

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

**Навчально-науковий інститут телекомунікаційних систем
Кафедра телекомунікацій**

До захисту допущено:

Завідувач кафедри

_____ Сергій КРАВЧУК

«__»_____ 2024 р.

Дипломна робота

на здобуття ступеня бакалавра

**за освітньо-професійною програмою «Інженерія та програмування
інфокомунікацій»**

спеціальності 172 «Телекомунікації та радіотехніка»

**на тему: «Побудова інтеграційного рівня управління мережі IoT на базі
протоколу ZigBee»**

Виконав:

студент IV курсу, групи ТЗ-01

Скрекотень Владислав Ігорович _____

Керівник:

Доцент кафедри ТК НН ІТС, доцент, к.т.н.

Нестеренко Микола Миколайович _____

Рецензент:

Доцент кафедри ЕКІР НН ІТС, доцент, к.т.н.,

Бердников Олег Михайлович _____

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

Студент _____

Київ – 2024 року

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

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інженерія та програмування інфокомунікацій»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Сергій КРАВЧУК

«___» _____ 2024 р.

ЗАВДАННЯ
на дипломну роботу студенту
Скрекотню Владиславу Ігоровичу

1. Тема роботи «Побудова інтеграційного рівня управління мережі IoT на базі протоколу ZigBee», керівник роботи Нестеренко Микола Миколайович, доцент, к.т.н., затверджені наказом по університету від «22» травня 2024 р. № 2064-с.
2. Термін подання студентом роботи 10 червня 2024 р.
3. Вихідні дані до роботи: Модель OSI, основи IoT, технології безпроводових мереж: ZigBee, Z-Wave, Bluetooth, Wi-Fi, системи розумного будинку.
4. Зміст роботи: 1) Використання Zigbee в Iot та основи IoT 2) Порівняння протоколу Zigbee з протоколами Z-Wave, Wi-Fi, Bluetooth 3) побудова власного інтеграційного рівня управління мережі IoT на основі протоколу Zigbee.
5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо):

Слайд 1: Основне поняття IoT;

Слайд 2: Приклад технологій в IoT;

Слайд 3: Zigbee в IoT;

Слайд 4: Архітектура Zigbee;

Слайд 5: Переваги та Недоліки Zigbee;

Слайд 6: Покоління протоколу Zigbee;

Слайд 7: Порівняння з протоколами WiFi, Bluetooth, Z-wave;

Слайд 8: Створення власної IoT платформи на базі НА на протоколі Zigbee;

Слайд 9: Що необхідно для керування розумним будинком;

Слайд 10: Схема управління розумним будинком через протокол Zigbee;

Слайд 11: Інтеграція розумного будинку в застосунок HomeKit.

6. Дата видачі завдання 24.03.2024 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1.	Написання першого розділу	24.03.2024-19.04.2024	Виконано
2.	Написання другого розділу	20.04.2024-09.05.2024	Виконано
3.	Написання третього розділу	10.05.2024-29.05.2024	Виконано
4.	Підготовка матеріалів до друку та оформлення пояснювальної записки	30.05.2024-05.06.2024	Виконано
5.	Підготовка та оформлення презентації для доповіді	10.06.2024	Виконано

Студент

Владислав СКРЕКОТЕНЬ

Керівник

Микола НЕСТЕРЕНКО

РЕФЕРАТ

Дипломна робота містить 79 сторінок, 30 рисунків, 4 таблиці, 25 джерел.

Актуальність роботи. Технології телекомунікаційних мереж постійно вдосконалюються, що робить швидкісний Інтернет доступним практично всюди з мобільним зв'язком. Це стимулює виникнення нових ідей і технологій. Розробка інтеграційного рівня управління мережею IoT з використанням протоколу ZigBee залишається актуальною в умовах стрімкого розвитку Інтернету речей і зростання числа підключених пристроїв, таких як сенсори, реле, контролери та інше обладнання. Використання протоколу ZigBee стає популярним вибором завдяки його низькому споживанню енергії та можливості створення масштабованих мереж. Управління такими розподільними мережами потребує ефективного інтеграційного рівня.

Метою роботи аналіз протоколу Zigbee та оцінку побудови інтеграційного рівня для управління мережею IoT на прикладі створення розумного будинку. Для досягнення цієї мети потрібно виконати такі завдання: дослідити особливості протоколу Zigbee, порівняти його з іншими протоколами, що використовуються в IoT для реалізації розумного будинку, та розробити власне середовище для керування функціями розумного будинку з використанням протоколу Zigbee.

Об'єкт дослідження – протокол Zigbee та порівняннями зі схожими протоколами, Інтеграційний рівень, практичні застосування та випробування в системі розумного будинку.

Предмет досліджень – особиста платформа для керування системою розумного будинку.

Методи дослідження. В роботі використовують методи критичного та порівняльного аналізу під час теоретичного дослідження безпроводових технологій та обладнання систем «розумного будинку». **Отримані результати.**

Результати порівнянь безпроводових технологій показали, що кожна з них по своєму унікальна у використанні, має свої переваги та недоліки під час застосування в системах розумного будинку. Також можна зазначити, що кожна середовище інтеграційного рівня особлива для кожного і здатна на розширення для побудови структури розумного будинку.

Галузь застосування. Результати роботи можна використовувати під час побудови систем розумного будинку. Результати порівняння допоможуть зрозуміти принцип використання таких мереж, обрати найбільш підходящу у конкретному випадку технологію та сформулювати бачення перспектив у своїй галузі.

Ключові слова: ІНТЕРНЕТ, РОЗУМНИЙ БУДИНОК, СТАНДАРТ, WIFI, BLUETOOTH, ZIGBEE, ЗВУКОВІ МЕРЕЖІ, БЕЗПРОВОДОВІ, OSI, ТЕХНОЛОГІЯ Z-WAVE, ІОТ, ДАТЧИКИ.

ABSTRACT

Diploma Thesis contains 79 pages, 30 figures, 4 tables, 25 sources.

Relevance of the work: Telecommunications network technologies are constantly improving, making high-speed Internet accessible almost everywhere with mobile connectivity. This stimulates the emergence of new ideas and technologies. The development of an integration layer for IoT network management using the ZigBee protocol remains relevant in the context of the rapid growth of the Internet of Things and the increase in the number of connected devices such as sensors, relays, controllers, and other equipment. The use of the ZigBee protocol is becoming a popular choice due to its low energy consumption and ability to create scalable networks. Managing such distributed networks requires an efficient integration layer.

The aim of the work: To analyze the ZigBee protocol and evaluate the construction of an integration layer for managing an IoT network using the example of a smart home. To achieve this aim, the following tasks need to be completed: investigate the features of the ZigBee protocol, compare it with other protocols used in IoT for implementing smart homes, and develop a custom environment for managing smart home functions using the ZigBee protocol.

Object of the research: The ZigBee protocol and comparisons with similar protocols, integration layer, practical applications, and testing in a smart home system.

Subject of the research: Personal platform for managing a smart home system.

Research methods: The work uses methods of critical and comparative analysis during the theoretical study of wireless technologies and smart home system equipment.

Results obtained: The comparison results of wireless technologies showed that each of them is unique in its use, has its own advantages and disadvantages when applied in smart home systems. It can also be noted that each integration layer environment is unique for everyone and capable of expansion to build a smart home structure.

Field of application: The results of the work can be used in the construction of smart home systems. The comparison results will help to understand the principle of using such networks, choose the most suitable technology in a specific case, and form a vision of prospects in their field.

Keywords: INTERNET, SMART HOME, STANDARD, WIFI, BLUETOOTH, ZIGBEE, SOUND NETWORKS, WIRELESS, OSI, Z-WAVE TECHNOLOGY, IOT, SENSORS.

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1	9
Основи інтернету речей та інтеграція Zigbee в систему	9
1.1 Основне поняття ІОТ	9
1.2 Процес роботи ІоТ	9
1.3 Технології, що використовуються в системах ІоТ	10
1.4 Безпека Internet of Things	11
1.5 Приклади пристроїв ІоТ	11
1.6 Типи платформ ІоТ	13
1.7 Архітектура ІоТ	14
1.8 Модель OSI	15
1.9 Zigbee в ІоТ	20
Висновки	21
РОЗДІЛ 2	22
АНАЛІЗ ПРОТОКОЛУ ZIGBEE ТА ПОРІВНЯННЯ З ІНШИМИ ПРОТОКОЛАМИ В СИСТЕМІ ІОТ	22
2.1. Загальні відомості технології Zigbee	22
2.2. Короткий опис протоколу Zigbee	22
2.3 Хто використовує та випадки використання Zigbee	23
2.4 Архітектура Zigbee.....	26
2.5 ZigBee в рамках моделі OSI	28
2.6 Переваги ZigBee	29
2.7 Недоліки ZigBee	30
2.8 Покоління протоколу Zigbee.....	31
2.9 Що таке ZigBee Alliance?	35
2.10 Як працює ZigBee Alliance?	36
2.11 Різниця між Zigbee і WiFi.....	36
2.11.1 Бездротовий діапазон	37

2.11.2 Тип мережі	37
2.11.3 Споживання енергії	38
2.11.4 Швидкість і пропускна здатність	39
2.11.5 Перешкоди	39
2.11.6 Що краще, Zigbee чи Wi-Fi?	40
2.12 Різниця між Zigbee і Z-Wave.....	40
2.13 Різниця між Zigbee та Bluetooth.....	45
2.14 Порівняльна таблиця між WiFi, Zigbee, Z-wave та Bluetooth.....	46
Висновки	47
РОЗДІЛ 3	48
Проектування та створення власного IoT на протоколі Zigbee на прикладі створення власного розумного будинку.	48
3.1 Підготовка та створення власного IoT платформи для керуванням розумним будинком.	48
3.2. Логіка управління розумним будинком	50
3.3. Схема побудови розумного будинку	51
3.3.1 Реалізація сервера для розумного будинку	52
3.4 Процес роботи контролю розумним будинком через протокол Zigbee а саме через Zigbee2MQTT.	54
3.5 Інтеграція вашого розумного будинку HomeKit	62
Висновки	66
ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ	68
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	69

ПЕРЕЛІК СКОРОЧЕНЬ

AES	Advanced Encryption Standard
IP	International Protection Hub
DAS	Directly Attached Storage
DTU	Data Transition Unit
IDE	integrated development environment
IOT	Internet of Things
ISO	International Organization for Standardization
MAC	Media Access Control
MQTT	message queuing telemetry transport
M2M	Machine to machine
NWK	Network
OSI	The Open Systems Interconnection model
PHY	Physical layer (Фізичний рівень)
RFID	Radio-frequency identification
SoM	System On Model
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
Wi-Fi	Wireless Fidelity
WPAN	Wireless personal area network

ВСТУП

У сучасному світі зростає популярність інтернету речей (IoT), який відкриває нові можливості для автоматизації і керування різноманітними пристроями в реальному часі. Протокол ZigBee займає важливе місце серед бездротових протоколів зв'язку в IoT системах, завдяки своїм перевагам у високій енергоефективності, низькому рівню споживання енергії та довгому часу автономної роботи пристроїв.

Ця дипломна робота спрямована на розробку та побудову інтеграційного рівня для управління мережею IoT на базі протоколу ZigBee. Основна мета роботи полягає в створенні централізованої системи, яка забезпечує зручний та ефективний механізм керування різноманітними пристроями, що підтримують ZigBee стандарт.

У рамках дипломної роботи будуть досліджені та реалізовані основні аспекти інтеграції пристроїв на базі ZigBee, включаючи підключення та керування датчиками, актуаторами, реле та іншими розумними пристроями. Особлива увага буде приділена аналізу протоколу ZigBee, його особливостям та можливостям, що сприяють створенню надійних та ефективних IoT рішень.

Дана робота також передбачає дослідження інтеграції із сучасними платформами управління розумним будинком, такими як Home Assistant, OpenHAB та іншими, що дозволить розширити функціональні можливості системи та забезпечити зручний інтерфейс для кінцевих користувачів.

РОЗДІЛ 1

ОСНОВИ ІНТЕРНЕТУ РЕЧЕЙ ТА ІНТЕГРАЦІЯ ZIGBEE В СИСТЕМУ

1.1 Основне поняття ІОТ

ІоТ є глобальною мережею підключених пристроїв і технологій, яка спрощує комунікацію між пристроями і хмарними ресурсами, а також між самими пристроями. Завдяки одноплатним чіпам і широкосмуговому зв'язку тепер ми маємо мільярди пристроїв, підключених до Інтернету[13].

RFID-мітки, початково використовувані для відстеження дорогоцінного обладнання, стали символом розвитку комп'ютерних мікросхем малої потужності. За допомогою радіохвиль вони розпізнають об'єкти як "свої" чи "чужі". Процес здійснюється зчитувачем, який запитує інформацію від RFID-мітки, яка містить необхідні дані (наприклад, в супермаркетах для сканування товарів).

ІоТ має потенціал, щоб впливати не тільки на те, як ми живемо, а й на те, як ми працюємо.

1.2 Процес роботи ІоТ

Система ІоТ працює за допомогою збору та обміну даними в реальному часі. ІоТ ділиться на 3 компоненти, а саме:

1. Розумні пристрої

Телевізор, камера відеоспостереження або кавоварка) Вони збирають дані зі свого середовища, дані користувачів або шаблони використання та передає дані через Інтернет у свою програму ІоТ і з неї.

2. Додаток IoT

Це набір служб і програмного забезпечення, яке об'єднує дані, отримані від різних пристроїв IoT. Він використовує технологію машинного навчання, щоб аналізувати ці дані та приймати зважені рішення. Ці рішення передаються назад до пристрою IoT, і вже потім наявний пристрій IoT реагує на вхідні дані[17].

3. Графічний інтерфейс користувача

Пристроєм IoT можна керувати через графічний інтерфейс користувача. Типовими прикладами є додаток який використовується для реєстрації та керування датчиками. В нашому дослідженні буде використовуватися кілька застосунків та один веб-сайт (Apple Homekit, Aqara та Home Assistant).

1.3 Технології, що використовуються в системах IoT

Засоби ідентифікації

Кожен фізичний об'єкт, що бере участь в Інтернеті речей, повинен завжди мати унікальний ідентифікатор. Для цього використовуються різні системи, такі як радіочастотні мітки, оптичні коди (штрих-коди, QR-коди) або інфрачервоні мітки.

Засоби вимірювання

Засоби вимірювання призначені для перетворення інформації про навколишнє середовище в дані, які можна передавати для обробки. Це включає датчики вологості, температури та інші вимірювальні пристрої, які можуть живитися від альтернативних джерел енергії, наприклад, сонячних батарей.

Засоби передачі даних

Для передачі даних використовуються різні технології, включаючи бездротові мережі, такі як Zigbee, Z-wave, Fibra, а також дротові технології, наприклад, передачу даних по лініях електропередач.

Засоби обробки даних

Центральною частиною Інтернету речей є хмарні системи, які забезпечують високу пропускну здатність і здатність швидко реагувати на зміни. Туманні обчислення доповнюють хмарні системи, оптимізуючи обробку даних безпосередньо на місці збору.

Виконуючі пристрої

Це пристрої, що обробляють цифрові сигнали з інформаційних мереж для здійснення певних дій, наприклад, керування побутовими пристроями через мобільні додатки або голосові асистенти.

1.4 Безпека Internet of Things

Безпека є однією з найбільших проблем у галузі Інтернету речей. Часто ці датчики збирають особисті дані, які є конфіденційними для користувачів. Захист цих даних є критично важливим для збереження довіри споживачів, проте рівень безпеки в Інтернеті речей залишається низьким. Недоліки в програмному забезпеченні регулярно виявляються, але багато IoT-пристроїв не мають можливості для встановлення оновлень або вимагають фізичної присутності для оновлення[13].

1.5 Приклади пристроїв IoT

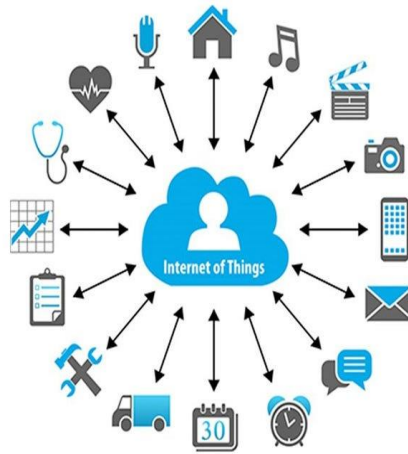


Рис 1.1 Схема прикладів пристроїв IoT

1. Дім.

