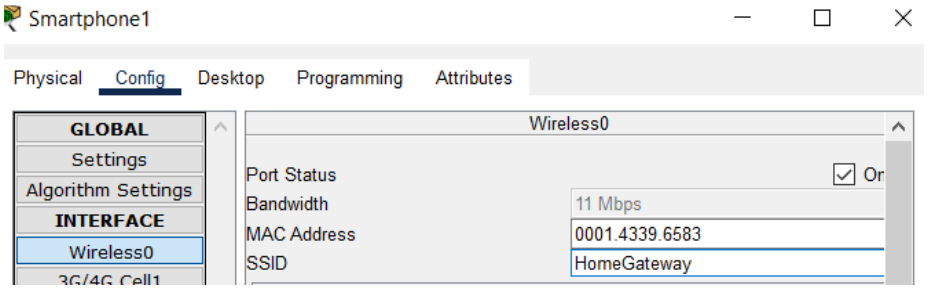

Рисунок 3.17 – Встановлення бездротового з’єднання смартфона з мережевим шлюзом

3) Заходимо у налаштування мережевого шлюзу, у вкладці Config обираємо LAN, змінюємо статичну IP-адресу на 1.1.1.1

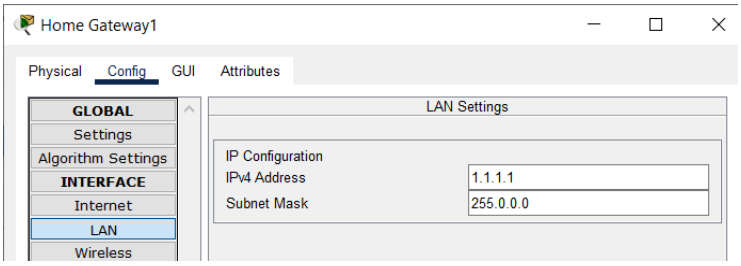

Рисунок 3.18 – Присвоєння IP адреси мережевому шлюзу

4) Заходимо у налаштування смартфону, у вкладці Wireless задаємо адресу мережевого щлюзу (1.1.1.1)

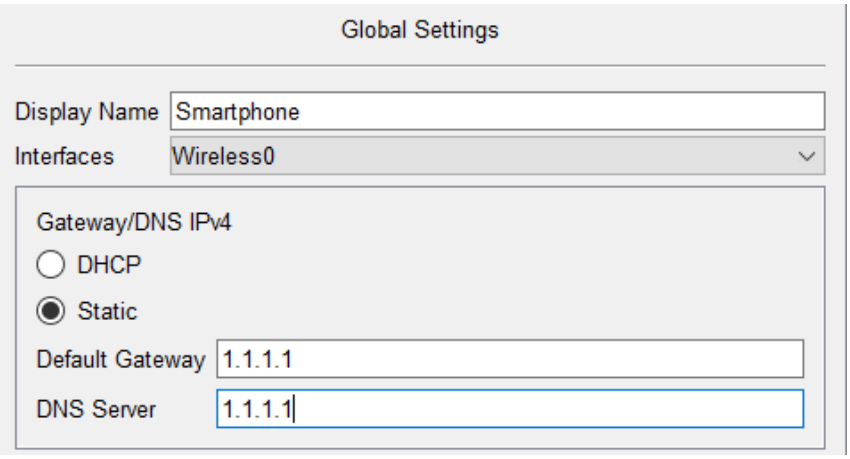

Рисунок 3.19 – Налаштовуємо роботу смартфона з мережевим шлюзом

5) Перемикаємо з Static на DHCP, залишаємо на режимі DHCP, адреса мережевого шлюзу має автоматично підв'язатися до смартфону в якості шлюзу по замовчуванню

Рисунок 3.20 – Перехід до режиму DHCP

6) Перевіряємо таким самим чином адресу за замовчуванням у налаштуваннях інших пристроїв, вона має бути теж 1.1.1.1

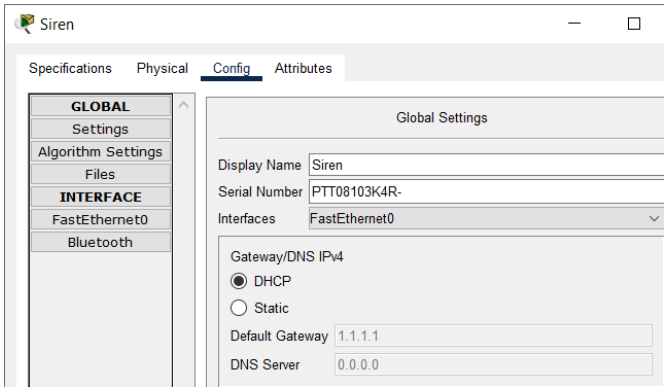

Рисунок 3.21 – Перевірка DHCP адреси всіх пристроїв

7) У вкладці Desktop на смартфоні обираємо IoT-Monitor, натискаємо та переходимо до вікна, у якому потрібно ввести адресу мережевого шлюзу, ім'я користувача та пароль

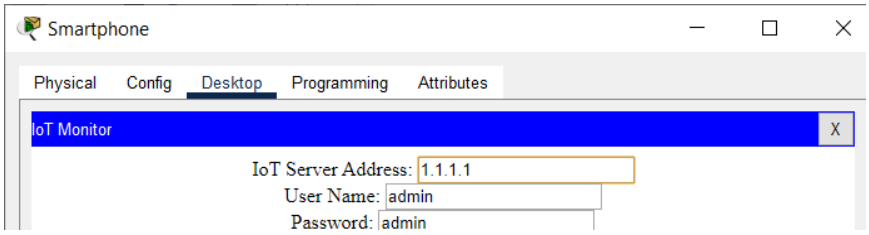

Рисунок 3.22 – Вхід до режиму моніторингу за допомогою адреси мережевого шлюзу

8) У вкладці Home бачимо три під'єднаних пристрої: сирена, детектор диму та ворота

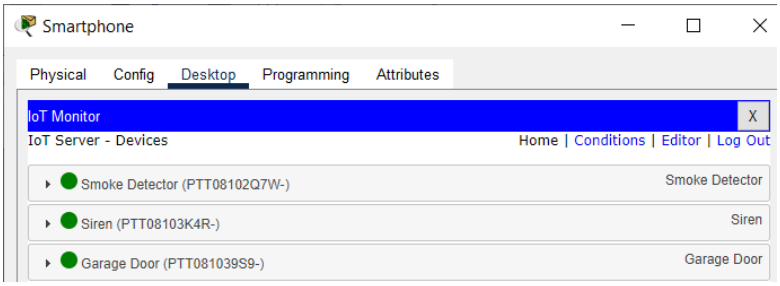

Рисунок 3.23– моніторинг під'єднаних пристроїв

9) Установимо правила роботи та взаємодії пристроїв у випадку надзвичайної ситуації. Якщо рівень диму в полі моделювання >=0.1, тоді спрацьовують автоматично ворота, що відчиняються та сирена. Якщо рівень диму менше за 0.08, тоді сирена та ворота не спрацьовують автоматично, так як рівень диму не перевищує допустиму норму у навколишньому середовищу.

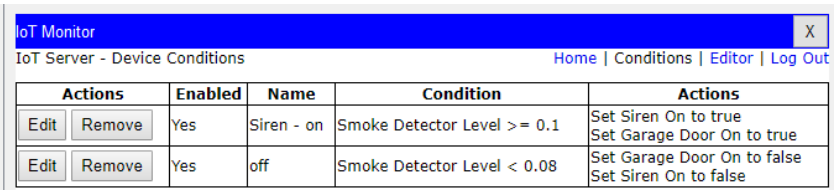

Рисунок 3.24 – встановлення правил роботи пристроїв при увімкненій та вимкненій сирені

10) Перевіримо роботу пристроїв. Для прикладу джерела диму візьмемо стару машину з багатьма поломками. Увімкнемо машину, подивимось на рівень диму, що у повітрі, та на роботу пристроїв, яку можна прослідкувати зі смартфону.

