

**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**ІМЕНІ ТАРАСА ШЕВЧЕНКА**

**ФАКУЛЬТЕТ РАДІОФІЗИКИ ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ**

**Кафедра радіотехніки та радіоелектронних систем**

До захисту допущено:

«На правах рукопису»

Завідувач кафедри \_\_\_\_\_ Ігор АНІСІМОВ

18 травня 2023 р.

**КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА**

на тему:

**«Інтелектуальна мережа: розробка розумного будинку  
з допомогою Cisco Packet Tracer 8.2»**

**Виконав:**

студент 2-го курсу магістратури  
денної форми навчання  
спеціальності 172 Телекомунікації та радіотехніка  
ОНП «Інформаційна безпека телекомунікаційних систем і мереж»  
Пасічник Андрій Миколайович \_\_\_\_\_

**Науковий керівник:**

к.т.н., ас. Муштак Аль Шурайфі \_\_\_\_\_

**Рецензент:**

д. т. н., проф. Хлапонін Юрій Іванович \_\_\_\_\_

Засвідчую, що у цій магістерській роботі  
немає запозичень з праць інших авторів без  
відповідних посилань

Студент \_\_\_\_\_

Робота допущена до захисту в ЕК рішенням кафедри радіотехніки та радіоелектронних систем від 18 травня 2023 р., протокол № 18.

Завідувач кафедри радіотехніки та радіоелектронних систем,  
доктор фіз.-мат. наук, професор  
Анісімов Ігор Олексійович \_\_\_\_\_

## ЗМІСТ

ВСТУП .....	3
РОЗДІЛ 1. РОЗУМНИЙ БУДИНОК .....	4
1.1 Що таке розумний будинок.....	4
1.2 Огляд протоколів управління «розумним будинком».....	6
1.2.1 Wi-Fi .....	7
1.2.2 Z-Wave .....	9
1.2.3 ZigBee .....	11
1.2.4 Bluetooth .....	15
1.2.5 Комунікаційна шина KNX.....	18
1.3 Постановка задачі роботи .....	20
РОЗДІЛ 2. Вибір методу вирішення завдань дипломного проекту .....	22
2.1 Огляд можливостей для моделювання в cisco packet tracer.....	22
2.2 Можливості мови Python для мікроконтролерів.....	25
2.3 Можливості мови JavaScript для мікроконтролерів.....	27
2.4 Можливості мови Blockly для мікроконтролерів .....	28
РОЗДІЛ 3. Програмна реалізація «розумного будинку» у симуляторі Cisco Packet Tracer 8.2.....	30
3.1 Система безпеки гаражу і освітлення.....	30
3.2 Система моніторингу пожежі та диму.....	35
3.3 Система пожежної сигналізації.....	38
3.4 Розумний будинок.....	41
Висновки.....	50
Список використаних джерел.....	51

## ВСТУП

**Актуальність роботи.** Тема розумного будинку актуальна, оскільки він дозволяє домогосподарству стати більш енергоефективним, дозволяє користувачам економити час і виконувати різні задачі дистанційно ( можливість керування пристроями розумного будинку з девайсів поза будинком) . Розумний будинок важливий через комфорт і безпеку , яку він забезпечує. Він максимально покращує, спрощує та автоматизує життя людини.

**Об'єкт роботи.** Дослідження процесів безпеки в інтелектуальній мережі «Розумний будинок».

**Предмет роботи.** Безпека в інтелектуальній мережі Розумний будинок за допомогою Cisco Packet Tracer 8.2.

**Мета роботи.** Покращення якості життя за рахунок забезпечення комфорту (можливість управління пристроями з телефону), безпеки (спостереження з камери за будинком, оповіщення в разі пожежі чи задимлення, попередження надзвичайних ситуацій).

## РОЗДІЛ 1

### РОЗУМНИЙ БУДИНОК

#### 1.1 Що таке розумний буднок

З появою нових гаджетів, які роблять управління будинком простішим і зручнішим, будинки, в яких широко використовуються розумні технології, тепер називають "розумними". В цьому розділі пояснюється, як працює розумний будинок і які його переваги та недоліки [1].

Розумний дім - це концепція житла, яка базується на використанні сучасних технологій для автоматизації різноманітних систем і пристроїв в будинку. Головною ідеєю є створення зручної і комфортної обстановки в будинку для мешканців.

У розумному домі можуть бути встановлені різні "розумні" системи, які дозволяють здійснювати управління електроприладами, опаленням, кондиціонуванням повітря, освітленням та іншими системами. Крім того, такі системи можуть контролювати безпеку в будинку, наприклад, за допомогою камер відеоспостереження, датчиків руху та інших пристроїв.

Зазвичай до центру управління розумного будинку [1,2] може підключатися велика кількість пристроїв.

Основними елементами Smart Home є:

1. Керування освітленням та жалюзі: здійснюється за допомогою датчиків руху та освітлення, або за допомогою телефону чи голосових команд.
2. Керування опаленням та кондиціонуванням повітря: встановлюються термостати, які можуть налаштовувати температуру в будинку в залежності від погодних умов або інших факторів.
3. Керування безпекою: встановлюються системи безпеки, які дозволяють контролювати доступ до будинку, а також використовують камери відеоспостереження, які надсилають відеозапис на смартфон чи комп'ютер.

4. Керування водопостачанням: встановлюються системи автоматичного вимикання водопостачання в разі виявлення протікання.
5. Керування енергоспоживанням: встановлюються системи, які дозволяють відстежувати та оптимізувати споживання електроенергії в будинку.
6. Розважальні системи: встановлюються домашні кінотеатри, аудіосистеми, системи звукової і графічної техніки та інші розважальні пристрої, якими можна керувати за допомогою пульта дистанційного керування чи голосу.

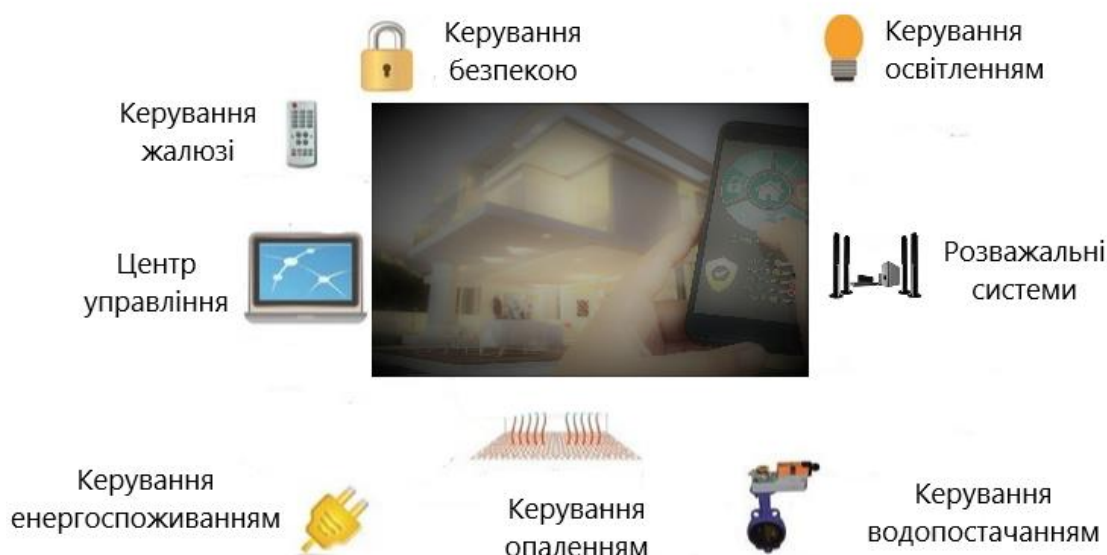


Рис. 1.1. Основні елементи Smart Home

З рис. 1.1 видно що до основних елементів розумного будинку входять: системи керування безпекою, освітленням та жалюзі, енергоспоживанням, опаленням, водопостачанням, розважальні системи та центр управління .

Управління системами може здійснюватися за допомогою голосових команд, мобільних додатків або ж кнопок на спеціальних пультах. Додатково можна налаштувати автоматичне виконання різних дій в залежності від певних умов, наприклад, включення світла в кімнаті при вході в неї або вимкнення під час виходу.

## **Переваги технології**

Переваги розумних будинків:

1. Можливість дистанційного вмикання та вимикання пристроїв. Виробники розумної техніки створюють спеціальні додатки, які потрібно встановити на смартфон для роботи зі смарт-приладом, не залежно від місця перебування власника.
2. Голосове керування. Вам навіть не доведеться вставати з дивана, щоб вимкнути світло, приготувати каву або вимкнути мультиварку.
3. Автоматичне оновлення. Смарт-пристрої мають модуль Wi-Fi, завдяки чому можуть оновлюватись автоматично, не вимагаючи втручання господарів.
4. Запобігає аварійним ситуаціям до того, як вони трапляться. У разі витoku газу, протікання води або пожежі система швидко відреагує і надішле сповіщення на ваш смартфон.

## **Недоліки технології**

Основним недоліком систем розумного будинку є висока вартість обладнання та різноманітних датчиків, що особливо неприємно, коли дороге обладнання виходить з ладу і потребує ремонту.

Ще одним недоліком є складність монтажу. Електрик або ремонтник без необхідного досвіду часто може заплутатися, тому необхідно вибирати майстра, який займався встановленням систем розумного будинку і точно знає, як це робити. Розумні будинки повинні працювати безперебійно і точно, оскільки всі елементи таких систем взаємопов'язані, і під час монтажу не повинно бути ні найменшої помилки.

Певні елементи розумного будинку повинні бути встановлені ще на етапі проектування та облаштування квартири. До них відносяться прокладка комунікаційних кабелів, установка розумного освітлення і регулювання температури [3].

### 1.2 Огляд протоколів управління «розумним будинком»

### 1.2.1 Wi-Fi

Wi-Fi - найпоширеніша технологія бездротового зв'язку, яка налічує мільярди користувачів у всьому світі. За даними галузевого консорціуму Wi-Fi Alliance, близько половини світового інтернет-трафіку передається за допомогою цього стандарту. Wi-Fi широко використовується в приватних будинках, офісах і громадських місцях. Найчастіше технологія використовується для підключення комп'ютерів, смартфонів і планшетів до глобальної мережі. Технічно Wi-Fi можна використовувати для з'єднання двох пристроїв з точки в точку та обміну інформацією між ними. Здається, що це ідеальна технологія для об'єднання в мережу різних пристроїв Інтернету речей і як основа для "розумних" будинків [4] [5]. Однак, незважаючи на те, що протягом багатьох років ведеться запекла війна за стандарти мережевих технологій для розумних будинків, Wi-Fi залишається поза увагою аутсайдерів. Більшість великих постачальників рішень не включили його в топ-список технологій, які претендують на лідерство на ринку домашньої автоматизації.

Технологія Wi-Fi базується на сімействі стандартів бездротових мереж IEEE 802.11x. Цей стандарт визначає лише перші два рівні моделі OSI (фізичний і каналний); мережі Wi-Fi мають топологію "зірка", що означає, що всі вузли підключаються безпосередньо до центрального елемента - бездротового маршрутизатора. Така топологія дозволяє додавати або видаляти кінцеві пристрої з мережі, не впливаючи на структуру мережі або цілісність передачі даних. Однак такий підхід створює унікальну точку відмови.

З точки зору мережевого і транспортного рівнів, Wi-Fi зазвичай використовує інші стандартні протоколи. Він використовує UDP або TCP для транспортного рівня і IPv4 або IPv6 для мережевого рівня. А прикладний рівень стосується сумісності пристроїв, взагалі не визначений і повністю відданий виробникам програмних або апаратних рішень.

#### **Переваги Wi-Fi**

Wi-Fi є одним з найпопулярніших протоколів бездротового зв'язку в розумних домах і має декілька переваг:

**Бездротовий доступ до Інтернету:** Wi-Fi дозволяє підключатися до Інтернету без проводів, що зручно для мобільних пристроїв і дає можливість контролювати домашні пристрої з будь-якої точки світу.

**Зручність встановлення:** Wi-Fi дуже простий у встановленні і налаштуванні, тому що не потребує проводів і спеціальної інфраструктури.

**Надійність:** Wi-Fi має високий рівень стабільності і надійності, що дозволяє забезпечити безперебійне підключення до Інтернету і контроль за домашніми пристроями.

**Широка підтримка:** Wi-Fi є стандартним протоколом для бездротового зв'язку, тому що його підтримують практично всі сучасні мобільні пристрої, комп'ютери і роутери.

**Висока швидкість передачі даних:** Wi-Fi може передавати дані з високою швидкістю, що дозволяє здійснювати контроль за домашніми пристроями у реальному часі і забезпечує швидку передачу відео та аудіо.

**Невисока вартість:** Wi-Fi має дуже низьку вартість, що дозволяє його використовувати для підключення до Інтернету і контролю за домашніми пристроями за доступну ціну.

Загалом, Wi-Fi є зручним, надійним і широко підтримуваним протоколом для бездротового зв'язку в розумних будинках і має багато переваг перед іншими технологіями.

### **Недоліки Wi-Fi в розумному будинку**

Протокол Wi-Fi є одним з найбільш поширених технологій бездротового зв'язку в розумних будинках. Однак, як і будь-яка технологія, він має свої недоліки. Ось кілька з них:

1. **Обмежена покриття мережі:** Wi-Fi є обмеженим у покритті мережі великих будинків або на вулиці, особливо в зонах з великою кількістю перешкод, таких як стіни, двері та інші перешкоди.
2. **Недостатня пропускна здатність:** Wi-Fi може бути обмеженим у

пропускній здатності, що може вплинути на швидкість передачі даних, особливо в тому випадку, якщо ви користуєтеся багатьма пристроями одночасно.

3. Незахищеність: Wi-Fi є вразливим до зламування, особливо якщо ви не застосували достатньо сильний пароль. Це може призвести до зламування вашої мережі і крадіжки конфіденційної інформації.
4. Вплив на здоров'я: Відомо, що електромагнітні хвилі від Wi-Fi можуть впливати на здоров'я людей, особливо на дітей, які можуть бути більш вразливими до їх впливу.
5. Висока споживання електроенергії: Wi-Fi може вимагати значної кількості електроенергії, що може збільшити розмір вашого рахунку за електроенергію.

Отже, перед тим, як вибрати Wi-Fi для розумного будинку, важливо враховувати його недоліки і вибрати найкращий варіант [6].