Ключовим елементом, що лежить в основі сучасних та безпечних будинків, є Інтернет речей (IoT). Різноманітні датчики, освітлення, сигналізаційні системи та камери (всі вони можуть бути управляються зі смартфона) підключаються через IoT для забезпечення режиму доступу.

2. Трекери активності.

Сенсорні пристрої, які можуть відстежувати та передавати ключові показники здоров'я в режимі реального часу. Як результат можна відстежувати та керувати своїм кров'яним тиском, фізичною активністю, рівнем кисню тощо.

3. Промислова безпека та охорона.

Системи виявлення, датчики та камери з підтримкою Інтернету речей розміщують в зонах з обмеженим доступом для виявлення порушників. Гарним прикладом такої системи є продукція охорони безпеки Ajax Systems.

1.6 Типи платформ IoT

Платформи підключення

Платформи підключення забезпечують технології для з'єднання фізичних об'єктів з центром обробки даних, будь то локальний або хмарний центр, та для передачі інформації між ними. Серед відомих протоколів і стандартів для Інтернету речей (IoT) варто виділити MQTT, Bluetooth, ZigBee, WiFi та інші[17].

Платформи аналітики

Платформи аналітики використовують інтелектуальні алгоритми для аналізу зібраної інформації з метою створення корисних ідей для клієнтів.

Наскрізні платформи Інтернету речей

Наскрізні платформи Інтернету речей охоплюють всі аспекти продуктів IoT, включаючи розробку, підключення, управління даними та візуалізацію.

Платформи розробки устаткування

Платформи розробки устаткування надають фізичні плати для створення пристроїв IoT, таких як мікроконтролери, мікропроцесори, системи на кристалі (SoC) та системи на модулі (SoM)[19].

Платформи розробки додатків

Платформи розробки додатків служать як інтегровані середовища розробки (IDE) з необхідними інструментами і функціями для програмування додатків.

Визначення:

- **System-on-a-Chip (SoC):** Це дизайн електронної схеми, який об'єднує всі функціональні складові цілого пристрою на одній мікросхемі.
- **System-on-Module (SoM):** Це фізичний вбудований модуль, що містить основні компоненти, такі як процесорні ядра, комунікаційні інтерфейси та блоки пам'яті, і який можна підключити до несучої плати для вбудованої системи.

- Integrated Development Environment (IDE): Це програмне середовище, яке допомагає розробникам ефективно писати програмний код.

1.7 Архітектура IoT

Архітектура IoT складається з 5 рівнів, щоб забезпечити збір, зберігання та обробку даних пристроїв, створених датчиками, у сховищі великих даних, а також виконавчими механізмами пристроїв команд, надісланих через програму користувача. Наступна діаграма відображає архітектуру IoT[18].

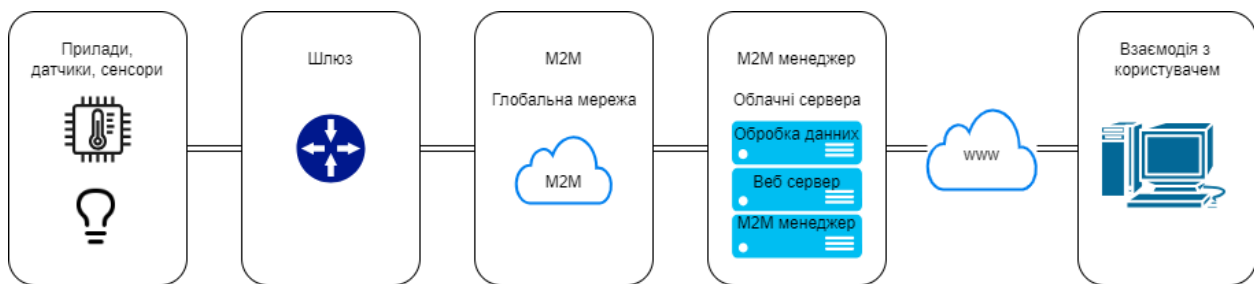


Рис 1.2 Схема архітектури IoT

Перший елемент системи IoT: датчики, детектори, приводи.

Датчики є пристроями або системами, які здатні виявляти та реагувати на зміни у своєму оточенні, перетворюючи фізичні параметри на електронні сигнали. Приводи — це компоненти, які перетворюють електричні сигнали в фізичні дії, і вони грають ключову роль у механізмах IoT. Машини та пристрої, оснащені цими компонентами, становлять основу інфраструктури IoT.

Другий елемент системи IoT: інтернет-шлюзи та системи збору даних.

Система збору даних (DAS) здійснює збір необроблених даних від датчиків, конвертує їх з аналогового формату в цифровий і готує до передачі через інтернет-шлюзи за допомогою бездротових або провідних мереж.

Третій елемент системи IoT: попередня обробка та аналітика.

Дані Інтернету речей проходять через попередню обробку, де вони агрегуються, аналізуються та оптимізуються ще до того, як вони будуть відправлені до центру обробки даних або у хмару. Цей процес може включати в себе машинне навчання для автоматизації реакцій на дані без чекання інструкцій з центрального центру.

Четвертий елемент системи IoT: аналіз у хмарі чи центрі обробки даних.

Дані піддаються детальному аналізу, управлінню та зберіганню за допомогою потужних IT-систем. Цей процес відбувається зазвичай у корпоративних центрах обробки даних або у хмарних сервісах, де дані IoT можуть бути аналізовані для виявлення ключових тенденцій, аномалій чи закономірностей.

П'ятий елемент системи IoT: надання оброблених даних користувачам.

Оброблені дані доступні для менеджерів системи або інших користувачів. Ці дані дозволяють виявляти тенденції, розуміти закономірності та реагувати на аномалії у реальному часі.

1.8 Модель OSI

Модель взаємодії відкритих систем (OSI) є фундаментальною конструкцією для всіх мережевих сутностей, визначаючи та розподіляючи мережеві протоколи на 7 логічних рівнях[21]. Протокол - це набір правил, що керує обміном даними. У кожному мережевому процесі управління передається від одного рівня до іншого, послідовно з'єднуючи протоколи на кожному рівні.

Різні технології бездротового зв'язку розроблялися для вирішення різних завдань. З огляду на це, їх функціонування можна розглядати в контексті моделі OSI. Модель OSI була розроблена Міжнародною організацією стандартизації

(ISO) ще в 80-х роках минулого століття і є основоположною для стандартів взаємодії мережевих систем.

Модель OSI виглядає наступним чином:

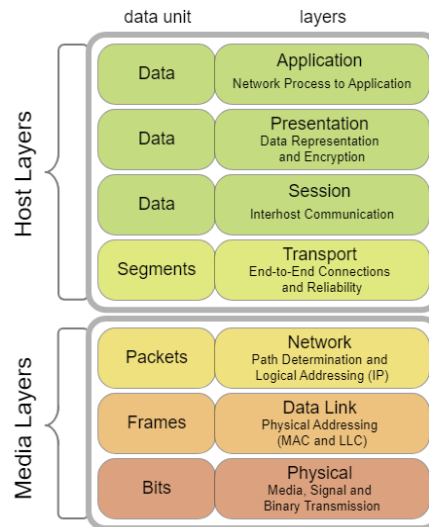


Рис.1.3 Схема 7 рівнів моделі OSI

- Прикладний рівень (Application).

На цьому рівні знаходяться мережеві служби, які дають змогу нам, як кінцевим користувачам, робити пошуки в інтернеті. Він починає використовуватися, коли найближчим часом потребується мережева взаємодія. Прикладний рівень це інтерфейс взаємодії між дійсними застосунками.

- Рівень представлення (Presentation).

На шостому рівні відбувається перетворення форматів повідомлень, таке як кодування або стиснення. Наприклад (JPEG, PNG, GIF). Так само рівень відповідальний за передачу потоку на четвертий (транспортний рівень). Ціль - направлення даних в правильний формат. Функція перелога надає дані передані з одного пристрою прочитаному на іншому пристрої.

- Сеансовий рівень (Session).

Сеансовий рівень займається тим, що керує з'єднаннями, або просто кажучи, сесіями. Відповідає за встановлення, підтримкою та завершення сеансу зв'язку. Координує зв'язок між системами і організовує зв'язок в одному з трьох режимів: сімплекс, напівдуплекс та дуплекс.

- Транспортний рівень (Transport).

Транспортний рівень, як можна зрозуміти з назви, забезпечує передачу даних мережею. Передача даних може бути гарантійною або ж не гарантійною. Найпопулярніші протоколи даного рівня - TCP і UDP.

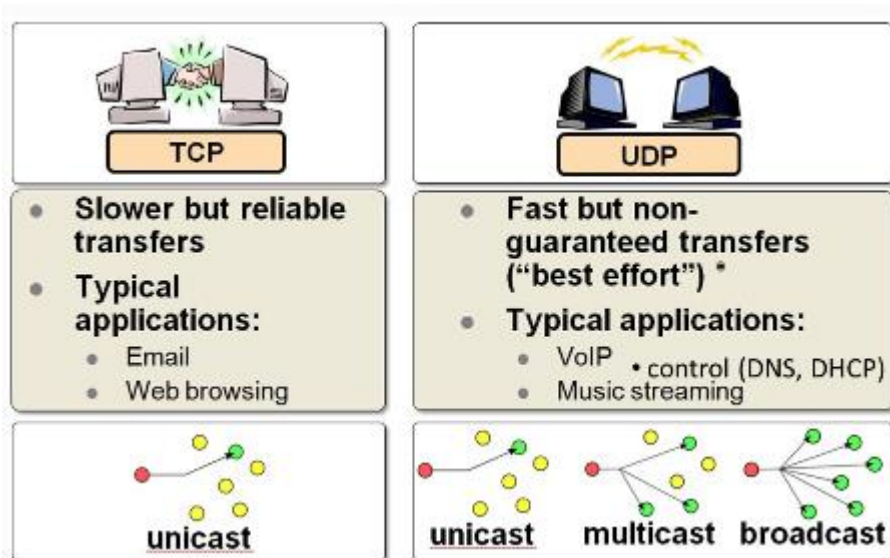


Рис. 1.4 Порівняльна таблиця TCP та UDP

Протокол UDP є дуже простим і призначений для доставки пакетів до застосунків через вказаний UDP-порт. Він не забезпечує контроль доставки, цілісності повідомлень або фрагментації. Це забезпечує його високу швидкість, оскільки не потребує додаткових полів у заголовку, що знижує обробку службової інформації. UDP використовується тоді, коли важливо швидко доставити дані, навіть за умови втрати пакетів. Прикладом може бути запуск стрімінгового відео на платформі YouTube.

TCP призначений для гарантованої доставки даних. Для цього він встановлює сеанс зв'язку перед обміном даними між застосунками. Встановлення сеансу включає домовленість із передачею службових повідомлень, що підтверджують правильність передачі та отримання даних. Ці службові процедури забезпечують надійність, хоча це призводить до повільнішої передачі даних порівняно з UDP. Прикладом може служити відправлення електронного листа колегам на роботу.

- Мережевий рівень (Network).

Мережевий рівень вводить термін «маршрутизація» і, відповідно, IP-адресу.

Саме на цьому рівні відбувається маршрутизація трафіку. Якщо ми хочемо потрапити на сайт, то ми відправляємо DNS-запит, отримуємо відповідь у вигляді IP-адреси і підставляємо її в пакет. Взагалі відповідає за логічне посилення даних на більш ефективному шляху. Загалом працює з IP-адресами. Прилади: маршрутизатор та роутер.

Ip-адресація використовує IPv4 та IPv6.

Маршрутизація - процес встановлення напрямку інформації в мережах зв'язку. Відповідає за доставку пакетів в інші мережі. Ip ділиться на 2 частини: адрес мережі та адрес приладу в мережі.

Маршрутизація буває статичною та динамічною. Шлях за замовчуванням відзначається, як 0.0.0.0 (адрес шлюза). Якщо шляхів декілька, то зрівнюються метрики. Чим нижче метрика, тим більший пріоритет у шляху.

Протокол маршрутизації - мережевий протокол, який використовується маршрутизаторами для виявлення можливих маршрутів слідування даних в конкретних комп'ютерних мереж. Він може працювати тільки з пакетами, які

належить одному із протоколів маршрутизатора. Наприклад Ip, Ipx, Xerox Network system.

- Канальний рівень (DataLink).

Це набір напруг різної амплітуди, хвиль і радіочастот. Під час отримання, на другому рівні перевіряються і виправляються помилки передачі. Тут з'являються перші ідентифікатори — MAC-адреси. Вони складаються з 48 біт і мають приблизно такий вигляд: 00:16:52:00:1f:03.

Канальний рівень відповідає за фізичну доставку даних. Прилади: комутатор або мережева карта.

Канальний рівень складний. Тому, його умовно кажучи ділять на два підрівні: управління логічним каналом (LLC, Logical Link Control) і управління доступом до середовища (MAC, Media Access Control)[21].

MAC - адрес - управління доступом до середи - унікальний ідентифікатор, який присвоєний мережевому інтерфейсу в мережах Ethernet.

- Фізичний рівень (Physical).

На першому рівні моделі OSI відбувається передача фізичних сигналів (струмів, світла, радіо) від джерела до одержувача. На цьому рівні ми оперуємо кабелями, контактами в роз'ємах, кодуванням одиниць і нулів. Фізичний рівень задає рівні сигналів. Можливі прилади: Патч - панель, кабель Ethernet, коннектор RJ-45.

1.9 Zigbee в IoT



Рис. 1.5 Коротка схема роботи з приладами на протоколі Zigbee

Zigbee відрізняється своєю низькою енергоспоживанням і швидкістю передачі даних, що робить його ідеальним для застосування в IoT та вбудованих системах, таких як домашня автоматизація, бездротові сенсорні мережі, оповіщення про дим і вторгнення, автоматизація будівель та інше. Наприклад, у розумних будинках контролер на протоколі Zigbee може підключати та управляти значною кількістю пристроїв, обробляючи дані локально перед їх відправленням на хмарну платформу для дистанційного контролю.

В промисловому секторі датчики Zigbee збирають дані про температуру, вологість, тиск, потік тощо, які потім передаються через блок передачі даних (Zigbee DTU) до центральної обробної системи або хмарної платформи для подальшого аналізу і обробки. Технологія також дозволяє дистанційно керувати пристроями, такими як регулювання температури, відкриття та закриття клапанів, контроль дверей тощо.

Однак, як і інші IoT рішення, Zigbee потребує уважного управління безпекою через можливість вразливостей, що можуть стати проблемою в разі недостатньої уваги до захисту даних та пристроїв.

Висновки

Інтернет речей є однією з найбільш перспективних галузей сучасних технологій, яка значно впливає на розвиток сучасного суспільства і промисловості. Ця технологія відкриває безліч можливостей для автоматизації, оптимізації і збільшення ефективності різних секторів, включаючи будівництво, медицину, промисловість, транспорт та побутове використання. Інтеграція ZigBee в систему IoT вимагає ретельного проектування та налагодження інтеграційного рівня, що забезпечить сумісність з іншими протоколами і стандартами, ефективне керування мережею та забезпечує високий рівень безпеки і захисту даних. Основні виклики включають управління ресурсами, підтримку масштабування та відповідність з стандартами забезпечення конфіденційності та інформаційної безпеки.