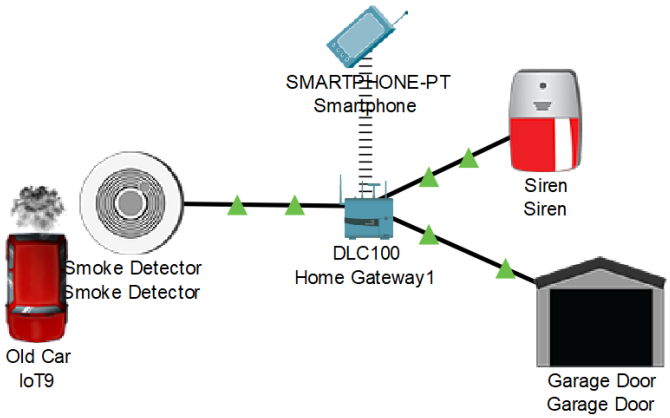

Рисунок 3.25 – Перевірка рівня диму у повітрі за участі несправного автомобіля

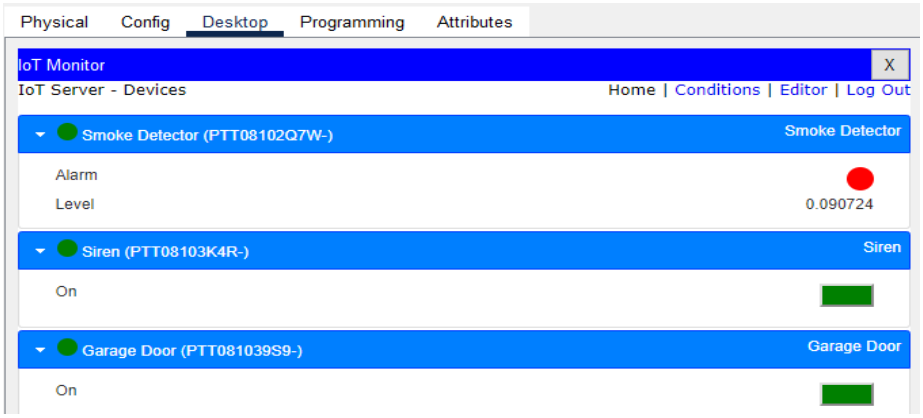

Рисунок 3.26 – моніторинг рівня повітря та синхронізації розумних пристроїв

11) Як ми можемо спостерігати, рівень диму у повітрі в полі моделювання перевищив за 0,08, тому сирена та ворота спрацювали автоматично.

3.3 Установка пожежного спринклеру, детектора диму та пожежі за допомогою мікроконтролера, запрограмованого мовою Python

1) Відкриємо програму Cisco Packet Tracer оберемо необхідні елементи: Fire Monitor, Fire Sprinkler, MCU-PT(мікроконтролер), з’єднаємо за допомогою кабелю IoT Custom Cable (D0 – D1, D0 – D0)

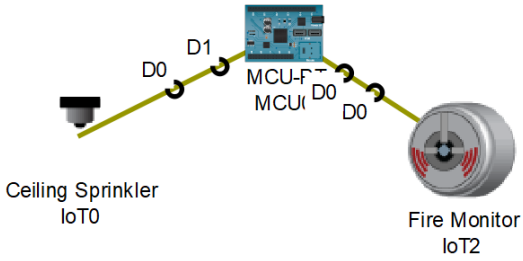

Рисунок 3.27 – Моделювання установки пожежного спринклеру

2) Заходимо в налаштування мікроконтролера та натискаємо вкладку Programming, натискаємо на New зліва у вікні для того, щоб створити новий проект. Називаємо проект firedetector, у template обираємо Empty – Python та натискаємо Create

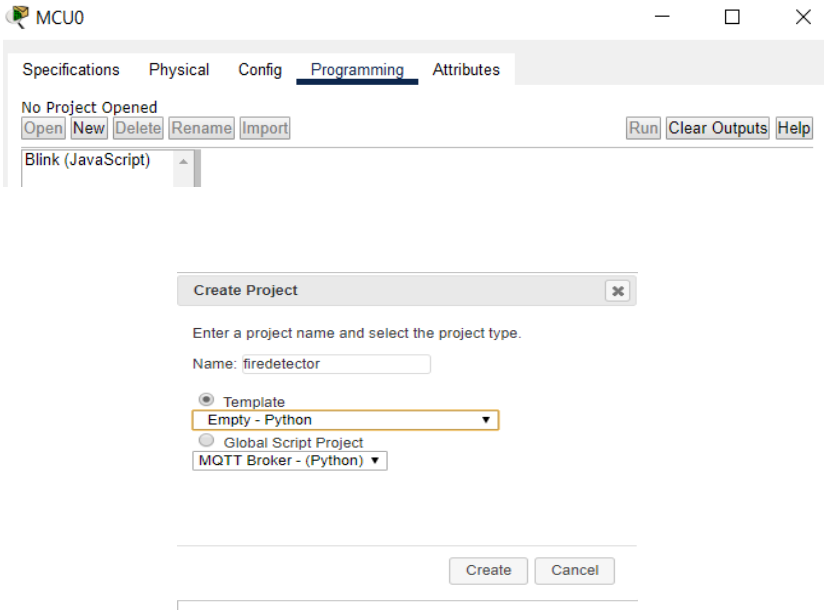

Рисунок 3.28 – Налаштовуємо мікроконтролер

3) Запрограмуємо мікроконтролер та запустимо на виконання таким чином, щоб детектор диму та пожежі міг реагувати на навколишнє середовище

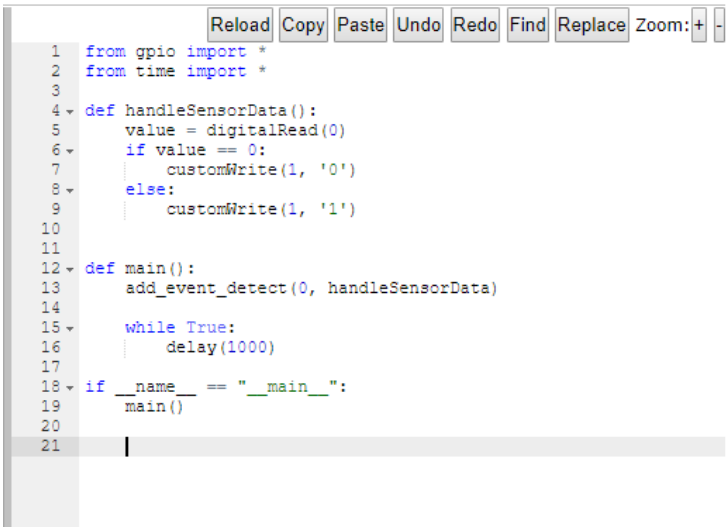

Рисунок 3.29 – Програмування мікроконтролеру

4) Запрограмуємо джерело вогню та запустимо на виконання

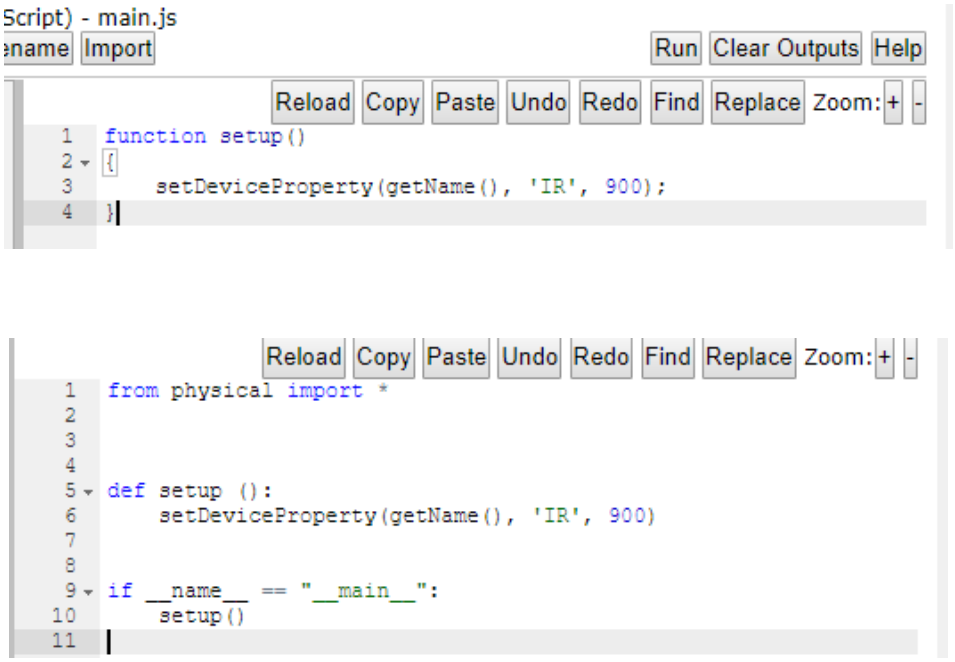

Рисунок 3.30 – Програмування джерела вогню

5) Після того, як усі програми були написані та запущені, можемо піднести джерело вогню та диму безпосередньо до детектора вогню, як ми бачимо на моделі, пожежний спринклер спрацьовує автоматично

