Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет __Комп'ютерної інженерії та управління_____

(повна назва)

Кафедра ___Автоматизації проектування обчислювальної техніки_____

(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти ___другий (магістерський)_____

(рівень вищої освіти)

__Технології аналізу моделей передачі даних для системи розумного будинку_.

_____.

(тема)

Виконав: студент 2 курсу, групи Чумак____

__Владислав Ігорович_____

(прізвище, ініціали)

Спеціальність _123 Комп'ютерна інженерія__

(код і повна назва спеціальності)

Тип програми _освітньо-професійна_____

(освітньо-професійна або освітньо-наукова)

Освітня програма _Спеціалізовані_____

__комп'ютерні системи_____

(повна назва освітньої програми)

Керівник ___доц. каф. АПОТ Філіппенко І. В.

(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _-_____ Чумаченко С.В.

(підпис) (прізвище, ініціали)

2022 р.

Харківський національний університет радіоелектроніки

Факультет ___Комп'ютерної інженерії та управління_____

Кафедра ____Автоматизації проектування обчислювальної техніки_____

Рівень вищої освіти ___другий (магістерський)_____

Спеціальність _____123 Комп'ютерна інженерія_____

(шифр і назва)

Тип програми _____Освітньо-професійна_____

(освітньо-професійна або освітньо-наукова)

Освітня програма _____Спеціалізовані комп'ютерні системи_____

(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри

_____

(підпис)

«___»_____20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студентові _Чумаку Владиславу Ігоровичу_____

(прізвище, ім'я, по батькові)

1. Тема роботи _Технології аналізу моделей передачі даних для системи_____ розумного будинку_____

затверджена наказом університету від _14_ _листопада_2022 р. №__1478Ст

2. Термін подання студентом роботи до екзаменаційної комісії 20.12.2022 р.

3. Вихідні дані до роботи _____

__технології передачі даних WiFi, Bluetooth _____

_____

_____

_____

_____

4. Перелік питань, що потрібно опрацювати в роботі _____

аналіз предметної області_____

___сумісність передачі даних різними технологіями_____

___перешкодостійкість та перешкодозахищеність_____

_____

_____

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) _____
_____18 слайдів_____
_____
_____
_____
_____

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання	04.11.2022 - 05.11.2022	
2	Аналіз літератури	12.11.2022 - 16.11.2022	
3	Розробка моделі	17.11.2022 - 26.11.2022	
4	Реалізація моделі	29.11.2022 - 05.12.2022	
5	Тестування отриманих даних	06.12.2022 - 10.12.2022	
6	Оформлення пояснювальної записки	13.12.2022 - 20.12.2022	

Дата видачі завдання __05___ ___09_____2022 р.

Студент _____

(підпис)

Керівник роботи _____ ___доц. Філіппенко І.В.___

(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить 55 сторінок, 18 рисунків, 3 таблиці та 27 джерел за переліком посилань.

РОЗУМНИЙ БУДИНОК, МОДЕЛІ ПЕРЕДАЧІ ДАНИХ, ХАБ, ЗВ’ЯЗОК, ПРОТОКОЛИ, ОБМІН ТА ПЕРЕДАЧА ДАНИХ, МОДЕЛІ РОЗУМНОГО БУДИНКУ

У роботі розглянуті питання структурування, аналізу та порівняння моделей передачі даних для системи розумного будинку, а також виявлення основних переваг та недоліків цих моделей.

Наведені таблиці аналізу моделей передачі даних для системи розумного будинку, приклади реалізації цих технологій. Проведено аналіз впливу роботи WiFi появи помилок у приймачі Bluetooth.

ABSTRACT

The explanatory note contains 55 pages, 18 figures, 3 tables and 27 references.

SMART HOME, DATA TRANSMISSION MODELS, HUB, COMMUNICATION, PROTOCOLS, DATA EXCHANGE AND TRANSMISSION, SMART HOME MODELS.

The work deals with structuring, analysis and comparison of data transmission models for the smart home system, as well as identifying the main advantages and disadvantages of these models.

Tables of analysis of data transmission models for the smart home system, examples of the implementation of these technologies are presented. An analysis of the effect of WiFi operation was carried out, an error appears in the Bluetooth receiver.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

РБ – розумний будинок

WWAN – безпровідна глобальна мережа

VPN – віртуальна приватна мережа

PC, ПК – персональний комп’ютер

USB – кабель універсальної послідовної шини

DSL – цифрова абонентська лінія

WiFi – один із стандартів безпровідної локальної мережі (Wireless Fidelity)

WLAN – безпровідна локальна мережа

LAN – локальна обчислювальна мережа

IBSS – незалежний базовий сервісний набір

AP – точка доступу (Access Point)

ESS – розширений сервісний набір (Extended Service Set)

IP – унікальний числовий ідентифікатор пристрою у комп'ютерній мережі (Internet Protocol)

OSI – базова еталонна модель взаємодії відкритих систем

TCP – протокол керування передаванням

TCP/IP – набір протоколів мережі Інтернет

FTP – протокол передавання файлів

SMTP – протокол пересилання пошти

WWW – всесвітня мережа (World Wide Web)

HTTP – протокол передачі гіпертексту

DNS – ієрархічна розподілена система перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в IP-адресу

SNMP – протокол керування мережами зв'язку на основі архітектури TCP/IP

PGR – бібліотека функцій, що дозволяє виконувати операції шифрування та цифрового підпису повідомлень (Pretty Good Privacy)

SET – стандартизований протокол для проведення операцій з кредитної/банківської картки через інтернет (Secure Electronic Transaction)

UPD – протокол датаграм користувача, один із протоколів в стеку TCP/IP

SSL/TLS – криптографічні протоколи, що забезпечують захищену передачу даних у комп'ютерній мережі.

FR – протокол канального рівня мережевої моделі OSI

RIP – протоколів маршрутизації в невеликих комп'ютерних мережах (Routing Internet Protocol)

OSPF – протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (Open Shortest Path First)

ICMP – міжмережевий протокол керуючих повідомлень (Internet Control Message Protocol)

IPsec – набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу IP

IrDA – інфрачервоний-порт (Infrared Direct Access)

CVSD – спосіб перетворення аналогового сигналу в цифрову форму (Continuous Variable Slope Delta Modulation)

RF – радіочастота (Radio Frequency)

WPAN – безпровідна персональна мережа

D2D – Device-to-Device, зв'язок між пристроями

ID – ідентифікатор (Identity Document)

ВСТУП

Сучасні технології використовуються не тільки в промисловості, але і в домашній автоматизації, зокрема у системах розумного будинку, для підвищення комфорту проживання людей. Розумний будинок (англ. smarthome) – це автоматизована система, що складається із сукупності датчиків, виконавчих пристроїв, здатних виконувати дії, та програмного забезпечення для реалізації певних повсякденних завдань без участі людини. Дана технологія дозволяє управляти всіма підключеними елементами з одного місця в будинку (пульта управління, хаба тощо), з різних місць (через смартфон, планшет, комп'ютер, управління голосом тощо) за межами будинку через Інтернет. Це дозволяє відстежувати стан всіх датчиків, приладів, камер відеоспостереження та керувати ними дистанційно в режимі реального часу, або переглядати архів записів.

Робота «розумного будинку» передбачає декілька обмінів даними: між елементами системи та між користувачем і системою.

Обмін даними між елементами системи може відбуватися дротовим та бездротовим шляхом за допомогою різноманітних протоколів. Популярні моделі передачі даних у системі розумний будинок: Z-Wave, ZigBee, Wi-Fi, Bluetooth.

Обмін між користувачем та системою також може відбуватися дротовим (безпосередньо при введені даних через пристрої системи) та бездротовим шляхом (наприклад, через мережу Інтернет).

Комбінація декількох моделей передачі даних утворює повноцінну модель розумного будинку. Таким чином є актуальною проблема розробка моделей передачі даних за допомогою різноманітних технологій з урахуванням їх сумісності для розумного будинку.

1 ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО РОЗУМНИЙ БУДИНОК

1.1 Поняття системи розумний будинок

Розумний будинок (РБ) – це автономна система побутових електроприладів та датчиків, яка забезпечує безпеку та життєдіяльність людини в квартири чи будинку без її безпосередньої участі та програмного забезпечення. Всі прилади у домі об'єднані в єдину систему і працюють в автоматичному режимі.

Система РБ дозволяє «спілкуватися» зі своїм будинком через телефон. Людина не тільки отримує повну інформацію про поточний стан всіх електроприладів та датчиків, але й отримує можливість дистанційного керування кожною з них. Якщо господаря будинку немає, і хтось захоче поговорити з ним через домофон, дзвінок буде автоматично переведено на мобільний телефон. Також, при потребі двері можна відкрити дистанційно, через додаток в телефоні.

1.2 Складові системи розумний будинок

Більшість проектів «розумного будинку» діляться на окремі системи для комфортного, більш простішого та вдалого керування системою. Основні системи РБ.

1) Управління освітленням. Одним із найбільш очевидних проявів «інтелекту» є управління освітленням. З системою «розумний будинок» можливо розумно та економно управляти освітленням в квартирі, дачі або офісу. Робота системи освітлення залежить від вимикачів, кнопкових панелей на мікроконтролерах, сенсорних панелей. Автоматична робота системи здійснюється за допомогою різних датчиків (зовнішніх і внутрішніх), таймерів для програмованого включення / вимкнення світильників, ламп у заданий час. Система дозволяє регулювати яскравістю освітлення, вмикати джерела світла за

таймером та часом доби, створювати ефект присутності господарів будинку та світлові сцени.

Для безперебійного електроживлення та електропостачання, також встановлюють акумуляторні батареї, перетворювачі напруги, зарядні пристрої, бензинові та дизельні генератори. При короткочасному відключенні живлення система здатна згладжувати коливання напруги. При довготривалій відсутності струму відбувається автоматичне відключення зайвого електрообладнання (виключення для систем безпеки, зв'язку та хабу).

2) Мікроклімат. Наше здоров'я та працездатність значною мірою залежать від мікроклімату та навколишнього середовища у житлових та громадських приміщеннях. У разі використання у системі «розумний будинок» опалювально-вентиляційних системам, освітлювальної техніки та електропобутового обладнання, сучасний будинок стає дедалі складнішим. Системи автоматизації дозволяють не лише контролювати та керувати будинком, але й можуть подбати про наше здоров'я. Роботу системи забезпечують припливна вентиляція, кондиціонери, електричне або водяне опалення (у тому числі тепла підлога), приводи відкривання / закривання вікон. Для керування застосовують датчики, які фіксують поточний стан мікроклімату в будинку, а також засоби керування – перемикачі та панелі та виконуючі пристрої.

Система виконує функції:

– управління якістю повітря (температура, вологість, озонування) залежно від пори року та доби;

– режим провітрювання за допомогою автоматичного відкривання вікон;

– керування радіаторами опалення;

– управління теплими підлогами;

– автоматичної підтримки температури та вологості у спеціальних приміщеннях (оранжерея, бібліотека, галерея тощо).

Система мікроклімату дозволяє індивідуально контролювати такі параметри, як температура, вологість, провітрювання, включати/вимикати систему фільтрації повітря, створювати індивідуальну кліматичну систему для

кожної людини, що значно економить кошти і вирішує проблему енергозбереження.

3) Безпека. Система безпеки захищає будинок від будь-яких надзвичайних ситуацій. Зазвичай це: захист від вторгнення за допомогою різноманітних датчиків (наприклад, руху) та камер відеоспостереження, автоматизації дверей, воріт, рольставнів, охоронної сигналізації, запобігання аварійним ситуаціям. Можливість вимкнення залишеної праски, щипців або духовки. У разі пожежі або задимлення автоматично спрацює пожежна сигналізація, РБ сповістить господаря та спеціальні служби.

Система безпеки забезпечує:

– контроль цілісності периметра (двері та вікна);

– імітацію присутності господарів;

– контроль доступу до приміщення;

– відеоспостереження за прилеглою територією;

– автоматичне підсвітлення території під час проникнення;

– керування захисними пристроями (жалюзі);

– виклик служби охорони;

– отримання картинки з будь-якої камери відеоспостереження через інтернет;

– запобігання ситуаціям, що загрожують здоров'ю людини, а саме захист від пожежі, витоків газу тощо;

– необхідний комфорт та безпеку для забезпечення оптимального догляду за дитиною (відеоняня) та ін.

Поточний стан зон контролюють провідні та / або безпровідні датчики (датчики вікон, дверей, руху, задимленості). Залежно від типу сигналу вони викликають відповідну реакцію системи керування.

Однією з найважливішою підсистемою системи безпеки є відеоспостереження. Зв'язатися з камерою можна з будь-якої точки земної кулі. Будинок ділиться на кілька зон, і в найважливіших встановлюються керовані відеокамери. Як правило, об'єктами захисту та контролю є прилегла до будівлі територія, включаючи огорожу та будівлі, що окремо стоять; вхідні ворота,

двері, хвіртки, підходи та під'їзди до них; вхідні та ліфтові ходи під'їздів. Камера може працювати постійно або вмикатися від руху щоб не фіксувати зайву інформацію. Сигнали від камер зводяться до центру керування.