### 1.2.2 Z-Wave

Z-wave - це протокол бездротового зв'язку, спеціально розроблений для мереж розумних будинків, розроблений компанією Zensys в Данії в 1999 році, представлений в США в 2002 році і розроблений для мереж розумних будинків в США в 2003 році. Зі зростанням кількості "розумних" будинків Z-wave став фактичним бездротовим рішенням для домашньої автоматизації. В даний час на світовому ринку представлено понад 3000 продуктів з підтримкою Z-wave і більше 100 мільйонів пристроїв Z-wave, що працюють в "розумних" будинках по всьому світу.

Z-wave використовує низькоенергетичні радіохвилі в діапазоні частот ISM 800-900 МГц для передачі даних між пристроями зі швидкістю 100 Кбіт/с. Ця бездротова мережа має радіус дії 40 метрів і може використовувати до чотирьох вузлів для розширення. Передаючи дані на більші відстані за допомогою хвиль з низькою енергією та оптимізованою швидкістю передачі

даних, Z-wave є ідеальним рішенням для пристроїв домашньої автоматизації порівняно з Wi-Fi та Bluetooth. Майже всі типи систем керування та датчиків, такі як керування освітленням, дистанційно керовані замки, розумні клавіатури, керування опаленням, відкривання гаражних воріт тощо, можуть використовувати Z-wave для передачі даних; обладнання для домашньої автоматизації може підтримувати Z-wave за допомогою цього чіпа.

Мережа Z-wave складається з двох типів пристроїв: контролерів/головних і підлеглих. Контролер зазвичай є шлюзом Z-wave, який контролює передачу даних між іншими вузлами і підключений до Інтернету. Контролер попередньо запрограмований з мережевим ідентифікатором HomeID. Це 32-бітний ідентифікатор, який ідентифікує конкретну мережу Z-wave. Ведені пристрої вводяться в мережу шляхом призначення NodeID, а також HomeID, NodeID - це 8-бітний ідентифікатор, який ідентифікує конкретний Z-wave вузол або пристрій в мережі. Присвоєння NodeID, HomeID (унікальний для конкретного Z-wave унікальний для конкретної мережі Z-wave), процес введення веденого пристрою в мережу називається "активація". Якщо підлеглий пристрій потрібно видалити з мережі, HomeID та NodeID буде видалено з підлеглому пристрою, а пристрій буде скинуто до заводських налаштувань.

Z-wave використовує радіочастоти в діапазоні 800-900 МГц. Фактична частота залежить від країни, в якій використовується пристрій.

Пристрої Z-wave можуть взаємодіяти один з одним, лише якщо вони мають однаковий HomeID. Два підлеглих пристрої Z-wave з різними ідентифікаторами HomeID належать до різних мереж Z-wave і не можуть взаємодіяти один з одним. Контролер з певним попередньо запрограмованим HomeID підтримує таблицю маршрутизації для управління передачею даних між дійсними вузлами, тобто пристроями Z-wave в мережі Z-wave з використанням топології комірчастої мережі. Таким чином, пристрої (ведені) не повинні бути підключені до контролера для зв'язку з іншими пристроями (введеними) в мережі. Вони можуть спілкуватися безпосередньо один з одним.

Деякі Z-wave пристрої також передають власні Z-wave сигнали. Такі пристрої є пристроями, що підключаються і діють як ретранслятори. За допомогою цих пристроїв Z-wave контролер може зв'язуватися з пристроями за межами свого початкового діапазону. Зазвичай, Z-wave пристрої не можна підключити безпосередньо до інтернету. Вони можуть підключатися до Інтернету тільки через контролер, який також є Z-wave-шлюзом до Інтернету.

Протокол Z-wave розроблений для розумних будинків і найкраще підходить для цього сегменту. На відміну від інших стандартів бездротового зв'язку, призначених для ширшого застосування, Z-wave призначений для домашньої автоматизації та подібних застосувань. Z-wave пропонує оптимізовану швидкість передачі даних на великі відстані, топологію комірчастої мережі і повну функціональну сумісність, а як бездротове рішення Z-wave підтримує достатню кількість вузлів, щоб бути придатним для додатків "розумного будинку" [6].

### **Переваги Z-Wave**

- Популярний серед багатьох пристроїв розумного будинку;
- Безпечна передача;
- Низький рівень перешкод;
- Сумісний з різними пристроями.

### **Недоліки протоколу Z-Wave**

- Потрібен хаб для керування пристроями;
- Існує максимальна кількість пристроїв, які можна підключити до одного хабу;
- Закрита система [7] .

#### **1.2.3 ZigBee**

Zigbee була розроблена для мереж управління і сенсорних мереж, що використовують стандарт IEEE 802.15.4 для бездротових персональних мереж (WPAN) і є продуктом Zigbee Alliance. Він визначає фізичний рівень і рівень

керування доступом до середовища (MAC) для роботи з декількома пристроями на низьких швидкостях передачі даних. Zigbee WPAN працює на частотах 868 МГц, 902-928 МГц і 2,4 ГГц; швидкість передачі даних 250 Кбіт/с найкраще підходить для переривчастої і проміжної двосторонньої передачі даних між датчиками і контролерами.

Zigbee - це дешева, малопотужна комірчаста мережа, яка широко використовується в системах управління та моніторингу в діапазоні від 10 до 100 метрів. Ця система зв'язку дешевша і простіша, ніж інші бездротові сенсорні мережі малого радіусу дії (Bluetooth і Wi-Fi).

Zigbee підтримує різні мережеві конфігурації, включаючи зв'язок "майстер-майстер" і "майстер-підлеглий". Мережі Zigbee можуть бути розширені за допомогою маршрутизаторів, що дозволяє декільком вузлам підключатися один до одного, щоб створити ширшу мережу.

Технологія Zigbee працює в поєднанні з цифровими радіостанціями, що дозволяє різним пристроям спілкуватися один з одним. Пристроями, що використовуються в цій мережі, є маршрутизатори, координатори та кінцеві пристрої. Основна функція цих пристроїв - передавати інструкції та повідомлення від координатора до окремих пристроїв, наприклад, лампочок.

У цій мережі координатор є найважливішим пристроєм на чолі системи. У кожній мережі є лише один координатор, який використовується для виконання різних завдань. Координатор не тільки сканує канали, але й обирає найбільш підходящий канал з найменшим рівнем перешкод і присвоює унікальну адресу та ідентифікатор кожному пристрою в мережі, щоб можна було надсилати повідомлення або інструкції в межах мережі.

Маршрутизатори розташовані між координатором і кінцевими точками і відповідають за маршрутизацію повідомлень між різними вузлами. Маршрутизатори отримують повідомлення від координатора і зберігають їх доти, доки кінцева точка не буде готова їх отримати. Маршрутизатори також можуть дозволяти іншим кінцевим пристроям підключатися до мережі так само, як і маршрутизатори.

Ця мережа дозволяє кінцевим пристроям контролювати невеликі фрагменти інформації за допомогою зв'язку з головним вузлом, таким як маршрутизатор або координатор, залежно від типу мережі Zigbee. Кінцеві пристрої не спілкуються безпосередньо один з одним. Спочатку весь трафік може бути направлений на батьківський вузол, наприклад, маршрутизатор, який зберігає ці дані до тих пір, поки кінцевий пристрій не зможе їх переслати. Кінцеві пристрої використовуються для запиту будь-яких повідомлень, очікуваних від батьківського вузла.

Структура системи Zigbee складається з трьох пристроїв: координаторів, маршрутизаторів і кінцевих пристроїв. Кожна мережа Zigbee складається з одного координатора, який виступає в ролі кореня і моста мережі. Координатор відповідає за обробку та зберігання інформації під час прийому та передачі даних.

Маршрутизатор діє як проміжний пристрій, і дані можуть передаватися на інші пристрої через пристрій та передавати з них. Зрештою, можливість зв'язку пристрою та батьківського блоку обмежена, що допомагає заощадити акумулятор. Кількість маршрутизаторів, координаторів та кінцевого пристрою залежить від типу мережі, наприклад, зірки, дерева або комірчастої мережі.

Архітектура протоколу складається зі стека різних рівнів, з IEEE 802.15.4, визначеного на фізичному рівні, і рівня MAC, який доповнюється мережевим рівнем самого протоколу Zigbee і інтеграцією прикладного рівня.

Фізичний рівень: рівень виконання модуляційних та демодуляційних функцій при передачі та отримання сигналів.

Рівень MAC: Цей рівень забезпечує надійну передачу даних за допомогою CSMA, отримуючи доступ до різних мереж. Цей рівень також надсилає маркер листа для синхронно спілкування.

Мережевий рівень: Цей рівень виконує всі функції, пов'язані з мережею, такі як конфігурація мережі, підключення та відключення кінцевих пристроїв до мережі, маршрутизація та конфігурація пристроїв.

Підрівень підтримки додатків: Цей рівень дозволяє об'єктам пристроїв

Zigbee та об'єктам додатків взаємодіяти з мережевим рівнем для надання послуг з управління даними. Цей рівень відповідає за сполучення двох пристроїв відповідно до їхніх послуг і потреб.

Інфраструктура додатків: надає два типи послуг передачі даних у вигляді пар ключ-значення і спільних служб обміну повідомленнями. Загальне повідомлення - це структура, визначена розробником, тоді як пара ключ-значення використовується для отримання атрибутів з об'єкта додатку. ZDO забезпечує інтерфейс між об'єктом додатку і рівнем APS пристрою Zigbee. ZDO - це служба, яка забезпечує роботу інших пристроїв і відповідає за виявлення, завантаження і підключення їх до мережі.

Zigbee підтримує різні мережеві топології, найбільш часто використовувані конфігурації - топологія "зірка", топологія "сітка" і топологія "кластер". Кожна топологія складається з одного або декількох координаторів. Топологія "зірка" складається з одного координатора, який відповідає за завантаження і керування пристроями в мережі. Всі інші пристрої називаються кінцевими і взаємодіють безпосередньо з координатором [8] .

### **Переваги**

Низьке споживання енергії: ZigBee характеризується дуже низьким енергоспоживанням обладнання. Це робить його придатним для пристроїв з живленням від батарей, таких як камери спостереження.

Низька затримка: ZigBee має низьку затримку, а це означає, що швидкі дані, такі як зображення та відео, можуть легко передаватися.

Надійний захист: ZigBee використовує надійні алгоритми шифрування та аутентифікації для захисту даних від кіберзагроз.

Інтероперабельність: До Альянсу ZigBee входять різні виробники пристроїв ZigBee, що гарантує надійну роботу вашого пристрою з іншими пристроями ZigBee.

Простота встановлення: Пристрої ZigBee легко встановлювати, оскільки їх можна використовувати з широкодоступними Wi-Fi і Z-Wave шлюзами та системами домашньої автоматизації.

## Недоліки

Обмежений радіус дії: пристрої ZigBee мають обмежений радіус дії і можуть підключатися лише до інших пристроїв ZigBee.

Пристрої ZigBee мають обмежену пропускну здатність: Пристрої ZigBee менш сумісні і можуть обмінюватися даними лише з іншими пристроями ZigBee. Це може бути недоліком для деяких користувачів, особливо якщо вони хочуть підключити пристрої ZigBee до таких пристроїв, як хости Wi-Fi або комп'ютери [9] .

### 1.2.4 Bluetooth Low Energy

Він використовує радіохвилі, щоб змусити пристрої спілкуватися один з одним. Але він має набагато більш обмежений діапазон, ніж два попередніх протоколи.

Bluetooth охоплює всі рівні базової моделі OSI, від фізичного до прикладного. Група спеціальних інтересів Bluetooth (SIG), яка здійснює нагляд за розробкою та ліцензуванням Bluetooth, має рідкісний привілей вносити прямі та незалежні зміни до стандарту.

BLE фокусується на передачі даних невеликими пакетами і зменшенні часу автономної роботи пристроїв в робочому режимі. Цим він відрізняється від класичного Bluetooth, до якого ми звикли, де пристрої BLE підключаються один до одного тільки тоді, коли їм потрібно надсилати та отримувати дані.

На прикладному рівні забезпечує сумісність між рішеннями різних виробників. Цей принцип був запозичений з оригінальної класичної специфікації Bluetooth. Це дозволяє виробникам застосовувати необхідні профілі до своїх пристроїв і забезпечує сумісність з іншими продуктами Bluetooth Smart, що підтримують ту ж саму специфікацію.

Слід також зазначити, що кілька профілів можуть бути інтегровані в одне рішення, що дозволяє розробникам гнучко налаштовувати функціональність своїх пристроїв. Однак пристрої від різних розробників

можуть повноцінно взаємодіяти лише тоді, коли вони мають принаймні один спільний профіль.

### **Переваги**

Bluetooth Low Energy - технологія з низьким енергоспоживанням, але з високою швидкістю передачі даних до 1 Мбіт/с (у новій версії Bluetooth 5 - 2 Мбіт/с). Чим вища швидкість, тим більше даних можна передати за одиницю часу. Це означає, що передавачі Bluetooth можуть швидше випускати сигнали, зменшуючи ймовірність зіткнень. Це важливо при роботі в дуже перевантажених частотних діапазонах, таких як 2,4 ГГц.

Bluetooth Smart підтримує сплячі вузли (пристрої, які проводять більшу частину свого часу в неактивному стані, періодично «прокидаючись» для виконання завдання на короткий проміжок часу, а потім негайно повертаючись до режиму сну), що забезпечує достатню, хоча й не провідну в галузі, термін роботи батареї та дозволяє певним датчикам і виконуючим пристроям працювати протягом року або більше від невеликої батареї планшета.

Крім того, Bluetooth Smart має цікаву функцію, якої немає в жодній із розглянутих вище технологій. Її називають маяками; використовуючи можливості наближення Bluetooth, маяки можуть змусити смартфон виконувати певні дії, коли користувач знаходиться поблизу. Маяки дозволяють використовувати різні унікальні програми, такі як push-сповіщення на основі місцезнаходження та служби точного позиціонування. Особливо важливою є можливість передавати функціональні можливості маяка на інтелектуальні пристрої з підтримкою Bluetooth за допомогою лише кількох рядків коду, доданих до стеку програмного забезпечення.