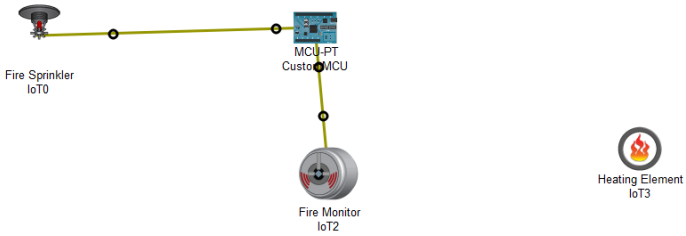

Рисунок 3.31– Вигляд сенсора та спринклера в неробчому стані

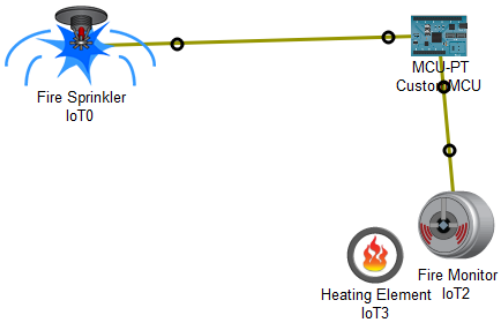

Рисунок 3.32– Вигляд сенсора та спринклера в робочому стані

3.3 Розробка IoE проекту з’єднань Інтернет-провайдера, клієнтів для модему та 3G/4G

1) Знайдемо усі необхідні елементи для побудови моделі.

Для цього нам потрібні Smartphone (телефон), Cell-Tower (базова станція), Centrall Office Server(центральний офіс), Cloud-PT("Cloud-PT" для емуляції WAN), ISP (роутер), Switch(мережевий комутатор), DNS-Server, IoT-Server, Cable-Modem-PT(кабельний модем), Home Gateway(мережевий шлюз), Laptop(ноутбук), Smart devices: Window, Light, Webcam, Siren, Door, Ceiling Fan. Підключимо пристрої один до одного використавши наступні з’єднання. Centrall-Offece-Server та Cell-Tower (коаксіальний кабель, coax0/0 – coax0/0), Centrall-Offece-Server та маршрутизатор (крос-кабель, Fa0/0 – Gig0/2), маршрутизатор та комутатор (прямий кабель типу «вита пара», (Gig0/0 –

Gig0/1), свіч та сервери DNS і IoT (також прямий кабель типу «вита пара», Fa0/1 – Fa0, Fa0/2 – Fa0), Cloud-PT та Cable Modem підключаємо за допомогою коаксіального кабелю, мережевий шлюз та кабельний модем підключаємо, використовуючи прямий кабель типу «вита пара», мережевий шлюз, ноутбук та деякі розумні пристрої підключені бездротово, інші розумні пристрої підключені за допомогою прямого кабелю типу «вита пара» до мережевого шлюзу.

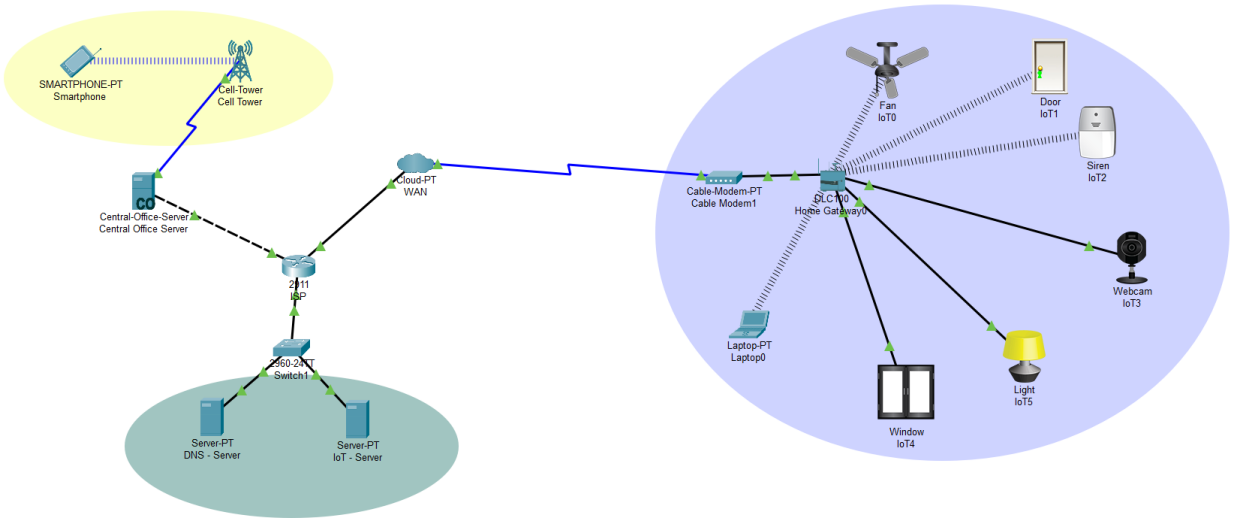

Рисунок 3.33– Вигляд готової моделі

2) Налаштуємо Home Gateway. Заходимо у режим конфігурації, обираємо Wireless, для бездротової мережі встановимо параметри. SSID присвоюємо найменування SMARTIOT, обираємо тип шифрування бездротової мережі WPA2-PSK, Pass Phrase встановлюємо 1234abcd, Encryption type –AES.

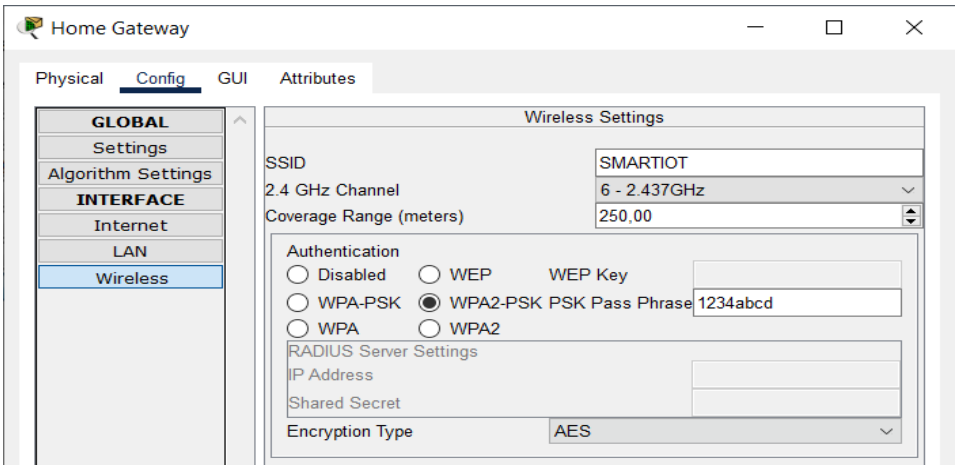

Рисунок 3.34– Налаштування Home Gateway

3) Натискаємо на вкладку Internet та обов'язково перевіряємо, щоб був підключений DHCP

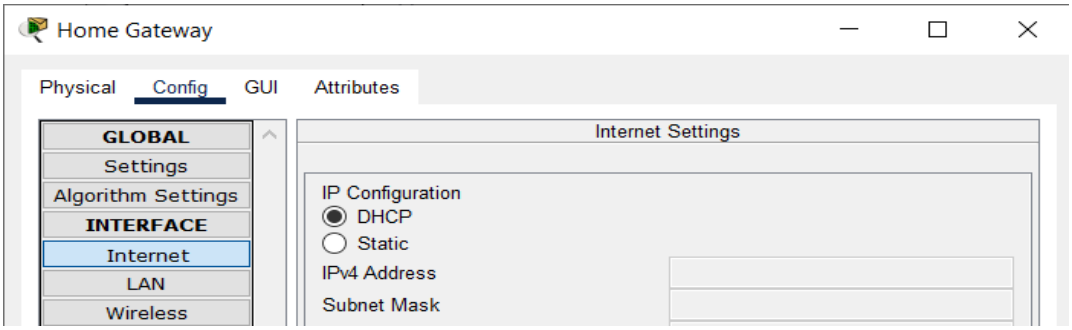

Рисунок 3.35 – Первірка підключення DHCP

4) Налаштуємо ноутбук. Вставляємо йому радіомодем. Для цього
   1. Вимкнемо ноутбук. (1)
   2. Перетягнемо карту (2) на місце (3)
   3. Перетягуємо модуль Linksys-WPC300N з місця (3) в ноутбук місце (2)
   4. Ввімкнемо ноутбук

Модуль Linksys-WPC300N забезпечує один бездротовий інтерфейс 2,4 ГГц, придатний для підключення до бездротових мереж. Модуль підтримує протоколи, які використовують Ethernet для доступу до локальної мережі.