Система Безпеки забезпечує:

– захист від протікання;

– захист від короткого замикання електромережі;

– захист від спалахів (датчик задимлення);

– автономне енергопостачання (дизель-генератор);

– автоматичну систему пожежогасіння;

– аварійну сигналізацію для виклику сервісних служб.

4) Мультирум. Функція мультирум розподіляє аудіо- та відеосигнал, дозволяючи прослуховувати джерело сигналу (один або кілька) у незалежних зонах (кімнатах), керувати джерелом з будь-якої зони та регулювати гучність. Кількість зон і джерел сигналу може бути не обмеженою. При цьому вся апаратура зосереджена лише в одному місці Вашої оселі. Управління системою здійснюється за допомогою стаціонарних (настінних та настільних) кнопкових панелей, пульта дистанційного керування або сенсорних панелей. Вони допомагають керувати параметрами джерела сигналу з кожної зони.

Зараз домашній кінотеатр, звук та відео у кожній кімнаті стали звичними. Система «розумного будинку» дозволяє керувати стереосистемою, домашнім кінотеатром або звуком у різних кімнатах, не сходячи з місця.

Підключення домашнього кінотеатру до системи «розумного будинку» забезпечує автоматизоване керування комплексом аудіо- та відео- обладнання, а також низку допоміжних функцій. Ідеальний домашній кінотеатр включає одне або кілька джерел звуку і зображення (HD-плеєр, DVD-програвач, мультимедіа-сервер), багатоканальний AV-ресивер, комплект акустичних систем (зазвичай це наявність п'яти або семи колонок та сабвуфера), плазмову панель, РК-телевізор або проектор з екраном.

Перегляд фільмів, телепередач, прослуховування музики далеко не повний список того, що може запропонувати сучасна технологія «розумний дім». Підключення домашнього кінотеатру до системи «Розумний дім» дає

можливість автоматизованого керування комплексом аудіо- та відео обладнання з єдиного пульт керування або сенсорної панелі. Програмування сценарію дозволяє виконувати список команд за допомогою однієї кнопки. При активізації функції перегляд фільму опускається моторизований екран, висувається захований в ніші проектор, закриваються жалюзі на вікнах, освітлення переходить в режим "Кіно" і світло гасне.

Телебачення та зв'язок. Однією з основних можливостей, що надаються системою "розумний дім", є телебачення та зв'язок, які забезпечують структуровані кабельні мережі (супутникове, ефірне телебачення, телефонія, комп'ютерна мережа). Система "розумний дім" дозволяє, перебуваючи в будинку, завжди бути в центрі подій, інтегруючи джерела отримання інформації (телебачення та інтернет) в навколишнє середовище. Система дозволяє вести прийом та розподіл ефірного або супутникового ТБ по всіх приміщеннях на будь-яке джерело відтворення, а також розподіляти інші потоки цифрових даних (інтернет) по дому. Інтеграція із системою відеоспостереження дозволить отримувати зображення від камер спостереження на будь-якому екрані або телевізорі у будинку. Сигнал телевізійного/супутникового телебачення з антени надходить у систему «мультирум», а далі розподіляється між телевізорами у різних кімнатах, ТВ-тюнерами та керуючими пристроями.

Всі ці пристрої повинні передавати та приймати данні у реальному часі, причому вони не повинні заважати одне одному, тому актуальною є проблема вибору каналів зв’язку за різноманітними технологіями таким чином, щоб всі системи працювали без перешкод.

2 МОДЕЛІ ПЕРЕДАЧІ ДАНИХ ТА ТЕХНОЛОГІЇ ЇХ РЕАЛІЗАЦІЇ

2.1 Безпровідна глобальна мережа (WWAN)

Бездротова глобальна мережа або WWAN – це спосіб підключення до Інтернету без проводів, що досягається за допомогою технології стільникової вежі. Компанії мобільного зв'язку пропонують цей тип підключення за щомісячну плату або по черзі на платній основі.

Можливість підключення дозволяє користувачеві з ноутбуком та спеціальною карткою виходити в Інтернет, перевіряти електронну пошту або підключатися до віртуальної приватної мережі (VPN) з будь-якої точки в межах регіональних меж стільникового зв'язку.

Оскільки люди стають все більш залежними від онлайнових технологій для ведення бізнесу та підтримки потоку інформації, бездротовий зв'язок став віртуальною необхідністю. Багато готелів та спільноти пропонують місцеве з'єднання, але покриття часто нечітке або відсутнє. WWAN може гарантувати підключення лише тоді, коли це необхідно користувачеві.

Щоб скористатися цією технологією, користувач повинен спочатку придбати комп'ютерну картку WWAN для свого ноутбука, якщо підключення не є вбудованим. Купуючи картку та оплачуючи щомісячну плату, користувачеві необхідно лише вставити картку в слот для PC-карток (іноді званий слотом PCMCIA), щоб отримати доступ до послуги. Плани варіюються між постачальниками, але більшість із них оцінюються відповідно до обмежень завантаження даних.

У деяких випадках людині може не знадобитися цілодобовий доступ до Інтернету, але він хотів би використовувати його час від часу, коли безкоштовні локальні мережі недоступні. Деякі провайдери мають плани, які дозволяють користувачам платити за підключення за день. Використовуючи карту WWAN, людина вносить невелику плату, отримує 24-годинний допуск. Після

закінчення 24-годинного періоду користувач більше не зможе підключитися, якщо тільки він або він не придбає ще одну картку.

Як альтернатива платі WWAN деякі мобільні телефони можна підключати безпосередньо до ноутбука за допомогою кабелю універсальної послідовної шини (USB). Мобільний телефон виступає в ролі модему для підключення ноутбука до Інтернету. Це можливо лише для певних моделей телефонів та планів, і швидкість передачі даних буде нижчою, ніж при підключенні за допомогою картки WWAN. Перед використанням цього методу користувачі повинні перевірити у свого оператора стільникового зв'язку, щоб дізнатися, які витрати можуть стягуватися, якщо такі є.

Хоча в багатьох випадках, безумовно, існують менш дорогі способи отримання бездротового підключення, лише небагато покривають територію, яку пропонує WWAN для тих, хто відвідує, живе або працює у віддалених або «непровідних» районах. Послуга зазвичай доступна в регіонах, де такі послуги, як цифрова абонентська лінія (DSL) та кабельний зв'язок, можуть бути відсутніми. Це також може бути міжнародним рішенням для мандрівників у всьому світі, пропонуючи ще одну можливість залишатися на зв'язку.

Передача сповіщень безпеки та контроль в розумному будинку найчастіше йде через використання технологій WWAN. В телефоні встановлюється спеціальний додаток, через який йде підключення до центрального контролера, використовуючи стільниковий зв’язок (рис 2.1). WWAN дозволяє вводити зміни та налаштовувати систему РБ. У разі виникнення аварії чи спрацювання тривоги надсилається SMS.

Рисунок 2.1 – Модель передачі даних через стільниковий зв’язок

2.2 Безпровідна локальна мережа (WLAN)

WiFi – стандарт передачі даних між пристроями на короткі дистанції без проводів. Пристрої, підключені за бездротовою технологією, утворюють мережу.

Технологія WiFi одна з найперспективніших на сьогоднішній день у галузі комп'ютерного зв'язку. WiFi (Wireless Fidelity) – у перекладі з англійської – "бездротова відданість". Технологією Wi-Fi називають один із форматів передачі цифрових даних по радіоканалах.

Спочатку пристрої WiFi були призначені для корпоративних користувачів, щоб замінити традиційні кабельні мережі. Для дротової мережі потрібна ретельна розробка топології мережі та прокладка вручну багатьох сотень метрів кабелю.

Мережа WLAN (Wireless Local Area Network (безпровідна локальна мережа) – вид локальної обчислювальної мережі (LAN), який використовує для зв'язку та передачі даних між вузлами високочастотні радіохвилі, а не кабельні з'єднання. Це гнучка система передачі даних, яка застосовується як розширення або альтернатива кабельної локальної мережі всередині одного офісу, будівлі або в межах певної території.

Ця технологія дозволяє заощаджувати Ваші кошти за рахунок відсутності необхідності прокладати метри кабелю, а простота установки не забирає час на складні ремонтно-технічні роботи. Розширення та реконфігурація мережі для WLAN не є складним завданням: пристрої користувача можна інтегрувати в мережу, встановивши на них бездротові мережні адаптери.

Бездротові мережі використовують радіочастоти, оскільки радіохвилі всередині приміщення проникають через стіни та перекриття. Діапазон або область охоплення більшості систем WLAN досягає 160 м, залежно від кількості та виду перешкод, що зустрічаються. Бездротові мережі зазвичай надійніші, ніж кабельні. Швидкість роботи можна порівняти зі швидкістю кабельної мережі. Так само, як і в звичайній мережі, пропускна здатність

мережі WLAN залежить від її топології, завантаження, відстані до точки доступу і т.д. Кількість користувачів практично необмежена. Його можна збільшувати, просто встановлюючи нові точки доступу. За допомогою точок доступу, що перекриваються, налаштованих на різні частоти (канали), бездротову мережу можна розширити за рахунок збільшення числа користувачів в одній зоні.

Ядром такої мережі є точка доступу (Access Point). Навколо неї утворюється територія радіусом 50-100 метрів, яка називається хот-спотом, або зоною Wi-Fi.

Топологія мережі WiFi. Тимчасова мережа ad-hoc у сімействі стандартів 802.11x називається мережею IBSS (Independent Basic Service Set). Для створення IBSS необхідна наявність принаймні двох пристроїв (наприклад комп'ютерів), оснащених бездротовими мережевими картами. Така мережа не підключена до проводової мережі, тому в ній неможливий обмін даними з магістральною мережею (наприклад, доступ до ресурсів Інтернету). Мережа ad-hoc не потребує точок доступу.

Залежна мережа (BSS – Basic Service Set) використовує пристрої звані точками доступу (AP – Access Point). Їх завданням є посилення та відновлення прийнятих сигналів, контроль руху та забезпечення доступу до провідної частини інфраструктури. Дальність покриття залежної мережі обмежена однієї точки доступу, у межах якої рухома станція може пересуватися без втрати з'єднання.

Складна мережа ESS – Extended Service Set отримаються в результаті об'єднання принаймні двох підмереж BSS, з'єднаних мережею LAN і є найрозвиненішим прикладом комбінованої мережі, який з успіхом може використовуватися для створення великих, змішаних, локальних комп'ютерних мереж.

Маршрутизатор. Маршрутизатор (роутер) – мережевий пристрій, необхідний перенаправлення пакетів даних у однієї чи кількох підмережах з допомогою тієї чи іншої принцица. Маршрутизатор може аналізувати дані, визначає адресата та вибирає маршрут вже виходячи з отриманої інформації.

Якщо комутатор (світч) може створити локальну мережу між кількома комп'ютерами, маршрутизатор здатний з'єднати кілька мереж одночасно, причому з різними ip-адресами (рис. 2.2).

Рисунок 2.2 – Приклад використання маршрутизатора

Розташований у будинку маршрутизатор дає змогу, окрім безпровідного підключення усіх гаджетів та ПК до глобального інтернету, підключити певні датчики та пристрої до центрального контролеру (хаба) системи розумного будинку. Також за допомогою WiFi можливо з будь якої точки світу отримати дані про поточний стан датчиків та пристроїв підключених у систему РБ, налаштувати їх та внести зміни (рис. 2.3).

Рисунок 2.3 – Модель передачі даних з використанням стандарту WiFi у системі розумний будинок

IP-мережа відрізняється від глобальних мереж тим, що є складовою мережею з підмереж, кількість яких вимірюється тисячами. Для Інтернету характерно використання стека протоколів не OSI, а моделі TCP/IP (рис. 2.4). Відмінною особливістю TCP/IP є також те, що IP-пакети можуть передаватися з використанням різних технологій складових мереж. Особливістю моделі TCP/IP на відміну моделі OSI розробили під конкретну складову мережу (internet). Підмережі, яка становить цю складову мережу, з'єднуються між собою маршрутизаторами. Такими підмережами можуть бути як локальні, і глобальні мережі різних технологій.

