МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Факультет електроніки та інформаційних технологій
Кафедра електроніки,
загальної та прикладної фізики

Кваліфікаційна робота магістра

ВИКОРИСТАННЯ МІКРОКОНТРОЛЕРІВ В РОЗПОДІЛЕНИХ БЕЗПРОВІДНИХ СИСТЕМАХ МОНІТОРИНГУ

Виконав
студент групи ЕП.м – 92 Д. О. Ніколаєнко

Науковий керівник,
к. ф.-м. н., ст.викл. К. В. Тищенко

Завідувач кафедри ЕЗПФ
д-р фіз.-мат. наук, професор І. Ю. Проценко

Суми 2020

РЕФЕРАТ

Об’єктом дослідження кваліфікаційної роботи магістра є безпровідні мікроконтролерні модулі та їх прикладне використання в системах моніторингу і керування.

Мета роботи полягає у вивченні принципів роботи та особливостей реалізації безпровідних систем моніторингу на базі стандартних протоколів зв’язку; Реалізації функціоналу розподіленої mesh-мережі на базі апаратних мікроконтролерних пристроїв, які працюють за стандартним протоколом ZigBee.

У роботі розглянуто найбільш популярні безпровідні протоколи зв’язку, та особливості їх застосування в системах моніторингу, показано їх основні переваги, недоліки та проаналізовано відмінності. У результаті проведених досліджень встановлено, що для використання в системах малої автоматизації та інтернеті речей доцільно використовувати пристрої з підтримкою протоколу ZigBee, оскільки вони характеризуються низьким енергоспоживанням, відносно низькою вартістю та простотою налаштування.

На основі датчиків з підтримкою протоколу ZigBee було запропоновано архітектуру IoT системи моніторингу в межах концепції розумного будинку. Описано функціональні можливості та можливі області застосування компонентів розподіленої безпровідної мережі.

Робота викладена на 38 сторінках, зокрема містить 11 рисунків, 2 таблиці, список цитованої літератури із 16 джерел.

КЛЮЧОВІ СЛОВА: БЕЗПРОВІДНИЙ ПРОТОКОЛ, МІКРОКОНТРОЛЕР, ДАТЧИК, СИСТЕМА МОНІТОРИНГУ, ZIGBEE.

ЗМІСТ

ВСТУП

Розробка складних систем керування та моніторингу сьогодні, переважно, виконується із застосуванням електронних пристроїв на базі мікроконтролерів. Для побудови ефективної розподіленої системи керування і моніторингу доцільним є застосування безпровідних пристроїв, оскільки вони не потребують проектування інфраструктури провідного зв’язку і забезпечують хорошу автономність роботи у важкодоступних місцях.

Об’єднання окремих безпровідних пристроїв у цілісну систему вимагає застосування спеціального набору правил, які визначають принципи та методи взаємодії окремих пристроїв між собою [1]. З цією метою прийнято використовувати стандартизовані протоколи безпровідної передачі даних, які описують повний алгоритм комунікації між пристроями, починаючи із фізичного рівня (частотний діапазон передачі даних) до логічного (набори команд, розмір пакетів даних та ін.).

Насьогодні існує велика кількість протоколів безпровідного зв’язку, і для кожного з них є області, де їх застосування буде доцільним або ж не прийнятним [1, 2]. На це впливає ряд факторів, таких як, топологія мережі, кількість окремих вузлів, швидкість передачі даних, вимоги до енергоефективності та ін.

Метою роботи є огляд сучасних систем і технологій для проектування і розробки безпровідних систем моніторингу з використанням мікроконтролерів, які забезпечують віддалений доступ до контролю фізичних величин, та керування обладнанням в режимі реального часу.

РОЗДІЛ 1
ОСОБЛИВОСТІ МЕРЕЖЕВИХ ПРОТОКОЛІВ ДЛЯ ПРОЕКТУВАННЯ БЕЗПРОВІДНИХ МЕРЕЖ

1.1 Вимоги до бездротових технологій для застосування у системах моніторингу

Системи моніторингу, котрі працюють із використанням контролерів та датчиків, підключених до безпровідних мереж можуть мати різноманітну архітектуру та використовувати різні технології і протоколи зв’язку [1]. При проектуванні таких систем потрібно виконати їх всебічний аналіз і обрати найбільш підходящу конфігурацію системи, виходячи із сукупності засобів моніторингу та задач, поставлених перед нею.