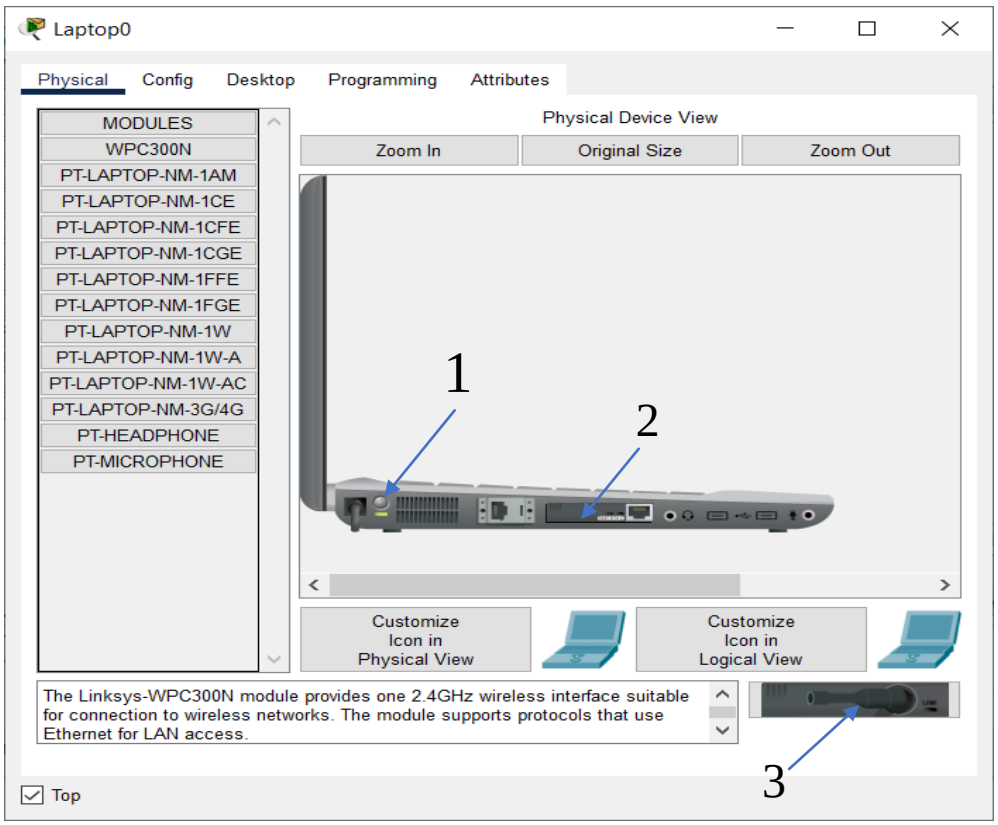

Рисунок 3.36 – Налаштування ноутбука

5) Заходимо у бездротове з’єднання.

Рисунок 3.37 – Бездротове з’єднання

6) У вкладці Connect натискаємо Connect

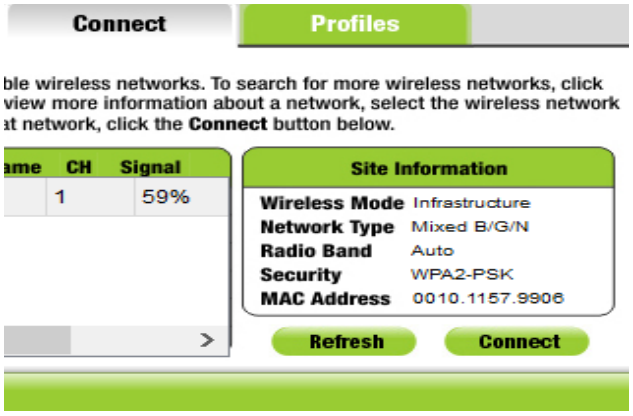

Рисунок 3.38 – Підключення до мережі

7) Вводимо пароль 1234abcd та ще раз натискаємо Connect

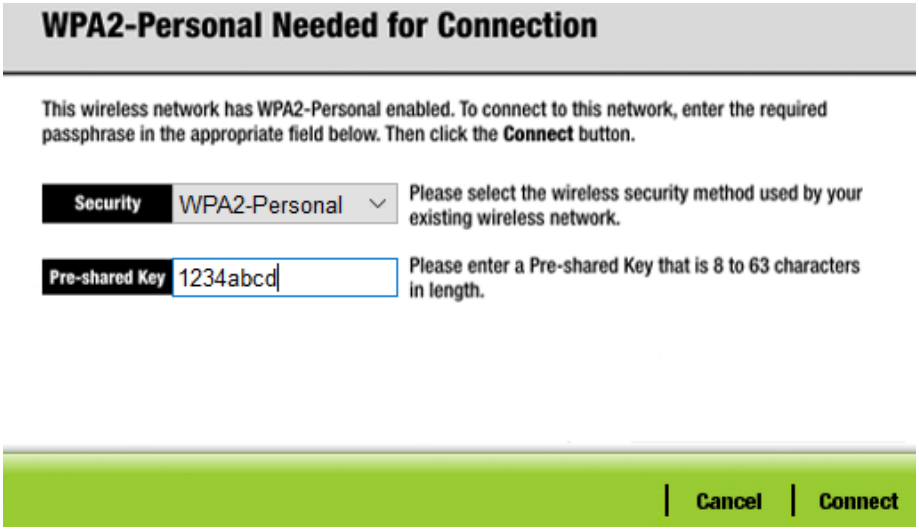

Рисунок 3.39 – Введення паролю

Рисунок 3.40 – Вигляд підключення до мережі

8) Налаштуємо веб-камеру. Добавимо модуль PT-IOT-NM-1W та введемо SSID - SMARTIOT і пароль – 1234abcd . Аналогічним чином налаштуємо решту IoT пристроїв: сирену, вікно, двері, вентилятор, лампу.

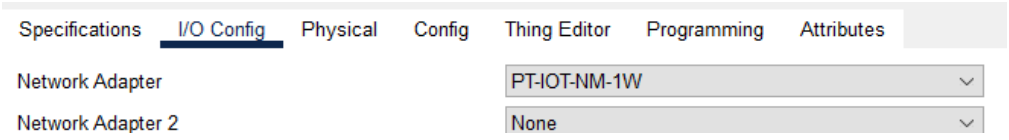

Рисунок 3.41 – Налаштування веб-камери

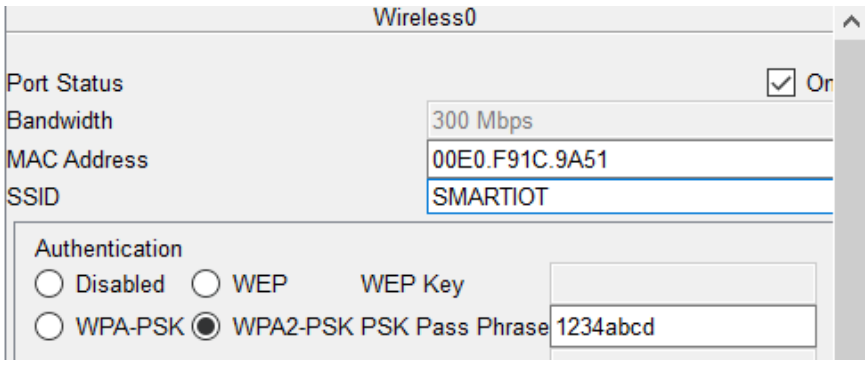

Рисунок 3.42 – Додавання модуля, SSID та пароля

9) Налаштуємо ISP (маршрутизатор). Налаштуємо ISP на роботу з Home Gateway через WAN.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip address 10.0.0.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#
Router(config-if)#no sh
Router(config-if)#int g0/2
Router(config-if)#ip address 209.165.201.225 255.255.255.224
Router(config-if)#no sh
Router(config-if)#int g0/1
Router(config-if)#ip address 209.165.200.225 255.255.255.224
Router(config-if)#no sh
Router(config-if)#
Router(config-if)#exit
Router(config)#ip dhcp excluded-address 209.165.201.225 209.165.201.229
Router(config)#ip dhcp pool CELL
Router(dhcp-config)#network 209.165.201.224 255.255.255.224
Router(dhcp-config)#default-router 209.165.201.225
Router(dhcp-config)#dns-server 10.0.0.254
Router(dhcp-config)#
```

```
Router(config)#ip dhcp excluded-address 209.165.200.225 209.165.200.209
Router(config)#ip dhcp pool WAN
Router(dhcp-config)#network 209.165.200.224 255.255.255.224
Router(dhcp-config)#default-router 209.165.200.225
Router(dhcp-config)#dns-derver 10.0.0.254
                       ^
% Invalid input detected at '^' marker.