РОЗДІЛ 2

АНАЛІЗ ПРОТОКОЛУ ZIGBEE ТА ПОРІВНЯННЯ З ІНШИМИ ПРОТОКОЛАМИ В СИСТЕМІ ІОТ

2.1. Загальні відомості технології Zigbee

Zigbee - це мережевий протокол для бездротових пристроїв з низьким споживанням енергії, який об'єднує їх через сітчасту мережу на основі радіопротоколу IEEE 802.15.4.[22] Протокол забезпечує спільну взаємодію пристроїв з такими характеристиками: висока надійність, довговічність пристроїв від однієї батареї, підтримка багатьох підключень і сумісність пристроїв різних виробників. Zigbee спеціально розроблено для бездротових персональних мереж (WPAN) і є продуктом альянсу Zigbee. Цей стандарт визначає фізичні та контрольні рівні доступу до мережі (MAC) для обробки даних з низькою швидкістю передачі. Zigbee WPAN працюють на частотах 868 МГц, 902-928 МГц і 2,4 ГГц. Швидкість передачі даних 250 кбіт/с ідеально підходить для періодичної та інтерактивної двосторонньої передачі інформації між датчиками та контролерами. Протокол підтримує роботу у 27 каналах трьох частотних діапазонах: 2,4 ГГц (16 каналів), 915 МГц (10 каналів) та 868 МГц (1 канал)[8]. Кінцеві пристрої можуть входити в режим сну для збереження заряду батареї і забезпечення безпеки інформації.

2.2. Короткий опис протоколу Zigbee

Для кращого розуміння та чіткого уявлення в наступній таблиці надано підсумок усіх технічних аспектів:

Таблиця 2.1

Технічні характеристики протоколу Zigbee

Характеристика	Опис
Частота	2,4 ГГц, 868/915 МГц та інші частоти в залежності від регіону
Швидкість передачі даних	Від 20 до 250 кбіт/с
Екскурсія	Від 10 до 100 метрів
Топологія мережі	Mesh-мережа, де кожен пристрій може діяти як маршрутизатор для розширення охоплення мережі
Безпека	Шифрування AES-128 для безпечного зв'язку
Споживання енергії	Низька потужність, призначена для роботи від невеликих батарей або інших джерел малої потужності
сумісність	Сумісність з іншими пристроями Zigbee, незалежно від виробника
Стандартний	Відкритий стандарт, не прив'язаний до якогось конкретного постачальника чи продукту.

2.3 Хто використовує та випадки використання Zigbee

Список того, хто використовує протокол Zigbee:

- Побутові та комерційні користувачі
- Розробники апаратного забезпечення IoT
- Постачальники/екосистеми послуг IoT
- Утиліти IoT

Приклади та випадки використання:

- Розумний будинок;

В основному в сучасних будинках реалізовано багато електричних та електронних пристроїв. Наприклад: світильник, освіжувач повітря, розумний пилесос, холодильник, кондиціонер, витяжка, пральні машини, кондиціонери тощо. Але також можуть бути наявні, система антипотоп, контроль отопленням, кліматом, розумні штори, реле для контроль світла та інше обладнання. У минулому можна було досягти керування «точка-точка», але якщо використовувати технологію ZigBee, ці електронні пристрої можна з'єднати, щоб утворити єдину мережу. Все це можна приєднати до Інтернету через hub і люди через це здатні швидко керувати системою розумного будинку з будь-якої точки без необхідності прокладання кабелю в житлі. Застосування даної технології ладна підвищити зручність експлуатації та знизити вартість будинку, з одного боку зі сторони монтажу.

- Складська логістична система;

З просуванням складських і логістичних систем попит на необмежені системи передачі даних демонструє тенденцію до зростання. Він пропонує високу ефективність і низьку вартість для технології бездротового зв'язку. ZigBee особливо підходить для складських і логістичних систем завдяки своїй безпеці та надійності.

Його практика має форму:

1. Планування транспортних засобів на місці.
2. Мережева структура технології бездротового зв'язку ZigBee mesh може бути застосована до складського господарства та логістики, покладаючись на пересилання даних, динамічну маршрутизацію та інші засоби для забезпечення надійності та ефективності загального зв'язку системи.

3. Транспортні засоби на складах і в логістиці завжди повинні постійно рухатися, а звичайні протоколи бездротового зв'язку завжди демонструють проблему недостатньої гнучкості в пошуку найкращого маршруту.

- Розумний догляд за людьми похилого віку

Рішення IoT для домашнього догляду за людьми похилого віку дозволяють використовувати непомітні бездротові датчики, розміщені по всьому будинку, щоб вивчати щоденні моделі поведінки людей похилого віку та виявляти зміни поведінки, які можуть викликати занепокоєння. Розумна система догляду за людьми похилого віку була успішно випробувана в інтернатних закладах протягом кількох років.

- Медичний моніторинг

Електронний медичний моніторинг в даний час активно вивчається. Багато датчиків розташовано на тілі людини для вимірювання пульсу, артеріального тиску та стану здоров'я. Монітори та системи сигналізації також розміщені в палатах лікарень для постійного моніторингу фізичного стану. Якщо виникає проблема, оперативно реагують, наприклад, сповіщаючи медичний персонал лікарні.

Завдяки технології ZigBee ці датчики, монітори та системи сигналізації можуть бути підключені для створення мережі моніторингу. Оскільки вона працює бездротово, не потрібне провідне з'єднання між датчиками, і пацієнт може вільно рухатися.

- Сенсорна мережева програма

Сенсорні мережі зараз активно вивчаються і мають значні перспективи застосування у моніторингу навантаження, контролі будівель та охороні навколишнього середовища. Дешеві вузли, низьке енергоспоживання, автоматичне об'єднання в мережі, просте обслуговування та висока надійність є ключовими вимогами до таких мереж.

ZigBee відмінно підходить для мережевих застосувань сенсорів завдяки своїм мережевим перевагам і низькому енергоспоживанню.

- Автоматичне зчитування лічильників

Датчики перетворюють показання лічильників у цифрові сигнали, які надсилають показання безпосередньо до газової чи водопровідної компанії через мережу ZigBee. Наприклад водопровідна компанія може надіслати деяку інформацію безпосередньо користувачеві або поєднати її з енергозбереженням.

2.4 Архітектура Zigbee

Стандарт IEEE 802.15.4 визначає рівні PHY (фізичний) і MAC (доступ до середовища), які використовуються в Zigbee. Zigbee Alliance використовує ці рівні для визначення структури NWK (мережевий рівень) і рівня додатків. В рамках цієї структури також присутній підрівень підтримки додатків, включаючи об'єкти пристрою Zigbee (ZDO) і об'єкти додатків виробників, які контролюються Zigbee Alliance.

В Zigbee Stack існують три нижні рівні: фізичний, каналний і мережевий. Останні чотири шари - транспортний, сеансовий, презентаційний і прикладний - охоплюються підрівнем підтримки додатків і ZDO. Між цими шарами забезпечені точки доступу до послуг, що ізолюють роботу кожного рівня від шарів над ним і під ним.

- Фізичний рівень.

Як згадувалося раніше, найнижчі два рівні, тобто. PHY і MAC визначаються специфікацією IEEE 802.15.4. Фізичний рівень конвертує дані у пакети бітів для передачі через радіоканал і навпаки при отриманні. Рівень MAC відповідає за інтерфейс між фізичним рівнем та мережевим рівнем (NWK). Він керує ідентифікацією PAN (Personal Area Network) і визначенням мережі через маяки. Рівень MAC також відповідає за управління формуванням та маршрутизацією мережі. Крім цього, рівень NWK забезпечує безпеку мережі Zigbee, зокрема, шифрує всі дані в рамці NWK.

- Рівень додатків.

Рівень додатків у стеку Zigbee є найвищим рівнем протоколу, що включає підрівень підтримки додатків (APS) і об'єкт пристрою Zigbee (ZDO). Він включає програми, розроблені виробником для взаємодії з мережевим стеком. Підрівень APS відповідає за виявлення та зв'язування служб. Об'єкт пристрою Zigbee (ZDO) управляє локальним і бездротовим мережевим керуванням. Application Framework містить Application Objects, які контролюють і керують рівнями протоколу в пристрої Zigbee. Фрейм додатка може вміщувати до 240 об'єктів додатка.

Згідно зі стандартом IEEE 802.15.4, існують два типи пристроїв: FFD (повнофункціональні пристрої) та RFD (пристрої з обмеженими функціями). Пристрої FFD можуть спілкуватися з будь-яким іншим пристроєм у мережі та завжди активні, слухаючи мережу. Пристрої RFD можуть спілкуватися лише з FFD та призначені для простих застосувань, таких як управління вмикачами.

Зігбі створив три типи пристроїв: координатор Zigbee, маршрутизатор Zigbee та кінцевий пристрій Zigbee. Координатор Zigbee виступає як координатор

PAN у мережі IEEE 802.15.4 і відповідає за створення мережі та призначення мережесих адрес. Маршрутизатор Zigbee також є координатором у стандарті IEEE 802.15.4 і розширює покриття мережі Zigbee, дозволяючи підключати більше пристроїв. Кінцевий пристрій Zigbee фізично підключається до датчиків або виконує керуючі операції.

Топології мережі Zigbee включають зіркову, кластерну деревну та мешову структури. У кожній з цих топологій координатори та маршрутизатори використовуються для забезпечення комунікації між кінцевими пристроями. Мережа Zigbee застосовується у домашній автоматизації, охороні здоров'я та інших сферах, де важливе бездротове зв'язку та управління пристроями.

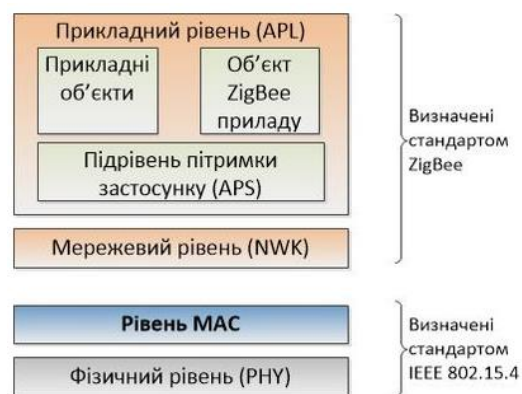


Рис 2.1. Схема архітектури Zigbee

2.5 ZigBee в рамках моделі OSI

Протокол ZigBee використовує лише верхні рівні моделі OSI - мережесий, транспортний і прикладний. Він базується на стандарті IEEE 802.15.4, який встановлює нижні рівні безпроводової мережі для до 47 кінцевих пристроїв, не користувачів, аплікацій. Стандарт IEEE 802.15.4 використовується не тільки ZigBee, але й в інших протоколах, підтримуваних кількома постачальниками чіпів. Він працює на неліцензованих частотах 2,4 ГГц (по всьому світу), 915 МГц

(Америка і Австралія) і 868 МГц (Європа), з швидкістю до 250 Кбіт / с в 2,4 ГГц, 40 Кбіт / с в 915 МГц і 20 Кбіт / с в 868 МГц діапазонах.

У мережах ZigBee маршрутизація відбувається від адресата, у відмінність від Z-Wave, яка використовує маршрутизацію від джерела. Мережа включає три класи пристроїв: координатор, маршрутизатор (який постійно діє і забезпечує зв'язок до 32 кінцевих пристроїв), і кінцеві пристрої (які в основному сплять, щоб заощадити енергію, і можуть ініціювати або приймати пакети, але не ретранслюють їх).

2.6 Переваги ZigBee

Однією з головних переваг Zigbee є спрямованість на економних споживачів. Це сприяється не лише відкритістю стандарту, але й простота процесу сертифікації нових товарів, що дозволяє виробникам впроваджувати власні конфігурації.

З точки зору енергоефективності Zigbee також вражає. Деякі пристрої можуть працювати до 3 років без заміни батарей, що робить їх привабливими для ринку домашньої автоматизації. Хоча швидкість передачі даних у Zigbee дещо обмежена (до 250 Кбіт/с), технологія має потужний потенціал масштабування, підтримуючи до 65 000 вузлів[22].

Проте, на практиці, мережі з великою кількістю вузлів можуть зіткнутися з проблемами, такими як затримки в обміні даними, особливо в умовах високого навантаження. Такі проблеми можуть виникати навіть при розгортанні маленьких мереж.

Усупереч цим обмеженням, Zigbee залишається привабливим вибором для виробників, орієнтованих на витратоємні рішення у бездротовій домашній

автоматизації, завдяки своїй ефективності, гнучкості та широкому колу підтримуваних пристроїв.

2.7 Недоліки ZigBee

У сьогоднішній день Zigbee часто має проблеми з перешкодами від інших пристроїв у зоні дії мережі, особливо у забрудненому діапазоні 2,4 ГГц, який використовують також Wi-Fi і Bluetooth. Оскільки Zigbee працює на одному каналі, він не завжди ефективно справляється з конкуренцією за смугою. З роками завантаженість цієї смуги лише зростає, що загрожує погіршенням ситуації для Zigbee.

Ще однією проблемою є обмеження стандарту IEEE 802.15.4, яке визначає фізичний рівень для Zigbee, з максимальною швидкістю передачі даних 250 Кбіт/с. Цей стандарт підконтрольний IEEE і застосовується в багатьох інших технологіях, що робить важким внесення змін в конфігурації без довгих переговорів з IEEE.

З погляду безпеки, Zigbee пропонує широкий спектр заходів, таких як 128-бітовий AES алгоритм для шифрування і аутентифікації даних. Однак з часом виявляються нові вразливості, які можуть стати загрозою для безпеки мереж Zigbee, навіть за наявності таких заходів захисту.

Найбільшою проблемою для Zigbee є сумісність між пристроями різних виробників. Часто пристрої різних брендів не можуть взаємодіяти прямо між собою, що ускладнює використання цієї технології в розумному будинку. Хоча Zigbee Alliance розробила стандартизовані профілі, які мають сприяти сумісності, на практиці проблеми все ще існують через велику вольність виробників у виборі функцій захисту і надзвичайною практикою створення пропрієтарних рішень.

2.8 Покоління протоколу Zigbee

Zigbee 1.0

Zigbee (раніше відомий як HomeRF Lite) був ратифікований як протокол бездротового зв'язку на основі стандарту IEEE 802.15.4 у 2004 році, а 13 червня 2005 року Альянс Zigbee оголосив про доступність специфікації 1.0, також відомої як специфікація ZigBee 2004.

Zigbee 1.1

Zigbee 1.0 є першою версією специфікації Zigbee, яка мала свої недоліки. Для вирішення цих проблем було введено ZigBee 1.1. Кластерна бібліотека Zigbee замінила попередню структуру пар значень, що використовувалась у стеку 2004 року. Це дозволяє пристроям Zigbee асинхронно повідомляти клієнтів про зміни атрибутів, що забезпечує можливість оновлення атрибутів і сповіщень у реальному часі. Приклади назв кластерів включають Zigbee Light Link, Home Automation і Smart Energy. Важливо відзначити, що цей новий протокол несумісний з ZigBee 1.0.

Zigbee Pro

Незважаючи на те, що ZigBee 1.1 внесло значні зміни порівняно з ZigBee 1.0, визнано, що оригінальне бачення ще не було повністю досягнуто. У 2007 році специфікація Zigbee пройшла ще один перегляд з метою забезпечення зворотної сумісності і була доповнена версією ZigBee Pro. Це дозволило пристроям ZigBee Pro підключатися до застарілих мереж Zigbee і працювати в них, а також навпаки. ZigBee Pro операційно працює в діапазоні ISM 2,4 ГГц і додає підтримку діапазону нижче ГГц, що забезпечує більшу гнучкість у використанні частот.

Спеціалізовані протоколи Zigbee:

Zigbee Home Automation (ZHA)

Ця версія Zigbee призначена для більш загального використання в широкому спектрі додатків домашньої автоматизації і має функціональність, що дозволяє інтегрувати складні мережеві топології і різноманітні пристрої в одну систему. Основні особливості ZHA включають використання профілів додатків Zigbee (ZAP), що забезпечують безпроблемну сумісність між різними типами пристроїв.

ZHA використовує стек Zigbee Home Automation, який менш надійний порівняно зі стеком Zigbee Pro, але має більшу енергоефективність, що особливо важливо для пристроїв з живленням від батарейок.

Zigbee Light Link (ZLL)

Це спеціалізована версія Zigbee, оптимізована для освітлення. Вона має наступні особливості:

ZLL спеціально розроблено для управління освітленням та включає функції, які дозволяють контролювати колір і інтенсивність освітлення.

ZLL використовує простіший процес налаштування мережі, що спрощує додавання пристроїв до мережі без необхідності використання центрального концентратора чи координатора. ZLL також включає функцію "Light Link", яка дозволяє групувати та керувати освітленням одночасно, сприяючи створенню сценаріїв і автоматизації освітлення в розумному домі або будівлі. ZLL також сумісний з іншими пристроями Zigbee, що забезпечує можливість працювати з іншими продуктами і екосистемами, що базуються на Zigbee.