Перш за все необхідно вияснити різницю між популярними протоколами зв'язку і їхню роль у проектуванні ефективної системи моніторингу. У загальному випадку протоколом називається набір правил, які забезпечують пристроям у мережі обмінюватися даними один з одним.

Для побудови розподіленої системи моніторингу найбільш ефективним буде рішення із використанням системи безпровідних контролерів, датчиків та інших пристроїв. До технологій і пристроїв бездротової комунікації пред'являється ряд вимог, виходячи із наступних пунктів [1 – 3]:

- енергоефективність;
- радіус дії і безпека;
- можливість роботи за наперед заданими правилами і умовами;
- відмовостійкість;
- сумісність з іншими пристроями у мережі.

Розглянемо кожен із цих пунктів більш детально.

Енергоефективність пристроїв безпровідної комунікації. Насьогодні широкого розповсюдження набула велика кількість різноманітних технологій

для забезпечення безпровідного зв'язку між пристроями у мережі. У більшості випадків до них пред’являються жорсткі вимоги до споживання енергії та пропускної здатності каналу зв’язку. Дані фактори збільшують час роботи від портативного джерела живлення і дозволяють використовувати пристрої моніторингу у просторі домашньої або промислової автоматизації. Доступний для описаних задач виділений частотний спектр значною мірою обмежений, тому для одночасної роботи великої кількості компонентів важливим є питання оптимізації його використання кожним окремим складовим елементом системи [2, 3].

Тому, кожен елемент бездротової мережі моніторингу та керування повинен забезпечувати використання якумога меншої кількість енергії, для забезпечення тривалого часу роботи пристрою в автономному режимі без необхідності підзарядження чи зміни батареї живлення. Остання також повинена бути невеликою, оскільки її розмір впливає на кінцеві габарити готового датчика, чи іншого автономного пристрою. З цього випливає, що вимоги до споживаної потужності пристроями безпровідної системи моніторингу повинні бути дуже жорсткими [1].

Радіус дії і безпека. У окремій розподіленій мережі сигнал між окремими вузлами повинен стабільно і з мінімальними затримками досягати приймача іншого пристрою, встановленого максимально віддалено від нього. Наприклад, найшвидша реакція повинна досягатись у системах, де є критичним час прийняття рішення, прикладом такої системи є пожежна сигналізація на основі датчиків задимленості, горіння чи наявності у приміщенні газу. Тому сигнали від будь-якого пристрою у мережі повинні без перешкод поширюватися через елементи будівельних конструкцій, таких, як, стіни і підлога у межах всієї площі роботи системи моніторингу. Всі розумні гаджети, у межах однієї екосистеми автоматизації, незалежно від її обширності, повинні працювати синхронно та забезпечувати стійке з’єднання між вузлами. Тому, при розгортанні мереж моніторингу і керування, слід врахувати можливі перешкоди від інших безпровідних пристроїв, котрі

працюють у тому ж частотному діапазоні, і за можливості, вони повинні бути усунуті або мінімізовані [1 – 3].

Будь-які дані, що передаються у мережі, повинні бути зашифровані, або захищені іншими способами, а підключення нових пристроїв в мережу повинно здійснюватись швидко і з забезпеченням максимального захисту. Але підвищення безпеки не повинно ускладнювати підключення [1]. Дана проблема стоїть насьогодні достатньо гостро, оскільки бездротові пристрої на базі мікроконтролерів все частіше стають жертвами хакерських атак і стають частиною бот нет мереж.

Підтримка календаря і сценаріїв роботи. Забезпечений популярними додатками та технологіями керування безпровідними засобами автоматизації і моніторингу функціонал, дозволяє підтримувати розклад для подій в екосистемах IoT та ін., як, наприклад, увімкнення кліматичної техніки, освітлення, планування прибирання. Але багато подій у системах керування і моніторингу не можна спланувати заздалегідь, наприклад поява диму, протікання води чи витік газу. Велику кількість пристроїв автоматизації не можуть працювати за наперед заданими сценаріями, тому необхідно, щоб пристрої у системі моніторингу та автоматизації могли відпрацьовувати команди дій в залежності від стану системи, або подій, що відбуваються в конкретний момент часу [1].