Router(dhcp-config)#dns-server 10.0.0.254
Router(dhcp-config)#
```

Рисунок 3.43 – Налаштування маршрутизатора

10) У налаштуваннях WAN обираємо відповідно підключення через Coaxial та Ethernet.

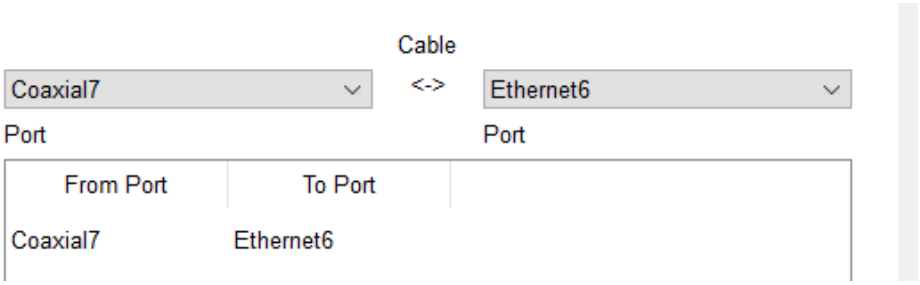

Рисунок 3.44 – Первірка підключення

11) Перевіряємо, щоб адреси обновились в Home Gateway (натискаємо по черзі DHCP-Static- DHCP).

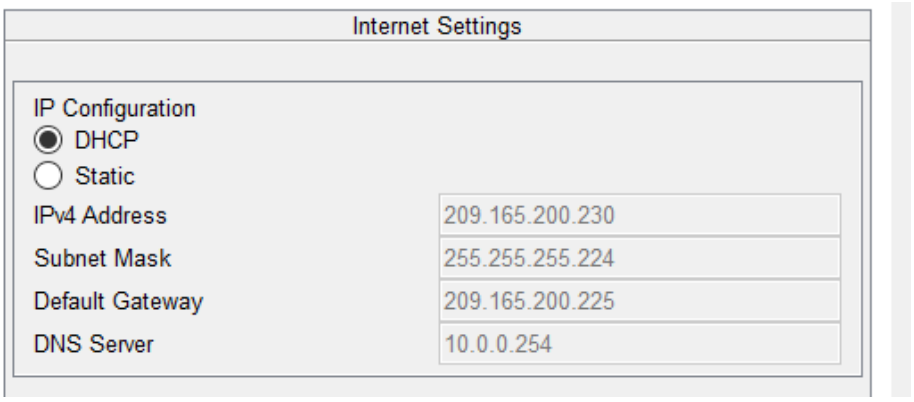

Рисунок 3.45 – Первірка оновлення DHCP

12) Оновлюємо параметр мережі в Laptop.

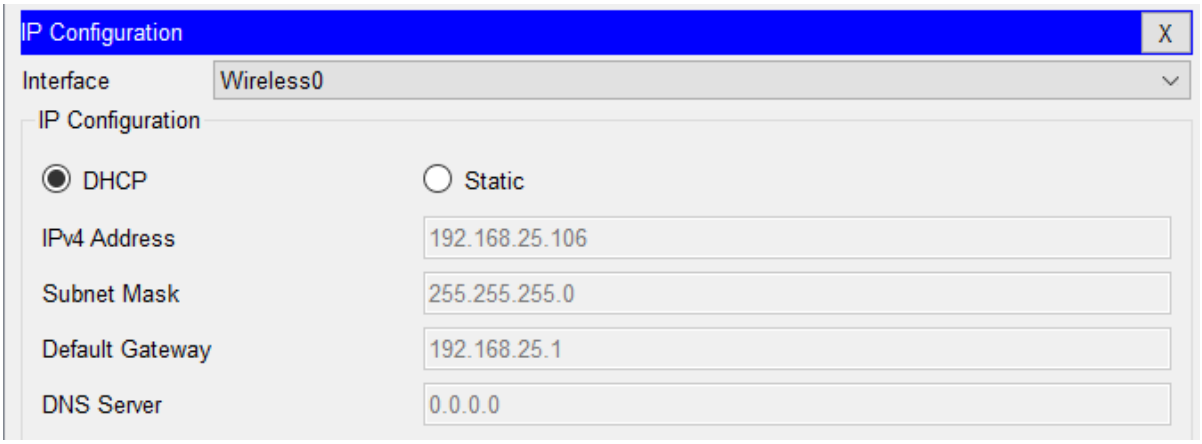

Рисунок 3.46– Оновлення параметрів

13) Оновлюємо параметри мережі у всіх інших IoT пристроях Home

Рисунок 3.47 – Оновлення параметрів мережі у всіх інших безпровідних пристроях

14) Налаштовуємо DNS-Server. Заходимо в Desktop натискаємо IP Configuration та вводимо статичні адреси

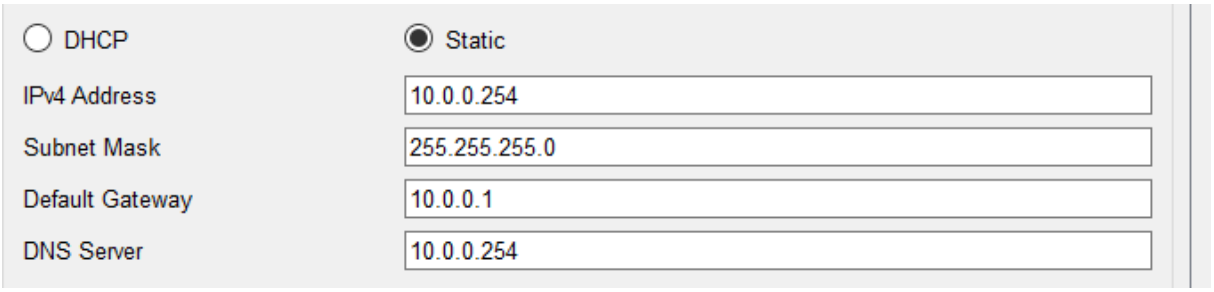

Рисунок 3.48 – Налаштування DNS сервера

15) Переходимо у вкладку Services та вмикаємо DNS-Service

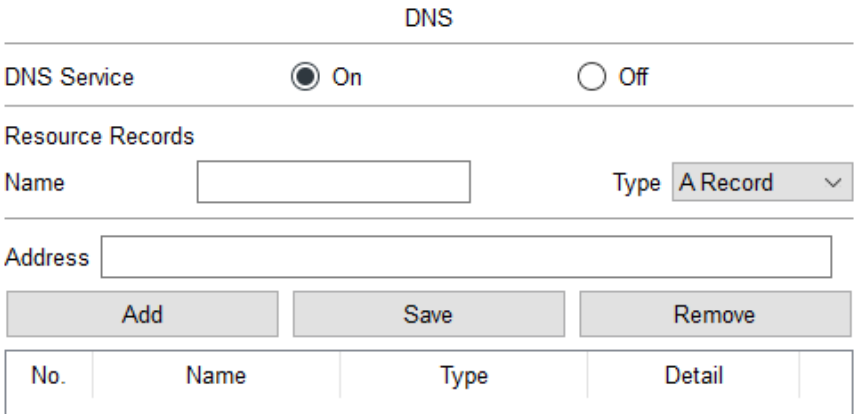

Рисунок 3.49 – Увімкнення DNS сервера

16) Аналогічно конфігуруємо IoT-Server. Вмикаємо сервіс IoT

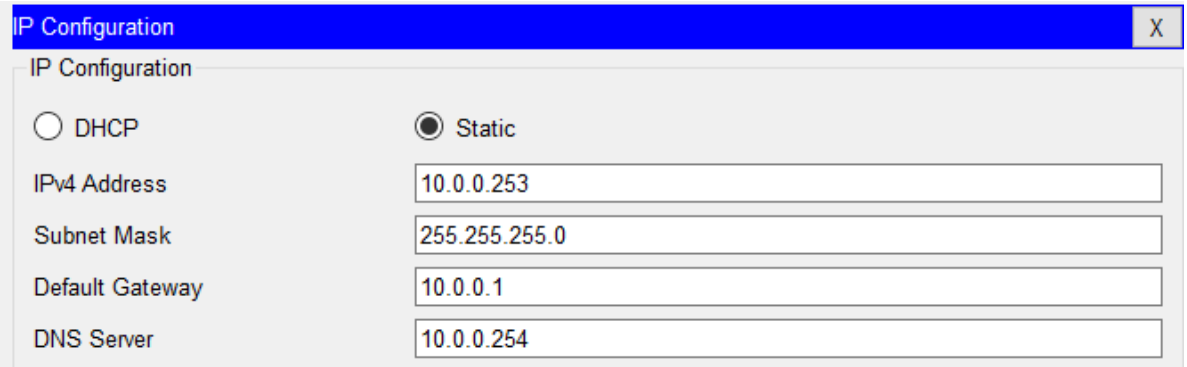

Рисунок 3.50 Конфігурація IoT сервера

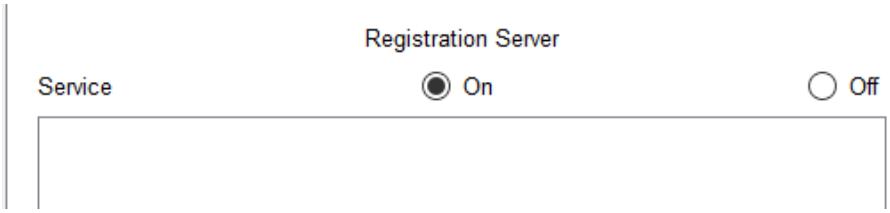

Рисунок 3.51 – Увімкнення IoT сервера

17) Асоціюємо IoT-пристрої з IoT-Server. Заходимо в налаштування веб-камери та підключаємо її до IoT-Server. Обираємо підключення через Remote Server. User Name та Password однакові admin. Після чого натискаємо клавішу Connect.

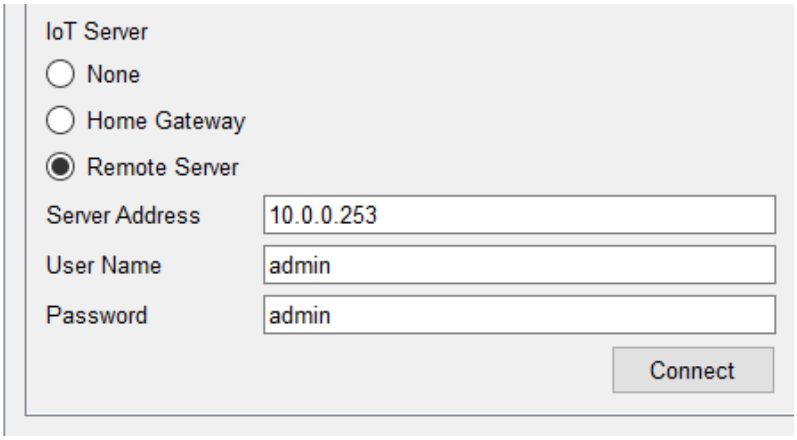

Рисунок 3.52 – Налаштування роботи розумних пристроїв на роботу з сервером

18) Перевіряємо підключення ноутбука до серверів командами ping

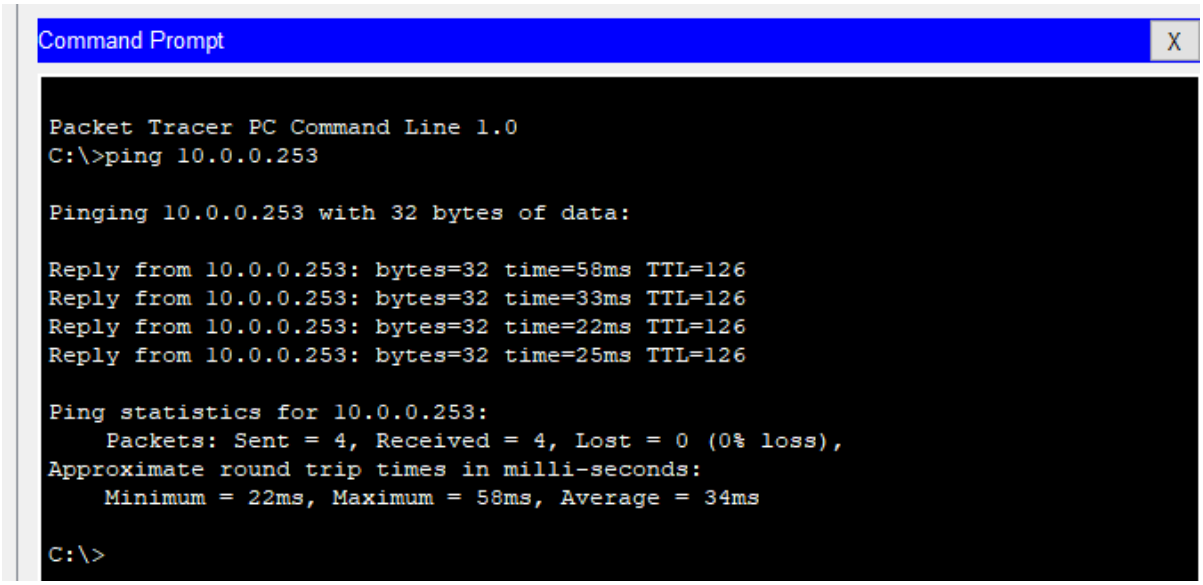

Рисунок 3.54 – Перевірка підключення ноутбука до серверів за допомогою команди ping

19) Заходимо в IoT monitor на ноутбуці. Міняємо адресу IoT Server 10.0.0.253 . Реєструємо новий сервер. Вводимо логін і пароль admin.

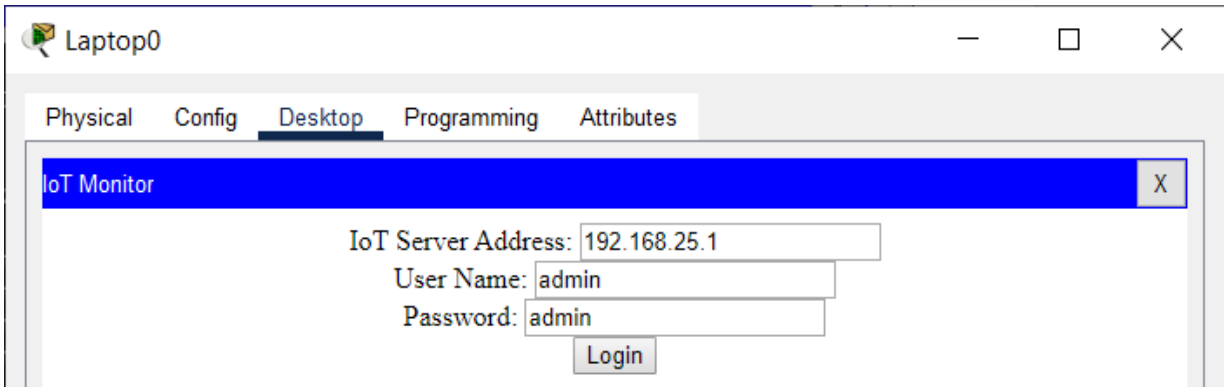

Рисунок 3.55 – Зміна адреси з 192.168.25.1 на 10.0.0.253

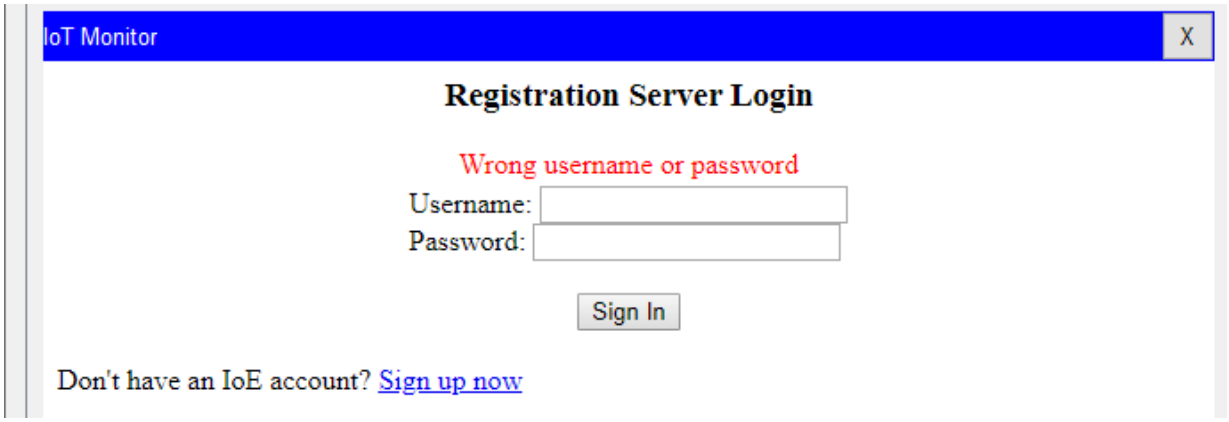

Рисунок 3.56 – Реєстрація нового сервера

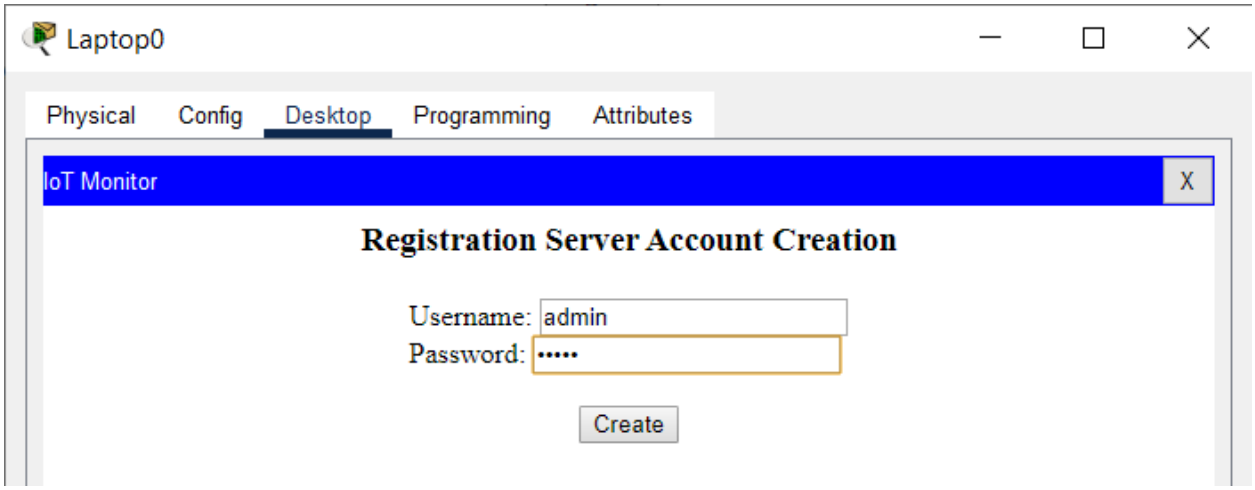