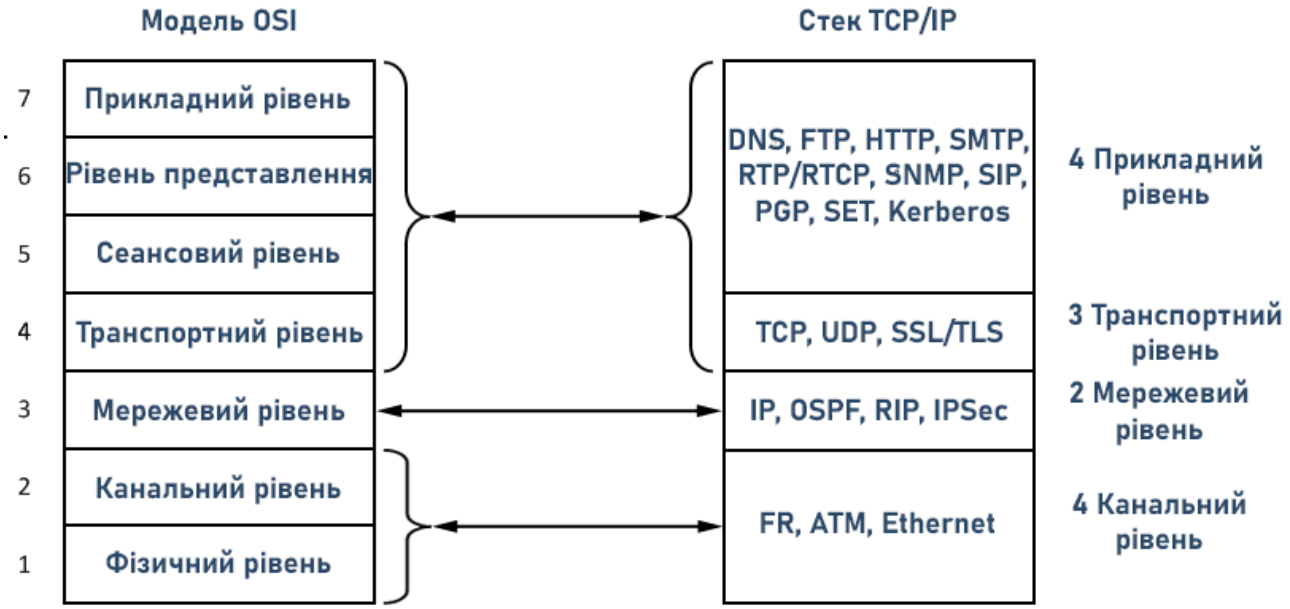

Рисунок 2.4 – Стек протоколів TCP/IP та його відповідність рівням моделі OSI

Прикладний рівень стека TCP/IP (рівень 4) відповідає трьом верхнім рівням моделі OSI. До протоколів прикладного рівня належать протокол перенесення файлів (FTP); протокол електронної пошти (SMTP); протокол, що використовується для створення сторінок у всесвітньому павутинні WWW (HTTP) - основа для доступу до пов'язаних між собою документів; протокол перетворення (DNS) текстових імен у мережеві IP-адреси, простий протокол мережного управління (SNMP), протоколи відповідно сигналізації та передачі даних в IP-телефонії або мова поверх IP (VoIP-Voice over IP) та ін. До

протоколів прикладного рівня відносяться також протоколи інформаційної безпеки Kerberos, PGP, SET та ін.

Транспортний рівень стека TCP/IP (рівень 3) забезпечує передачу даних між прикладними процесами. Транспортний рівень включає два протоколи TCP та UDP. Протокол управління передачею TCP (Transmission Control Protocol) є надійним протоколом із встановленням з'єднання, що дозволяє управляти потоком, тобто. без помилок доставляти байтовий потік з однієї машини на іншу машину складової мережі. Щоб забезпечити надійну доставку даних, протокол TCP передбачає встановлення логічного з'єднання. Це дозволяє йому нумерувати пакети, підтверджувати їх прийом квитанціями, у разі втрати організовувати повторні передачі, розпізнавати та знищувати дублікати, доставляти прикладному рівню у тому порядку, у якому їх було відправлено. Пакети, що надходять на транспортний рівень, організуються як безліч черг до точок входу прикладних процесів. У термінології TCP/IP такі черги, що однозначно визначають додаток у межах хоста, називається портами. За портами кожної стандартної програми визначено номер, наприклад, порт TCP № 21 – за протоколом передачі файлу FTP (File Transport Protocol). Номер порту разом із номером мережі та номером кінцевого вузла має назву сокет (socket). Кожна логічна сполука ідентифікується парою сокетів взаємодіючих процесів. Другий протокол транспортного рівня – протокол користувачів дейтаграм UDP (User Data Protocol) є найпростішим дейтаграмним протоколом (тобто без встановлення з'єднання). До протоколу транспортного рівня належить протокол інформаційної безпеки SSL/TLS. Протоколи прикладного та транспортного рівнів стека рівнів TCP/IP встановлюються на кінцевих станціях (хостах) мережі.

Мережевим рівнем, є основним всієї архітектури TCP/IP. Саме цей рівень, функції якого відповідають мережевому рівню моделі OSI, забезпечує перенесення пакетів даних у межах усієї складової мережі. Протоколи мережевого рівня підтримують інтерфейси з транспортним рівнем, отримуючи від нього запити на передачу даних по складовій мережі. Основним протоколом мережевого рівня є мережевий протокол IP (Internet Protocol). Він забезпечує

просування пакета між підмережами – від одного прикордонного маршрутизатора до іншого, доки пакет не потрапить до мережі призначення.

Протокол IP як і, як і протоколи функцій комутації глобальних мереж зв'язку (FR, ATM та інших.), встановлюється як на кінцевих пунктах (хостах), а й у всіх маршрутизаторах мережі. Маршрутизатор є процесором, який зв'язує між собою дві мережі (підмережі). Протокол міжмережевого рівня працює в режимі без встановлення з'єднання (дейтаграмний режим), відповідно до якого він не відповідає за доставку пакета до вузла призначення. При втраті пакета мережі IP не намагається відновити його.

У заголовку IP-пакета міститься IP-адреса відправника та одержувача - по 4 байти кожен. До міжмережевого рівня належать також протоколи, що виконують функції складання та корекції таблиць маршрутизації RIP (Routing Internet Protocol), OSPF (Open Shortest Path First), протокол міжмережевих керуючих повідомлень ICMP (Internet Control Message Protocol). До протоколу мережного рівня належить протокол інформаційної безпеки IPSec. Рівень мережного доступу стека TCP/IP (рівень 1) відповідає за організацію інтерфейсу із приватними технологіями підмереж складової мережі. Переміщення пакета можна розглядати як послідовність стрибків від одного маршрутизатора до іншого. На черговому маршрутизаторі на мережному рівні визначається мережна адреса наступного маршруту маршрутизатора. Щоб передати пакет IP цьому маршрутизатору, треба перенести через деяку підсіть. Для цього необхідно використати транспортні засоби цієї підмережі. Завдання рівня мережного доступу зводиться до інкапсуляції (вкладання) пакета в блок даних цієї проміжної мережі та перетворення мережних адрес граничних маршрутизаторів цієї підмережі в новий тип адреси, прийнятої в технології проміжної мережі.

2.3 Bluetooth

Bluetooth – технологія бездротового зв'язку, розробленого групою Bluetooth Special Interest Group (Bluetooth SIG), яка була заснована 20 травня

1998 році. У неї увійшли компанії Ericsson, IBM, Intel, Toshiba і Nokia. Потім багато компаній, включаючи Microsoft, Lenovo і Motorola, вступили в неї як асоційовані члени. Будь-яка компанія, яка планує розробляти пристрої Bluetooth, може безкоштовно увійти в цю групу. У SIG вже складається близько 2000 компаній. Згодом Bluetooth SIG і IEEE досягли угоди, на основі якої специфікація Bluetooth стало частиною стандарту IEEE 802.15.1. Роботи із створення Bluetooth компанія Ericsson Mobile Communication почала в 1994 році. Спочатку ця технологія була пристосована під потреби системи FLYWAY у функціональному інтерфейсі між мандрівниками та системою.

На відміну від технології інфрачервоного зв'язку IrDA (Infrared Direct Access), що працює за принципом "точка-точка" в зоні прямої видимості, технологія Bluetooth розроблялася для роботи як за принципом "точка-точка", так і в якості багатоточкового радіоканалу, керованого багаторівневим протоколом , схожим на протокол мобільного зв'язку GSM. Bluetooth стала конкурентом таких технологій, як IEEE 802.11, HomeRF і IrDA, хоча остання і не призначена для побудови локальних мереж, але є найпоширенішою технологією бездротового з'єднання комп'ютерів і периферійних пристроїв.

Основне призначення Bluetooth – забезпечення економного (з точки зору споживаного струму) і дешевого радіозв'язку між різноманітними типами електронних пристроїв, таких як мобільні телефони та аксесуари до них, портативні та настільні комп'ютери, принтери та інші. Причому, велике значення приділяється компактності електронних компонентів, що дає можливість застосовувати Bluetooth у малогабаритних пристроях розміром з наручний годинник. Bluetooth забезпечує обмін інформацією між такими пристроями як кишенькові і звичайні персональні комп'ютери, мобільні телефони, ноутбуки, принтери, цифрові фотоапарати, мишки, клавіатури, джойстики, навушники, гарнітури на надійній та недорогій радіочастоті для ближнього зв'язку. Bluetooth дозволяє цим пристроям обмінюватись інформацією, коли вони знаходяться в радіусі від 10 до 100 метрів один від одного, навіть в різних приміщеннях. Дальність дуже сильно залежить від механічних та радіо перешкод.

Технологія Bluetooth спеціально розроблена для забезпечення дешевою, стійкої, ефективної, високоємного зв'язку, для роботи з голосом і передачі даних, з наступними характеристиками:

– швидкість передачі/прийому 1 Мбіт/с, при використанні каналу з максимально можливою шириною смуги;

– швидкі перемикання частоти, щоб уникнути інтерференції;

– адаптивна вихідна потужність для мінімізації перешкод;

– короткі пакети даних для мінімізації потужності під час перешкод;

– швидке впізнання (підтвердження);

– CVSD (Continuous Variable Slope Delta Modulation) голосове кодування, яке дає можливість роботи з високими частотами помилок по бітам;

– гнучкі типи пакетів, які підтримують широкий спектр додатків;

– ненапружений "бюджет зв'язку", що підтримує недорогу інтеграцію окремих елементарних сигналів;

– інтерфейс передачі/прийому, спеціально пристосований для мінімізації енергоспоживання.

Ці властивості дають технології Bluetooth можливість забезпечувати надзвичайно гнучкий зв'язок з високими швидкостями передачі даних навіть за наявності серйозних перешкод. При завідомо хорошому прийомі в сприятливих умовах передачі сигналу, в міру посилення перешкод, падіння якості переданого сигналу буде залишатися мінімальним і поступовим, що дає можливість збереження стабільного зв'язку.

Bluetooth має RF (Radio Frequency) специфікації для передачі голосу і даних на короткі відстані, "точка-мультиточка".

Принцип роботи. Радіус роботи пристроїв BT2 не перевищує 15 метрів, для BT1 до 100 м (клас А). Ці числа декларуються стандартом для прямої видимості, в реальності не варто чекати роботу на відстані більше 10-20 метрів. Такого дальнодії недостатньо для ефективного застосування атак на практиці. Тому, ще до детального опрацьовування алгоритмів атаки, на Defcon-2004 публіці була представлена антена-гвинтівка BlueSniper, розроблена Джонном Херінгтоном (John Herington). Пристрій підключається до портативного

пристрою ноутбуку/КПК і має достатню спрямованість і потужність (ефективна робота до 1,5 км.)

Радіозв'язок Bluetooth здійснюється в ISM діапазоні (англ. Industry, Science and Medicine - смуга промислового, наукового та медичного застосування), який використовується в різних побутових приладах і безпровідних мережах (вільний від ліцензування діапазон 2,4-2,4835 Ггц). Спектр сигналу формується по методу FHSS (Frequency Hopping Spread Spectrum псевдовипадкова перебудова робочої частоти). Метод FHSS простий в реалізації, забезпечує стійкість до широкосмугових перешкод, а устаткування коштує недорого.

Згідно алгоритму FHSS, в Bluetooth частота сигналу, що несе, стрибкоподібно міняється 1600 разів в секунду (всього виділяється 79 робочих частот шириною в 1 Мгц, а в Японії, Франції і Іспанії смуга вже 23 частотних каналу). Послідовність перемикання між частотами для кожного з'єднання є псевдовипадковою і відома тільки передавачу і приймачу, які кожні 625 мкс (один часовий слот) синхронно перебудовуються з однієї частоти, що несе, на іншу. Таким чином, якщо поряд працюють декілька пар приймач-передавач, то вони не заважають один одному. Цей алгоритм є також складовою частиною системи захисту конфіденційності передаваної інформації: перехід відбувається по псевдовипадковому алгоритму і визначається окремо для кожного з'єднання. При передачі цифрових даних і аудіосигналу (64 Кбіт/с в обох напрямах) використовуються різні схеми кодування: аудио-сигнал не повторюється (як правило), а цифрові дані у разі втрати пакету інформації будуть передані повторно. Без перешкодостійкого кодування це забезпечує передачу даних зі швидкостями 723,2 Кбіт/с із зворотним каналом 57,6 Кбіт/с, або 433,9 Кбіт/с в обох напрямах.