Здатність пристроїв Bluetooth визначати близькість можлива через прямий зв'язок між інтелектуальними пристроями та смартфонами. Це найбільша перевага Bluetooth: з бездротових технологій, що використовуються в IoT, лише Bluetooth і Wi-Fi спочатку сумісні майже з усіма смартфонами, планшетами і ноутбуками. Однак Wi-Fi, окрім того, що

не підходить для більшості додатків IoT, вимагає, щоб усі комунікації проходили через центральну точку доступу. Тільки Bluetooth дає пряме з'єднання між телефоном і пристроєм. Це велика перевага, адже лише за допомогою спеціального додатку гаджет може стати «дистанційним дисплеєм» для інтелектуальної домашньої мережі розумних пристроїв. Ця топологія дозволяє дуже легко додавати нові пристрої до існуючої мережі: з Bluetooth усі дії спрощені, інтуїтивно зрозумілі та безпечні.

### **Недоліки**

Bluetooth використовує той самий діапазон 2,4 ГГц, що й інші бездротові технології, охоплюючи не лише вищезгадані протоколи, а й численні пристрої, такі як бездротові телефони та мікрохвильовки. Незважаючи на те, що Bluetooth оснащений інструментами (технологією адаптивного перемикавання частоти, яка дає можливість динамічного перемикавання між 40 іншими каналами під час передачі даних), запровадження діапазону частот 2,4 ГГц є певним недоліком. На додаток до того факту, що радіохвилі в діапазоні 2,4 ГГц завжди створюють перешкоди при проходженні крізь стіни та інші перешкоди, включно з людськими тілами, оскільки вони затухають швидше, ніж частоти нижче 1 ГГц, є ще один серйозний недолік.

З тієї ж причини діапазон, у якому переважає технологія BLE, невеликий. Незважаючи на радіус дії до 100 метрів у зоні прямої видимості, Bluetooth версії 4 може планувати відстань до 10 метрів під час роботи двох пристроїв у приміщенні. Це число регулюється не тільки перешкодами, які стоять на шляху розповсюдження сигналу, але й опціями виробника, такими як Bluetooth Smart, наприклад, де є можливість регулювати потужність сигналу пристроїв у певному діапазоні (наприклад збільшення вихідної потужності та споживання електроенергії), що, здається, додає турбот.

Головним недоліком BLE є конкуренція в діапазоні частот 2,4 ГГц з Wi-Fi та іншою побутовою технікою.

Основна причина, чому Bluetooth Smart, який був навмисно створений, щоб відповідати викликам швидко зростаючого ринку Інтернету речей,

буквально не розглядається як варіант для потужного впровадження Інтернету речей, включаючи створення великих мереж домашньої автоматизації. Фактично, він був розроблений для підтримки відносно простих сітчастих мереж із зіркоподібною топологією. Mesh-мережі вважаються необхідною топологією для багатьох додатків, особливо тих, які потребують більш ширшого спектру та однорангового зв'язку між пристроями. Тому всі відомі протоколи в категорії низької пропускної здатності маршрутизують повідомлення через сітчасті мережі. Однак Bluetooth, за рідкісним винятком, представленим декількома пропрієтарними рішеннями (і несумісними одне з одним), не пропонував цю функціональність [10-11].

#### 1.2.5 Комунікаційна шина KNX

KNX (KONNEX) - це технологія, яка керує автоматизацією критично важливих функцій у всіх житлових, комерційних і промислових установках, включаючи системи опалення, вентиляції та кондиціонування повітря, системи освітлення, мультимедіа, безпеки та управління енергоспоживанням [12].

Для того, щоб надсилати керуючі дані всім елементам управління будівлею (або пристроям/функціям розумного будинку), необхідна система, яка дозволяє уникнути проблеми ізольованих пристроїв, що розмовляють "різними мовами".

Пристрої KNX можуть керувати освітленням, жалюзі та ролетами, опаленням, вентиляцією та кондиціонуванням, системами безпеки, енергоменеджментом, аудіо-відео, приладами, моніторами, пультами дистанційного керування та багато іншого.

Крім того, KNX є єдиним у світі відкритим стандартом для управління будинком і будівлею відповідно до EN 50090, EN 13321-1 і ISO/IEC 14543.

На відміну від пропрієтарних протоколів, KNX є відкритим глобальним стандартом, в якому понад 300 виробників випускають продукти, що

безперешкодно спілкуються та співпрацюють один з одним.

KNX працює, дозволяючи всім компонентам, пристроям, функціям і особливостям будівлі (або зовнішнього простору) спілкуватися безпосередньо і віддалено на спільній мові.

Шина KNX - це головна центральна нервова система для всього обладнання для автоматизації: шина KNX - це зелений кабель, який встановлюється поряд зі звичайною електромережею в нових будівлях і під час реконструкції.

Всі різні технічні компоненти будівлі з'єднуються один з одним через шину KNX відповідно до стандарту KNX для автоматизації будівель.

Система проводки контролюється датчиками, детекторами та параметрами, якими кінцевий користувач може легко керувати за допомогою ноутбука, смартфона або планшета.

Шина KNX працює паралельно з електроживленням всіх пристроїв і систем в мережі:

Датчики (кнопки, термостати, анемометри, датчики руху тощо) збирають інформацію та надсилають її на шину у вигляді інформаційних повідомлень.

Виконавчі пристрої (регулятори освітленості, опалювальні клапани, монітори) отримують телеграми даних і перетворюють їх у дію.

Логічні функції, такі як контролери (наприклад, контролери температури в приміщенні, контролери жалюзі).

### **Переваги**

Ця технологія не асоціюється з будь-яким конкретним брендом або виробником. Існує багато сертифікованих виробників, і їх кількість зростає з кожним роком.

Децентралізована, тобто немає центрального елемента управління, і система продовжить працювати навіть у разі виходу з ладу одного блоку (якщо система розумного будинку має кілька джерел живлення).

Перевірена, перспективна і високонадійна технологія.

Її можна розширити за допомогою інших технологій. Завдяки популярності цієї системи, всі виробники випускають модулі розширення для шини KNX.

Кабелі (шинні кабелі) можуть бути використані для інших рішень автоматизації.

Система використовує топологію "зірка", де кожен пристрій підключається безпосередньо до плати живлення.

Існує багато систем управління або віртуалізації (управління розумним будинком) під Android, iOS тощо.

### **Недоліки**

Встановлення програмного забезпечення KNX ETS вимагає наявності досвідчених і кваліфікованих інсталяторів/інтеграторів та ліцензій. Хоча це дійсно так, це не тільки забезпечує якість виконаних робіт, але й подальше обслуговування системи.

Початкова інсталяція може бути дорогавартісною. Це пов'язано з вартістю програмного забезпечення, навчання та сертифікації[13].

### 1.3 Постановка задачі роботи

Провівши теоретичне дослідження «розумних будинків» можна стверджувати, що ми опинимося в ідеально організованій та продуманій екосистемі розумних пристроїв, які спілкуються між собою, щоб покращити, спростити та зробити безпечнішим наше життя. Тому постановку задачі для дипломного проекту формулюємо наступним чином:

- дослідити принципи проектування інтелектуальної мережі «Розумний будинок»;
- спроектувати власну мережу «розумного будинку» використовуючи різні пристрої;
- створити систему використовуючи бездротовий та дротовий зв'язок;
- розробити схему, в якій на приладах зконфігуровані правила взаємодії

з іншими приладами системи та з навколишнім середовищем або їх поєднанням;

- створити внутрішню мережу Wi-Fi та надати доступ планшету до управління інтелектуальними пристроями ;

- протестувати інтелектуальну мережу «Розумний будинок».

У результаті виконання поставленої задачі буде створена мережа «розумного дому» з бездротовим та дротовим типом зв'язку, можливістю налаштування конфігурацій через веб-інтерфейс.

## РОЗДІЛ.2

### Вибір методу вирішення завдань дипломного проекту

#### 2.1 Огляд можливостей для моделювання в cisco packet tracer

Cisco Packet Tracer — це комплексна програма навчання мережевим технологіям, яка пропонує унікальні можливості поєднання реалістичного моделювання та візуалізації, оцінювання та авторських можливостей діяльності та можливості для багатокористувацької співпраці та конкуренції. Інноваційні функції Packet Tracer допоможуть студентам і викладачам співпрацювати, вирішувати проблеми та вивчати концепції в захоплюючому та динамічному соціальному середовищі. Деякі з переваг Packet Tracer є такими:

- Забезпечує реалістичне навчальне середовище моделювання та візуалізації, яке доповнює обладнання класу, включаючи можливість бачити внутрішні процеси в режимі реального часу, які зазвичай приховані на реальних пристроях;
- Забезпечує багатокористувацьку співпрацю в реальному часі та змагання для динамічного навчання;
- Дозволяє створювати та локалізувати структуровані навчальні дії, такі як лабораторні роботи, демонстрації, вікторини, іспити, та ігри;
- Дає студентам можливість досліджувати концепції, проводити експерименти та перевіряти своє розуміння побудови мережі;
- Дозволяє студентам і викладачам проектувати, будувати, налаштовувати та виправляти складні мережі за допомогою віртуальних мереж обладнання;
- Підтримує різноманітні можливості для викладання та навчання, такі як лекції, групові та індивідуальні лабораторні роботи, домашні завдання, ігри, конкурси;

- Підтримує розширення функцій через зовнішні програми за допомогою API для покращення функціональності Cisco Packet Tracer у таких сферах, як навчальний план і оцінювання, ігри, доступність і взаємодія з справжнім обладнанням [14].

Cisco Packet Tracer (CPT) - це програмне забезпечення для моделювання мережі та налагодження її роботи. Воно може бути використане для моделювання розумного будинку, але має деякі обмеження, що потрібно враховувати.

Для моделювання розумного будинку в CPT можна використовувати такі компоненти:

1. Маршрутизатори: Маршрутизатори можуть бути використані для керування мережею розумного будинку та забезпечення доступу до Інтернету. Це може включати підключення до мережі домашнього Інтернет-провайдера або підключення до хмарних сервісів.
2. Пристрої IoT: Для моделювання розумного будинку, в CPT можна використовувати пристрої IoT, такі як сенсори, датчики, пристрої розумного дому та інші пристрої з підтримкою протоколів IoT.
3. Сервери: Сервери можуть бути використані для зберігання даних, таких як відео, зображення, музика, документи та інші файли. Вони також можуть використовуватися для запуску додатків, що контролюють розумний будинок.
4. Комутатори: Комутатори можуть використовуватися для керування трафіком в мережі розумного будинку та забезпечення доступу до мережевих пристроїв.
5. Камери відеоспостереження: Для моделювання системи відеоспостереження можна використовувати камери відеоспостереження та записуючі пристрої.
6. Пристрої звукового контролю: Для моделювання системи звукового контролю можна використовувати пристрої звукового контролю, такі як динаміки, ресивери та інші пристрої.

Обмеження:

1. СРТ не підтримує всіх протоколів IoT.
2. Моделювання реальних умов розумного будинку може бути складним у СРТ, оскільки воно є програмою для моделювання мереж, а не фізичних пристроїв.
3. Не всі пристрої розумного будинку можуть бути доступні в СРТ, що може обмежити можливості моделювання.
4. СРТ може мати обмеження на кількість пристроїв, які можуть бути додані до мережі, залежно від версії програмного забезпечення та комп'ютерної конфігурації.
5. СРТ не має можливості підключення до реальних пристроїв та систем, що можуть бути використані в розумному будинку.

Хоча СРТ має деякі обмеження для моделювання розумного будинку, воно все ж може бути корисним інструментом для вивчення та тестування мережі розумного будинку, включаючи розгортання, конфігурування та налагодження мережевих пристроїв, які можуть використовуватися в розумному будинку.

В Cisco Packet Tracer розділення мережі на логічний та фізичний рівні можна виконати з використанням різних мережевих пристроїв та інструментів. Для розділення мережі на фізичний рівень можна використовувати комутатори та маршрутизатори, які дозволяють створювати фізичні підмережі. Наприклад, використовуючи комутатори, можна створити окрему підмережу для комп'ютерів, окрему для серверів, а також окрему для інших мережевих пристроїв, таких як принтери або маршрутизатори.

Для розділення мережі на логічний рівень можна використовувати віртуальні локальні мережі (VLAN, Virtual Local Area Network). В Packet Tracer це можна зробити за допомогою віртуальних комутаторів. Для цього необхідно налаштувати віртуальні інтерфейси на комутаторі та розділити пристрої на різні VLAN. За допомогою VLAN можна забезпечити безпеку мережі, зменшити розмір мережі та забезпечити легкість управління мережею.

Також у Cisco Packet Tracer можна використовувати віртуальні приватні мережі (VPN, virtual private network) для забезпечення безпеки підключення до мережі. VPN дозволяє підключати пристрої до мережі через інтернет з захистом від несанкціонованого доступу до мережі.

Застосування підсередовищ залежить від потреб користувачів та мережевої інфраструктури. Використання комутаторів та маршрутизаторів дозволяє розділити мережу на фізичний рівень, а використання VLAN та VPN дозволяє розділити мережу на логічний рівень.

Cisco Packet Tracer дозволяє програмувати пристрої, які можуть імітувати поведінку мікроконтролера, отримувати сигнали від різних датчиків і надсилати команди до пристроїв виконання. Для програмування можна використовувати JavaScript, Python і Blockly у вкладці «Програмування мікроконтролерів». У цій роботі використовувався Python.

## 2.2 Можливості мови Python для мікроконтролерів

Мова програмування Python, яка спочатку була призначена для розробки програмного забезпечення на комп'ютерах, тепер також підтримується на деяких мікроконтролерах. Python для мікроконтролерів може бути корисним в різних випадках, наприклад, для розробки вбудованих систем або для створення прототипів пристроїв.

Ось деякі з можливостей мови Python для мікроконтролерів:

1. Мінімальний розмір коду: Python є інтерпретованою мовою, що означає, що програмний код може бути коротким і простим у порівнянні з іншими мовами програмування. Це дозволяє зменшити розмір програми та пам'яті, необхідної для її виконання.
2. Простота використання: Python має простий синтаксис, що дозволяє швидко та легко писати програми. Це може знизити час розробки, а також спростити утримання та оновлення коду.

3. Багаті бібліотеки: Python має велику кількість бібліотек, які дозволяють працювати з різними пристроями та сенсорами. Це забезпечує широкі можливості для створення різних типів пристроїв, таких як IoT-пристрої, датчики, контролери тощо.
4. Підтримка різних платформ: Python може бути виконаний на різних мікроконтролерах та платформах, таких як Arduino, Raspberry Pi, ESP8266 та ESP32. Це дозволяє розробникам використовувати Python для різних проектів та пристроїв.
5. Інтерактивне програмування: Python має інтерактивне середовище розробки (REPL), що дозволяє розробникам взаємодіяти з мікроконтролером в режимі реального часу та тестувати свої програми на ходу. Це дозволяє зменшити час розробки та полегшити відлагодження коду.
6. Можливість розширення: Python може бути поєднаний з іншими мовами програмування, такими як C та C++, що дозволяє розробникам використовувати Python для написання програмного забезпечення для мікроконтролерів та переключатися на мову C або C++ для написання частин коду, що потребують високої продуктивності.
7. Легкість навчання: Python є однією з найбільш поширених мов програмування у світі. Це означає, що для навчання Python для мікроконтролерів можна знайти багато ресурсів та курсів онлайн, що забезпечує легкий та доступний спосіб навчання.