Відмовостійкість. Топологія кінцевої безпровідної мережі, яка забезпечується підтримкою одним із протоколів зв’язку, має вирішальне значення для забезпечення відмовостійкості. Сучасні уявлення про топологію і архітектуру бездротових мереж передбачають використання комірчастих мереж (mesh-мереж), котрі забезпечують децентралізований підхід до реалізації комунікативних принципів між вузлами [1, 2]. Кожен пристрій, що входить до складу такої мережі повинен зв'язуватися, без використання засобів шлюзування, з іншим, у радіусі своєї дії. Якщо два пристрої знаходяться на великій відстані один від одного, то сигнали можуть передаватися через проміжні вузли, які, водночас, є пристроями цієї самої мережі, таким способом

можна розширити зону дії пристроїв. Також, за такого підходу до проектування мережі, нові компоненти системи можуть бути включені, а старі видалені без впливу на надійність роботи мережі і стабільність роботи системи загалом. Однак для переважної більшості комірчатих мереж також необхідним елементом є базовий мережевий контролер для забезпечення координації спільної роботи пристроїв в мережі. Такий контролер повенен бути підключений до стабільного джерела живлення, а також, за можливості, продубльований, для того, щоб у разі виходу з ладу головного контролера, дублюючий пристрій міг забезпечити керування мережею. Ця властивість mesh-мереж є ключовою для забезпечення її безперебійної роботи.

Взаємна сумісність. Концепція бездротових мереж моніторингу полягає в тому, що всі наші пристрої повинні об'єднуватися в мережу і безперешкодно обмінюватись даними один з одним. Основним питання є сумісність пристроїв в рамках одного стандарту безпровідного зв’язку, тобто, не кожна технологія, яка може бути обрана як базова для побудови розподіленої системи моніторингу, може дати гарантію того, що різні пристрої, з підтримкою одиного стандарту, будуть без перешкод обмінюватись даними між собою. Наприклад, може виникнути ситуація, коли безпровідний датчик відправив пакет даних з повідомленням до комунікаційного пристрою, а останній можете не отримати відправлене повідомлення, оскільки, датчик і контролер, хоч і використовують один стандарт передачі даних, та вироблені різними компаніями можуть по різному передавати і отримувати інформацію [1 – 3].

Питання сумісності не є проблемою лише мережевих протоколів, котрі забезпечують підключення пристроїв у системі. Проблеми полягають у відсутності стандартизованих форматів (протоколів) даних або універсальних інтерфейсів програмування (API). Але базовою потребою, яку необхідно задовольнити, щоб розподілена система, з великою кількістю пристроїв, працювала правильно і без збоїв є забезпечення сумісності її компонентів не залежно від виробника кожного із них.

1.2 Протоколи безпровідного зв’язку для побудови розподілених систем моніторингу

Оскільки більшість конкуруючих безпровідних стандартів мають подібні характеристики, може скластися враження, що вони забезпечують аналогічні можливості та характеристики. Однак при більш детальному аналізі проявляються принципові відмінності між ними. Кожна із технологій була розроблена для виконання різних задач, як наслідок, вони по-різному і працюють [1]. Багато моментів, що стосуються особливостей роботи кожного із протоколів, стануть більш зрозумілими, якщо їх розглядати спираючись на стек протоколів (модель) OSI [2, 3].

OSI (Open Systems Interconnection) – модель взаємодії відкритих систем, розроблена у 80-х р.р. XX ст. Це основа для координації розробки стандартів зв'язку, котра є базовою моделлю для комунікаційних мереж. Стек протоколів OSI розглядає процес взаємодії елементів мережі як ієрархію, що складається з семи рівнів. Кожен з цих рівнів забезпечує певні функції і вирішує чітко визначені завдання в його рамках, а також взаємодії з сусідніми рівнями. Узагальнена модель OSI показана на рис. 1.1 [2].