Для повнодуплексної передачі використовується дуплексний режим з тимчасовим розділенням (TDD). Підтримується ізохронна і асинхронна передача даних і забезпечується проста інтеграція з TCP / IP. Енергоспоживання пристроїв Bluetooth має бути в межах 0.1 Вт. Кожен

пристрій має унікальну 48-бітову мережеву адресу, сумісний з форматом стандарту локальних мереж IEEE 802.

В багатьох датчиках чи пристроях, зараз, вбудована технологія Bluetooth і це дає змогу активно використовувати їх для автоматизації будинку в системі розумного будинку. Центральний контролер встановлює зв’язок з датчиком та отримує від нього потрібні данні та передає на екран хабу (рис. 2.5).

Рисунок 2.5 – Приклад моделі передачі даних через технологію Bluetooth

2.4 Zigbee

Відкритий стандарт Zigbee призначений для програм з низьким рівнем передачі даних та енергоспоживанням та підтримує нижчі швидкості і використовує протокол комірчастої (mesh) мережі для створення архітектури, що самовідновлюється.

Протокол Zigbee заснований на специфікації 802.15 та створений для мереж керування та датчиків за бездротовим стандартом IEEE для безпровідна персональних мереж (WPAN). Мережі працюють на частотах 2,4 ГГц, 900 МГц та 868 МГц. Zigbee пристрої взаємодіють між собою в екосистемі розумного

будинку, що використовують топологію мережі. Пристрої знаходять активні девайси на його околицях, ініціюють зв'язок без переривань. Ефективність системи збільшується за допомогою зв'язку D2D.

Швидкість Zigbee – 250 кбіт/с, найкраще підходить для періодичної та проміжної двосторонньої передачі даних між датчиками та контролерами. За технологією Zigbee дальність зв'язку заявлено 10-100 метрів.

Основні характеристики Zigbee:

– підтримує кілька мережевих топологій («точка-точка», багатоточкові, комірчасті мережі);

– має низький робочий цикл збільшуючи термін служби батареї;

– має низьку затримку відгуку;

– забезпечує спектр поширення прямої послідовності (DSSS);

– допускає наявність 65 000 мережних вузлів;

– має шифрування 128-bit для безпечного підключення до даних;

– запобігає зіткненням, повторним спробам, підтвердженням.

Структура системи Zigbee складається з трьох типів пристроїв: координатор, маршрутизатор та кінцевий пристрій. Кожна мережа повинна складатися щонайменше з одного координатора, який діє як корінь і міст (хаб) мережі. Координатор відповідає за обробку та зберігання інформації при виконанні операцій прийому та передачі даних. Маршрутизатори виступають ролі проміжних пристроїв, які забезпечують обмін між компонентами (рис. 2.6).

За допомогою Zigbee в системі розумний будинок можна автоматизувати:

– моніторинг безпеки та керування домашніми програмами з віддалених місць;

– дистанційне керування приладами;

– автоматичні двері, вікна із датчиками руху;

– прогнозують датчики диму, води та газу;

– розумні світлові рішення з програмами для керування зі смартфона;

– підключене освітлення із опціями енергозбереження;

– інтелектуальні перемикачі, які не потребують батарейного джерела живлення;

– інтелектуальні програми для роздрібної торгівлі: відстеження розташування, датчики, торгові марки електроніки;

– моніторинг безпеки харчових продуктів;

– удосконалені бездротові пристрої для покращення покупок.

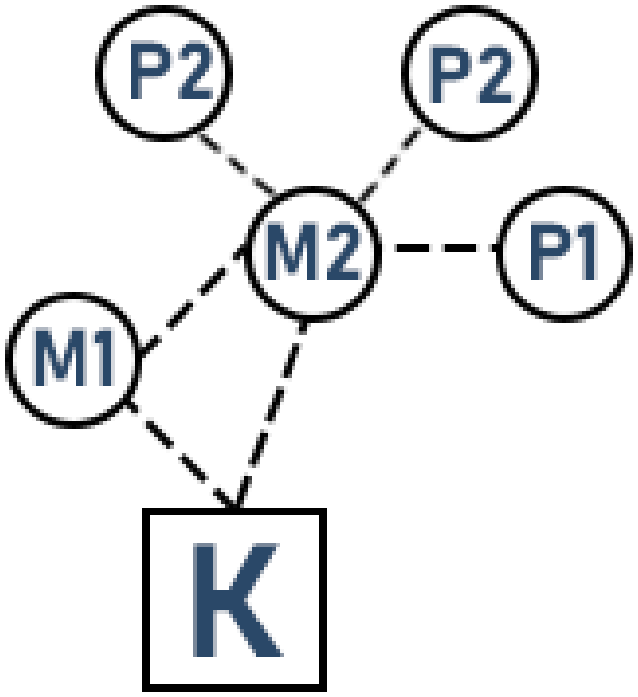

Рисунок 2.6 – Модель передачі даних Zigbee в системі розумний будинок (К – координатор Zigbee; М1, М2 – маршрутизатори, які передають і приймають сигнал Zigbee; Р1, Р2, Р3 – кінцеві прилади)

2.5 Z-Wave

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

Приклади використання технології Z-Wave:

– управління освітленням (реле/димери), шторами, рольставнями та воротами;

– управління жалюзі та іншими моторами (10-230 В);

– увімкнення/вимкнення будь-яких навантажень до 3.5 кВт (модуль в розетку або реле, що вбудовується);

– управління обігрівом (електричні теплі підлоги із захистом від перегріву, електро котли та радіатори, термостати для водяних клапанів радіаторів);

– управління кондиціонерами (через ІЧ інтерфейс імітуючи пульт);

– детектування тривожних подій (датчики руху, відкриття дверей/вікна, протікання, сухі контакти);

– моніторинг стану (датчики температури, вологості, освітленості);

– управління A/V апаратурою (за протоколом Z-Wave або через ІЧ інтерфейс імітуючи пульт);

– зв'язок із будь-яким програмним забезпеченням через ПК контролер;

– збір даних із лічильників.

Протокол Z-Wave був розроблений для квартир та невеликих будинків. Зазвичай такі системи містять від 10 до 150 пристроїв. Основна особливість Z-Wave у тому, що він належить до формату "зроби сам", встановлення та налаштування системи власник житла може зробити самостійно. Протокол розроблявся спеціально керувати такими пристроями як світло, жалюзі, ворота, термостати та інші шляхом передачі коротких команд, потребують невеликого енергоспоживання. Типові невеликі завдання, які вирішуються за допомогою Z-Wave – це встановлення прохідних вимикачів, перенесення вимикачів на більш зручний рівень, дистанційне керування воротами та жалюзі, включення світла за датчиками руху. Всі ці завдання не вимагають перекладання дротів. Існують і складніші проекти автоматизації квартир, що не поступаються за складністю промисловим системам автоматизації.

Модель стека мережевих протоколів Z-Wave має 6 рівнів логічної роботи:

Фізичний рівень. Передача даних здійснюється на частоті 869.0 МГц (Росія), 868.42 МГц (Європа, Китай, Сінгапур, ОАЕ, ПАР), 908.42 МГц (США, Мексика), 921.42 МГц (Австралія, Бразилія, Нова Зеландія, Гонконг), 865.2 МГц (Індія), 868.2 МГц (Малайзія), Японія (951-956 та 922-926 МГц). Модуляція FSK (частотна маніпуляція). Швидкість передачі: 42 кбіт/с, 100

кбіт/с та 9.6 кбіт/с (для сумісності зі старими пристроями). Добре не більше 1%. Гранична потужність передачі 1 мВт.

Канальний рівень. Використовуються пакети з контролем цілісності даних (контрольна сума) та адресацією одержувача та відправника. Як одержувач може використовуватися multicast адресу чи broadcast (у разі пакет приймається всіма учасниками мережі з включеним радіо-модулем).

Мережевий рівень. Протокол Z-Wave визначає алгоритм маршрутизації, що дозволяє передавати дані між пристроями поза прямою видимістю. Всі вузли мережі, що постійно працюють (бувають ще сплячі і "часто слухають" вузли) можу брати участь у пересиланні пакетів між іншими учасниками мережі. Z-Wave використовує механізм Source Routing, тобто. маршрут проходження визначається відправником. Broadcast та multicast пакети не маршрутизуються. Якщо неможливо знайти потрібний вузол за маршрутами, записаними в пам'яті, існує механізм пошуку вузла по всій мережі шляхом надсилання спеціального пакета Explorer Frame всім вузлам мережі. Після успішного знаходження вузла новий маршрут записується відправником на згадку для подальшого використання.

Транспортний рівень. На цьому рівні Z-Wave гарантує підтвердження доставки та повторне відправлення у випадку, якщо пакет не був доставлений до одержувача. Кожен вузол, що у пересиланні, підтверджує факт отримання повідомлення. Для зменшення завантаження ефіру в Z-Wave використовується механізм "мовчазних підтверджень": вузол (А), що передав пакет наступному вузлу (Б) на шляху проходження пакета не чекає підтвердження від нього, а бачить, що Б відправив пакет далі вузлу С і сприймає це як факт підтвердження успішного пересилання пакета від А до Б. Отримавши пакет, кінцевий вузол передає назад підтвердження доставки, яке подорожує назад тим самим маршрутом до вихідного відправника. Таким чином, відправник завжди знає, чи дійшов пакет до точки призначення чи ні.

Сеансовий рівень. Використовується лише при використанні шифрування, де визначаються короткі сеанси з одноразовим ключем.

Прикладний рівень. Z-Wave також визначає алгоритм інтерпретації одержуваних на прикладному рівні команд. Даний рівень описаний набором класів команд (Command Classes). Для деяких класів існує кілька варіантів інтерпретації команд, які залежать від класу пристрою (Device Class), що визначає тип пристрою.

З 2012 року фізичний та канальний рівні протоколу Z-Wave увійшли до стандарту ITU-T G.9959 (рекомендації сектора стандартизації електрозв'язку Міжнародного союзу електрозв'язку).

Рівні від транспортного до канального реалізовані у програмному коді Sigma Designs і постачаються у прекомпільованому вигляді (у комплекті SDK). З одного боку, пропрієтарний код — це мінус, але в закритості даного протоколу є і свої плюси: жоден виробник не може змінити нижні рівні протоколу, що дозволяє легше забезпечувати сумісність — всі пристрої засновані на одному добре налагодженому коді.

Усі команди Z-Wave гранично компактно упаковані. Це необхідно для зменшення розміру пакета, що позитивно впливає займане в ефірі час, і навіть зменшення втрат під час передачі. Z-Wave призначений передачі коротких команд без відкриття сесії, тобто. Не підходить для потокової передачі потокових даних. Максимальний корисний розмір даних становить 46 байт (розмір даних прикладного рівня без шифрування).

Типи вузлів в структурі Z-Wave.

Портативний контролер (Portable Controller) Пристрій, що зберігає інфомацію про сусідів всіх вузлів мережі (топологію мережі) та здатний на базі цієї інформації знайти маршрут до будь-якого вузла мережі. Крім того, цей пристрій може переміщуватися в мережі і здатний достукатися до всіх вузлів мережі з будь-якої точки мережі (звичайно за умови, що мережа однозв'язна). До пристроїв цього типу не можна звернутися, т.к. вони не фігурують у таблиці маршрутизації (будучи портативними) — їм можна лише відповідати на їхній запит. Можливе застосування: пульт дистанційного керування. Такий пристрій потребує енергонезалежної пам'яті EEPROM.

Статичний контролер (Static Controller) Аналогічний портативному, але він повинен переміщатися у просторі і покликаний бути завжди доступним іншим учасникам мережі. Типове застосування: контролер ПК, виконавець. Такий пристрій потребує енергонезалежної пам'яті EEPROM.

Дочірний пристрій (Slave) Пристрій, здатне лише відповісти запит, що прийшов до нього, т.к. не знає топології мережі та не зберігає жодних маршрутів. Такі пристрої можуть бути лише датчиками, які живляться від мережі та опитуються іншими вузлами, або виконавцями. Вони не вміють ініціювати відправлення даних самостійно (надсилати непрохані пакети — unsolicited packets).

Дочірній маршрутизатор (Routing Slave) Пристрій, здатний зберігати до 4 маршрутів для 5 вузлів (так звані "зворотні маршрути"). Ці пристрої можуть ініціювати відправлення даних (надсилати непрохані пакети — unsolicited packets), а також можуть бути сплячими або "часто слухають". Типове застосування: датчики, виконавці, нерухомі пульти керування (датчик руху, кнопка вмикання на батарейках).

Просунутий дочірній маршрутизуючий пристрій (Routing Enhanced Slave) Як і дочірній маршрутизуючий пристрій, але що зберігає маршрути до всіх вузлів мережі, а не тільки до 5. Такому приладу потрібна енергонезалежна пам'ять EEPROM.

Більшість вузлів знають маршрути до деяких вузлів через своїх сусідів. Повні списки сусідів усіх вузлів зберігаються на контролерах, які покладаються на їхню достовірність при формуванні маршрутів (рис. 2.7).