Zigbee Building Automation (ZBA)

Призначений для програм автоматизації комерційних і промислових будівель, забезпечує інтеграцію та контроль різних систем, включаючи освітлення, вентиляцію, кондиціонування, контроль доступу та управління енергією в комерційних будівлях.

Zigbee Healthcare (ZHC)

Відповідає особливим потребам програм охорони здоров'я, включаючи моніторинг медичних пристроїв, моніторинг пацієнтів і віддалені медичні послуги.

Zigbee Green Power (ZGP)

Це спеціалізована версія Zigbee, оптимізована для пристроїв із низьким енергоспоживанням, що живляться від батареї, і має функції, які забезпечують енергоефективний зв'язок і безпеку в мережі пристроїв. Основні характеристики:

ZGP використовує унікальний метод зв'язку під назвою "Green Power Tunneling", що дозволяє пристроям спілкуватися один з одним без необхідності використання центрального концентратора чи координатора. Це зменшує енергоспоживання та подовжує термін служби батареї ваших пристроїв. Протокол Zigbee Green Power споживає менше енергії завдяки впровадженню різних функцій енергозбереження, таких як режим сну, зниження активності бездротової передачі даних, зниження швидкості передачі даних, енергозберігаюча конструкція та збір енергії.

ZGP використовує стек Zigbee Pro, який є більш надійним, ніж стек Zigbee Home Automation, що дозволяє використовувати більші мережі та більше пристроїв, а також має покращені функції безпеки.

Zigbee Smart Energy (ZSE)

ZSE спеціально призначено для використання в додатках управління енергією, таких як розумні лічильники, контроль навантаження та AMI (Advanced Metering Infrastructure). Він використовує Zigbee Smart Energy Application Profile (SEP), який визначає протоколи зв'язку та моделі даних, що використовуються пристроями в мережі. Це забезпечує сумісність різних типів пристроїв для управління енергією. ZSE включає такі функції, як автоматичне зчитування лічильників (AMR), дистанційне відключення/повторне підключення та реагування на потреби, корисні для управління споживанням енергії та витратами. ZSE також включає розширені функції безпеки, такі як шифрування Advanced Encryption Standard (AES), безпечне встановлення ключа та безпечне оновлення по повітрю (OTA), щоб захистити вашу мережу та підключені до неї пристрої.

Zigbee 3.0

Zigbee 3.0 уніфікував раніше згадані протоколи прикладного рівня, такі як ZHA, ZLL, ZBA та ZHC. Для того щоб забезпечити сумісність пристроїв різних виробників, від підключення до мережі до операцій пристрою, таких як увімкнення та вимкнення, кожен аспект повинен бути чітко визначений. Зигбі 3.0 також стандартизував процедури виявлення пристроїв і підключення до мережі, використовуючи різні протоколи прикладного рівня, що значно спрощує взаємодію пристроїв Зигбі у мережі і сприяє розробці нових продуктів. Наприклад, користувачі можуть з легкістю підключати та керувати розумними вимикачами та лампочками різних виробників через мережу Zigbee.

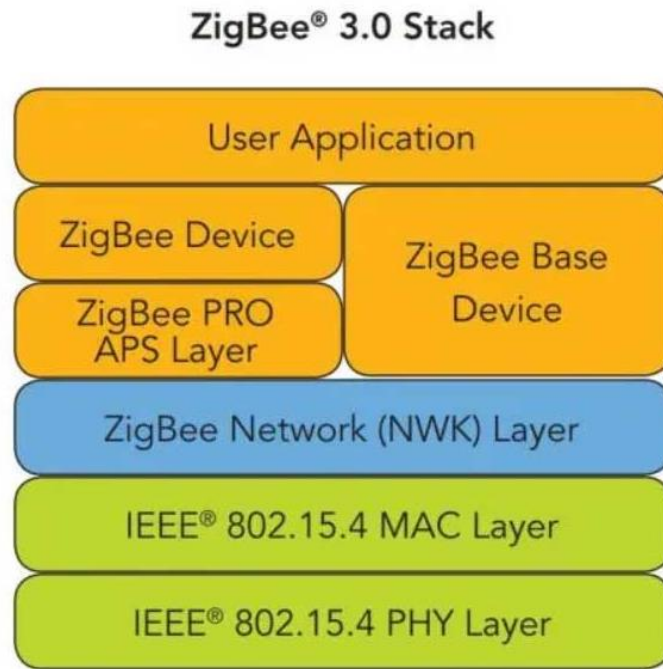


Рис 2.2. Zigbee 3.0 Stack

2.9 Що таке ZigBee Alliance?

ZigBee Alliance — некомерційна організація, що об'єднує близько 400 технологічних компаній, заснована у 2002 році.



Рис 2.3 Частина компаній, які є частиною zigbee alliance

На сьогодні ZigBee Alliance випустив три покоління стандартів:

ZigBee 1.0 (2004);

ZigBee 2.0 (2007);

ZigBee 3.0 (2014);

2.10 Як працює ZigBee Alliance?

Мета альянсу Zigbee полягає в створенні надійної, доступної та енергоефективної цифрової інформації та управління для промислового та комерційного використання. Це підкреслює важливість, яку вони враховували під час розробки. Іншими словами, Zigbee Alliance розробляє специфікації для бездротових технологій, які функціонують у мережі.

Цей визначний альянс продемонстрував свій швидкий розвиток, річно випускаючи понад 50 мільйонів розумних пристроїв ZigBee. Найпопулярнішими застосунками ZigBee є системи домашньої автоматизації, де користувачі можуть віддалено управляти освітленням, замками, термостатами та іншими пристроями за допомогою своїх смартфонів або планшетів.

2.11 Різниця між Zigbee і WiFi

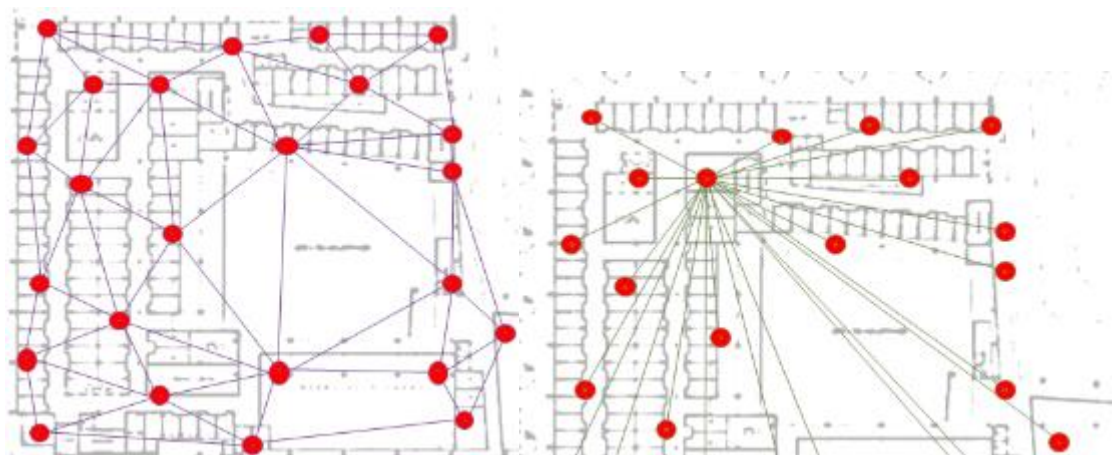


Рис 2.5 Приклад різниці роботи протоколу Zigbee та WiFi

WiFi і ZigBee мають свої переваги, але вони, очевидно, мають і певні недоліки. Розберемо позитивні і негативні відмінності між цими двома протоколами.

2.11.1 Бездротовий діапазон

Розумні пристрої з підтримкою WiFi і Zigbee використовують бездротовий зв'язок, що забезпечує їм більшу зручність і спрощує процес встановлення. Обидва типи пристроїв працюють на частоті 2,4 ГГц, що забезпечує ширший радіус дії та можливість проникнення крізь стіни та двері. Однак через те, що вони використовують одну і ту ж частоту, вони можуть взаємно перешкоджати один одному, особливо якщо декілька пристроїв розташовані поруч.

Пристрої, які працюють через Wi-Fi, мають значно більший зону охоплення, ніж Zigbee, здатні взаємодіяти та працювати на відстані від 30 до 100 метрів. Натомість, пристрої Zigbee мають зону охоплення лише близько 20 метрів. Проте завдяки можливості пристроїв-ретрансляторів Zigbee розширювати мережу, а також можливості придбати спеціальні підсилювачі мережі, цей недолік компенсується.

2.11.2 Тип мережі

Тип мережі, що використовується в системі, визначає спосіб підключення кожного пристрою до центрального контролера (або концентратора), який виступає центральним блоком керування для всіх підключених компонентів. Системи розумного дому переважно використовують два типи мереж: зіркові і мережі з маршрутизацією.

У зірковій мережі кожен пристрій спілкується безпосередньо лише з центральним концентратором (наприклад, роутером для розумних пристроїв

WiFi). Якщо пристрій виходить за межі діапазону центрального концентратора, він втрачає з'єднання з мережею.

Мережі з маршрутизацією (mesh) дозволяють кожному пристрою в мережі виступати як ретранслятор, який може передавати сигнал іншому пристрою. Це дозволяє мережам з маршрутизацією подолати великі відстані і обходити перешкоди.

WiFi використовує зіркову мережу, де всі пристрої підключаються до WiFi-рутера. Натомість пристрої Zigbee використовують мережу з маршрутизацією і підключаються один до одного для зв'язку з контролером Zigbee. Це дозволяє системі розумного дому з пристроями Zigbee працювати більш координаційно та мати більший радіус охоплення загалом[23].

Важливо відзначити, що пристрої Zigbee, що працюють від батарейок, не функціонують як ретранслятори і не можуть посилати сигнали на інші пристрої.

2.11.3 Споживання енергії

При розгляді енергоефективності систем, системи WiFi зазвичай споживають значно більше енергії, ніж їхні аналоги на базі Zigbee. Мережі Zigbee, наприклад, зазвичай використовують менше 25% енергії в порівнянні з WiFi. Пристрої Zigbee працюють з низьким енергоспоживанням, споживаючи мікроампери. Термін служби батарейок у пристроїв Zigbee є значно довшим, ніж у пристроїв WiFi, що є великою перевагою. Цей аспект потрібно ретельно враховувати при плануванні розумного будинку, особливо якщо ваші пристрої працюватимуть від акумуляторів або батарейок.

2.11.4 Швидкість і пропускна здатність

Пристрої, які використовують Wi-Fi, мають значно вищу швидкість передачі даних порівняно з Zigbee. Більшість Wi-Fi мереж можуть досягати максимальної швидкості передачі даних 11 Мбіт/с, що ідеально підходить для потокового відео у форматі Full HD, що важливо для камер спостереження як усередині, так і зовні. Протокол Zigbee, натомість, має значно меншу швидкість передачі даних - лише 250 Кбіт/с. Проте для більшості розумних пристроїв вдома ця швидкість виявляється більш ніж достатньо. Наприклад, система захисту від протікання може реагувати миттєво на виявлення витoku води, затримуючи його за доли секунди до закриття клапана подачі води. Через низьку швидкість передачі даних пристрої Zigbee зазвичай споживають менше енергії. Більшість розумних пристроїв не мають проблем з обмеженою швидкістю передачі даних у порівнянні з Wi-Fi, зокрема через переваги в енергоефективності.

2.11.5 Перешкоди

Пристрої Wi-Fi більш схильні до перешкод. По-перше, пристрої, які підключені безпосередньо до вашого роутера Wi-Fi, можуть значно навантажувати вашу Wi-Fi мережу і з'єднання з Інтернетом. Це може призвести до зниження швидкості Інтернету або погіршення якості з'єднання Wi-Fi у випадку, коли підключено занадто багато пристроїв і навантаження стає великим.

Натомість, пристрої Zigbee мають менші ймовірності зазнати подібних проблем. Центральний контролер Zigbee обробляє всі дані локально і не вимагає хмарних обчислень. Це означає, що немає навантаження на вашу існуючу Wi-Fi мережу. Крім того, за допомогою Zigbee ваш розумний будинок може продовжувати функціонувати навіть при відсутності Інтернету, оскільки пристрої продовжують взаємодіяти з контролером Zigbee локально. Zigbee не

залежить від Інтернет-з'єднання, і пристрої зберігають свою функціональність, доки працює контролер Zigbee.

2.11.6 Що краще, Zigbee чи Wi-Fi?

Розглянуто переваги і недоліки кожного протоколу для розумного будинку, тому вибір залежить від ваших конкретних цілей і потреб. Якщо вам потрібно встановити бездротові пристрої з довгим терміном служби від батарейок і уникнути прокладання додаткових проводів, то варто вибрати пристрої Zigbee. Якщо ж вам необхідний відеонагляд або інші пристрої, які потребують високої швидкості зв'язку (наприклад, домофони чи викличні панелі), то найкращим рішенням будуть пристрої Wi-Fi.

Але що, якщо у вас потрібно поєднати обидва типи пристроїв в одному розумному будинку? В такому випадку, вам на допомогу прийде інноваційна платформа для розумних пристроїв - TuYa Smart.

2.12 Різниця між Zigbee і Z-Wave

Z-Wave — це протокол передачі даних, призначений для домашньої автоматизації. Характерною особливістю Z-Wave є стандартизація від фізичного рівня до рівня програми. протокол покриває всі рівні OSI класифікації, що дозволяє забезпечувати сумісність пристроїв різних виробників під час створення гетерогенних мереж[3].

Основною відмінністю між Z-Wave і Zigbee є радіочастота, яку вони використовують для спілкування з іншими пристроями Z-Wave або Zigbee. Z-Wave використовує низькочастотні радіодіапазони, які не заважають Wi-Fi. З іншого боку, Zigbee використовує IEEE 802.15.4. Ця частота не схильна до перешкод, особливо якщо у вас вдома мережа Wi-Fi 2,4 ГГц. Окрім частот, Z-

Wave та Zigbee відрізняються швидкістю передачі даних, радіусом дії та сумісністю з іншими пристроями Z-Wave чи Zigbee. ZigBee значно швидший за Z-Wave. ZigBee передає дані зі швидкістю 250 Кбіт/с порівняно зі швидкістю передачі Z-Wave 100 Кбіт/с. Протокол ZigBee справді працює швидше – навіть у 25 разів. Але це не означає, що це матиме суттєве значення, і це справедливо, лише якщо ви використовуєте дійсно старі пристрої ZWave. Більшість новіших пристроїв Z-Wave працюють зі швидкістю 100 Кбіт/с, тоді як ZigBee працює зі швидкістю 250 Кбіт/с[1]. Однак - це не означає, що ви повинні помітити суттєву різницю - обидва протоколи повинні працювати досить швидко, і якщо ви бачите 5-6 секундні затримки, то, ймовірно, це спричинено мережевими тайм-аутами. ZigBee працює трохи краще, ніж ZWave, оскільки кілька транзакцій можуть бути незавершеними одночасно.

Протокол Zigbee використовує частоту 915 МГц у США та частоту 2,4 ГГц у Великобританії. Передача сигналу на пристрій із такою частотою може призвести до відсутності або хитромудрості сигналів. Це виникає через перешкоди та перевантаження будь-якого Wi-Fi, мікрохвильової печі або пристрою, що працює на високій частоті в цій зоні. З іншого боку, протокол Z-Wave використовує діапазон частот 900 МГц, а саме 908,42 МГц. Також існує ймовірність виникнення перешкод із пристроями, які використовують частоти в діапазоні 900 МГц, як-от стаціонарні телефони. Однак це втручання мінімальне. Протокол Zigbee підтримує мережеві підключення між 65 000+ пристроями одночасно. Протокол Z-Wave підтримує сітчасті з'єднання з максимум 232 пристроями. Цей діапазон підключення може бути придатним для невеликих організацій, підприємств середнього розміру, розумних будинків та інших малих і середніх випадків використання IoT[3].