Кожен з рівнів стеку протоколів OSI є невід’ємною складовою будь якої комунікаційної мережі, тому, що визначає завдання, які є частиною процесу взаємодії пристроїв в кінцевій системі зв’язку. Вони дозволяють їм, що використовують один і той же протокол для спілкуватися між собою, забезпечуючи необхідний функціонал для стабільної роботи мережі, безпеки і обміну даними. Згідно цієї моделі прикладний рівень є основним критерієм для забезпечення сумісності кінцевих пристроїв. У разі, коли, прикладний рівень не стандартизований, пристрої різних виробників не зможуть комунікувати між собою. Якщо пристрої забезпечують використання одного протоколу, вони все одно не зможуть підтримувати комунікацію, якщо в ньому не стандартизований прикладний рівень моделі OSI.

Для визначення оптимальної моделі розподіленої безпровідної системи

моніторингу розглянемо особливості найбільш популярних протоколів безпровідних мереж.

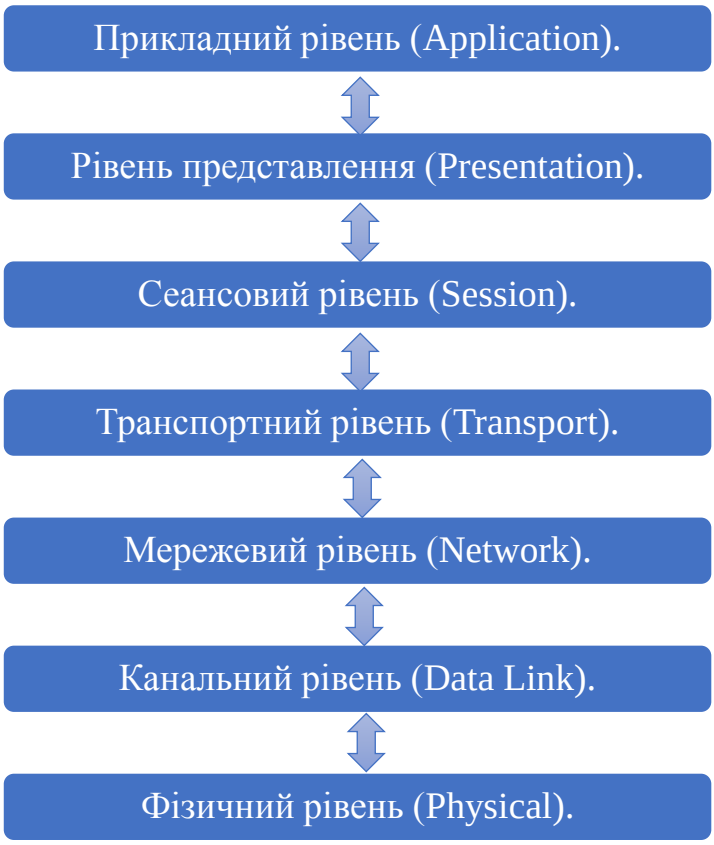


Рис. 1.1 – Модель стеку мережевих протоколів OSI. Адаптовано з роботи [2]

1.2.1 Безпровідна мережа Wi-Fi

Wi-Fi – це найбільш розповсюджена, на сьогодні бездротова мережева технологія з великою кількістю підключених користувачів. За допомогою цього стандарту забезпечується передача близько половини інформації в мережі інтернет [4]. Wi-Fi активно застосовується в приватних будинках, квартирах, організаціях і публічних просторах. Така технологія, на сьогодні, найбільш популярна для підключення смартфонів і ноутбуків до мережі. Технічно, із застосуванням Wi-Fi можна організувати з'єднання декількох пристроїв, для організації обміну інформацією, але ця потужна бездротова технологія вважається найгіршим рішенням для концепції IoT (інтернету

речей) з усіх можливих.

Технологія Wi-Fi заснована на стандарті безпровідних комунікаційних мереж IEEE 802.11x. Вони визначають перші два рівня моделі OSI – фізичний і канальний (Рис. 1.2). Мережа Wi-Fi розгортається за топологію «Зірка», коли всі її вузли з'єднуються з центральним елементом – маршрутизатором або комутатором, який і бере на себе базові функції керування і взаємодії. У такій мережі можна змінювати склад, не впливаючи на цілісність структури і передачу даних. Але такий підхід не забезпечує достатньої надійності, внаслідок того, що існує єдина точку відмови (комутатор), при виході з ладу якого функціонування мережі стане не можливим [3, 4].