В цілому, Python може бути корисним для розробки програмного забезпечення для мікроконтролерів, якщо ви шукаєте простий та ефективний спосіб для створення вбудованих систем, пристроїв Інтернету речей (IoT) та датчиків. Однак, перед використанням Python на мікроконтролерах, важливо вивчити його можливості та обмеження

для впевненості в правильному виборі мови програмування для вашого проекту.

### 2.3 Можливості мови JavaScript для мікроконтролерів

Мова JavaScript, зазвичай використовується для програмування на веб-сторінках, але також може бути використана для програмування мікроконтролерів. Для цього потрібно мати підтримку відповідних інструментів та апаратної платформи.

Деякі з можливостей використання мови JavaScript для програмування мікроконтролерів на сьогоднішній день включають:

Використання JavaScript на базі Node.js на мікроконтролері: можливо встановити Node.js на платформу мікроконтролера, наприклад, на Raspberry Pi, і використовувати JavaScript для програмування підключених пристроїв.

Використання спеціалізованих бібліотек: на сьогоднішній день існує кілька спеціалізованих бібліотек, таких як Johnny-Five, Espruino та Firmata, які дозволяють використовувати JavaScript для програмування мікроконтролерів.

Використання вбудованих JavaScript-інтерпретаторів: деякі мікроконтролери мають вбудовані JavaScript-інтерпретатори, які дозволяють виконувати JavaScript-код безпосередньо на мікроконтролері.

Використання спеціалізованих мов програмування, які компілюються в JavaScript: деякі мови програмування, такі як MicroPython та Lua, можуть бути скомпільовані в JavaScript, що дозволяє

використовувати їх для програмування мікроконтролерів безпосередньо на JavaScript.

Необхідно мати на увазі, що хоча JavaScript може бути використаний для програмування мікроконтролерів, він не є найбільш оптимальним варіантом для деяких завдань, оскільки може виникнути проблема з ресурсами, в тому числі з пам'яттю та швидкістю виконання.

## 2.4 Можливості мови Blockly для мікроконтролерів

Мова програмування Blockly є графічною мовою програмування, яка забезпечує зручний і доступний інтерфейс для програмування мікроконтролерів. Blockly заснований на парадигмі програмування за блоками, що дає можливість створювати програми шляхом з'єднання графічних блоків, які відповідають певним операціям та функціям.

Однією з основних переваг мови Blockly для програмування мікроконтролерів є її простота та доступність. Графічний інтерфейс дозволяє легко створювати програми, навіть користувачам без досвіду в програмуванні. Крім того, Blockly має багато готових блоків, що можуть бути використані для різних операцій, таких як робота з сенсорами, виведення даних на дисплей, робота з мережевими протоколами тощо.

Blockly також підтримує різні мікроконтролери, такі як Arduino, Raspberry Pi тощо. Це дозволяє легко програмувати різні мікроконтролери з одного інтерфейсу.

Крім того, Blockly дозволяє ефективно використовувати мікроконтролери, зменшуючи витрати пам'яті та швидкість виконання

програм. Це особливо важливо для пристроїв з обмеженими ресурсами, таких як мікроконтролери.

Отже, мова програмування Blockly є зручним та ефективним інструментом для програмування мікроконтролерів, що дозволяє швидко та легко створювати програми без потреби великого досвіду в програмуванні.

## РОЗДІЛ.3

## Програмна реалізація «розумного будинку» у симуляторі Cisco Packet Tracer 8.2

## 3.1 Система безпеки гаражу і освітлення

Розміщуємо прилади на їх логічних і остаточних місцях.

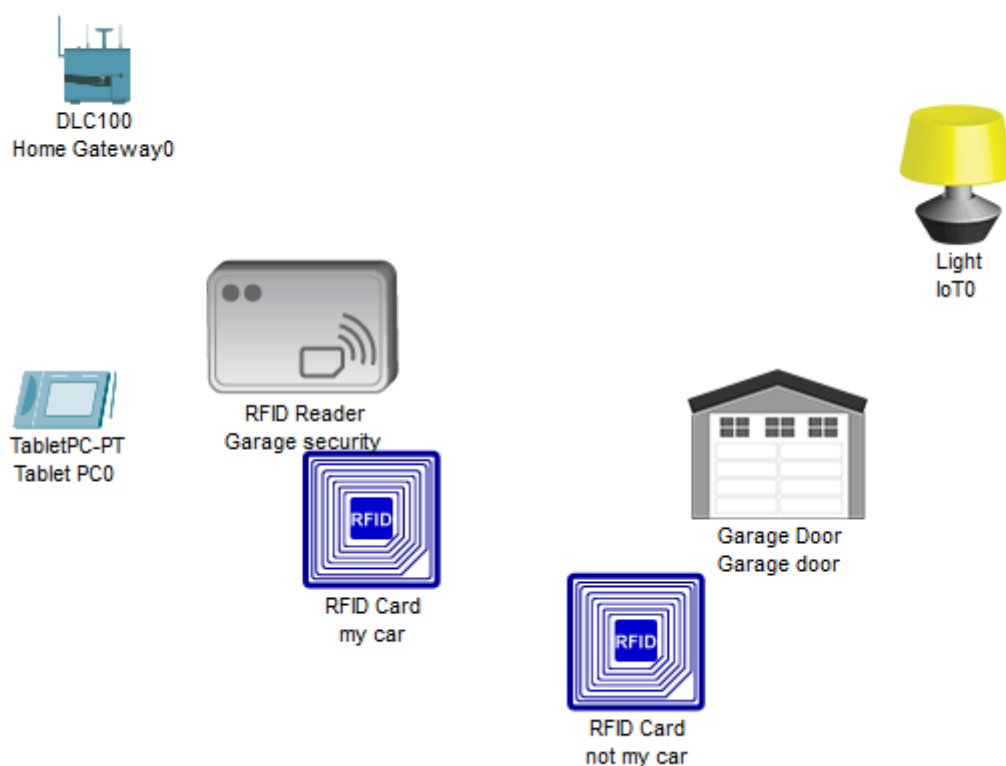


Рис. 3.1. Датчики та пристрої системи безпеки гаражу

На рис. 3.1 представлено датчики та пристрої системи безпеки гаражу, а саме: двері гаражу, планшет, радіочастотний ідентифікатор та дві радіочастотні карти.

Починаємо з налаштування домашнього шлюзу. Пристрої відправляють сигнали на домашній шлюз. На рис. 3.2 зображено налаштування домашнього шлюзу. Для подальшої роботи задаємо SSID - HomeGateway, та WPA2-PSK кодування і пароль шлюзу.

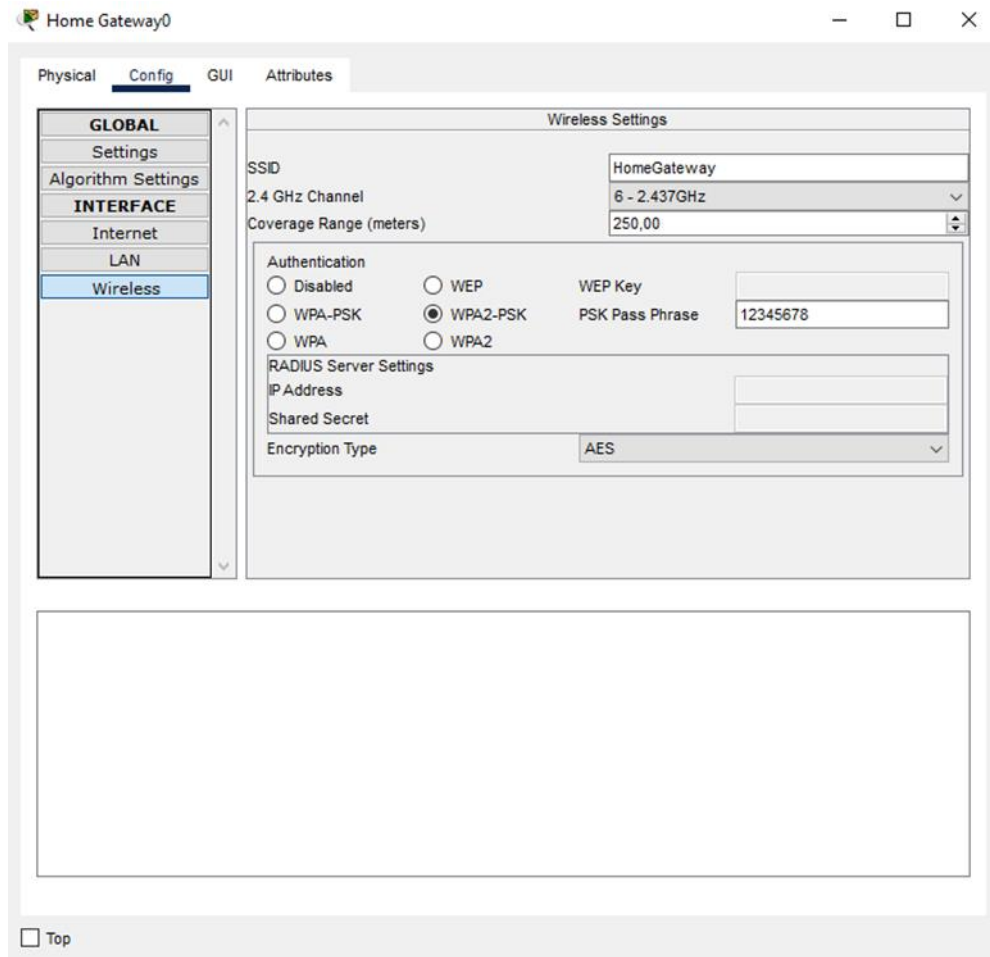


Рис. 3.2. Налаштування домашнього шлюзу

На рис.3.2 зображено налаштування домашнього шлюзу .Для подальшої роботи задаємо SSID - HomeGateway, та WPA2-PSK кодування і пароль шлюзу.

Далі налаштовуємо та підключаємо всі девайси. На рис. 3.3 зображено вкладку Config для налаштування пристроїв .

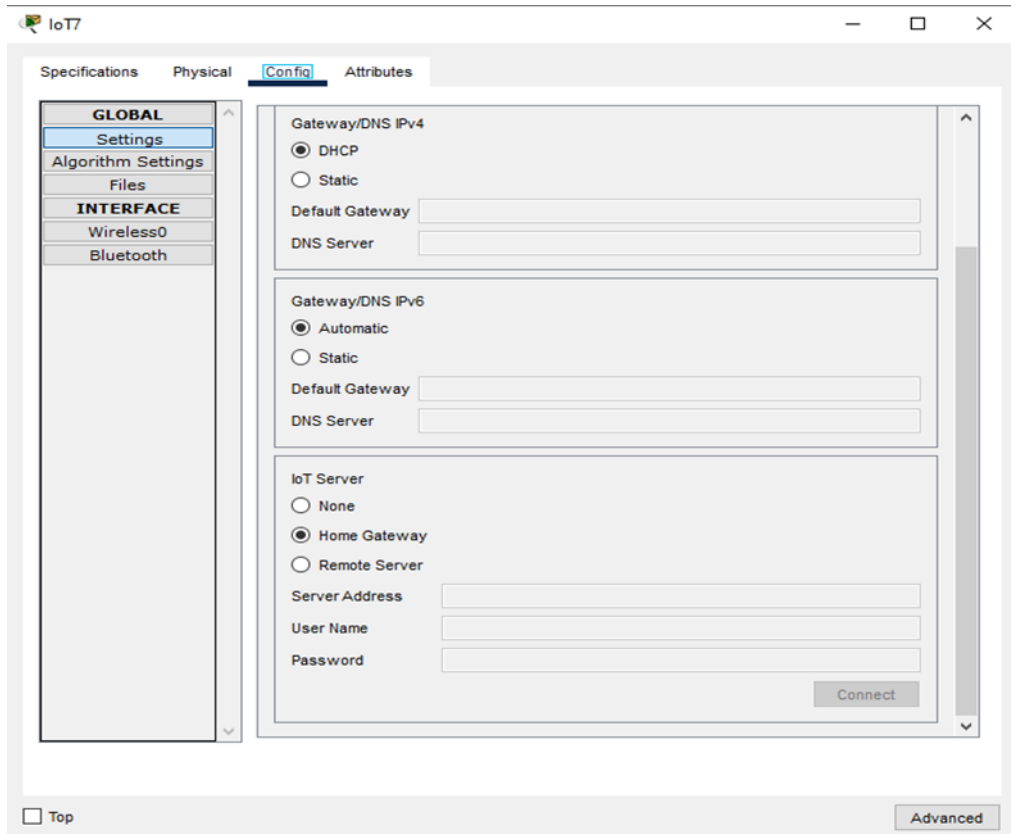


Рис. 3.3. Вкладка Config для налаштування пристроїв

З рис. 3.3 видно, що ми на вкладці Config задали імя та IoT-сервер – Home Gateway. На вкладці Wireless0 вказано SSID – HomeGateway, тип автентифікації WPA2-PSK та пароль.

Світильник, RFID та двері гаражу запрограмуємо на вмикання за певними правилами, які зображені на рис. 3.4.

Actions	Enabled	Name	Condition	Actions
<div>Edit</div> <div>Remove</div>	Yes	RFID KEY	Garage security Card ID = 1	Set Garage security Status to Valid
<div>Edit</div> <div>Remove</div>	Yes	garage open	Garage security Status is Valid	Set Garage door On to true
<div>Edit</div> <div>Remove</div>	Yes	garage close	Match any: <ul style="list-style-type: none"> <li>Garage security Status is Invalid</li> <li>Garage security Status is Waiting</li> </ul>	Set Garage door On to false
<div>Edit</div> <div>Remove</div>	Yes	light on	Garage door On is true	Set IoT0 Status to On
<div>Edit</div> <div>Remove</div>	Yes	light off	Garage door On is false	Set IoT0 Status to Off

Рис. 3.4. Налаштування на вмикання за певними правилами

Як впливає з рис.3.4 при валідній автентифікації відкриваються двері гаражу та при відкритті двері автоматично вмикається світло. Це забезпечує комфорт та безпеку для господаря. При невалідній автентифікації двері залишаються зачиненими.