Протокол Zigbee дозволяє здійснювати незліченну кількість переходів за одну передачу. Протокол Zigbee підтримує з'єднання між будь-якою кількістю

пристроїв, які ви бажаєте підключити. протокол Z-Wave дозволяє лише чотири стрибки на передачу. Це означає, що сигнали можуть передаватись лише між чотирма пристроями, і якщо цільовий пристрій є п'ятим пристроєм у з'єднанні, сигнал не досягне його — зв'язок розривається після четвертого пристрою.

Протокол Z-Wave має додатковий рівень безпеки. Рівень безпеки 2 (S2) також позначено як обов'язковий для кожного пристрою, який потребує сертифікації Z-Wave. Цей рівень захищає розумні пристрої від використання в DDOS-атаці. Цей додатковий захист не обов'язково робить Zigbee менш безпечним, оскільки він також використовує симетричне шифрування AES128.

Обидва протоколи споживають низьку енергію, але протокол Zigbee краще використовує менше енергії, ніж протокол Z-Wave. Протокол Zigbee побудований на основі стандарту протоколу IEEE 802.15.4. Серед інших переваг цей стандарт протоколу дає перевагу Zigbee у мінімізації енергоспоживання інтелектуальними пристроями[3].

Zigbee використовує стандарти відкритої мережі. Таку форму мережі також називають гоночною мережею з відкритим кодом. Це тому, що код протоколу, що керує операціями передачі, доступний кожному.

Перевага відкритої мережі Zigbee полягає в тому, що кожен може перевірити код. Це також недолік, оскільки кожен може змінити код відповідно до своїх потреб. Z-Wave використовує стандарти закритої мережі. У цьому стандарті код, який замінює операції передачі, не оприлюднюється та не може бути змінений[1].

Закритий стандарт Z-Wave забезпечує додаткову безпеку. Кожен пристрій, підключений до концентратора, має унікальний ідентифікатор для легкої ідентифікації. Це підвищує безпеку безпечної мережі та забезпечує взаємодію лише з пристроями Z-Wave.

Zigbee, так і Z-wave мають радіус дії до 100 метрів на відкритому просторі, чого більш ніж достатньо для реалізації аспектів, сценаріїв та можливості реалізації розумного будинку.[1] Обидва протоколи використовують невелику кількість енергії, пристрої, на яких вони реалізовані, зможуть працювати набагато довше, перш ніж знадобиться підзарядка або заміна батареї, та надає можливість включення передачі зв'язку в момент дії самого користувача (запит дії через смартфон або ж фізичний контакт через вимикач).

Зараз буде надана порівняльна таблиця між двома якби дуже подібними протоколами:

Таблиця 2.2

Порівняльна таблиця між протоколами Zigbee та Z-Wave

	Zigbee	Z- Wave
Частота	2.4 ГГц (у всьому світі), 784 МГц (Китай), 868 МГц (Європа), 915 МГц (Америка)	Промисловий стандарт, підтримує кілька виробників і типів пристроїв
Діапазон	До 70 метрів у приміщенні, до 400 метрів на вулиці	До 100 метрів у приміщенні, до 400 метрів на вулиці
Ширина смуги	250 Кбіт	100 Кбіт
Топологія	Мережева мережа	Мережева мережа
Втручання	На нього можуть впливати Wi-Fi та інші пристрої з частотою 2.4 ГГц	Менш сприйнятливий до перешкод Wi-Fi
Прилади	Більше 1,000 сертифікованих пристроїв від різних виробників	Понад 2,400 сертифікованих пристроїв переважно від одного виробника
Коштувати	Середня або висока вартість концентраторів і пристроїв	Помірна вартість концентраторів і пристроїв
Споживання енергії	Більш низьке споживання енергії	Більше споживання електроенергії
Безпека	AES-128 шифрування	Шифрування AES-128 плюс S2
Взаємодія	Промисловий стандарт, підтримує кілька виробників і типів пристроїв	Запатентований, в основному використовується одним виробником

На відміну від Zigbee, Z-Wave має кращу сумісність пристроїв, оскільки кожен пристрій Z-Wave проходить сувору сертифікацію від Z-Wave Alliance, що гарантує їхню сумісність із усіма іншими сертифікованими пристроями. На відміну від цього, у Zigbee є два рівні сертифікації – для апаратного і програмного забезпечення, що може призводити до сумнівної сумісності між пристроями, що мають різні рівні сертифікації.

Zigbee використовує сітчасту топологію мережі, що підвищує надійність та радіус дії, так як кожен пристрій може служити як повторювач сигналу. Це дозволяє зберігати стабільність мережі навіть у разі втрати зв'язку деяких пристроїв. З іншого боку, Z-Wave також використовує сітчасту топологію, що робить його менш чутливим до перешкод від інших бездротових пристроїв, таких як Wi-Fi роутери, що забезпечує йому високу надійність і стабільність навіть у навантажених мережних середовищах[6].

Щодо безпеки, обидва стандарти – Zigbee і Z-Wave – використовують шифрування AES128, що забезпечує високий рівень захисту. Однак Z-Wave впроваджує додатковий стандарт безпеки S2, який зменшує ризик DDOS атак та забезпечує швидше встановлення зв'язку та зменшує споживання енергії.

У висновку, обидва протоколи – Zigbee і Z-Wave – мають свої унікальні переваги та особливості, і вибір між ними залежить від конкретних вимог і умов вашого розумного будинку.

2.13 Різниця між Zigbee та Bluetooth

Таблиця 2.3

Порівняльна таблиця протоколів Bluetooth та Zigbee[24]

Bluetooth	Zigbee
Bluetooth Special Interest Group — організація, відповідальна за керування стандартами та пристроями Bluetooth.	Альянс Zigbee відповідає за керування Zigbee, тестування та затвердження пристроїв на основі Zigbee. IEEE стандартизує всі протоколи на основі Zigbee.
Діапазон частот, підтримуваний Bluetooth, коливається від 2,4 ГГц до 2,483 ГГц.	Частотний діапазон в Zigbee, в основному становить 2,4 ГГц.
У Bluetooth є сімдесят дев'ять радіочастотних каналів.	У zigbee є шістнадцять радіочастотних каналів.
У Bluetooth є максимум 8 вузлів стільникового зв'язку.	В zigbee є понад шістдесят п'ять тисяч (65 000) вузлів клітинок.
В мережі Bluetooth побудова підходу «точка-точка головний-підлеглий», у якому є один головний і до семи підлеглих пристроїв утворюють пікомережу, що призводить до формування розсіяної мережі, яка є з'єднанням двох або більше пікомереж.	Пристрої Zigbee можна об'єднувати в мережу в різних загальних топологіях, включаючи зірку, сітку та інші. Кластер можна створити шляхом з'єднання різних мережевих топологій на основі Zigbee. Вузли Zigbee Coordinator, Zigbee Router і Zigbee Endpoint складають будь-яку мережу Zigbee.
вимагає низьку пропускну здатність.	також потребує низької пропускну здатність, але в більшості випадків більшої, ніж Bluetooth.
Діапазон радіосигналу Bluetooth становить десять метрів.	Тоді як дальність радіосигналу zigbee становить від десяти до сотні метрів.
Bluetooth розроблено відповідно до IEEE 802.15.1.	Тоді як він був розроблений відповідно до IEEE 802.15.4.
Акумулятори Bluetooth можна заряджати.	Хоча батареї ZigBee не можна заряджати, вони служать довше.
Синій зуб використовує високу швидкість передачі даних і багато енергії на пристроях з великою передачею пакетів.	Zigbee використовує низькі швидкості передачі даних і малу потужність на пристроях з малими пакетами.
У Bluetooth використовується стрибкоподібна зміна частоти. Під час стрибкоподібної зміни частоти сигнал несучої частоти змушений коливатися.	Zigbee використовує техніку прямого розширення спектру. У прямому розширеному спектрі; вихідний сигнал змішується та відновлюється з псевдовипадкового коду на передавач і приймач.
Швидкість мережі до 250 мегабіт в секунду.	Швидкість мережі до 1 мегабіт в секунду.
Час, необхідний для підключення до мережі за допомогою Bluetooth, становить приблизно 3 секунди.	Час, необхідний для приєднання до мережі за допомогою Zigbee, становить приблизно 30 мілісекунд.

Продовження таблиці 2.3

Розмір стека протоколу Bluetooth становить 250 КБ.	Розмір стека протоколу Zigbee становить 28 Кбайт.
Комп'ютерні периферійні пристрої, такі як бездротові клавіатури, миші, гарнітури та інші периферійні пристрої, є основними варіантами використання програм на базі Bluetooth. Крім того, кілька бездротових пультів дистанційного керування та пристроїв, що керуються жестами, передають дані через Bluetooth.	Системи, побудовані на протоколі Zigbee, призначені для бездротової роботи в сенсорній мережі, і вони більш популярні серед компактних і енергоефективних гаджетів. Мережа на основі Zigbee використовується в різноманітних програмах, включаючи датчики системи SCADA, медичні пристрої та пульти дистанційного керування телевізорами.

2.14 Порівняльна таблиця між WiFi, Zigbee, Z-wave та Bluetooth

Таблиця 2.4

Порівняльна таблиця протоколів

Характеристика	ZigBee	Wi-Fi	Bluetooth	Z-Wave
Діапазон частот	2,4 ГГц	2,4 ГГц і 5 ГГц	2,4 ГГц	908,42 МГц
Екскурсія	30-100 м	30-100 м	10-30 м	30-100 м
Максимальна кількість пристроїв	65 000	254	7-8	232
Споживання енергії	Бас	Помірний	Бас	Бас
Безпека	AES-128	WPA2-AES	AES-128	AES-128
Додатки	пристрої IoT	Інтернет і мультимедіа	Підключення персонального пристрою	Домашня автоматизація
Топологія мережі	свєтр	зірка	Piconet	свєтр
Швидкість передачі даних	40-250 Кбіт/с	Від 600 Мбіт/с до 3 Гбіт/с	1 Мбіт/с	Кбіт/с 100
Стек протоколів	IEEE 802.15.4	IEEE 802.11	Bluetooth 4.2	UTI G.9959

Висновки

Протокол ZigBee виявляється потужним інструментом для реалізації мереж Internet of Things (IoT) завдяки своїм унікальним характеристикам і можливостям. В порівнянні з іншими популярними протоколами, такими як Z-Wave, WiFi та Bluetooth, ZigBee відзначається значними перевагами, особливо у контексті високої енергоефективності та можливості створення масштабованих мереж з великою кількістю вузлів.

Основні переваги ZigBee включають низьке споживання енергії, високу пропускну здатність, низьку вартість компонентів і відмінну підтримку мереж зі зниженим рівнем потужності. Це робить ZigBee ідеальним вибором для застосування в розумних будинках, де важлива надійність, довговічність і ефективне використання енергії.

Порівнюючи з іншими протоколами, такими як Z-Wave з його спеціалізованою орієнтацією на побудову розумних систем, або WiFi та Bluetooth, які надають більшу швидкість передачі даних, але вимагають значно більшого споживання енергії, можна зробити висновок, що вибір протоколу повинен базуватися на конкретних вимогах проекту.

Для проектів, де критичне значення має низьке споживання енергії та можливість взаємодії з великою кількістю пристроїв у різних мережах, ZigBee може бути оптимальним вибором. В той час як для задач, які вимагають високої швидкості передачі даних або інтеграції зі смартфонами і комп'ютерами, WiFi та Bluetooth можуть надавати більше переваг.

РОЗДІЛ 3

ПРОЕКТУВАННЯ ТА СТВОРЕННЯ ВЛАСНОГО ІОТ НА ПРОТОКОЛІ ZIGBEE НА ПРИКЛАДІ СТВОРЕННЯ ВЛАСНОГО РОЗУМНОГО БУДИНКУ.

3.1 Підготовка та створення власного IoT платформи для керуванням розумним будинком.

В даному дослідженні використовується сервер у вигляді міні ПК, на якому встановлена операційна система Debian. На цьому сервері запущений Proxmox, який є гіпервізором для віртуалізації, і надає можливість створювати віртуальні машини та контейнери. Один з таких контейнерів використовується для встановлення платформи IoT - Home Assistant. Home Assistant дозволяє керувати різноманітними датчиками та пристроями для розумного будинку, незалежно від їх бренду чи протоколу зв'язку.

Home Assistant — це універсальна вільна операційна система для керування пристроями інтернету речей різних виробників, а також їхньої автоматизації. Це локальне рішення, що не залежить від хмари чи наявності інтернету, та підтримує велику кількість протоколів: Wi-Fi, Zigbee, Z-wave, Bluetooth, Bluetooth-mesh, IR etc.

Основні характеристики та переваги Home Assistant:

- Універсальність та інтеграція: Підтримка широкого спектру пристроїв із різними брендами, протоколами (включаючи Zigbee, WiFi, Z-Wave, Bluetooth тощо) і системами автоматизації.
- Простота налаштування: Інтуїтивно зрозумілий інтерфейс для конфігурації та управління пристроями.
- Розширюваність: Можливість додавати нові пристрої і налаштовувати автоматизацію без значних зусиль.

- Спільнота та підтримка: Активна спільнота користувачів та регулярні оновлення програмного забезпечення.

Приклад сценаріїв:

Система безпеки: включає камери, сигналізацію, датчики диму, датчики відкриття, руху та вібрації.

Освітлення: включає регулювання яскравості, колірне підсвічування, теплоту світла та *ambilight*.

Побутова техніка: включає кондиціонер, пиросос, телевізор та електричний чайник.

Електропостачання: включає розетки, вимикачі, реле та лічильники.

Моніторинг: включає вимірювання температури, вологості, тиску, рівня CO₂ та виявлення протікання.

Встановлення та мінімальні вимоги для Home Assistant:

Для запуску Home Assistant на одноплатному ПК, такому як Raspberry Pi, рекомендується мати наступне:

- Мінімум 2 ГБ оперативної пам'яті: Для забезпечення плавної роботи системи, особливо при великій кількості підключених пристроїв.
- Мінімум 32 ГБ вільного місця у сховищі: Для зберігання даних та резервного копіювання конфігурації та інших даних.

Застосування протоколів Zigbee та WiFi у дослідженні:

- Zigbee: Використання Zigbee відображається у підключенні різних пристроїв розумного будинку до мережевого координатора через бездротову мережу Zigbee. Цей протокол відомий своєю низькою споживаною енергією та підтримкою великої кількості пристроїв у мережі.

- **WiFi:** Простота підключення та широкий охоплює забезпечують використання пристроїв WiFi у розумному будинку. Протокол WiFi забезпечує високу швидкість передачі даних і зручність у налаштуванні.

Ці два протоколи дозволяють проводити порівняльний аналіз їхніх характеристик та ефективності в умовах реального використання у розумних будинках.

3.2. Логіка управління розумним будинком

Управління розумним будинком через протокол Zigbee на платформі Home Assistant включає інтеграцію різноманітних пристроїв, таких як датчики, реле, вимикачі, термостати та інші, які підтримують цей стандарт бездротового зв'язку.

Основні аспекти логіки управління через Zigbee на Home Assistant охоплюють наступні кроки:

1. **Інтеграція з Zigbee координатором:** Початковим етапом є підключення Zigbee координатора до системи Home Assistant. Це зазвичай здійснюється за допомогою USB адаптера, який підтримує Zigbee стандарт (наприклад, ConBee II, Zigbee USB stick тощо).
2. **Додавання пристроїв до мережі:** Після підключення координатора, ви можете додавати пристрої Zigbee до мережі. Home Assistant підтримує автоматичне відкриття та додавання пристроїв через різноманітні інтеграції, такі як Zigbee2MQTT, ZHA (Zigbee Home Automation) або спеціалізовані платформи Zigbee.
3. **Керування та автоматизація:** Після успішного додавання пристроїв їх можна керувати через інтерфейс Home Assistant. Ви зможете включати/виключати пристрої, регулювати їх параметри (якщо підтримується), а також моніторити їх стан.