Технологія Wi-Fi використовує стандартизовані комунікаційні протоколи – UDP та TCP для транспортного рівня (згідно моделі OSI), та IPv4 або IPv6 для мережевого рівня. Прикладний рівень в мережах Wi-Fi, котрий забезпечує сумісність пристроїв, не визначений, і реалізується на програмному рівні пристроями чи додатками, розгорнутими на них.

Переваги Wi-Fi, як протоколу для побудови мереж моніторингу, полягають у тому, що Wi-Fi – це надійне та широко розповсюджене рішення, котре застосовується для розгортання локальних мереж уже тривалий час. У переважній більшості ситуацій, маршрутизатора бюджетної цінової категорії досить для забезпечення покриття площі усієї квартири. У великих приміщеннях, для збільшення площі покриття мережею, можна розмістити декілька окремих точок доступу чи застосувати пристрої розширення зони покриття – ретранслятори сигналу. Також головною перевагою Wi-Fi є доступність інфраструктури.

Wi-Fi як протокол для розподілених систем автоматизації має і велику кількість недоліків. Будучи високошвидкісним стандартом зв'язку, Wi-Fi споживає велику кількість енергії. Енергоспоживання не відіграє великої ролі, якщо пристрій підключено до джерела живлення, але воно починає бути проблемним моментом, коли необхідно забезпечити автономність роботи від портативних джерел, наприклад акумуляторних батарей або ж сонячних

панелей. На практиці майже неможливо розробити пристрій із комунікацією через мережу на основі Wi-Fi з підтримкою одночасного швидкого реагування та живленням від батарейок, які можуть забезпечувати стале живлення протягом тривалого періоду часу. Тому дивлячись на широку поширеність Wi-Fi не може ефективно працювати в автономних бездротових пристроях [4].

Рис 1.2 – Протокол Wi-Fi в моделі OSI. Адаптовано з роботи [4]

Також, значні обмеження виникають у зв’язку із самою топологією безпровідних мереж на основі Wi-Fi – залежність усієї комунікації (у тому числі і трафіку) від центрального вузла такої мережі (маршрутизатора) призводить до появи єдиної точки відмови. Щойно маршрутизатор перестає працювати, окремі пристрої мережі втрачають можливість взаємодіяти між собою, що призводить до порушення роботи всієї мережі автоматизації. Проблема сумісності пристроїв – найважливіший аспект у побудові систем автоматизації. Стандартом Wi-Fi не визначається прикладний рівень

мережевої моделі OSI, що робить неможливим передачу даних за принципом pear to pear (пристрій – пристрій), а це ускладнює розгортання мережі, здатної до самоорганізації.

1.2.2 Безпровідна мережа Z-Wave

Z-Wave, насьогодні, є лідером серед технологій домашньої автоматизації за кількістю пристроїв (понад 100 млн по всьому світу) [5]. Даний протокол безпровідного зв'язку забезпечує ультранизьке енергоспоживання і спеціально розроблений для забезпечення можливості віддаленого управління датчиками і виконуючими пристроями з максимальною ефективністю і надійністю у системах типу розумний будинок та IoT [1, 5].

Стартап Z-Wave був розроблений у 2003 році фірмою Zensys, і у 2008 році викуплений компанією Sigma Designs. У 2017 дана технологія була продана напівпровідниковій компанії Silicon Labs, після чого і почалась епоха її бурхливого розвитку. Silicon Labs ліцензує кожен модуль із підтримкою Z-Wave таким чином гарантуючи їх сумісність один з одним, також вона є найбільшим виробником модулів і компонентів Z-Wave [5]. Даний протокол, насьогодні, представляє собою недороге і просте рішення у системах типу розумний будинок та IoT та забезпечує найбільш важливих потреби в системах автоматизації. Z-Wave, як технологія, переросла у потужний стандарт бездротового зв'язку для керування і автоматизації.

Z-Wave покриває усі сім рівнів стеку протоколів моделі OSI [1, 2, 5], від фізичного до прикладного. Даний факт може гарантувати неперевершений рівень сумісності датчиків і керуючих пристроїв для домашньої автоматизації створених різними фірмами. Z-Wave – це протокол, орієнтований на обмін короткими командами і повідомленнями між пристроями, чим реалізується низьке навантаження на частину радіочастотного спектру, в якій працює даний протокол, та зменшується вірогідність втрати пакетів даних.