Для перевірки працездатності наводимо RFID my car на RFID reader рис. 3.5.

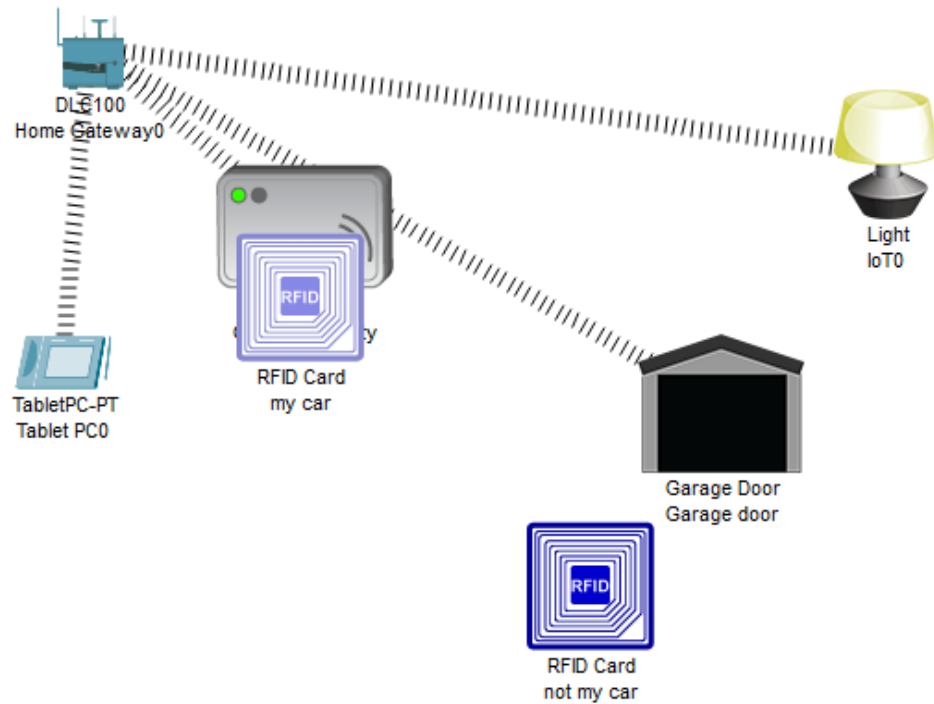


Рис. 3.5. Перевірка працездатності (1)

З рис. 3.5 видно, що система працює правильно, при валідній автентифікації двері гаражу відчиняються і вмикається світло. Далі піднесемо RFID not my car і перевіримо працездатність системи рис. 3.6.

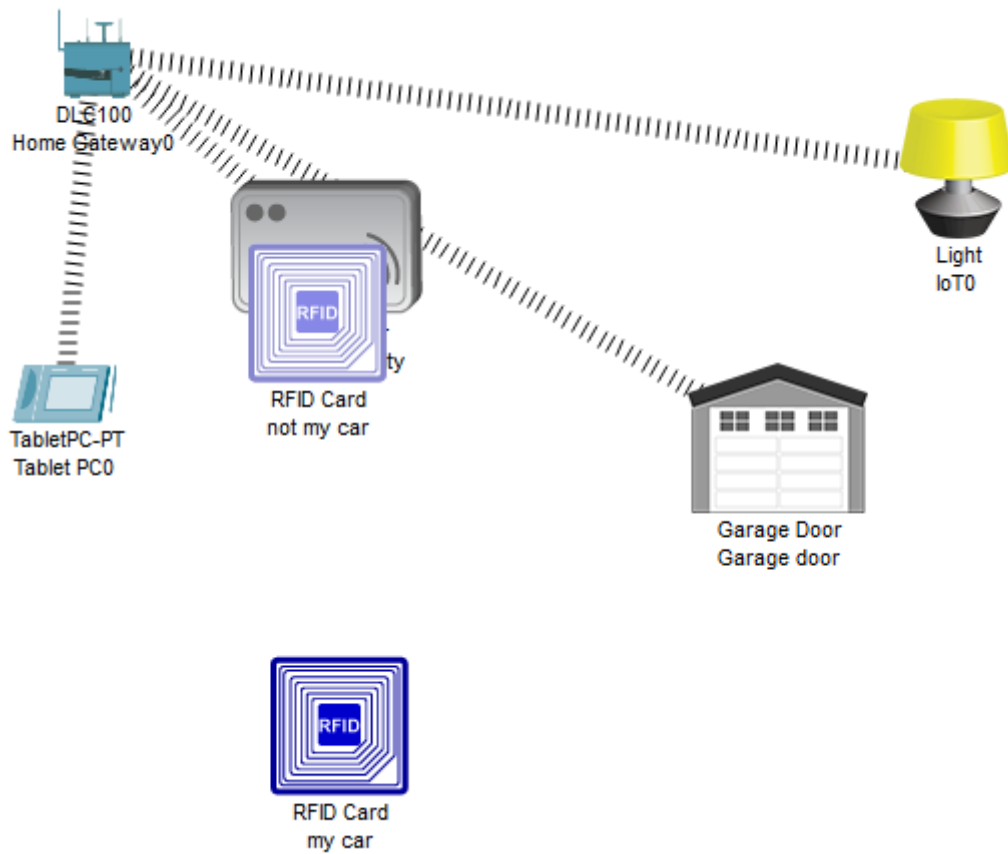


Рис. 3.6. Перевірка працездатності (2)

З рис. 3.6 випливає, що система працює правильно, при невалідній автентифікації двері гаражу невідчиняються і невимикається світло.

### 3.2 Система моніторингу пожежі та диму

Розміщуємо прилади на їх логічних і остаточних місцях як показано на рис. 3.7.

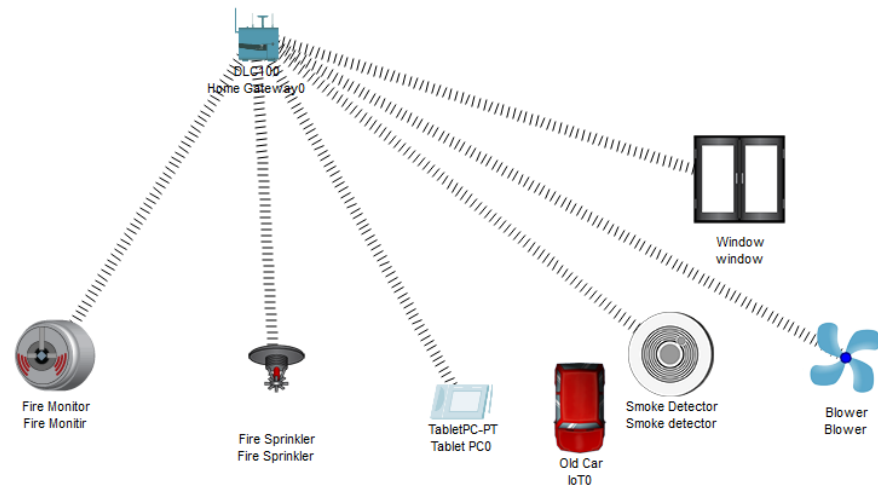


Рис. 3.7. Система моніторингу пожежі та диму

На рис. 3.7 зображено систему моніторингу пожежі та диму яка складається з : планшету , вентилятору, датчика диму, датчика вогню, вікна та розприскувача.

Далі налаштовуємо та підключаємо всі девайси. На вкладці Config задано імя та IoT-сервер – Home Gateway. На вкладці Wireless0 вказуємо SSID – HomeGateway, тип автентифікації WPA2-PSK та пароль.

Всі пристрої запрограмуємо за певними правилами, які зображені на рис. 3.8.

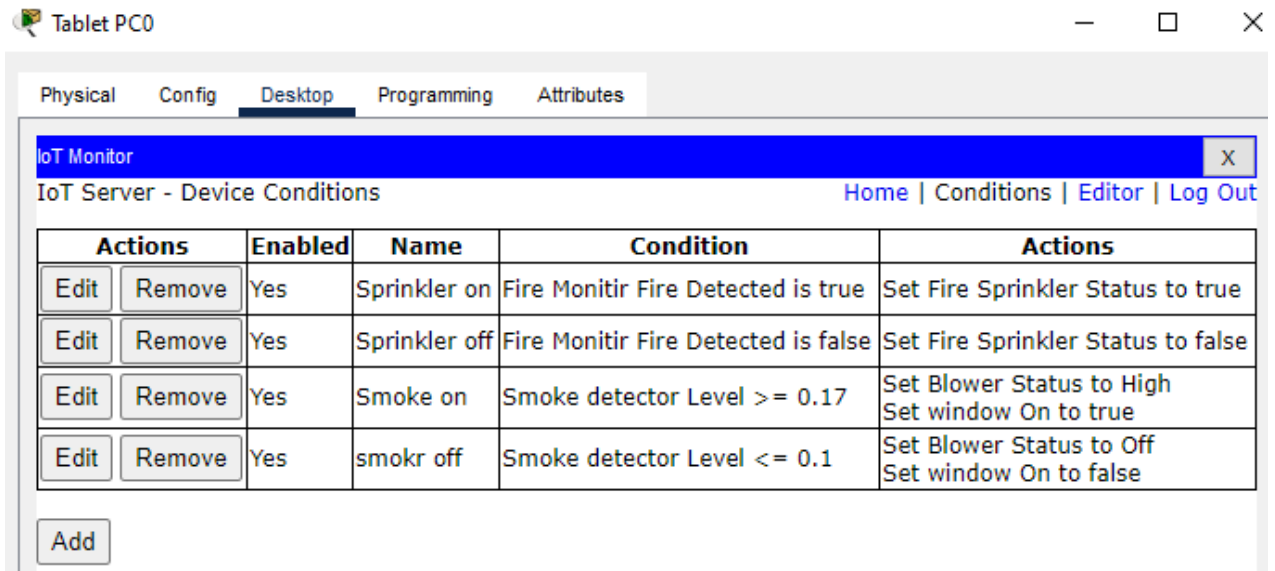


Рис. 3.8. Налаштування правил для системи моніторингу пожежі та диму

З рис. 3.8 видно, що при виявленні вогню має запрацювати розприскувач, а при виявленні диму включитися вентилятор та відкритися вікна.

Для перевірки працездатності піднесемо вогонь до датчику вогню рис. 3.9.

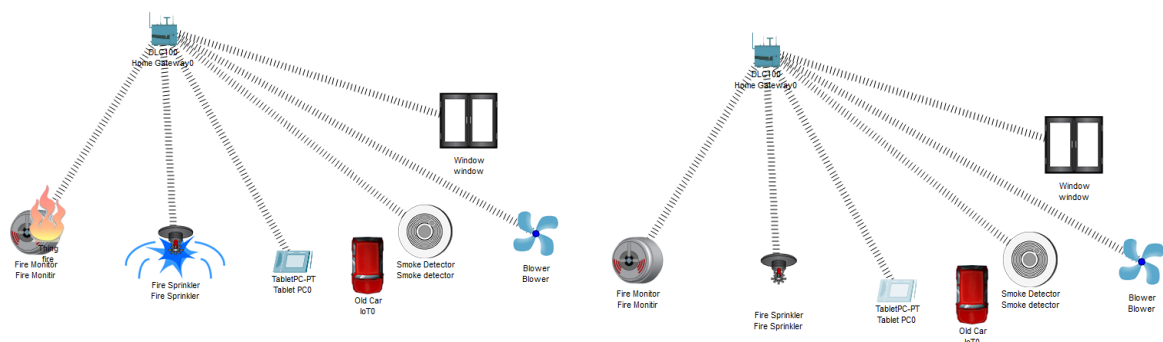


Рис. 3.9. Перевірка працездатності датчика вогню

З рис. 3.9 виходить, що при піднесенні вогню до датчика вогню починає працювати розприскувач. При віднесенні вогню від датчика розприскувач перестає працювати.

Далі перевіримо датчик диму, для цього розмістимо машину і включимо її, як зображено на рис. 3.10.

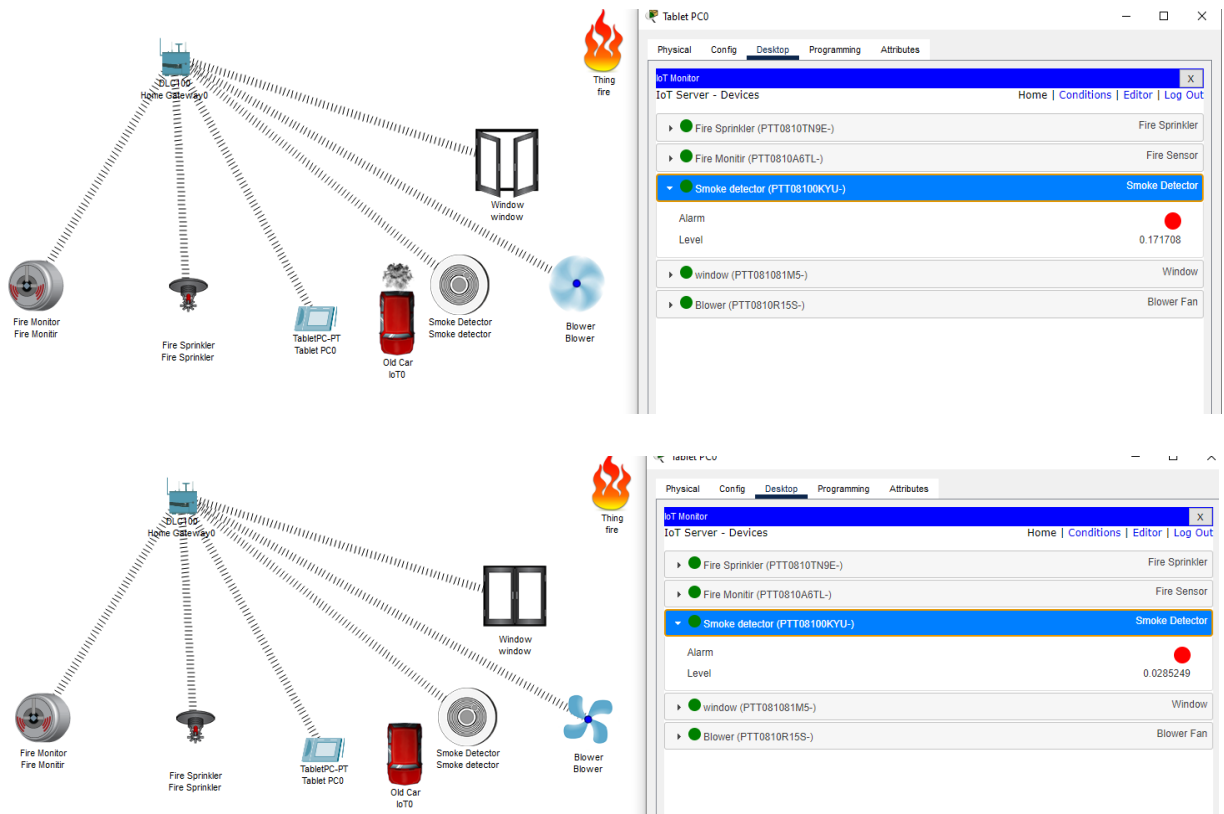


Рис. 3.10. Перевірка датчику диму

З рис. 3.10 випливає що, при досягненні рівня диму 0.17 відчиняється вікно і починає працювати вентилятор. При вимиканні старої машини рівень диму зменшується і вентилятор вимикається і вікно закривається. Система працює правильно.