3.3. Схема побудови розумного будинку

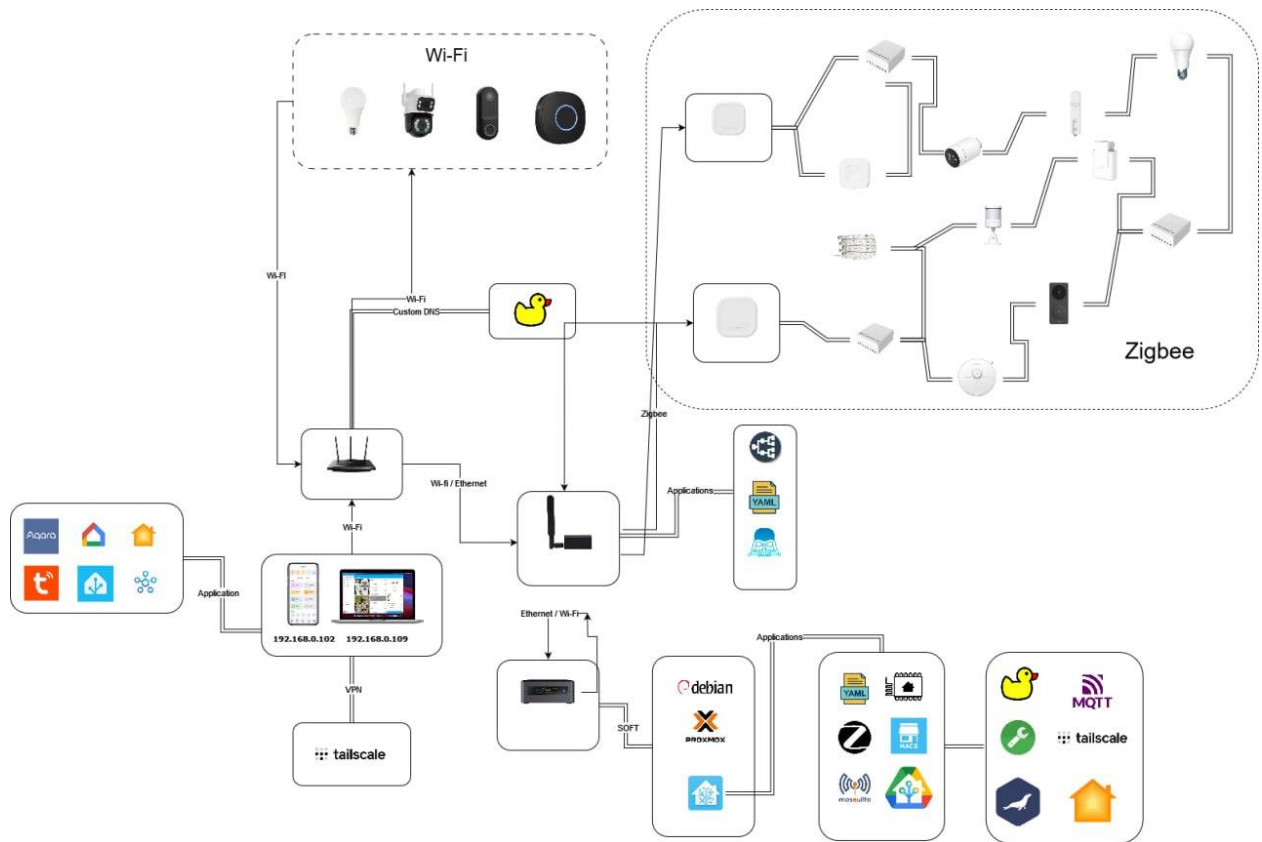


Рис 3.1 Схема побудови розумного будинку

3.3.1 Реалізація сервера для розумного будинку

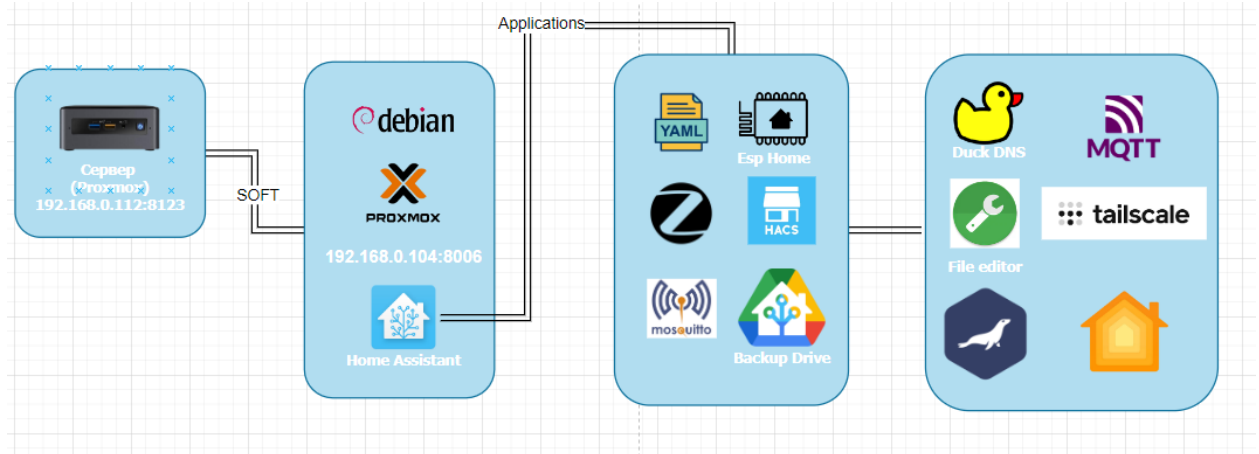


Рис 3.2 Схема реалізації сервера розумного будинку.

Схема реалізації розумного будинку (мережеве обладнання та програмне забезпечення) на протоколі Zigbee та WiFi).

3.3.2. Частина клієнта для контролю розумним будинком

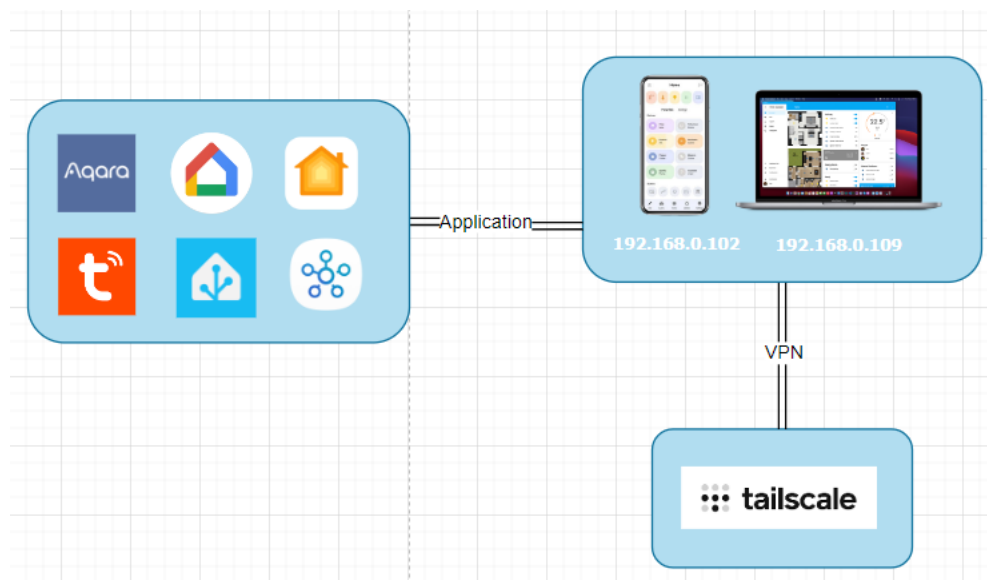


Рис 3.3 Схема реалізації частини клієнта

Керування розумним будинком через носії IoT, такі як смартфон або ноутбук, надає користувачам зручність і доступність управління різноманітними

пристроями з будь-якої точки світу, де є Інтернет. Ось детальніше про те, як це працює і які можливості це відкриває для користувачів:

Застосування смартфона або ноутбука для керування розумним будинком

1. Дистанційне керування: Ви можете управляти освітленням, опаленням, кондиціонуванням повітря, розетками, алармами та іншими пристроями з будь-якого місця, де є Інтернет. Наприклад, вмикаючи світло перед тим, як повернутися додому або регулюючи температуру в приміщенні задовго до вашого приходу.
2. Встановлення VPN: Щоб забезпечити безпечний доступ до вашої системи розумного будинку зовнішнім пристроям, ви можете встановити VPN (віртуальна приватна мережа) на вашому смартфоні або ноутбуці. VPN забезпечить зашифроване з'єднання із дому, що знижує ризик несанкціонованого доступу до вашої системи.
3. Застосунок Tailscale як приклад VPN: Tailscale є одним із популярних варіантів для налаштування VPN для дистанційного доступу до домашньої мережі. Він простий у встановленні та використанні, забезпечує зручну і безпечну зв'язність між вашим пристроєм і системою розумного будинку.

Інтеграція з іншими платформами IoT

1. Aqara Home: Інтеграція з Aqara Home дозволяє вам керувати пристроями, які підтримують цю платформу, використовуючи той самий інтерфейс, яким ви звикли користуватися.
2. Google Home: Google Home забезпечує можливість керувати розумними пристроями за допомогою голосових команд, інтегруючи їх у ваш побутовий екосистем Google.

3. HomeKit: Якщо ви користуєтесь пристроями, які підтримують Apple HomeKit, ви можете легко інтегрувати їх з вашою системою розумного будинку через Home Assistant, що дозволяє вам керувати їх через голосового асистента Siri.
4. TuYa Smart: TuYa Smart підтримує широкий спектр розумних пристроїв і забезпечує просте управління через один інтерфейс, який може бути інтегрований з Home Assistant.
5. SmartThings: Платформа SmartThings дозволяє підключати і керувати різноманітними пристроями IoT, інтегруючи їх з вашим розумним будинком через Home Assistant.

3.4 Процес роботи контролю розумним будинком через протокол Zigbee а саме через Zigbee2MQTT.

Zigbee2MQTT — це програмне забезпечення координатора (синоніми шлюз, хаб). Zigbee мережі, що дозволяє локально керувати пристроями різних виробників. Воно поєднує мережу Zigbee з MQTT-протоколом. Має якісну підтримку великої кількості (2245) пристроїв та відрізняється надійністю. Для його роботи необхідно мати один з підтримуваних шлюзів та прошити його (можна купити прошитий). є використання USB адаптера CC2531. Проте він вважається застарілим, деякі значення обладнання можуть відображатись некоректно. Більш сучасним і популярним варіантом (~550 грн) є використання CC2652P, наприклад smartlight, або sonoff. В власному випадку використовував прилад Ham Geek на прямому контакті Ethernet.

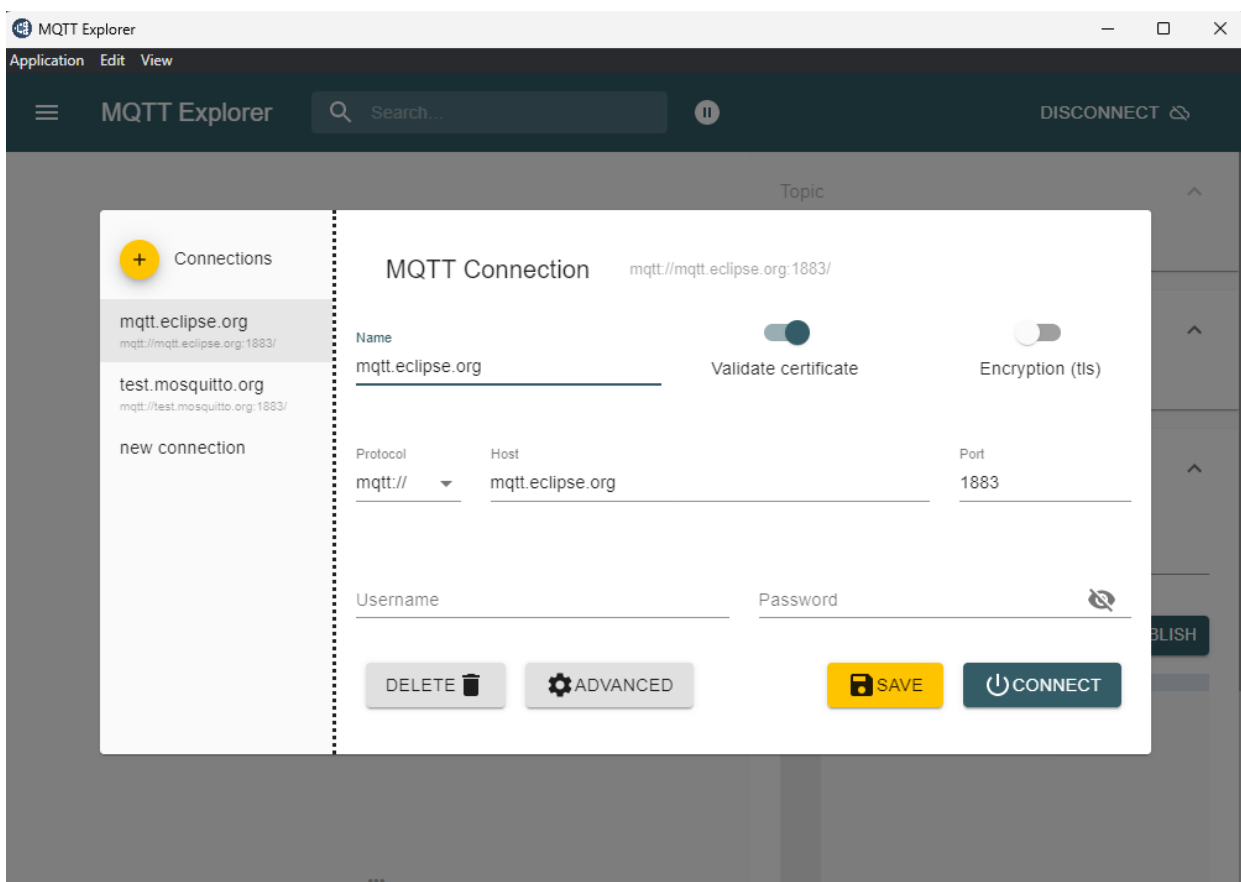


Рис. 3.4 Скріншот з застосунку MQTT Explorer

Для початку вам потрібно прошити ваш наявний координатор, щоб ви змогли через платформу Home Assistant керувати вашим розумним будинком. Для початку на вашому носії потрібно вказати ip та порт вашого координатора. В моєму випадку потрібно зайти на веб сторінку власного роутера TP link. Через ці дані ви можете зайти на веб сторінку вашого мережевого координатора та отримати дані заповнення в Iot платформі Home Assistant

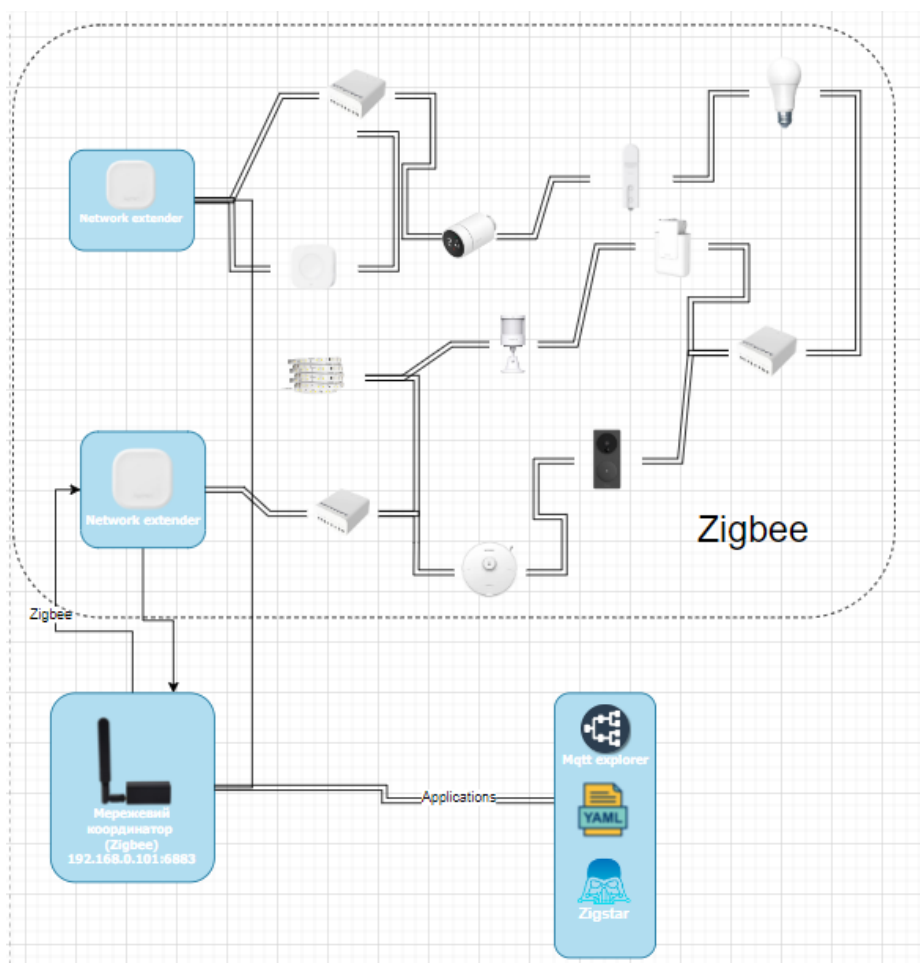


Рис. 3.5 Схема конфігурації мережевого координатора

1. Перейдіть в налаштування >> Додатки >> Магазин доповнень >> Знайдіть та встановіть Mosquito broker.