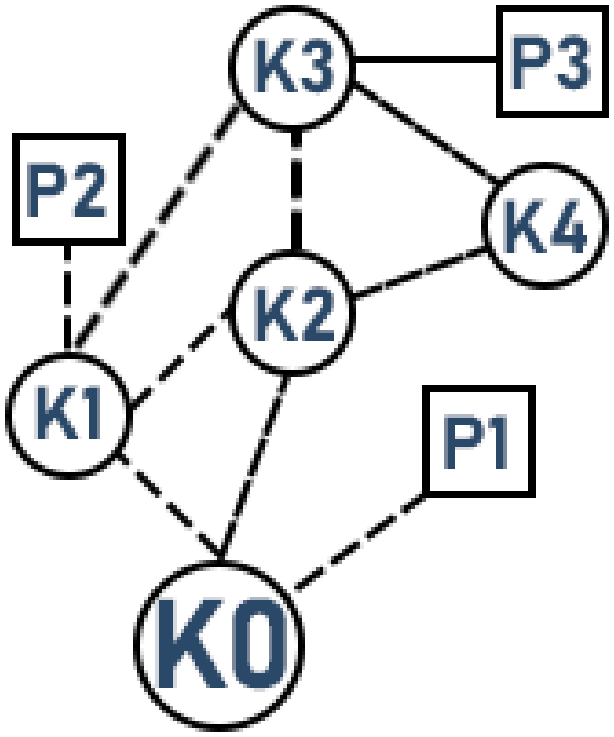

Рисунок 2.7 – Модель структури Z-Wave в системі розумний будинок (K0 – центральний контролер Z-Wave; K1, K2, K3, K4 – вторинні контролери; P1, P2, P3 – кінцеві прилади)

Мережа Z-Wave визначається унікальним параметром Home ID (генерується при створенні мережі генератором випадкових чисел з шумом від радіоприймача як джерело випадкових числа або призначається Sigma Designs для старих контролерів). На одній території може співіснувати кілька мереж Z-Wave із різними Home ID. При цьому вони не будуть бачити один одного і взаємодіяти один з одним. Завдяки обов'язковій вимогі шпаруватості (не більше 1% часу перебуває в стані передачі), ці мережі не заважатимуть один одному.

Кожен вузл в мережі має свій унікальний Node ID, який присвоюється первинним контролером при включенні пристрою в мережу. Також при включенні в мережу пристрій запам'ятовує Home ID первинного контролера для подальшого спілкування. Мережа може містити до 232 пристроїв.

Увімкнення відбувається переведенням контролера в спеціальний режим Увімкнення (Inclusion mode; зазвичай якоюсь спеціальною кнопкою або комбінацією клавіш), а пристрою, що включається в режим Навчання (Learn mode; зазвичай одинарним або потрійним натисканням на кнопку). При цьому

контролер і пристрій повинен перебувати в прямій видимості. Багато сучасних (версій протоколу 4.5x або 6.x) пристрої, що постійно живляться (не сплять), перші 3-5 хвилин після включення в мережу електроживлення самостійно переходять у спеціальний режим навчання (Network Wide Inclusion, NWI), якщо вони ще не включені в мережу . При цьому умова перебування у прямій видимості вже не потрібна. Це дозволяє легко включати в мережу нові пристрої, не бігаючи по будинку.

Виняток із мережі відбувається аналогічно: контролер переводиться у режим Виключення (Exclusion mode), а дочірній вузол у режим Навчання. Після виключення Node ID та Home ID пристрої скинуться на 0 (для контролерів NodeID скинеться на 1, а HomeID на заводське значення). Більшість пристроїв при виключенні скине і всі інші налаштування на заводські значення.

Варто зазначити, що пристрій, що вже прописаний в одній мережі, не включиться в іншу мережу. Але виключити з мережі може будь-який первинний контролер (навіть пристрій не зі своєї мережі).

Контролери та дочірні пристрої включаються до мережі та виключаються з неї однаковим чином.

При включенні до мережі первинний контролер отримує інформацію про тип включеного вузла та його NIF.

Commad Classes (Класи Команд).

Всі дані рівня програми передаються у вигляді коротких пакетів такого вигляду:

Command Class ID
Command ID
<специфічні дані для команди>

Спочатку йде Клас Команди, потім команда у цьому класі, далі дані специфічні для цієї команди. Завдяки строгому стандарту, який описує Класи Команд, пристрої різних виробників можуть розуміти один одного без будь-яких проблем.

Приклад популярних класів:

Basic – найпопулярніший клас, що дозволяє пристроям різного типу бути сумісними на мінімальному рівні. Наприклад, вимикач вміє посилати команди Включити/Вимкнути, які диммер і реле інтерпретуватимуть як включення/вимикання світла, термостат як перехід між режимами нормальний/енергозберігаючий, а пристрій управління жалюзі як хід/зупинка руху віконниць.

Switch Binary / Switch Multilevel – використовуються для керування освітленням (реле/діммер), а також для керування моторами (для віконниць або воріт).

Sensor Binary / Sensor Multilevel – для бінарного датчика (відкриття дверей, протікання, диму, руху) та багатопозиційного датчика (температури, освітленості, вологості).

Meter – використовується для зняття показань та скидання накопичених значень лічильників.

Association – дозволяє встановлювати зв'язки між пристроями. Наприклад, на пристрої є 3 кнопки. Для них є 3 відповідні кнопки групи асоціацій. При натисканні на кнопку надсилаються команди Basic Set Увімкнути відповідній групі. Клас Association використовується для ведення списку вузлів у цій групі. Такий підхід дозволяє легко та ефективно налаштовувати прямі взаємозв'язки між пристроями мережі.

Configuration – дозволяє змінювати деякі закладені виробником установки пристроїв. Наприклад, швидкість димування світла чи чутливість датчика руху.

Battery – дозволяє вимагати заряду батарей пристроїв.

Wakeup – для керування параметрами прокидання сплячих пристроїв.

MultiChannel – використовується для адресації до конкретної компоненти складного пристрою, що складається з кількох елементів. Звичайні класи команд (Basic, Switch/Sensor Binary/Multilevel, Meter) інкапсулюються в команду даного класу із зазначенням номера елемента. Наприклад, пристрій може містити два реле або три датчики (температури, вологості та руху).

Список підтримуваних пристроєм Класів Команд міститься в пакеті NIF (Node Information Frame – пакет опису пристрою). Завдяки ньому можна визначити Клас Пристрої (Device Class) та список можливостей пристрою. Цей пакет приходить первинному контролеру при включенні пристрою в мережу, а також при натисканні один або три рази на кнопку (у більшості пристроїв дивитися документацію до конкретного пристрою).

Device Classes. Кожен пристрій характеризується своїм функціональним типом (Класом Пристрою, Device Class). Кожен клас визначає обов'язкові класи команд, що підтримуються пристроєм, та способи інтерпретації їх команд. Наприклад, команди класу команд Basic можуть абсолютно по-різному інтерпретуватися для різних класів пристроїв: для двопозиційного реле Basic Set 0 вимикає, 1-99 або 255 включають, у той час як для термостата можуть інтерпретуватися як температура в одиницях або 1/10 градусів. , тобто. від 0 до 255 чи від 0 до 25.5 градусів, відповідно. Всі інші класи команд чітко прописані аж до інтерпретації кожної команди.

3 АНАЛІЗ МОДЕЛЕЙ ПЕРЕДАЧІ ДАНИХ ДЛЯ СИСТЕМИ РОЗУМНОГО БУДИНКУ

3.1 Сумісність моделей передачі даних

При створенні загальної моделі розумного будинку іноді приходиться комбінувати різні моделі передачі даних. Але, не всі вони можуть бути поєднані в одну систему РБ (таблиця 3.1).

Проблема сумісності одна із основних перешкод поширення пристроїв розумного будинку. Використання виробниками різних моделей передачі даних ускладнює використання пристроїв розумного будинку та їх інтеграцію один з одним. Наприклад, в системі розумному будинку з використанням моделі передачі даних WiFi об’єднують або поєднують в одну систему з моделлю Bluetooth. Але, якщо обрати моделі передачі даних через Zigbee або Z-Wave, то їх поєднання у загальну систему РБ не можлива. Ці моделі співпрацюють тільки самі з собою, причому системи розумних будинків однієї компанії на базі цих моделей не можуть об’єднатися у спільну систему з датчиками, приладами інших виробників.

Таблиця 3.1 – Таблиця сумісності моделей передачі даних в одні системі розумний будинок

Модель	Стільниковий зв’язок	WiFi або інтернет	Bluetooth	Zigbee	Z-Wave
Стільниковий зв’язок	Не існує системи РБ	Сумісні	Сумісні	Сумісні	Сумісні
WiFi або інтернет	Сумісні	Сумісні	Сумісні	Сумісні	Сумісні
Bluetooth	Сумісні	Сумісні	Сумісні	Не сумісні	Не сумісні
Zigbee	Сумісні	Сумісні	Не сумісні	Сумісні	Не сумісні
Z-Wave	Сумісні	Сумісні	Не сумісні	Не сумісні	Сумісні

Причому, моделей розумного будинку з використанням лише передач даних Bluetooth, Zigbee та Z-Wave – не існує. Всі вони використовують WiFi та/або стільниковий зв'язок для передачі даних на смартфон або ПК, користувачеві. Отже, виходячи з таблиці 3.1 є три основні моделі розумного будинку, об'єднані різними типами передачі даних:

1) модель РБ WiFi та Bluetooth (рис. 3.1);
2) модель РБ Zigbee (рис. 3.2);
3) модель РБ Z-Wave (рис. 3.3).

Невід'ємною частиною кожної такої системи розумного будинку є модель передачі даних через стільниковий зв'язок, яка дає доступ через спеціальний додаток в смартфоні до системи. Через цей додаток можна контролювати, переглядати, змінювати дані в датчиках або пристроях, для налагоджування всієї системи.

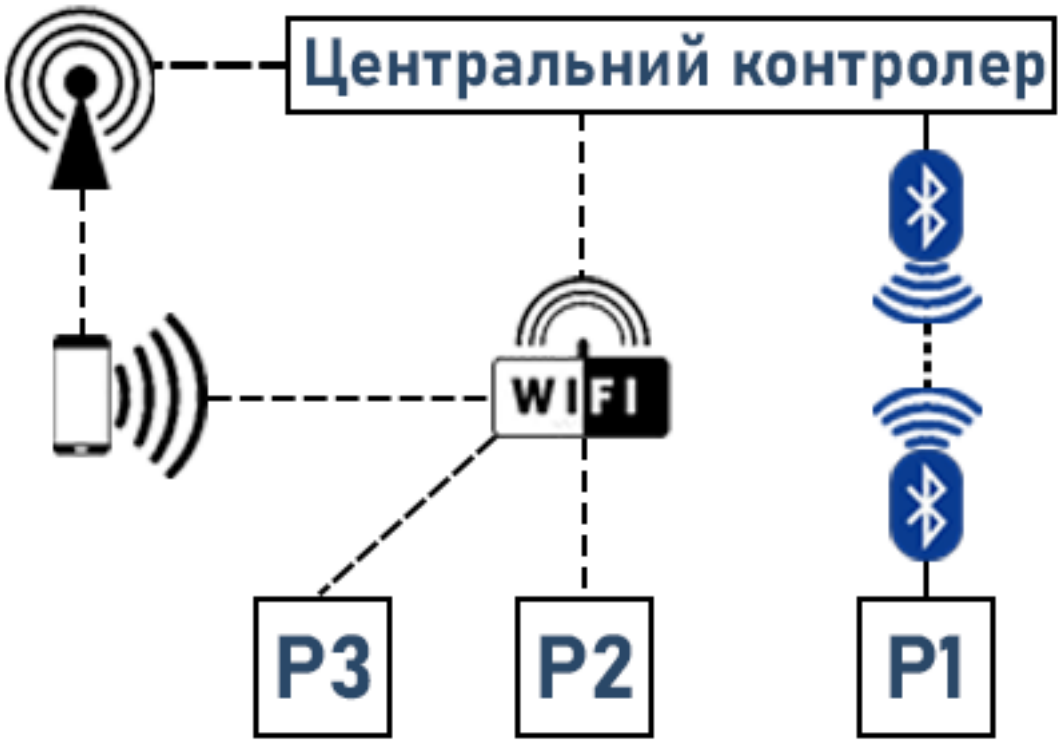

Рисунок 3.1 – Модель РБ WiFi та Bluetooth
(P1, P2, P3 – кінцеві прилади або датчики)

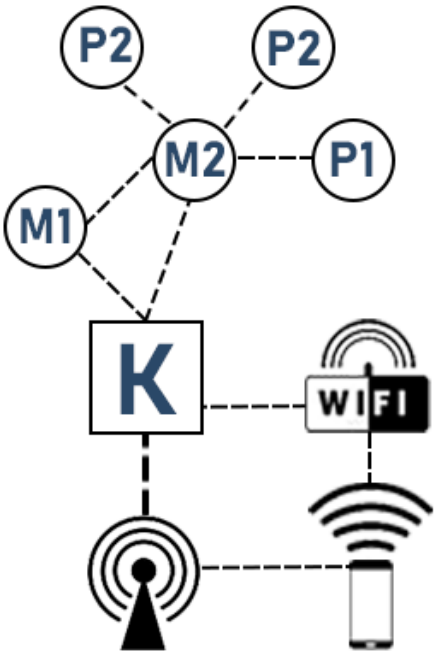

Рисунок 3.2 – Модель РБ Zigbee

(К – центральний контролер; М1, М2 – маршрутизатори сигналу Zigbee; Р1, Р2, Р3 – кінцеві прилади або датчики)

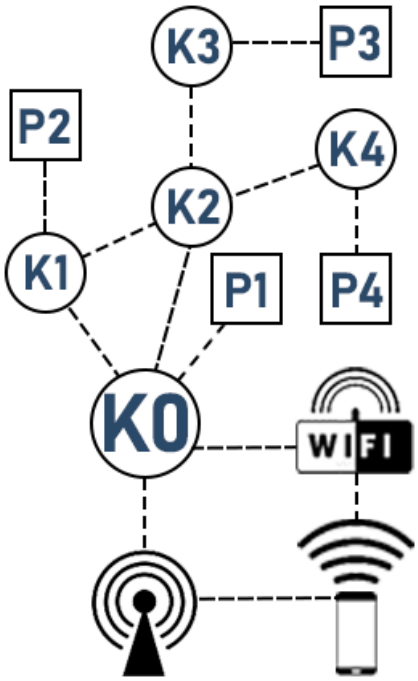

Рисунок 3.3 – Модель РБ Z-Wave

(К0 – центральний контролер Z-Wave; К1, К2, К3, К4 – вторинні контролери; Р1, Р2, Р3, Р4 – кінцеві прилади)

В Україні популярності набула модель РБ WiFi та Bluetooth (рис. 3.4). Це можна зрозуміти проаналізувавши ринок приладів та датчиків в популярних і офіційних магазинах в країні.