### 3.3 Система пожежної сигналізації

Розміщуємо прилади на їх логічних і остаточних місцях і з'єднуємо їх custom IoT cable ,як показано на рис. 3.11 .

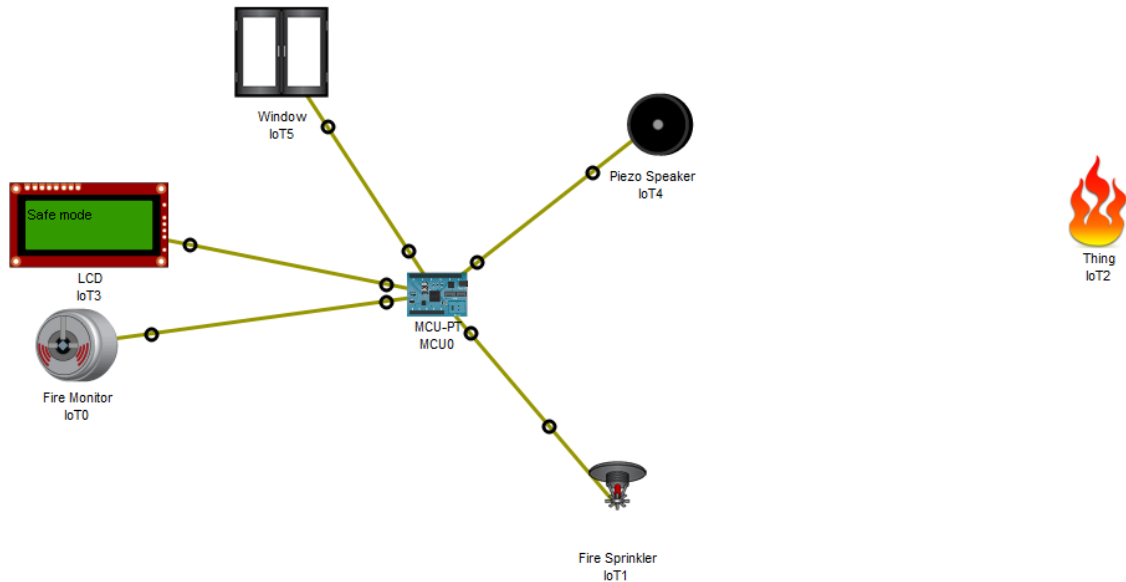


Рис. 3.11. Система пожежної сигналізації

На рис. 3.11 зображено систему пожежної сигналізації, яка складається з: мікроконтролера, динаміка, розприскувача, датчика вогню і LCD екрана.

Далі програмуємо плату для того щоб при вогні працював динамік , відкривалося вікно , працював розприскувач і на LCD екрані виводилися дані щодо пожежі (додаток А) .

Для перевірки працездатності підносимо вогонь до датчику рис. 3.12.

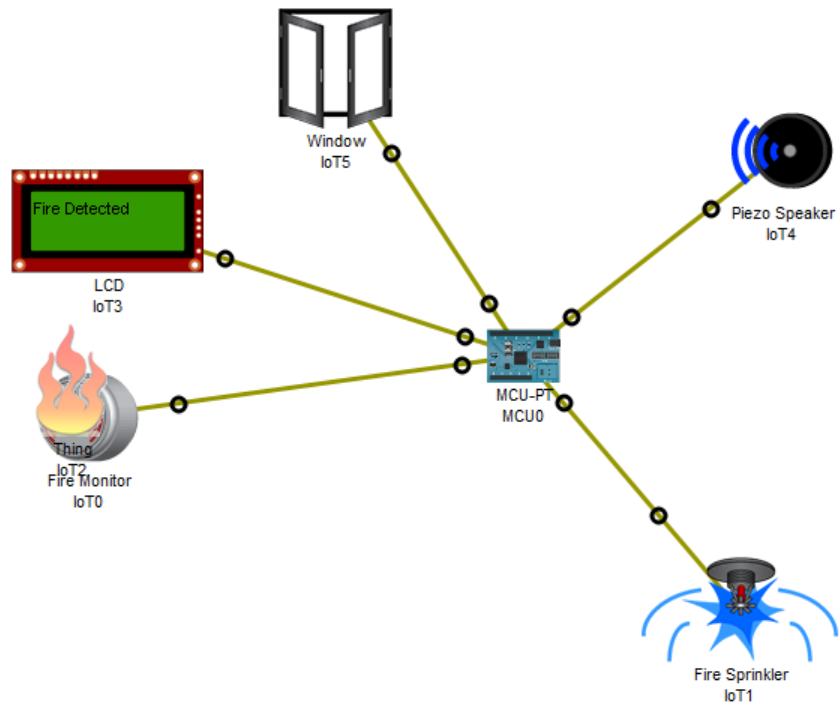


Рис. 3.12. Робота системи при пожежі

З рис. 3.12 видно, що при пожежі починає працювати розприскувач і динамік, відкривається вікно та на екрані виводиться надпис, що виявленна пожежа.

Далі прибираємо вогонь , як зображено на рис. 3.13.

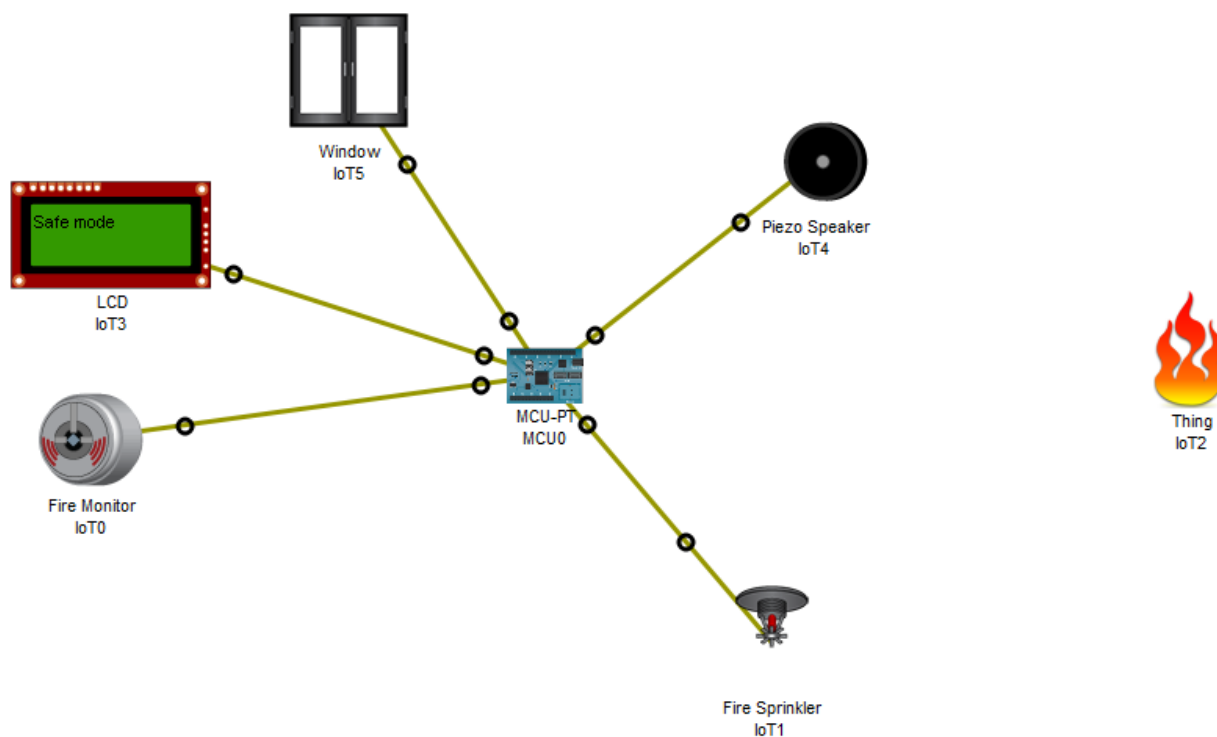


Рис. 3.13. Робота системи при відсутності пожежі

З рис. 3.13 виходить ,що система працює правильно, вікно закрите , динамік і розприскувач вимкнені та на екрані виведено безпечний режим .

### 3.4 Розумний будинок

Далі об'єднуємо все в розумному будинку. Для цього розставляємо все на своїх місцях . На схемі будинку розміщаємо усі прилади IoT, які утворюють необхідну інтелектуальну мережу всередині дому , як зображено на рис. 3.14.

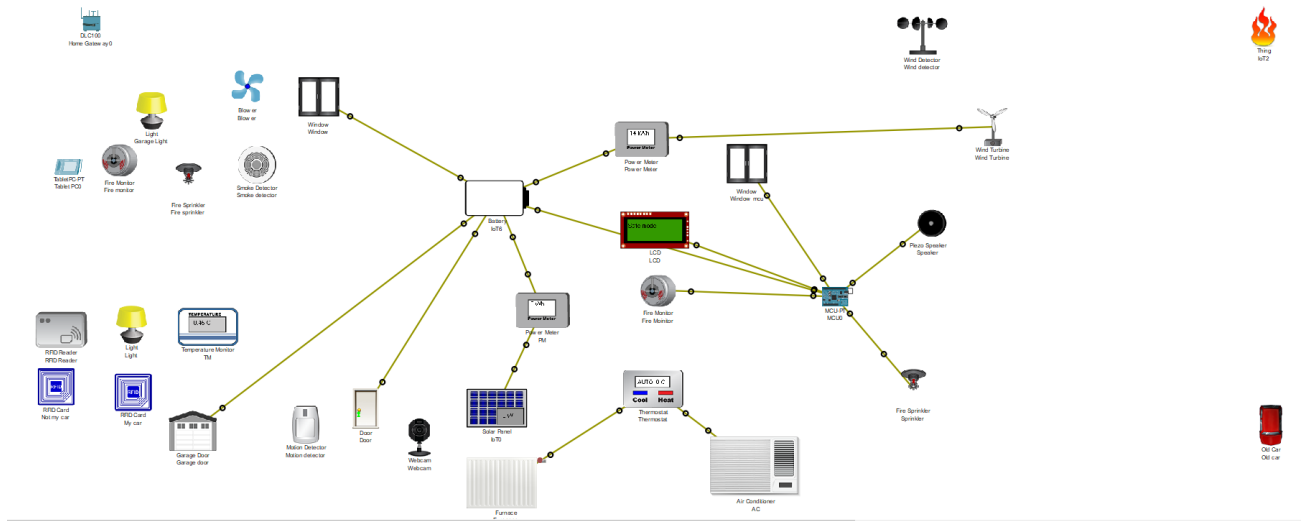


Рис . 3.14. Розумний будинок

На рис. 3.14 зображено розумний будинок складається з : система безпеки гаражу і освітлення, система моніторингу пожежі та диму, система пожежної сигналізації та інших пристроїв інтернету речей.

Починаємо з налаштування домашнього шлюзу. Пристрої інтелектуальної мережі відправляють сигнали на домашній шлюз. Для подальшої роботи задаємо IP-адреса шлюза, SSID - HomeGateway, та WPA2-PSK кодування і пароль шлюзу. На вкладці Config задаємо імя та IoT-сервер – Home Gateway. На вкладці Wireless0 вказано SSID – HomeGateway, тип автентифікації WPA2-PSK та пароль.

Тип з'єднання можна змінити у будь-який момент. Налаштовано доступ з кінцевих пристроїв для керування та моніторингу мережі – планшетом. Інші налаштування схожі з описаними вище.

Для моніторингу мережі через мобільні пристрої, на вкладці Desktop обрано IoT monitor як зображено на рис.3.15.

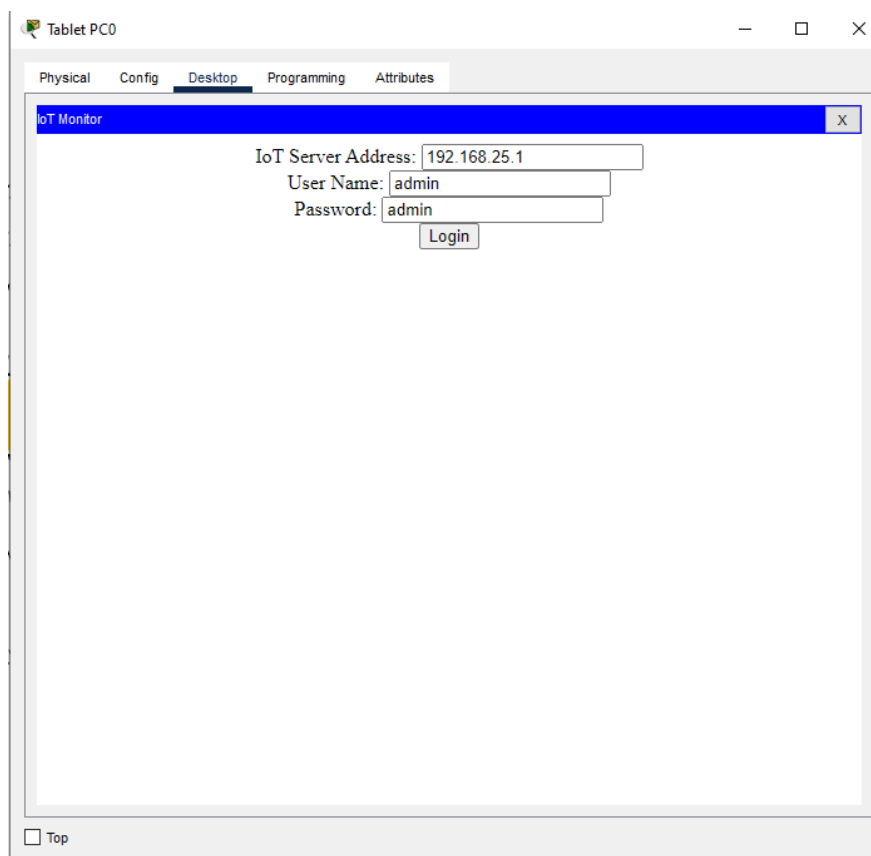


Рис. 3.15. Доступ до веб-інтерфейсу шлюзу через планшет

На рис. 3.15 показано вхід до екрану керування пристроями системи, де вказано адресу серверу, логін та пароль для логіну.