Рисунок 3.57 – Вхід у систему

20) Перевіряємо роботу усіх пристроїв з ноутбука та смартфону. Після входу до режиму моніторингу у вкладці Home мають відображатися усі пристрої, індикатори мають бути позначені зеленим кольором, що означає злагоджену роботу.

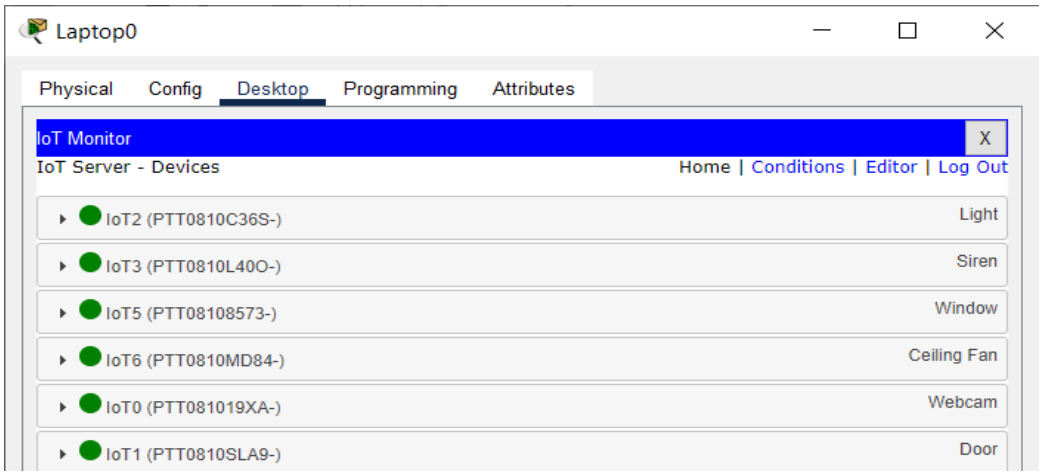

Рисунок 3.58 – Первірка підключення усіх пристроїв

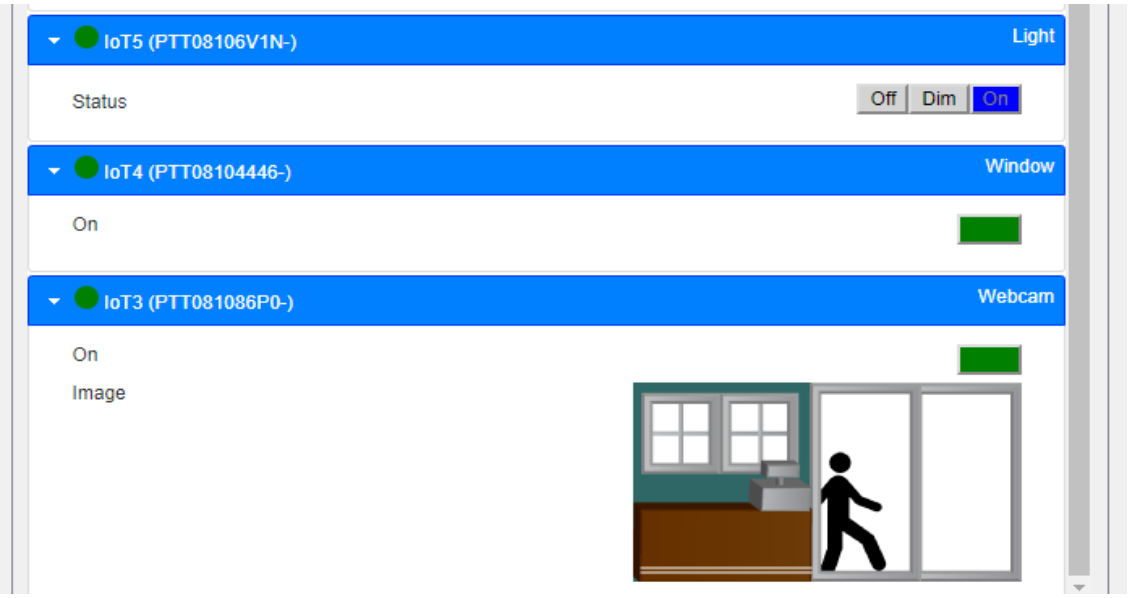

Рисунок 3.59 – Первірка підключення усіх пристроїв

21) Добавляємо адресу та ім’я www.ioe.org у конфігурації DNS-Server

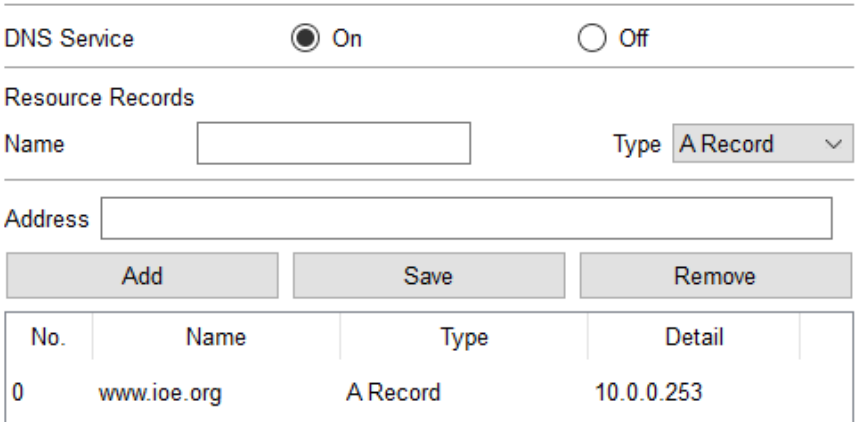

Рисунок 3.60 – Додавання адреси

22) Перевіряємо доступ з ноутбука та з смартфону за ім’ям www.ioe.org

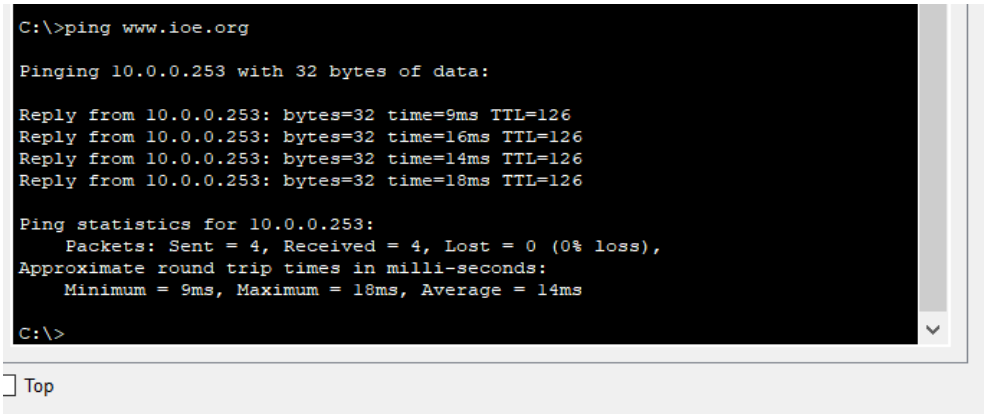

Рисунок 3.61– Первірка доступу з ноутбука

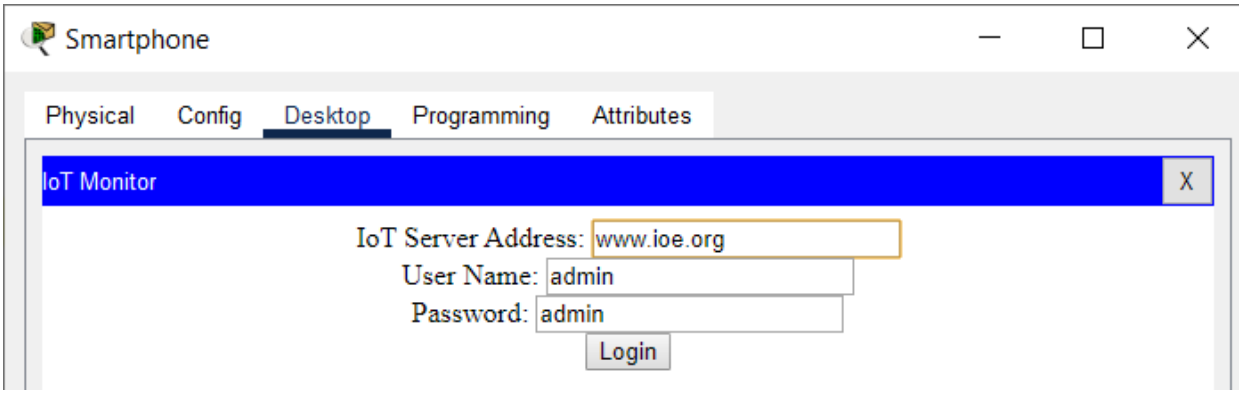

Рисунок 3.58 – Вхід до системи моніторингу за допомогою адреси www.ioe.org

ВИСНОВКИ

В ході даної дипломної роботи було розглянуто різні моделі побудови мереж з використанням сенсорних датчиків, які в свою чергу допомагають запобіганню уникнення та розповсюдження масштабу надзвичайної ситуації.

Також було запропоновано розглянути установку пожежного спринклеру, детектора диму та пожежі за допомогою мікроконтролера, запрограмованого мовою Python

Дана робота включає в себе взаємодія бездротових сенсорних мереж з мережами зв'язку загального призначення, таких як ZigBee та Wi-Fi

Оскільки неможливо передбачити кінцеві умови експлуатації, мережі повинні забезпечувати гнучкість і масштабованість залежно від кількості датчиків і щільності їх розміщення. Для забезпечення надійності рівень інтерференції повинен бути невисоким, і система повинна зберігати функціонування в разі відмови окремих вузлів. Підвищити надійність і зменшити затримку передачі можна за допомогою додаткових ресурсів, наприклад, за рахунок збільшення кількості бездротових каналів, збільшення кількості сусідніх пристроїв для кожного вузла, збільшення коефіцієнта посилення сигналу. При цьому зростає споживання, тому рекомендується проводити динамічний розподіл ресурсів.