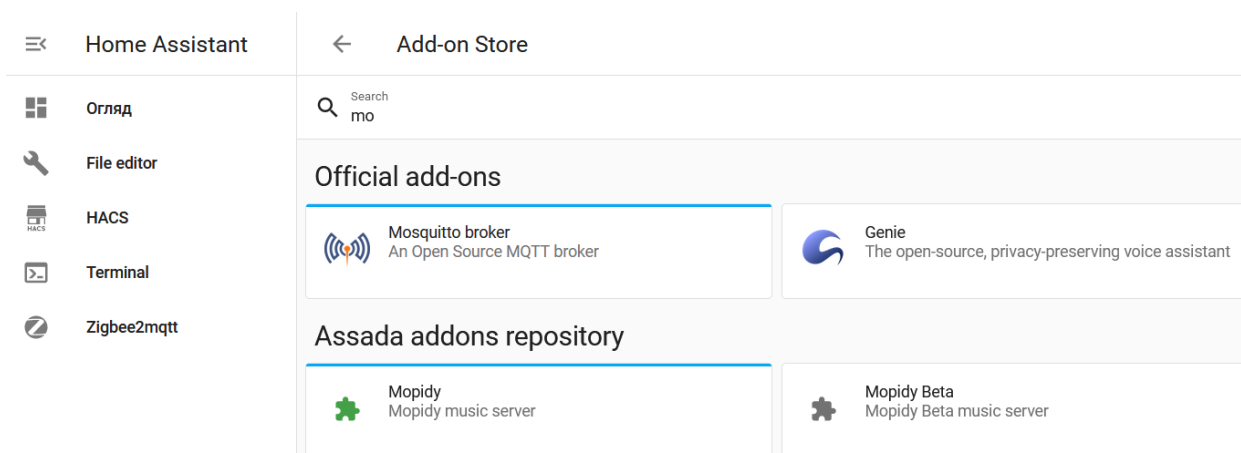


Рис 3.6 Скріншот застосунку Home Assistant

2. Перейдіть на сторінку додатку Mosquito broker >> вкладку Configuration.

У Параметрах в пункті logins впишіть:

username: mqtt

password: mqtt

В конфігураціях Home Assistant є два види редагування параметрів: користувацький та YAML. Змінити режим можна, натиснувши три крапки зверху.

В режимі YAML конфігурація виглядає так:

Мережа

Change the ports on your host that are exposed by the add-on

1883	1883/tcp	Normal MQTT
1884	1884/tcp	MQTT over WebSocket
8883	8883/tcp	Normal MQTT with SSL
8884	8884/tcp	MQTT over WebSocket with SSL

СКИНУТИ НАЛАШТУВАННЯ ЗА ЗАМОВЧУВАННЯМ ЗБЕРЕГТИ

Рис 3.7 Скріншот застосунку Home Assistant

3. Збережіть налаштування та запустіть додаток.

4. Перейдіть в налаштування >> Пристрої та сервіси >> Додати інтеграцію >> Встановіть інтеграцію MQTT.

5. З'явиться вікно підключення до MQTT брокера:

- в полі брокер введіть core-mosquitto;
- в полі імені користувача mqtt;

- в полі пароль mqtt;
- виділіть пункт автододавання пристроїв та збережіть.

Broker options ? ×

Введіть інформацію про з'єднання з вашим брокером MQTT.

Брокер*
core-mosquitto

Порт*
1883

Ім'я користувача
mqtt

Пароль
mqtt

ДАЛІ

Рис 3.8 Скріншот застосунку Home Assistant

6. Додайте репозиторій Zigbee2mqtt: Перейдіть в налаштування >> Додатки >> Магазин доповнень >> Натисніть меню зверху справа >> Репозиторії

У пустій стрічці знизу вставте адресу <https://github.com/Zigbee2mqtt/hassio-Zigbee2mqtt>

Натисніть додати:

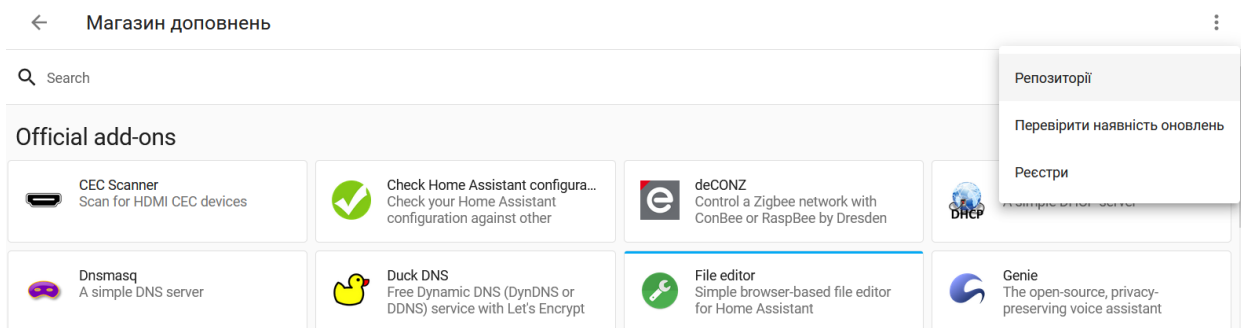


Рис 3.9 Скріншот застосунку Home Assistant

7. В магазині доповнень з'являться два нових додатки Zigbee2MQTT Edge — це розробницька гілка додатку, у ній раніше з'являється підтримка нових пристроїв. Натисніть та встановіть Zigbee2mqtt. Якщо додатки не з'явилися, необхідно очистити кеш або зайти в Home Assistant з іншого браузера.

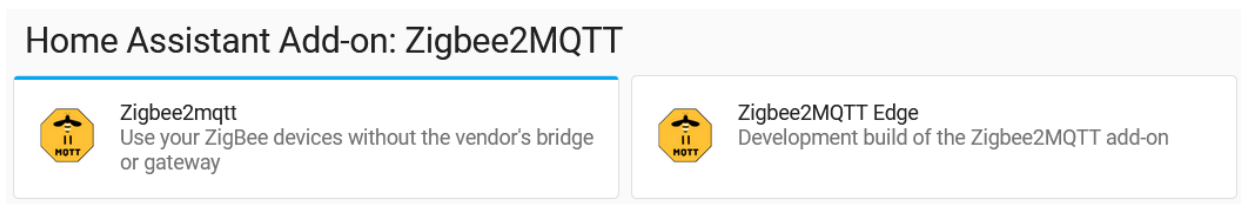


Рис 3.10 Скріншот застосунку Home Assistant

8. Перейдіть на сторінку додатку Zigbee2mqtt >> вкладку Configuration.

У параметрах запишіть наступні дані:

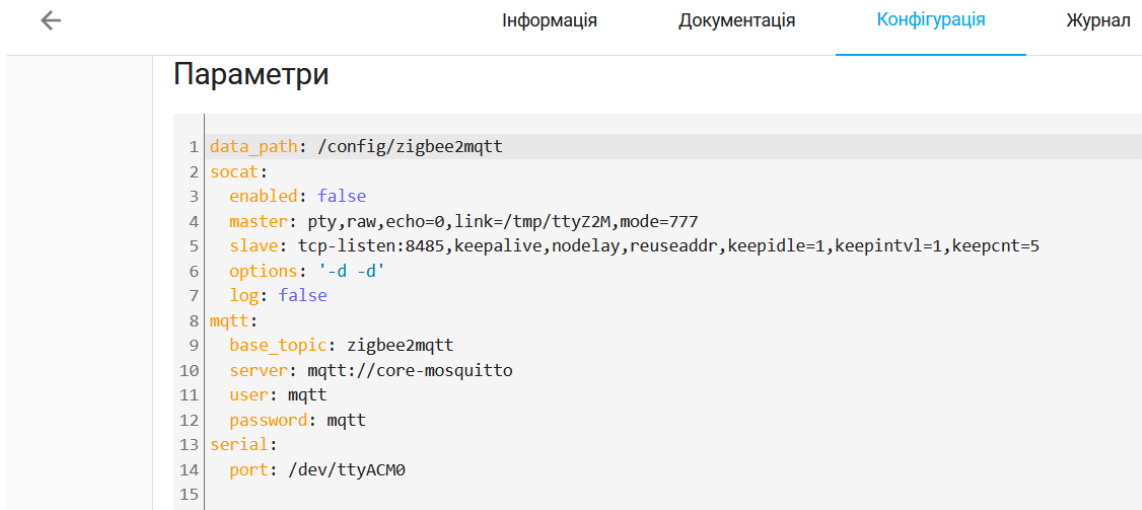


Рис 3.11 Скріншот застосунку Home Assistant

9. Запустіть додаток.

Як знайти порт

Перейдіть в налаштування >> Система >> Устаткування >> Верхнє праве меню >> Все обладнання.

Найчастіше ваш порт буде tty ACM0. Також ви можете скористатись пошуком і вписати назву вендора.

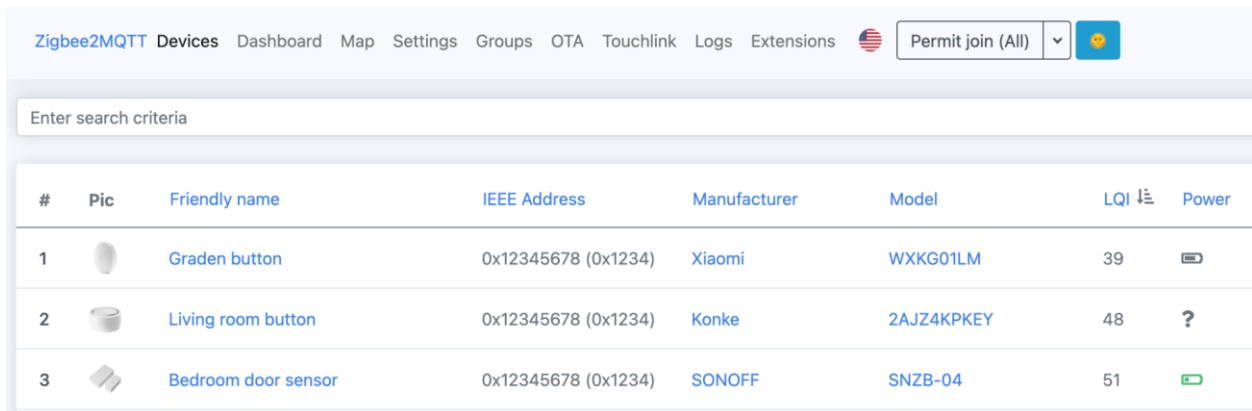


Рис 3.12 Скріншот застосунку Home Assistant

Якщо у вас мережевий координатор з ethernet портом на кшталт SLZB-05, в рядку «Порт» потрібно вказати IP та порт, наприклад:

port: tcp://192.168.0.237:6638

Як результата ви можете додавати прилади на протоколі Zigbee та керувати один між одним для отримання результату.



The screenshot shows the Zigbee2MQTT web interface. At the top, there is a navigation bar with links: Zigbee2MQTT, Devices, Dashboard, Map, Settings, Groups, OTA, Touchlink, Logs, Extensions. There is also a language selector (US flag) and a 'Permit join (All)' button. Below the navigation bar is a search input field labeled 'Enter search criteria'. The main content area displays a table of connected devices.

#	Pic	Friendly name	IEEE Address	Manufacturer	Model	LQI	Power
1		Graden button	0x12345678 (0x1234)	Xiaomi	WXKG01LM	39	
2		Living room button	0x12345678 (0x1234)	Konke	2AJZ4KPKEY	48	?
3		Bedroom door sensor	0x12345678 (0x1234)	SONOFF	SNZB-04	51	

Рис 3.13 Скріншот застосунку Home Assistant

Внизу вказана схема роботи один між одним приладів на протоколі Zigbee

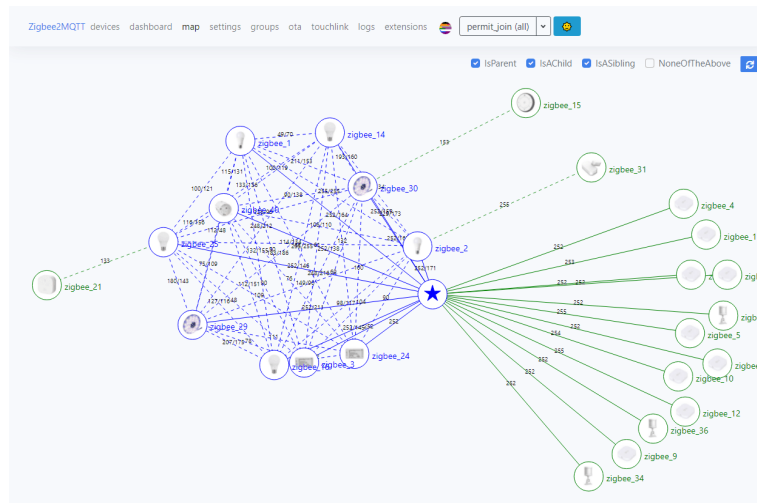


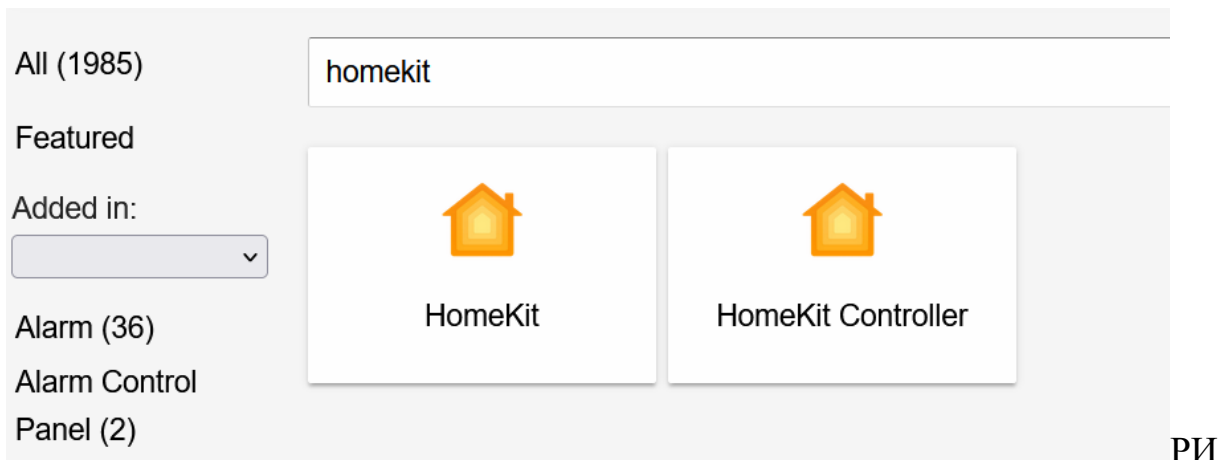
Рис 3.14 схема роботи один між одним приладів на протоколі Zigbee

3.5 Інтеграція вашого розумного будинку HomeKit

HomeKit - це платформа та протокол від Apple для керування розумними пристроями. Для віддаленого керування через програму "Дім" потрібно мати Apple TV (4-го покоління або новіше), HomePod або iPad з відповідними версіями ОС.