Панель де можна вмикати/вимикати, контролювати налаштування на рис. 3.16.

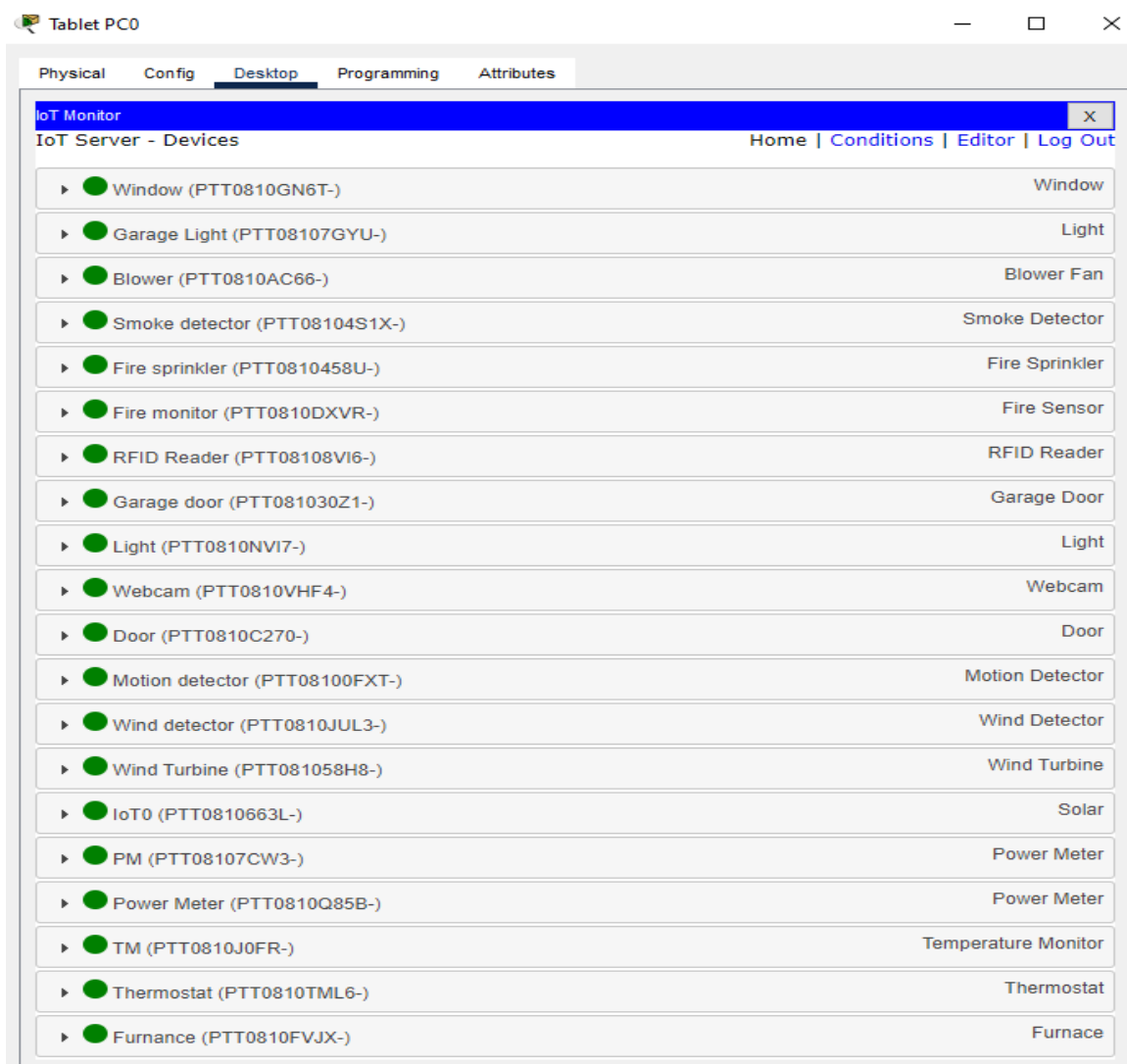


Рис. 3.16 Веб-інтерфейс планшету для керування інтелектуальною мережею

На рис. 3.16 показано інтерфейс для керування пристроями в розумному будинку.

На рисунку 3.17 зображена схема, отримана в результаті проекту «Smart Home». При необхідності цю мережу можна розширити аналогічними маніпуляціями з будь-яким із кінцевих пристроїв, доступних у симуляторі, через вже побудовані канали зв'язку.

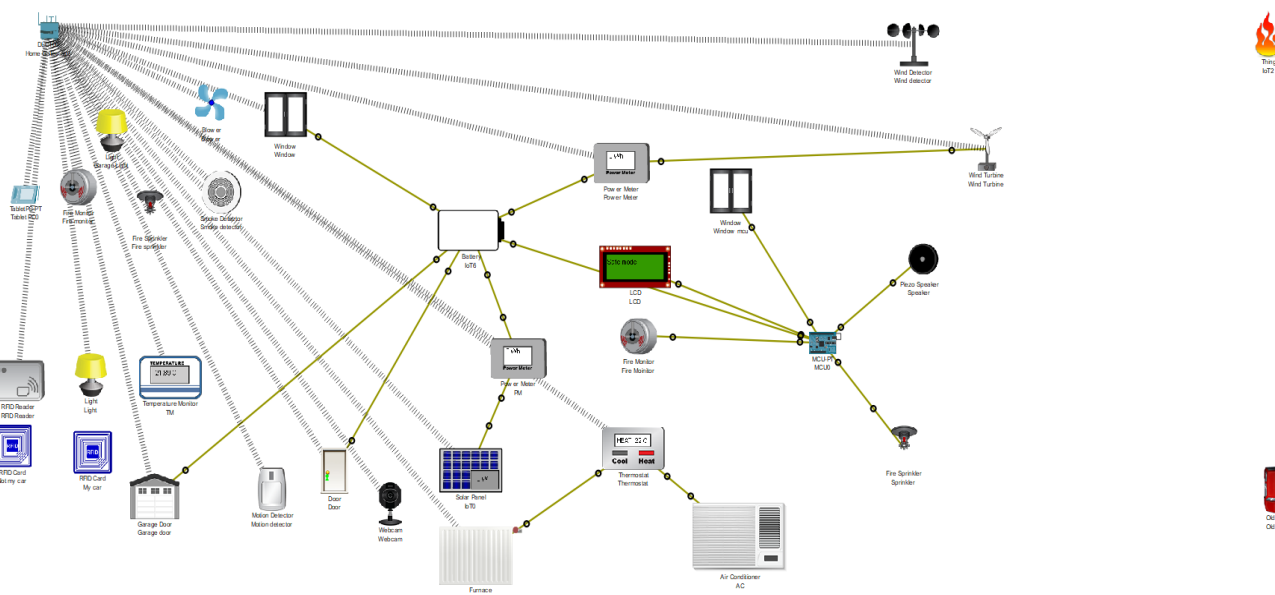


Рис. 3.17. Інтелектуальна мережа «розумного будинку»

На рис. 3.17 показано проект робочої мережі «розумного будинку», який було отримано в результаті базових налаштувань. Усі підключені пристрої перевірені та доступні для управління і контролю через веб-інтерфейс планшета.

У Cisco Packet Tracer користувач може побудувати модель «розумного будинку» та емулювати реальну поведінку датчиків, мікроконтролерів та пристроїв. Безперечно, деякі з них вимагають спеціального налаштування та програмування. Смарт-девайси можна активувати натиснувши на них лівою кнопкою миші з одночасним натискання клавiші Alt на клавіатурі. Пристрої також можуть активуватися самостійно, в залежності від змін параметрів навколишнього середовища. Конфігурувати правила взаємодії приладів можна використовуючи веб-інтерфейс.

У користувача є спеціальне вікно браузера для управління системою «розумного будинку». За потреби він може перейти на вкладку Conditions та створити власні правила, які визначають умови взаємодії інтелектуальних приладів. Правила програмуються на основі прості if-then умов. Це ще раз підтверджує легкість у конфігуруванні інтелектуальної системи для

звичайного користувача. Так, встановлено, що веб-камера активується, коли активується детектор руху. Інтерфейс взаємодії дуже зручний і зрозумілий.

Для забезпечення безперебійного живлення «розумного будинку» використано альтернативні джерела енергії. Так, у симуляторі імітована робота сонячної панелі, вітрової турбіни та акумулятора. Для цього пристрої з'єднані між собою спеціальним кабелем IoT і кожен з них підключено окремо до шлюзу. Графік сонячного світла налаштовано на вкладці «Навколишнє середовище» рис. 3.18.

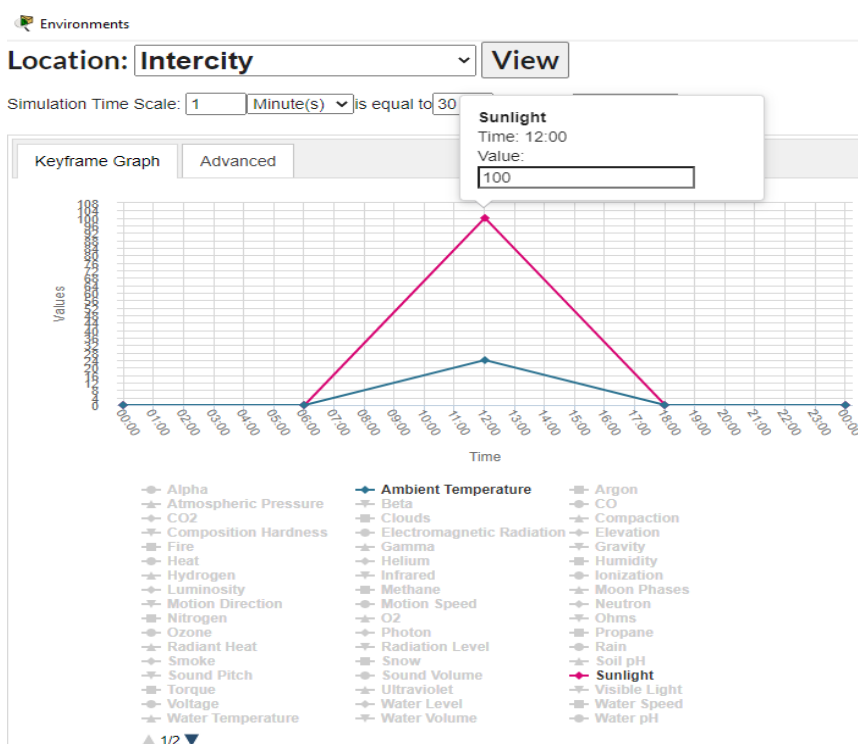


Рис. 3.18. Графік зміни температури та сонячного світла протягом доби

З рис. 3.18 видно, що з 6 години ранку починається зріст сонячного світла. Найбільша його частина припадає на дванадцятю годину дня. А потім, відповідно починає зменшуватися.

На рис. 3.19 показано графік зміни поривів та напрямлення вітру.

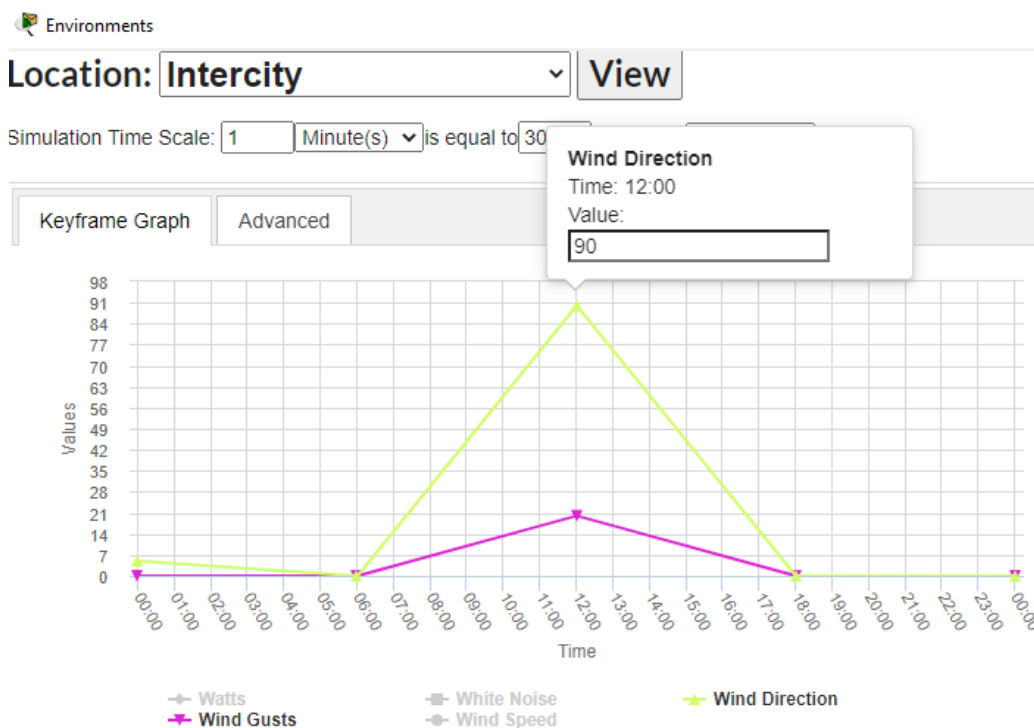


Рис. 3.19. Графік зміни поривів та напрямлення вітру

З рис. 3.19 видно, що з 6 години ранку починається зріст напрямлення вітру. Найбільша його частина припадає на дванадцяту годину дня. А потім, відповідно починає зменшуватися.

Світильник запрограмуємо на вмикання за певними правилами рис.

3.20.