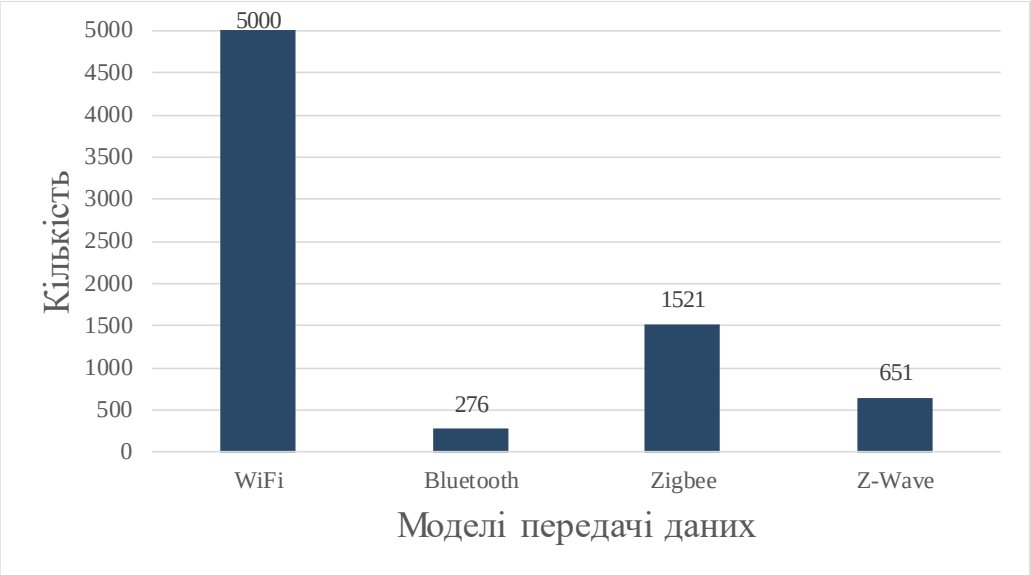

Рисунок 3.4 – Діаграма кількості кінцевих приладів та центральних контролерів для моделей розумного будинку WiFi, Bluetooth, Zigbee, Z-Wave на ринку України

Не зважаючи на те що в аналіз не увійшли системи розумного будинку центральним контролером яких виступає ПК, перевага обрання людьми в Україні моделі РБ WiFi та Bluetooth найпоширеніша. Також, це підтверджує кількість кінцевих приладів, виготовлених компаніями-гігантів, які випускають на ринок датчики, прилади з різними моделями передачі даних. Наприклад, китайська компанія Xiaomi, яка офіційно продає свої продукти в України, надає таку статистику свої товарів для автоматизації будинка: на базі WiFi випущено 100 приладів, Bluetooth – 24, Zigbee – 35.

3.2 Порівняння моделей РБ за основними характеристиками

Кількість кінцевих приладів (датчиків) в моделях розумного будинку, обмежена властивостями використаного при побудові системи РБ центрального контролера (хаб). Центральних контролерів існує багато від різних компаній і

вони зазвичай не поєднуються один з одним. Також, хабом може виступати персональний комп'ютер, на якому встановлений спеціальний додаток, наприклад: Apple HomeKit, Google, Amazon, Xiaomi та Control4.

До встановлення центрального контролера потрібно підходити особливо ретельно. Бажано це робити в центрі квартири або будинку, для того щоб він міг побачити і об'єднати усі кінцеві прилади в системі, інакше прийдеться докупляти подовжувачі сигналів або вторинні контролери (рис 3.5). Також, треба врахувати усі перешкоди на шляху сигналу.

В моделях розумного будинку Zigbee або Z-Wave кількість приладів та датчиків стандартизовано та вказано виробниками. Переважно, можна вмістити від 200 кінцевих приладів в модель РБ Zigbee, та 232 в Z-Wave.

В моделі розумного будинку WiFi та Bluetooth кількість кінцевих приладів залежить від марки та виробника розумних маршрутизаторів (роутерів), це може бути від 20 до 40 приладів. А для об'єднання з датчиками Bluetooth треба встановлювати ретранслятори сигналів.

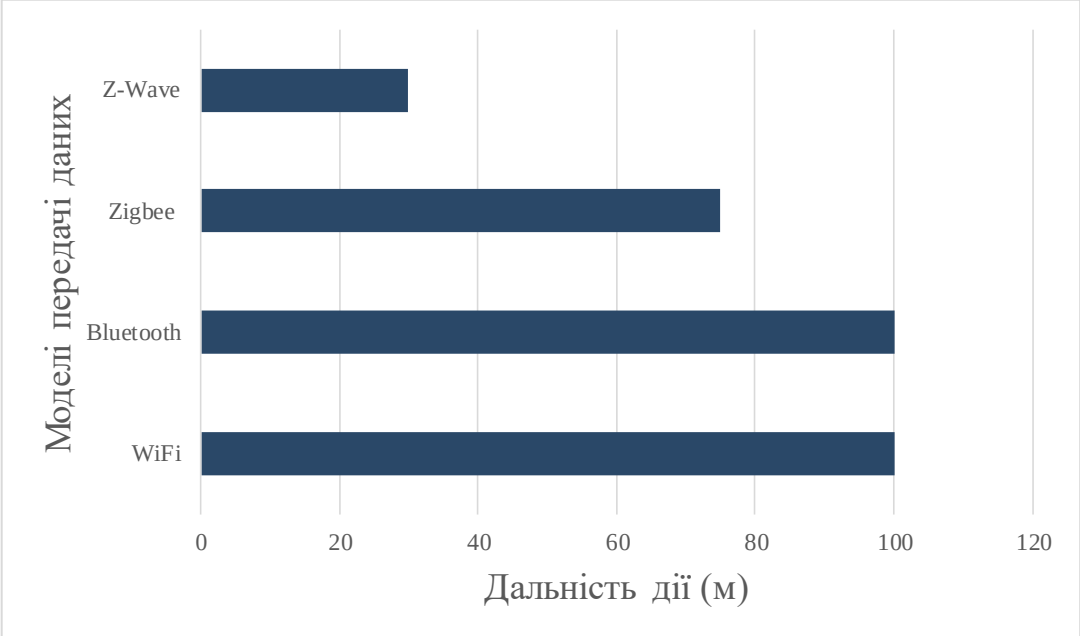

Рисунок 3.5 – Діаграма дальності дії сигналу моделей передачі даних в системі розумний будинок

Окрім дальності дії сигналів в моделях розумного будинку, найважливішим параметром є пропускна здатність. Пропускна здатність

залежить від моделі передачі даних та її стандарту, наприклад прилади або датчики оснащені Bluetooth v. 2.0 передають дані зі швидкістю до 3 Мбіт/с, тоді як Bluetooth v. 3.0 має пропускну здатність від 3 до 24 Мбіт/с. Детальніше про всі стандарти та їх пропускну здатність дивитися в таблиці 3.2.

Таблиця 3.2 – Порівняльна таблиця моделей передачі даних на пропускну здатність

Модель	Стандарт	Пропускна здатність
WiFi	IEEE 802.11a	до 54 Мбіт/с
WiFi	IEEE 802.11b	до 11 Мбіт/с
WiFi	IEEE 802.11g	до 54 Мбіт/с
WiFi	IEEE 802.11n	до 300 Мбіт/с
Bluetooth v. 1.2	IEEE 802.15.1	до 0,7 Мбіт/с
Bluetooth v. 2.1	IEEE 802.15.1	до 3 Мбіт/с
Bluetooth v. 3.0	IEEE 802.15.1	від 1 до 24 Мбіт/с
Bluetooth v. 4.2	IEEE 802.15.1	від 1 до 24 Мбіт/с
Bluetooth v 5.0	IEEE 802.15.1	від 2 до 48 Мбіт/с
Zigbee	IEEE 802.15.4	від 20 до 250 Мбіт/с
Z-Wave	ITU-T G.9959	від 40 до 100 Мбіт/с

Для більш докладнішого і правдоподібного визначення споживання електроенергії в моделях розумного будинку її розглядають у чотирьох стадіях (табл. 3.3):

1) режим сну;
2) режим очікування;
3) режим передачі даних;
4) режим отримання даних.

Виходячи з таблиці 3.3 було побудовано діаграму порівняння споживання електроенергії моделями передачі даних (рис 3.6).

Таблиця 3.3 – Таблиця споживання електроенергії моделями передачі даних

Режим	Модель передачі даних			
	WiFi	Bluetooth	Zigbee	Z-Wave
Режим сну	30 мкА	9 мкА	12 мкА	12 мкА
Режим очікування	245 мА	35 мА	50 мА	50 мА
Режим передачі даних	251 мА	39 мА	52 мА	50 мА
Режим отримання даних	248 мА	37 мА	54 мА	55 мА

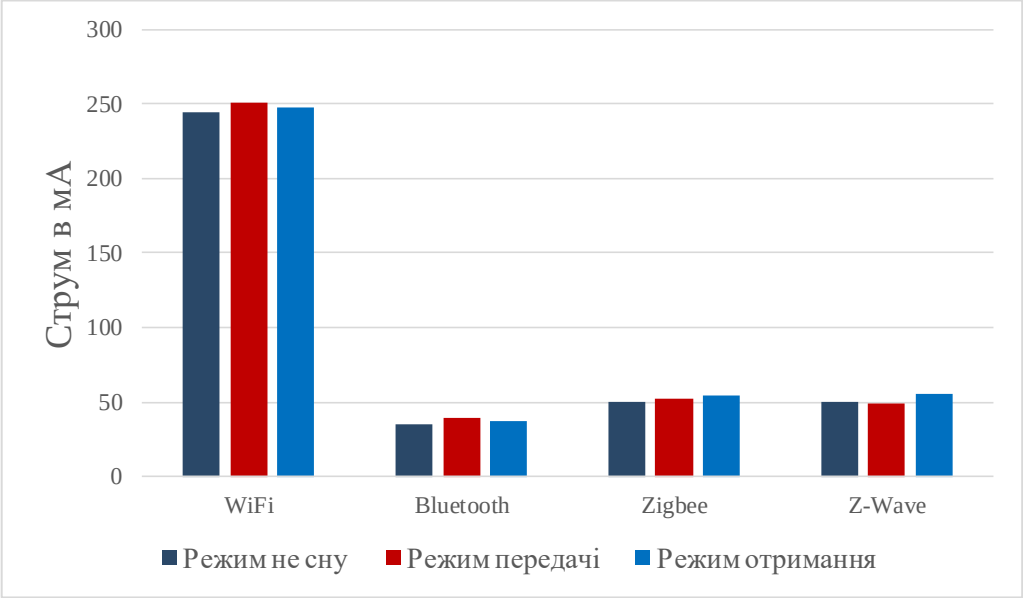

Рисунок 3.6 – Діаграма споживання електроенергії моделями передачі даних

3.3 Перешкодостійкість та перешкодозахищеність моделі РБ WiFi та Bluetooth

З аналізу, який наведено у підрозділі 3.1, було виявлено, що найпопулярнішою моделлю розумного будинку є WiFi та Bluetooth.