Інтеграція з HomeKit в Home Assistant включає дві опції:

1. **HomeKit Controller:** дозволяє додавати сертифіковані пристрої, що підтримують протокол HomeKit.
2. **HomeKit Bridge:** дозволяє додавати усі пристрої, включаючи несертифіковані, до програми "Дім" та керувати ними через Siri. Ця інтеграція створює віртуальний міст, що дозволяє взаємодіяти з пристроями Home Assistant через програму "Дім".



РИ

Рис 3.15 Скріншот застосунку Home Assistant

Важливо зазначити, що без використання домашнього хаба, ви не зможете дистанційно керувати пристроями з програми Дім, лише коли знаходитесь вдома.

Щоб додати пристрої Home Assistant до HomeKit, необхідно перейти до меню >> Конфігурація >> Пристрої та сервіси >> Додати інтеграцію >> обрати інтеграцію HomeKit.

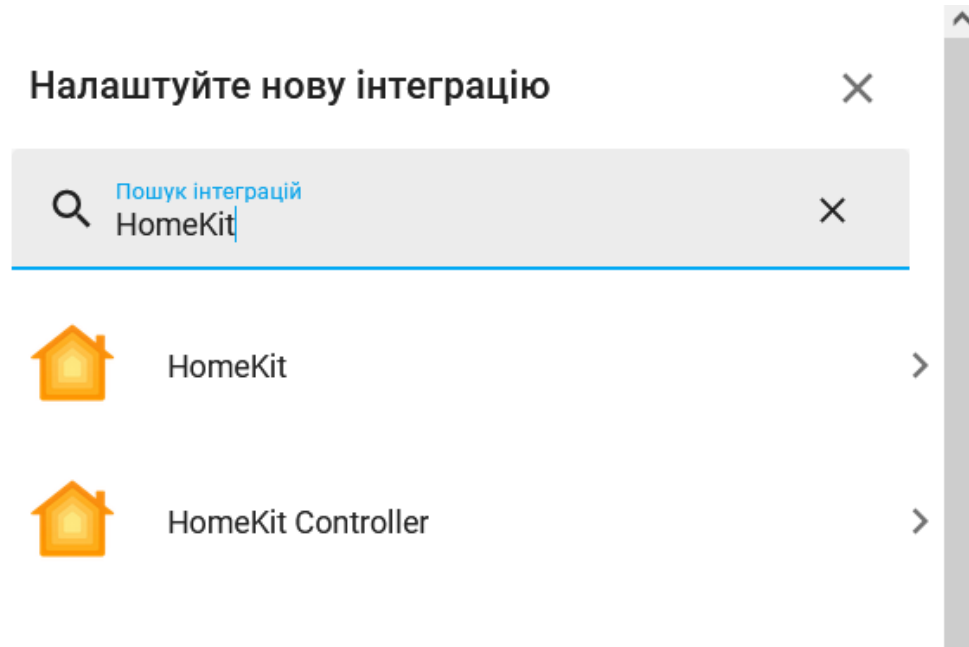


Рис 3.16 Скріншот застосунку Home Assistant

Після інтеграція попросить вас обрати домени обладнання (категорії, простіше кажучи). Якщо ви не знаєте, за що вони не відповідають, залиште так, їх можна налаштувати пізніше. До прикладу, датчики руху, температури, вологості — належать до домену Sensor.

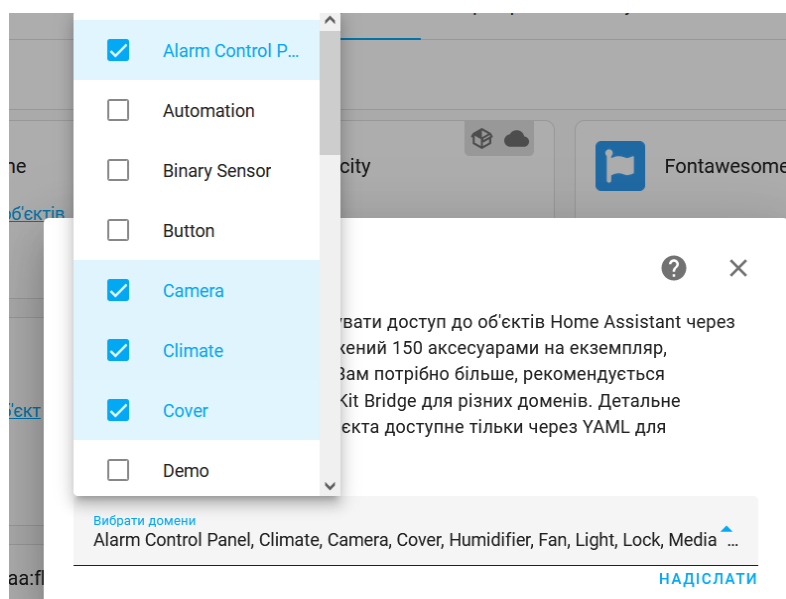


Рис 3.17 Скріншот застосунку Home Assistant

Після того, як ви натиснете кнопку «Надіслати», ви отримаєте повідомлення, про те, що код спарювання з HomeKit буде доступний в сповіщеннях. Натисніть кнопку «Надіслати» і після успішної конфігурації Home Assistant попросить вас обрати кімнату віртуального мосту. Натисніть кнопку «Закінчити».

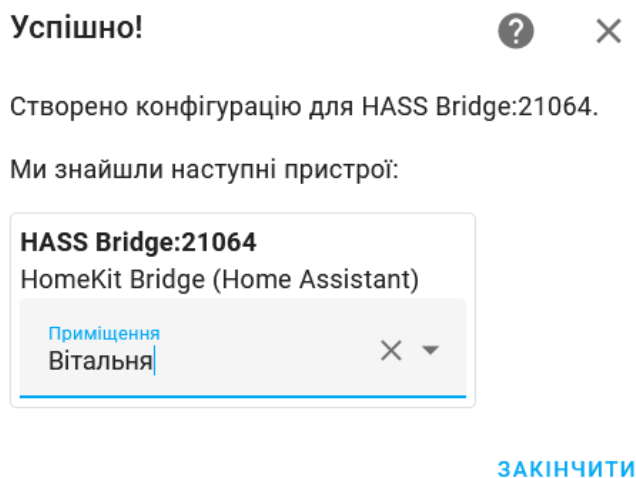


Рис 3.18 Скріншот застосунку Home Assistant

Відкрийте меню сповіщень Home Assistant та програму Дім на пристрої Apple. Натисніть кнопку «Додати прилад» та відскануйте код в меню сповіщень.

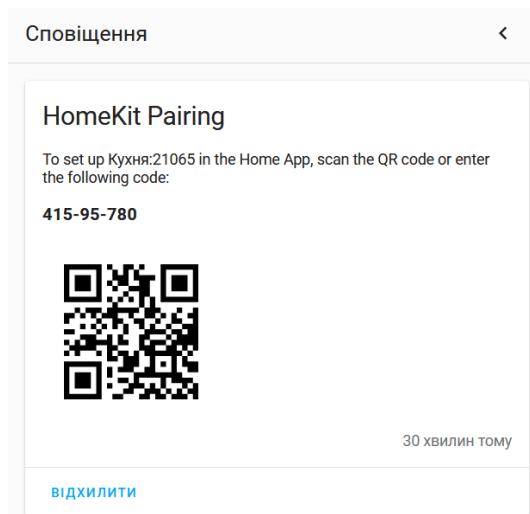


Рис 3.19 Скріншот застосунку Home Assistant

Дім сповістить вас, що пристрій, який ви додаєте, несертифікований. Натисніть «Все одно додати». Оберіть назву та кімнату пристроїв. Пристроїв може бути багато, непотрібні можна прибрати.

Щоб не показувати непотрібні пристрої, перейдіть до меню >> Конфігурація >> під іконкою інтеграції буде кнопка «Налаштувати, натисніть її.

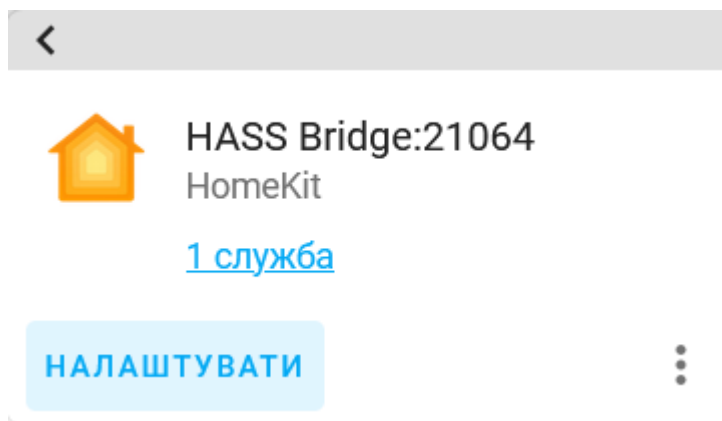


Рис 3.20 Скріншот застосунку Home Assistant

Інтеграція має два режими включення:

- **exclude** (виключити) — після вибору доменів (категорій) пристроїв, ви можете виключити з них непотрібні вам сутності. Відмічені галочкою пристрої та сутності не будуть відображатись в програмі Дім.
- **include** (включити) — після вибору доменів (категорій) пристроїв, ви можете включити потрібні вам пристрої. Відмічені галочкою пристрої та сутності будуть присутні в програмі Дім. Усе, що не відмічено, відображатись не буде.

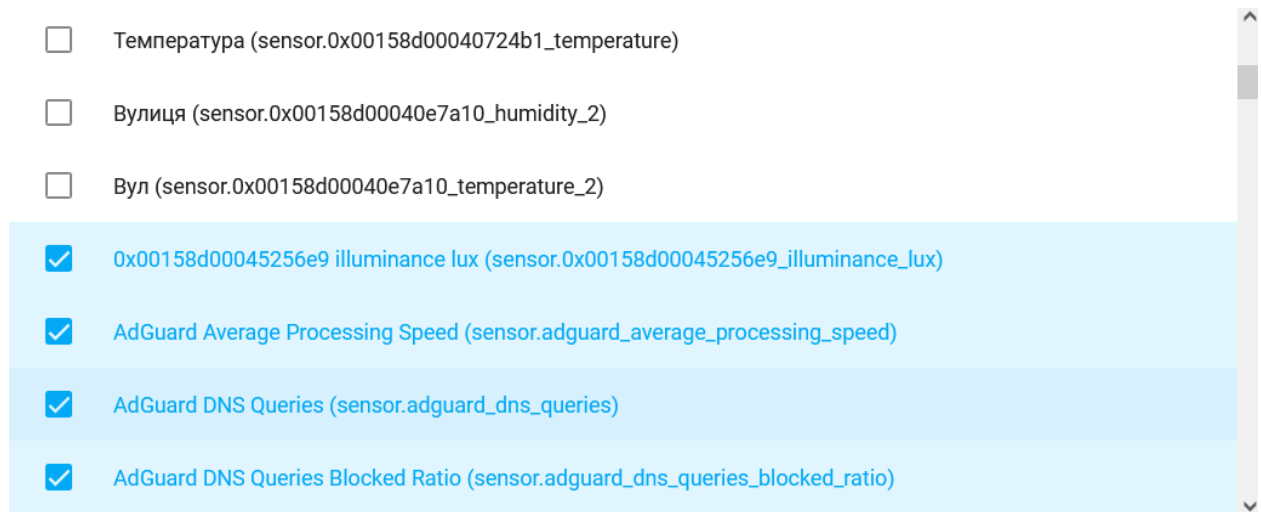


Рис 3.21 Скріншот застосунку Home Assistant

В результаті ви отримаєте ваші пристрої в програмі Дім від Apple та зможете керувати ними через Siri.

Висновки

Проектування та створення власного IoT на основі протоколу Zigbee для реалізації розумного будинку є складним і захоплюючим завданням, яке відкриває безліч можливостей для покращення комфорту, безпеки та енергоефективності у житловому просторі. В даному висновку розглянемо основні аспекти проектування та переваги використання протоколу Zigbee.

Однією з ключових переваг Zigbee є його здатність створювати масштабовані мережі з великою кількістю вузлів, що розширює функціональні можливості розумного будинку. Завдяки мережевим координаторам та маршрутизаторам, які оптимізують передачу даних, система може працювати ефективно навіть у великих приміщеннях.

Проектування такої системи вимагає ретельного планування і інтеграції компонентів, вибору відповідних пристроїв та платформ для управління. Важливо також забезпечити високий рівень безпеки для захисту особистих даних та конфіденційності користувачів.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

У дипломній роботі було проведено порівняння бездротових технологій доступу для систем управління розумним будинком, аналіз протоколу Zigbee та розроблено власний інтеграційний рівень для контролю системи розумного будинку.

Виявлено, що основними складовими розумного будинку є сервер і координатор, датчики для збору інформації, мікроконтролери для групування датчиків та передачі інформації, сервер для інтерфейсу з користувачем, канали передачі даних для різних послуг (наприклад, безпеки та швидкості), хмара як зовнішня служба бази даних і мобільні пристрої для управління системою через сервер.

До бездротових технологій, які можна застосовувати для керування системами розумного будинку, відносяться Wi-Fi, Z-Wave, Zigbee та Bluetooth. Виявлено, що Wi-Fi доцільно використовувати для стабільного зв'язку з віддаленими системами, такими як хмара.

Основними недоліками технологій Zigbee та Bluetooth для застосування в системах розумного будинку є прив'язка до зашумленого діапазону 2,4 ГГц, у той час як Z-Wave використовує менш зашумлений діапазон 869 МГц.

Запропоновано ряд критеріїв для визначення придатності бездротових технологій в системах управління розумним будинком, таких як надійність, використання частотного спектру, мережна конфігурація, безпека, потужність, глобальна сумісність і вартість.

Встановлено, що технології Z-Wave та Bluetooth відповідають критерію надійності та підтримки зв'язку на всіх рівнях моделі OSI, забезпечують високий рівень сумісності пристроїв.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. <https://dusuniot.com/uk/blog/zigbee-vs-z-wave-which-is-better-for-home-automation/>
2. <https://dusuniot.com/uk/blog/zigbee-vs-bluetooth-vs-wi-fi-which-one-is-the-best-for-smart-home/>
3. <https://www.spiceworks.com/tech/iot/articles/zigbee-vs-z-wave/>
4. <https://dusuniot.com/uk/blog/what-is-the-zigbee-alliance/>
5. <https://www.spiceworks.com/tech/iot/articles/zigbee-vs-z-wave/>
6. <https://reolink.com/blog/z-wave-vs-zigbee/>
7. <https://www.dusuniot.com/it/blog/what-is-zigbee/>
8. <https://www.dusuniot.com/it/blog/the-definitive-guide-for-zigbee-gateway-for-solution-vendors/>
9. <https://www.dusuniot.com/it/blog/the-definitive-guide-for-zigbee-gateway-for-solution-vendors/>
10. <https://aws.amazon.com/what-is/iot>
11. <https://dou.ua/forums/topic/46215/>
12. <https://iot.kpi.ua/web/site/about>
13. https://stud-point.com/blog/it_life/shcho-take-internet-of-things-iot/
14. <https://www.home-assistant.io/>
15. <https://pve.proxmox.com/pve-docs/>
16. <https://medium.com/@omaslyuchenko/hello-zigbee-world-part-4-zigbee-basics-e7039fbbe7b5>
17. <https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot>
18. <https://www.mongodb.com/resources/basics/cloud-explained/iot-architecture>

19. <https://deviceauthority.com/unpacking-iot-architecture-layers-and-components-explained/#:~:text=IoT%20architecture%20is%20an%20organised,processing%20and%20User%20interface%2Fapplication.>
20. <https://www.sciencedirect.com/science/article/pii/S2542660523001142>
21. <https://dou.ua/forums/topic/46215/>
22. <https://mk.fmuser.net/content/?21156.html>
23. https://www.geeksforgeeks.org/difference-between-zigbee-and-wifi/?ref=ml_lbp
24. <https://www.geeksforgeeks.org/difference-between-bluetooth-and-zigbee/>
25. https://www.geeksforgeeks.org/difference-between-zwave-and-zigbee/?ref=ml_lbp