Edit	Remove	Yes	light h on	Door Open is true	Set Light Status to On
Edit	Remove	Yes	light h off	Door Open is false	Set Light Status to Off

Рис. 3.20. Налаштування умов для ввімкнення світла

З рис. 3.20 випливає, що при відкритті дверей має автоматично вмикатися світло. Для перевірки працездатності відкриємо входні двері рис. 3.21.

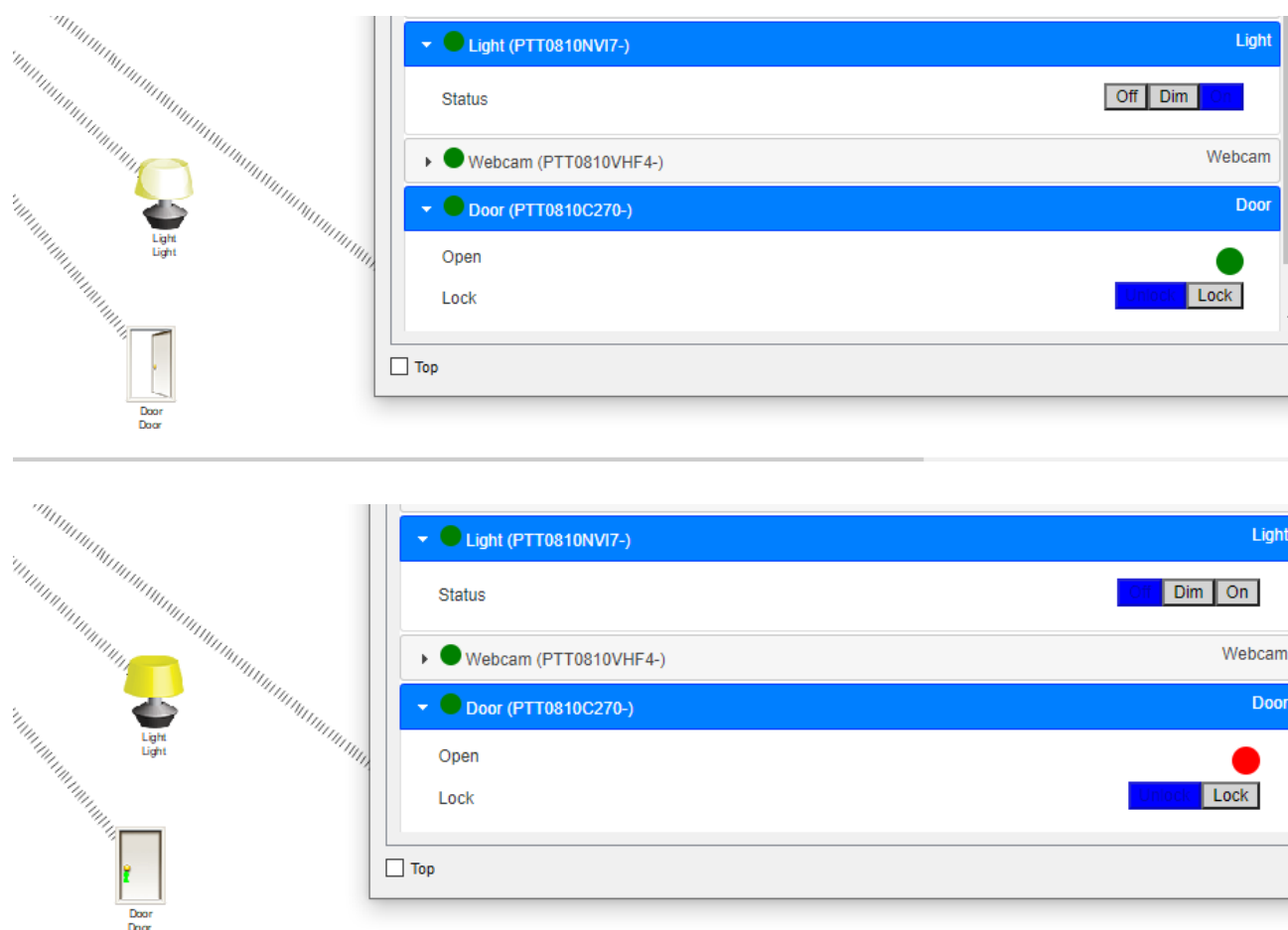


Рис 3.21 Перевірка виконання умов

З рис. 3.21 видно, що при відкритті дверей автоматично вмикається світло, а коли двері закриті світло вимкнене.

Далі налаштуємо активацію веб-камери, коли активується детектор руху рис. 3.22.

Edit	Yes	webcam on	Motion detector On is true	Set Webcam On to true
Remove				
Edit	Yes	webcam off	Motion detector On is false	Set Webcam On to false
Remove				

Рис. 3.22. Налаштування правил автовмикання веб-камери при активації детектору руху

На рис. 3.22 зображені правила автовмикання веб-камери при активації детектору руху, згідно з якими при активації детектору руху починає працювати камера.

Для перевірки руху детектора активуємо його переміщенням миші з натисканням клавіші Alt на клавіатурі як зображено на рис. 3.23.

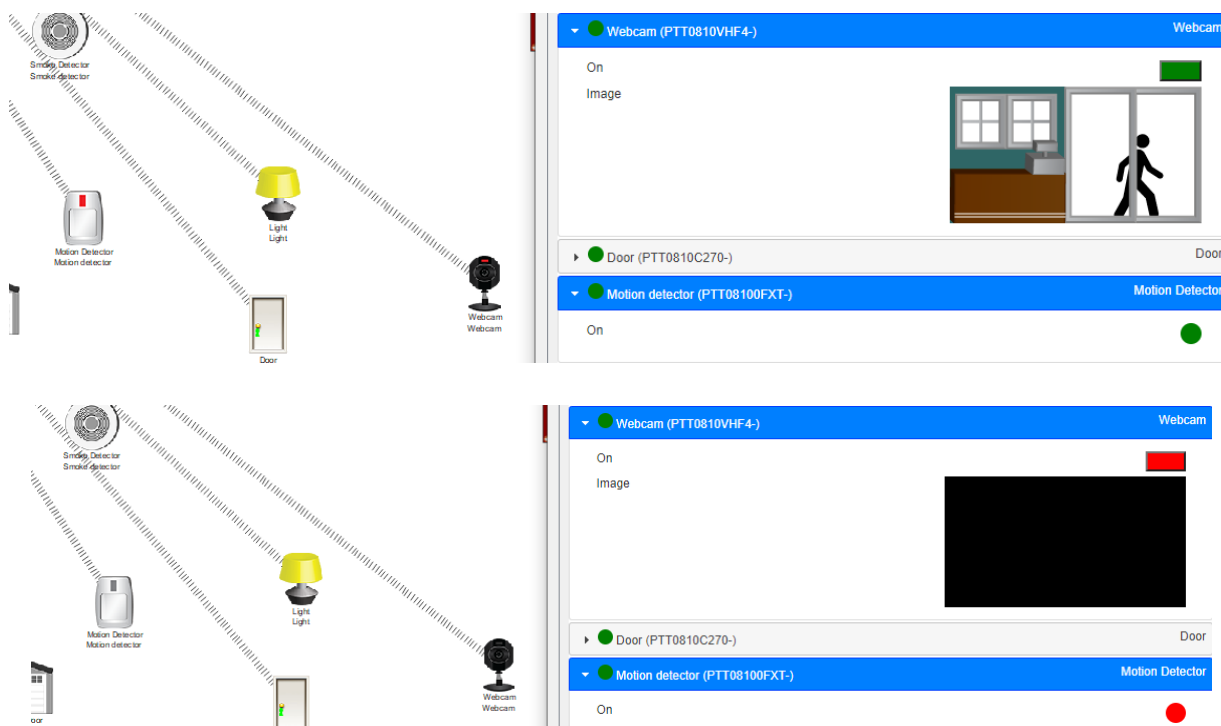


Рис. 3.23. Перевірка вебкамери та датчика руху

З рис. 3.23 видно, що коли курсор рухається до детектора, детектор включається і веб-камера активується.

Таким чином, було реалізовано інтелектуальну мережу «розумного будинку» з трьома системами безпеки у симуляторі Cisco Packet Tracer 8.2.

## ВИСНОВКИ

В ході виконання роботи було зібрано , з'єднано , запрограмовано та протестовано: система безпеки гаражу і освітлення , система пожежної сигналізації , система моніторингу пожежі та диму і проект робочої інтелектуальної мережі «Розумний будинок» у симуляторі Cisco Packet Tracer 8.2. Для проектування системи було використано бездротовий (Wi-Fi) та дротовий (IoT custom cable) зв'язок. Перевірено, що усі з'єднані пристрої доступні для керування та моніторингу через веб-інтерфейс планшету.

Було досягнуто покращення якості життя за рахунок забезпечення комфорту (можливість управління пристроями з планшету, вмикання світла при відкриванні входних дверей), безпеки (вмикання камери при активації детектора руху , оповіщення в разі пожежі чи задимлення).

Для програмування мікроконтролера було вибрано мову програмування Python, тому що вона:

- легка в вивченні: Python - це досить проста мова програмування, що дозволяє швидко засвоїти її основні принципи. Це може бути особливо корисним для початківців у програмуванні мікроконтролерів;
- багата екосистема: Python має велику кількість бібліотек і фреймворків, що дозволяє простіше розробляти програми для мікроконтролерів. Також існує багато онлайн-документації та підтримки спільноти.

## Список використаних джерел

1. V. Ricquebourg, D. Menga, D. Durand, B. Marhic, L. Delahoche and C. Loge, "The Smart Home Concept : our immediate future," 2006 1ST IEEE International Conference on E-Learning in Industrial Electronics, Hammamet, Tunisia, 2006, pp. 23-28, <https://doi.org/10.1109/ICELIE.2006.347206> .
2. Velivela, Gopinath & Srija, Arigela & Rao, Dr & Madhuri, Avula. (2018). Smart Homes: Steps, Components, Utilities and Challenges. International Journal of Engineering & Technology. 7(2.7):436. <https://doi.org/10.14419/ijet.v7i2.7.10858> .
3. Wilson, Charlie & Hargreaves, Tom & Hauxwell-Baldwin, Richard. (2017). Benefits and risks of smart home technologies. Energy Policy. 103. 72-83. <https://doi.org/10.1016/j.enpol.2016.12.047> .
4. Maheswari Muthusamy, M. Sujatha, Kolusu Tirumala Trilok Babu, Kolla Gokul Pratyush, Dasi Amrutha; IoT enabled smart home. AIP Conference Proceedings 18 November 2022; 2452 (1): 060006. <https://doi.org/10.1063/5.0130007> .
5. Jie Ding, Tian-ran Li and Xue-Li Chen; The Application of Wifi Technology in Smart Home; IOP Conf. Series: Journal of Physics: Conf. Series 1061 (2018) 012010; <https://doi.org/10.1088/1742-6596/1061/1/012010> .
6. S. J. Danbatta and A. Varol, "Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019, pp. 1-5, <https://doi.org/10.1109/ISDFS.2019.8757472> .
7. H. Krasniqi, Zijadin & Vershevc, Behar. (2020). Smart Home Automatic Control of Lighting through Z Wave IoT technology. IC-ISS 2020 : 9th International Conference on Information Systems and Security, Kosovo [https://www.researchgate.net/publication/345390600\\_Smart\\_Home\\_Automatic\\_Control\\_of\\_Lighting\\_through\\_Z\\_Wave\\_IoT\\_technology](https://www.researchgate.net/publication/345390600_Smart_Home_Automatic_Control_of_Lighting_through_Z_Wave_IoT_technology) (дата звернення 13.04.2023)
8. Obaid, Thoraya & Rashed, Haleemah & Abou-Elnour, Ali & Rehan, Muhammad & Hasan, Musaab & Tarique, Mohammed. (2014). Zigbee Technology and its Application in Wireless Home Automation Systems: A Survey. International journal of Computer Networks & Communications. 6. 115-131.

<https://doi.org/10.5121/ijcnc.2014.6411> .

9. Chellappa, Muthu & Madasamy, Shanmugaraj & Prabakaran, R.. (2011). Study on ZigBee technology. 297-301.

<https://doi.org/10.1109/ICECTECH.2011.5942102> .

10. Sofi, Mukhtar. (2016). Bluetooth Protocol in Internet of Things (IoT), Security Challenges and a Comparison with Wi-Fi Protocol: A Review. International Journal of Engineering Research and. V5.

<https://doi.org/10.17577/IJERTV5IS110266> .

11. Barua, Arup & Alamin, Md Abdullah Al & Hossain, Md & Hossain, Ekram. (2022). Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey. IEEE Open Journal of the Communications Society. 3. 1-1. <https://doi.org/10.1109/OJCOMS.2022.3149732> .

12. KNX BASICS URL:

[https://www.knx.org/wAssets/docs/downloads/Marketing/Flyers/KNX-Basics/KNX-Basics\\_en.pdf](https://www.knx.org/wAssets/docs/downloads/Marketing/Flyers/KNX-Basics/KNX-Basics_en.pdf) .

13. Branko Dvoršak, Juraj Havelka, Elena Mainardi, Hrvoje Pandžić, Tea Selič, Mario Tretinjak. SMART HOME SYSTEMS URL:

[https://ec.europa.eu/programmes/erasmus-plus/project-result-content/4df4e928-8958-4552-80da-146977e666b9/Smart\\_Home\\_systems\\_FINAL.pdf](https://ec.europa.eu/programmes/erasmus-plus/project-result-content/4df4e928-8958-4552-80da-146977e666b9/Smart_Home_systems_FINAL.pdf) .

14. Cisco Packet Tracer 8.2 Frequently Asked Questions URL: <https://www.netacad.com/courses/packet-tracer/faq> (дата звернення 13.04.2023)

15. Python documentation URL: <https://docs.python.org/3/> (дата звернення 13.04.2023)

## Додаток А. Код до мікроконтролера МС0

```
from gpio import *
from time import *

def main():
    pinMode(0, INPUT)
    pinMode(1, OUT)
    print("Fire Alarm System");
    while True:
        fire = digitalRead(0);
        print(fire);
        if(fire==1023):
            customWrite(1,'1');
            customWrite(4,"Fire Detected");
            customWrite(3,HIGH);
            digitalWrite(2,HIGH);
        else:
            customWrite(1,'0');
            customWrite(4,"Safe mode");
            customWrite(3,LOW);
            digitalWrite(2,LOW);

if __name__=="__main__":
    main()
```