У зв'язку з цим розрахуємо вплив роботи WiFi за протоколом 802.11b на ймовірність появи помилок приймача Bluetooth.

За приклад було взято передачу мультимедійного файла. Трафік бездротовими мережами більш схильний до впливу різних перешкод. Таким чином, завдання визначення можливості бездротових моделей передачі даних отримувати ті чи інші мультимедійні дані у певному місці мережі в умовах дії перешкод та підвищення стійкості перешкод мережі є актуальною.

Крім того, слід враховувати, що сучасна техніка проектується з розрахунком забезпечення максимальної мобільності та малих габаритів пристроїв, тому блоки Wi-Fi та Bluetooth монтуються на одній платі, що призводить до виникнення взаємних перешкод, що обумовлені близькістю робочих діапазонів частот: для стандартів IEEE 802.11b – 2,4 та 5 ГГц; для IEEE 802.15.1 – 2,4 ГГц. Таким чином, при оцінці перешкодостійкості WiFi та Bluetooth мереж необхідно враховувати канальну інтерференцію цих двох стандартів.

Під перешкодою розуміється будь-який вплив, що накладається на сигнал і утруднює його прийом. Сигнал на вході каналу зв'язку F_m може бути представлений як лінійна комбінація базових векторів:

$$F_m = a_1\overline{S_1}(t) + a_2\overline{S_2}(t) + a_3\overline{S_3}(t) + \cdots + a_n\overline{S_n}(t). \quad (3.1)$$

У разі дискретного каналу, як правило, один з $a_i = 1$, інші дорівнюють нулю. Для приймачів різних двох сигналів S_1 та S_2 – базисні вектори. На вхід приймача пристрою приходить: $x_1 = S_1(t) + \xi_1(t)$ або $x_2 = S_2(t) + \xi_2(t)$, де $\xi_i(t)$ – сигнал перешкоди. Імовірність помилки приймача у складі двійкового симетричного каналу:

$$P_{пм} = 0{,}5 \times \left(1 - \frac{2}{\sigma\sqrt{2\pi}} \times \int_0^{\frac{d}{2}} e^{\frac{-\xi^2}{2\sigma^2}}\, d\xi\right), \quad (3.2)$$

де σ – задане середньоквадратичне відхилення. Цей вираз оцінює ймовірність помилки $P_{пм}$ як ймовірність того, що проекція вектора перешкоди на вектор різниці $\bar{d} = \overline{S_1} - \overline{S_2}$ набуде значення, що перевищує $\frac{d}{2}$, де d – довжина

вектора $\bar{d}$. У цьому випадку кінець вектора $\bar{x} = \bar{S_1} - \bar{\xi_2}$ (при передачі сигналу S_1) опиниться у просторі другого сигналу $\bar{S_2}$, і інформація буде спотворена. При заміні змінної $\frac{\xi_n^2}{2\sigma^2} = \frac{z^2}{2}$ отримаємо $\xi_n = \sigma z$ та $d\xi_n = \sigma dz$. Тоді

$$P_{\text{пм}} = 0{,}5 \times \left(1 - \frac{2}{2\pi} \times \int_0^{\frac{d}{2\sigma}} e^{\frac{z^2}{2}} dz\right) = 0{,}5 \times \left(1 - \Phi(h)\right), \qquad (3.3)$$

де $h = \frac{d}{2\sigma}$ та $\Phi = \frac{2}{\sqrt{2\pi}} \int_0^h e^{\frac{-z^2}{2}} dz$ – функція Крампа для нормованої величини $z(0,1)$ з нульовим математичним очікуванням та одиничною дисперсією. При частотній модуляції (застосовуваній у пристроях Bluetooth) $S_1(t)$ і $S_2(t)$ вважаються ортогональними, отже $h = \sqrt{\frac{E}{N_0}}$, а

$$P_{\text{пм}} = 0{,}5 \times \left[1 - \Phi\left(\frac{E}{N_0}\right)\right]. \qquad (3.4)$$

Теоретичний графік залежності $P_{\text{пм}}$ (у межах зміни $P_{\text{пм}} = [0{,}001;\ 0{,}1]$) від співвідношення сигнал/шум $\left(\sqrt{\frac{E}{N_0}}\right)$ зображено на рис. 3.7.

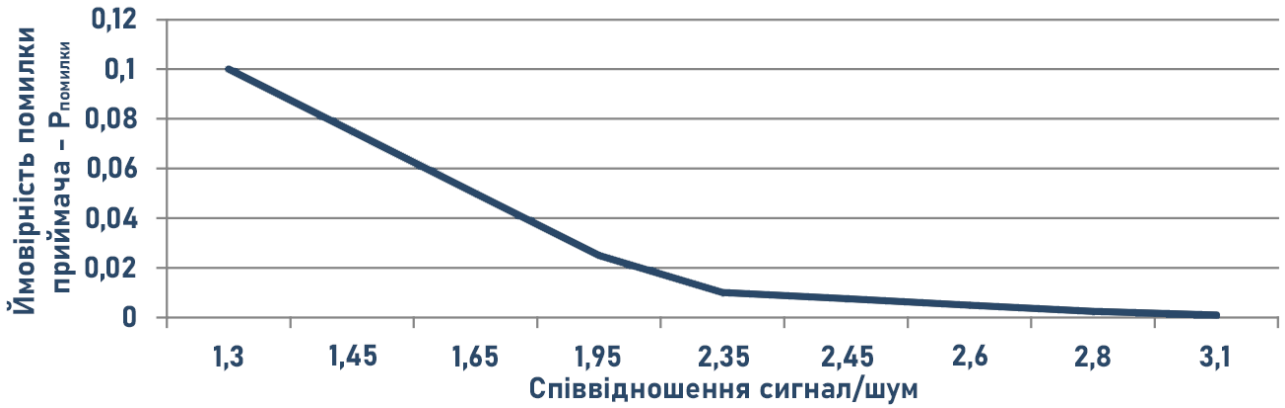

Рисунок 3.7 – Теоретична залежність помилки приймача від співвідношення сигнал/шум $\sqrt{\frac{E}{N_0}}$

Візьмемо вплив перешкоди типу білий шум, що виникає у бездротовій персональній Bluetooth-мережі, та працює на частоті 2,4 ГГц, при передачі голосового сигналу на короткі відстані з урахуванням впливу WiFi-мережі, стандарту IEEE 802.1b, що підтримує швидкість передачі до 11 Мбіт/с (табл. 3.1).

Перешкода типу білого шуму використовується як модель найважчої перешкоди у каналах зв'язку. Щільність розподілу ймовірності білого шуму підпорядковується нормальному закону. Енергетичний спектр перешкоди рівномірний у смузі частот сигналу і потужність білого шуму на виході каналу зв'язку $P_\xi = N_0 f\,[Вт]$, де N_0 – спектральна щільність потужності білого шуму [Вт/Гц].

Дослідження впливу перешкод на якість передачі звуку у моделі Bluetooth велося методом математичного моделювання із застосуванням вбудованого MatLab Demos Bluetooth Voice Transmitter, трансформованого відповідно до завдань дослідження.

Топ-рівень моделі Bluetooth Voice Simulink включає: Master Transmitter – передавальний пристрій, наприклад смартфон, AWGN (модель радіоканалу, в якому діє «білий шум», Free Space Path Loss – імітатор довгої бездротової лінії, що визначає втрати у вільному просторі, 802.11b Interferer – модель джерела перешкоди у вигляді передавача, що працює за протоколом Wi-Fi IEEE 802.11b, Slave Receiver – приймач підлеглого вузла (приймаючий пристрій).

При побудові моделі передавача сигналу враховувалося, що всі реальні безперервні повідомлення, що передаються в системах зв'язку відображають процеси, основна частина спектру яких зосереджена в кінцевому інтервалі частот. Це пояснюється частотними властивостями джерел повідомлень і абонентів (отримувачів повідомлень), які є реальними фізичними системами. Починаючи з деякої частоти, високочастотні складові спектру повідомлення виявляються значно нижчими від рівня перешкод і не сприймаються отримувачем. Таким чином усі реальні безперервні повідомлення можна розглянути як функції з обмеженим спектром, тобто у якому не міститься частот вище деякої граничної частоти f_c.

Відповідно до теореми Котельникова (Найквіста-Шеннона) сигнал, що має кінцевий (обмежений по ширині) спектр, може бути відновлений із заданою якістю за своїм відліком, взятим з частотою, строго більше подвоєної верхньої частоти f_c. Теорема справедлива і у випадку, коли безперервне повідомлення x(t) має спектр, замкнутий в обмеженій смузі частот від $f_н$ до $f_в$. Зокрема, під час передачі Bluetooth звукового сигналу, що має діапазон частоти $f = [0{,}3 – 3{,}4]$ кГц, смуга частот $\Delta f = 3{,}4 - 0{,}3 = 3{,}1$ кГц. У цьому випадку відліки слід брати через інтервал часу:

$$\Delta t = \frac{1}{2(f_в - f_н)} = \frac{1}{2\Delta f_{сп}}, \tag{3.5}$$

де $\Delta f_{сп} = (f_в - f_н)$ – ширина спектра функцій.

У випадку звукового сигналу $\Delta f = 3{,}1$ кГц і час дискретизації:

$$\Delta t = \frac{1}{2 \times f\eta} = 125 мкс, \tag{3.6}$$

де η = [1,1; 1,2] – інженерний коефіцієнт, що враховує не ідеальність пристроїв відновлення. Частота дискретизації $f_S = \frac{1}{\Delta t} = 8$ кГц, а швидкість передачі $v = 8$ біт $\cdot 8$ кГц $= 64$ Кбіт/с.

Крім того, при постановці модельного експерименту враховувалося, що на якість передачі значною мірою впливає загасання у вільному просторі між передавачем та приймачем, що визначається за формулою:

$$L_0 = 20Ig\frac{4\pi lf}{c} [дБ], \tag{3.7}$$

де L_0 – згасання; l – відстань, для якої це згасання вираховується; f – частота; c – швидкість світла. Розв'язавши (3.7) щодо відстані l, отримаємо формулу для визначення дальності передачі:

$$l = \frac{c \times 10^{\frac{L_0}{20}}}{4\pi f}. \quad (3.8)$$

У моделі Bluetooth існує можливості завдання втрат у вільному просторі при поширенні хвилі через задане згасання від 10 до 40 дБ і через задану частоту та дальність передачі.

Результати. Для радіообміну пристрою Bluetooth використовують діапазон частот 2400 МГц. Місткість цієї смуги частот – 79 підканалів із шириною смуги пропускання рівною 1 МГц. Несуча частота підканалів $f_k = 2402 + k$ (МГц), де k = 0, ..., 78. Таким чином, для центрального каналу 39 несуча частота $f_k = 2402 + 39 = 2441$ МГц, для термінального 79 каналу – $f_k = 2402 + 78 = 2480$ МГц.

Згасання у вільному просторі при $l = 2$ м (традиційна відстань, на яку працює Bluetooth на практиці) з (3.8): для 39 каналу $L_0 = 40{,}19312$ дБ, для 79 каналу – $L_0 = 40{,}3264$ дБ.

Дальність передачі при $L_0 = 40$ дБ з (3.7): для 39 каналу дальність передачі $l = 0{,}978011$ м, для 79 каналу $l = 0{,}996119$ м.

За відсутності канальної інтерференції помилка приймача у складі двійкового симетричного каналу передачі звуку Bluetooth (при зміні $P_{пм}$ в діапазоні від 10^{-1} до 10^{-3}) характеризується отриманою в результаті модельного експерименту залежністю (рис. 3.8). Спектрограма процесу передачі звуку Bluetooth на 39 каналі при співвідношенні сигнал/шум $\sqrt{\frac{E}{N_0}}$ представлена на рис. 3.9.