Стандартні рішення забезпечують нечутливість до збоїв в ланцюзі постачань одного з постачальників, а також відповідають керівним принципам роботи, таким як безпека архітектури.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Информационные технологии и телекоммуникации. Электронный научный журнал. [Електронний ресурс]. – Режим доступу: https://www.sut.ru/doci/nauka/review/1-15.pdf

2. В.А. Бабошин, Е.А. Бубнова, Р.В. Ковальчук. Особенности использования технологии сенсорных сетей всистеме связи специального назначения. [Електронний ресурс]. – Режим доступу: http://www.npomars.com/db/ru/news/ofic_inf/178-2014-04-07/sec1/3.pdf
3. Шахнович И. Персональные беспроводные сети стандартов IEEE 802.15.3 и 802.15.4/И. Шахнович/Электроника наука технология бизнес, №6. – 2004
4. Jiang Q. Routing Protocols for Sensor Networks / Q. Jiang, D. Manivannan // IEEE Consumer Communications and Networking Conference (CCNC'04). - 2004.
5. В. А. Иваненко. Анализ протоколов передачи данных от узлов в беспроводных сенсорных сетях. Восточно-Европейский журнал передовых технологий, 2/10 (50)/2011. [Електронний ресурс]. – Режим доступу: https://cyberleninka.ru/article/n/analiz-protokolov-peredachi-dannyh-ot-uzlov-v-besprovodnyh-sensornyh-setyah/viewer
6. Silicon Laboratories, The Evolution of Wireless Sensor Networks, 2013. [Електронний ресурс]. – Режим доступу: https://www.silabs.com/documents/public/white-papers/evolution-of-wireless-sensor-networks.pdf
7. Н.П. Букин, Р.М. Полстянкин, И.А. Толкунов. Системы обработки информации, 2014, випуск№9 (125)
8. International Journal of Distributed Sensor Networks. Evolution of wireless sensor network design from technology centric to user centric: An architectual perspective, August 10, 2020. [Електронний ресурс]. – Режим доступу: https://journals.sagepub.com/doi/full/10.1177/1550147720949138
9. L. Yang , S.H. Yang and L. Plotnick. How the Internet of Things Technology Enhances Emergency Response Operations. School of Business and Economics, Loughborough University, Loughborough, LE11 3TU, UK, [Електронний ресурс]. – Режим доступу: https://core.ac.uk/download/pdf/288379003.pdf

10. Anthony M. Townsend /Mitchell L. Moss, Center for Catastrophe Preparedness and Response & Robert F. Wagner, Graduate School of Public Service New York University, April 2005 [Електронний ресурс]. – Режим доступу: https://reliefweb.int/sites/reliefweb.int/files/resources/nyu-disastercommunications1-final.pdf