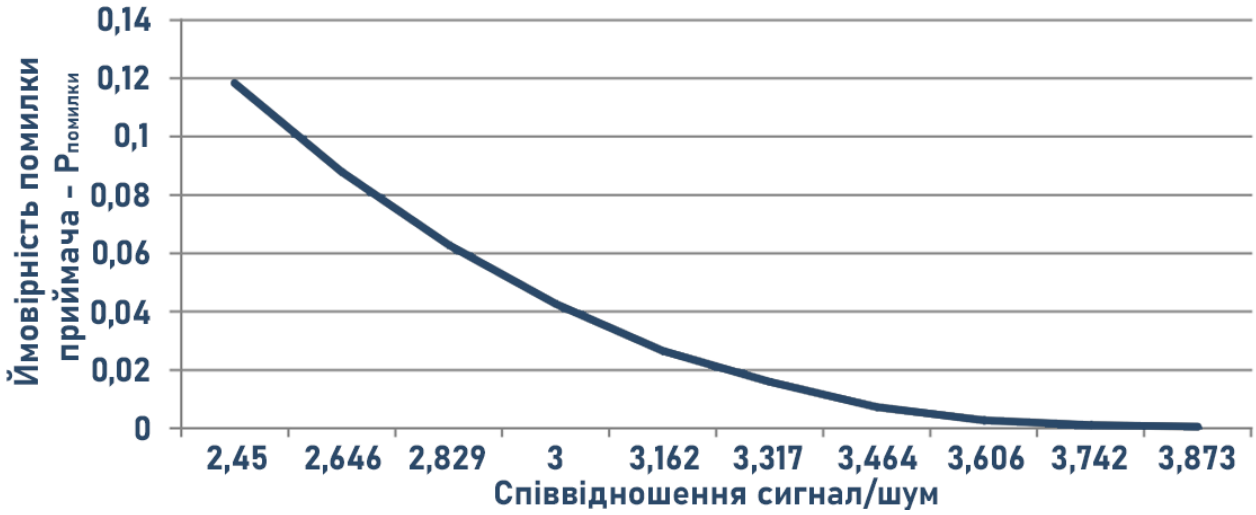

Рисунок 3.8 – Залежність помилки приймача від співвідношення сигнал-шум $\sqrt{\frac{E}{N_0}}$ за відсутності канальної інтерференції

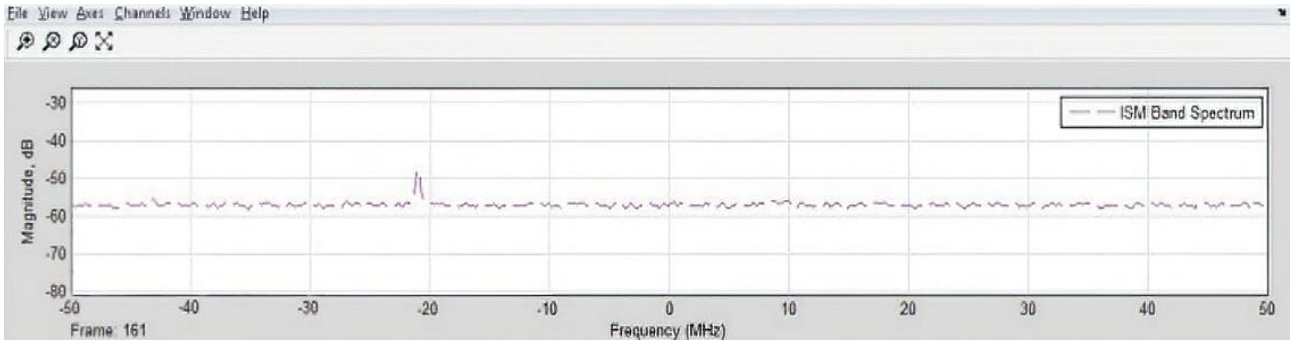

Рисунок 3.9 – Спектрограма звукового сигналу, що приймається при співвідношенні сигнал/шум $\sqrt{\frac{E}{N_0}} = \sqrt{6}$ у відсутності канальної інтерференції

Для врахування канальної інтерференції пристроїв WiFi і Bluetooth у модель вбудований блок 802.11b Interferer – модель джерела перешкоди у вигляді передавача, що працює за протоколом Wi-Fi IEEE 802.11b в розширеному діапазоні частот (2,4...5,5 ГГц).

Отже, робота WiFi за протоколом IEEE 802.1b (на частоті 5,5 ГГц) не робить істотної помилки при передачі звукових сигналів у системі Bluetooth. При цьому функція залежності помилки приймача у складі двійкового симетричного каналу передачі звуку через Bluetooth (в діапазоні $P_{пм} =$

[10– 1 до 10– 3]), отримана в результаті моделювання, втрачає гладкість (рис. 3.10). Це зміною фізики процесу, що наочно підтверджується отриманими спектрограммами (рис. 3.11).

Рисунок 3.10 – Залежність помилки приймача від співвідношення сигнал/шум $\sqrt{\frac{E}{N_0}}$ в умовах канальної інтерференції

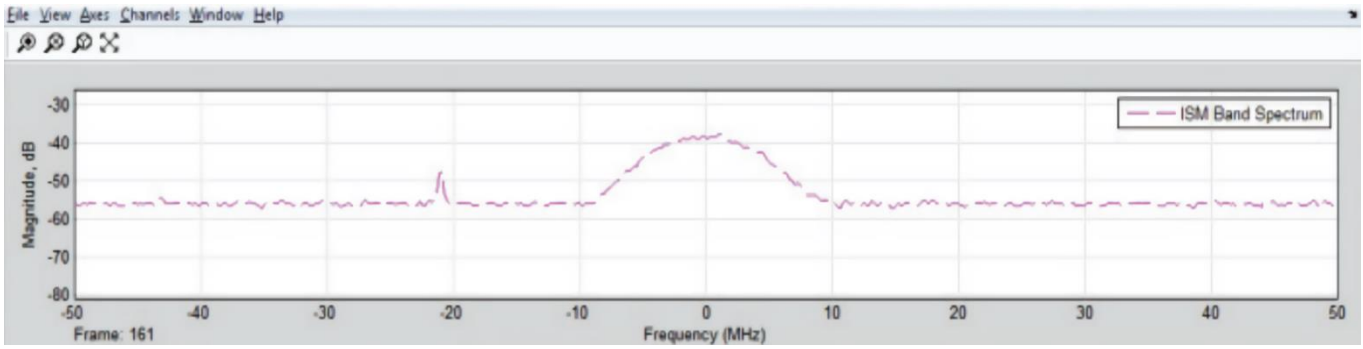

Рисунок 3.11 – Спектрограма звукового сигналу, що приймається при співвідношенні сигнал/шум $\sqrt{\frac{E}{N_0}} = \sqrt{6}$ в умовах канальної інтерференції

В результаті отримаємо, що вплив роботи WiFi за протоколом 802.11b на ймовірність появи помилок приймача Bluetooth не перевищує 0,01%.

Перешкодозахищеність Wi-Fi. Фактична швидкість з'єднання бездротової мережі залежить не тільки від відстані до точки доступу, але і від «засміченості» ефіру. Тобто від того, скільки пристроїв працює в конкретному діапазоні, а також кількості додаткових джерел перешкод. Як уже говорилося вище, найпопулярнішою частотою роботи Wi-Fi у нашій країні є 2.4 ГГц, тому з

високою ймовірністю на цій частоті працюватимуть роутери ваших сусідів. Строго кажучи, 2.4 ГГц, якщо говорить про Wi-Fi, не частотою, а спектром від 2400 до 2483,5 МГц, розділеним на 11 каналів. Для прискорення з'єднання можна спробувати змінити канал, але в умовах багатоквартирних будинків допомагає це не завжди, тому що для серйозного зниження рівня перешкод вільним має бути не тільки використовуваний, а й сусідні канали.

Діапазон 5 ГГц позбавлений цього недоліку і сприяє цьому як менша поширеність, а й більша кількість каналів, і навіть перевага, що є наслідком недостатньої «проникаючої здатності» хвиль із високою частотою.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було приведено загальну інформацію про розумний будинок, розглянуто основні складові системи. Проаналізовані безпровідні моделі передачі даних WiFi, Bluetooth, Zigbee, Z-Wave та стільниковий зв’язок.

Також було виконано аналіз сумісності моделей передачі даних одна з одною, в результаті чого було отримано три загальні моделі розумного будинку з поєднанням різних безпровідних моделей передачі даних: WiFi та Bluetooth, Zigbee, Z-Wave. Зі спільного в цих моделей можливість передачі повідомлень через стільниковий зв’язок.

Було проведено тестування впливу роботи WiFi, стандарт 802.11b, на ймовірність появи помилок приймачем Bluetooth не перевищує 0,01%.

Було проаналізовано моделі передачі даних у чотирьох режимах роботи: сну, очікування, передавання та отримання даних, було виявлено що енергоспоживання у WiFi врази більше ніж у інших. Не зважаючи, на поширеність в Україні, ця модель розумного будинку є найгіршою для зниження витрат на електроенергію, але найкращою в швидкості передачі даних на велику, відносно усіх моделей, відстань.

За результатами дослідження було побудовано моделі розумного будинку: модель розумного будинку WiFi та Bluetooth краще підходить для реалізації систем на великі відстані і при великому об’єму передачі даних, модель Zigbee – рекомендована при побудові системи розумного будинку для зменшення витрат енергоспоживання, модель Z-Wave – найкраще пристосована для систем розумного будинку на незначні відстані і при великій кількості кінцевих приладів у мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Дементьев А. Д. «Умный» дом XXI века [Текст] / А. Д. Дементьев – М. : Litres, 2016. - 168 с.

2. Розумний будинок [Електронний ресурс] Режим доступа: https://stylus.ua/uk/articles/528.html

3. Уінг Ч. Как работает ваш дом [Текст] / Ч. Уінг – К. : ДМК-Пресс, 2016.

4. Пєтін В. В. Создание умного дома на базе Arduino [Текст] / В. В. Пєтін – К. : ДМК-Пресс, 2017. – 180 с.

5. Умный Дом MiMi SMART. Що вміє Розумний будинок [Електронний ресурс] Режим доступа: https://www.smarthouse.ua/ua/chto_umeet_umnyj_dom.html

6. Блум Д. Изучаем Arduino. Инструменты и методы технического волшебства [Текст] / Д. Блум – К. : БХВ-Петербург, 2021. – 544 с.

7. Пєтін В. А. Практическа энциклопедия Arduino [Текст] / В. А. Петин, Біняковский А. А. – К. : ДМК Пресс, 2020. – 166 с.

8. KY-015 Temperature and humidity sensor module [Електронний ресурс] Режим доступа: https://win.adrirobot.it/sensori/37_in_1/KY-015-Temperature-and-humidity-sensor-module.htm

9. ZigBee Alliance, “Zigbee Specification,” 2006

10. Кон Е. Л., Фрейман В. І. Теория электрической связи. Помехоустойчивая передача данных в информационноуправляющих и телекоммуникационных системах: модели, алгоритмы, структуры. — Перм: Видавництво Перм.гос.техн.ун та, 2007.

11. Propagation of Radiowaves, Barclay L.W. (Ed.), 2nd Ed.- London: IEEE, 2003.

12. Безпровідні технології [Електронний ресурс] Режим доступа: https://wireless-e.ru/development/2-4-ghz/

13. A. Kamerman. Coexistence between Bluetooth and IEEE 802.11CCK: Solutions to avoid mutual interference. IEEE P802.11 Working Group Contribution. IEEE P802.11-00/162r0. July 2000.

14. B. Treister, A. Batra, K. C. Chen, O. Eliezer. Adapative Frequency Hopping: A Non-Collaborative Coexistence Mechanism. IEEE P802.15 Working Group Contribution. IEEE P802.15-01/252r0. Orlando, FL, USA. May 2001.

15. Group B. S. I., Specifications of the Bluetooth System, vol. 1, v. 1.0B 'Core' and vol. 2 v1.0B 'Profiles', December 1999.

16. Comparative Study of Communication Interfaces for Sensors and Actuators in the Cloud of Internet of Things [Електронний ресурс] Режим доступа: http://article.sapub.org/10.5923.j.ijit.20170601.02.html

17. Панфилов Д. Введение в беспроводную технологию ZigBee стандарта 802.15.4 / Д. Панфилов, М. Соколов. – 2004.

18. Черняк, А. А. Система «Умный дом» / А. А. Черняк. Текст : непосредственный // Молодой ученый. – 2020.

19. Архипов, В. Системы для «умного» здания / В. Архипов .- М.: "СтройМаркет", 1999.- № 45.- 182с.

20. Сопер М. Е.. Практичні поради та рішення щодо створення «Розумного будинку» / Сопер М. Е. - М.: НТ Пресс, 2007. - 432 с.

21. Харке В. Н. «Розумний будинок. Об'єднання в мережу побутової техніки та систем комунікацій у житловому будівництві »/ Харке В.Н.- М.: Техносфера, 2006. - 292с.

22. Гололобов В. Н.. «Розумний будинок» своїми руками./Гололобов В. Н.- М.: НТ Пресс, 2007. - 416 с

23. Yuan D. The design of smart home monitoring system based on WiFi electronic trash / D. Yuan, S. Fang, Y. Liu // Journal of Software. – 2014. – V. 9, No. 2. – P. 425-428.

24. Mowad M. A. L. Smart Home Automated Control System Using Android Application and Microcontroller / M. A. L. Mowad, A. Fathy, A. Hafez // International Journal of Scientific & Engineering Research. – 2014. – V. 5, No. 5. – 935-939.

25. Piyare R. Bluetooth Based Home Automation System Using Cell Phone / R. Piyare,Tazil // IEEE 15th International Symposium on Consumer Electronics, June 14-17, 2011. – 2011. – P. 192-195.

26. Hall J., Ramsey B., Rice M., Lacey T. Z-Wave network reconnaissance and transceiver fingerprinting using software-defined radios. International conference on cyber warfare and security. 2016, p. 163-171.

27. Fouladi B., Ghanoun S. Security evaluation of the Z-Wave wireless protocol / Presented at Blackhat, Fouladi, Ghanoun, 2013. USA. [Електронний ресурс] режим доступа: http://neominds.org/download/zwave_wp.pdf