11. Vandana Jindal, D.A.V College, Bathinda, History and Architecture of Wireless Sensor Networks for Ubiquitous Computing, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 2, February 2018 [Електронний ресурс]. – Режим доступу: http://ijarcet.org/wp-content/uploads/IJARCET-VOL-7-ISSUE-2-214-217.pdf
12. Dionisis Kandris, Christos Nakas , Dimitrios Vomvas and Grigorios Koulouras, Applications of Wireless Sensor Networks: An Up-to-Date Survey, 25 February 2020, [Електронний ресурс]. – Режим доступу: https://www.mdpi.com/2571-5577/3/1/14
13. Електронний журнал ELEC.RU, Особенности построения беспроводовых сенсорных сетей, [Електронний ресурс]. – Режим доступу: https://www.elec.ru/articles/osobennosti-postroenija-sensornykh-besprovodnykh-s/
14. Електронний журнал «Компьютер Пресс», Беспроводные сенсорные сети, 2018, [Електронний ресурс]. – Режим доступу: https://compress.ru/article.aspx?id=18943
15. Кучерявый, А. Е. Интернет вещей / А. Е. Кучерявый // Электросвязь. — № 1. — 2013. 34.
16. Кучерявый, А. Е. Самоорганизующиеся сети / А. Е. Кучерявый, А. В. Прокопьев, Е. А. Кучерявый // Издательство «Любавич». — СПб. — 2011.
17. Dr. Shu Yinbiao, Project Leader, MSB Member, SGCC Dr. Kang Lee, Project Partner, NIST, Wireless Sensor Networks project team, in the IEC Market Strategy Board. , [Електронний ресурс]. – Режим доступу: https://www.ipwea.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=e0619c58-f639-080a-86c2-055ae9c8af4d
18. Сергиевский М. Беспроводные сенсорные сети. Часть 1, 2, 3, 4 // Компьютер Пресс. – 2008. – №№ 4, 8, 11.
19. Національна доповідь про стан техногенної та природної безпеки в Україні у 2013 році. –: К.: УНДІЦЗ, 2014. – 542 с

20. IEEE Std 802.11s-2011, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 10: Mesh Networking, IEEE Computer Society, September 2011.
21. Y. Yu et al., "Supporting concurrent applications in wireless sensor networks," In proceedings of the 4th International Conference on Embedded Networked Sensor Systems, SenSys'06, Boulder, Colorado, 2006, pp.139-152