Протокол Z-Wave реалізує пористу топологію мережі (mesh-мережу)

(рис. 1.3). Він побудований таким чином, що окремі складові елементи мережі, котрі забезпечують функцію ретрансляторів, мають можливість перенаправляти повідомлення між вузлами, до моменту, поки воно не буде доставлене до адресата [6]. Такий підхід не тільки дозволяє значно розширити радіус дії бездротової мережі, але і підвищує її надійність. Якщо з певних причин відбулася втрата одного із елементів мережі, вона не припинить роботу, а повідомлення змінять маршрут проходження, тобто будуть проходити через інші вузли мережі.

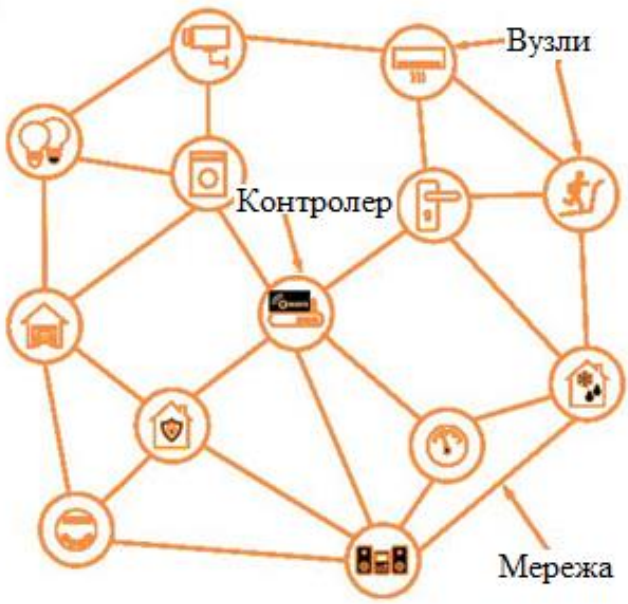


Рис 1.3 – Топологія мережі Z-Wave. Адаптовано з роботи [6]

Кожна логічна мережа Z-Wave може підтримувати роботу до 232 пристроїв. За потреби розгортання мережі із більшої кількості вузлів, можна реалізувати об’єднання декількох мереж в одну екосистему, оскільки окремі мережі Z-Wave можуть працювати, з частковим або повним перекриттям, не заважаючи одина одній. У мережі Z-Wave є центральний контролер (базова станція), котрий виконує підключення нових пристроїв до мережі і видаляє не потрібні, також він виконує динамічну побудову карти маршрутизації у режимі реального часу, забезпечує безпечне підключення, реалізує створення сценаріїв роботи окремих складових системи та інші функції, пов’язані з організацією роботи мережі.

Особливістю Z-Wave було те, що технологія навмисне розвивалася як закритий протокол, котрий захищений великою кількістю патентів. Починаючи з 2012 року компанія Sigma Designs відкрила частину специфікації Z-Wave, а у 2016 році було розміщено у відкритому доступі всю офіційну документацію по цьому протоколу. Зокрема, були опубліковані класи команд і класи пристроїв; опис специфікацій шифрування в мережах Z-Wave, які отримали назву Security 2 (S2). Насьогодні залишаються закритими мережевий і транспортний рівні, на яких описані алгоритми, котрі відповідають за стабільність роботи та маршрутизацію повідомлень, їх ретрансляцію і контроль отримання [5].

Перевагою Z-Wave є те, що з усіх представлених на ринку домашньої автоматизації рішень, пристрої Z-Wave є найбільш енергоефективними, надійними і безпечними. У таких мережах забезпечується використання до 4 проміжних точок при передачі даних між окремими пристроями. Зважаючи, що у зоні прямої видимості модулі Z-Wave забезпечують стабільну передачу даних на відстань приблизно 40 метрів то дальності передачі сигналу в одній мережі достатньо для реалізації обширних проектів типу інтернет речей та розумний будинок. Z-Wave використовує ті ж технології шифрування, що і системи онлайн-банкінгу. Стандарт безпеки Security 2 став обов'язковим для сертифікації всіх розумних пристроїв Z-Wave з 2017 року. Він удосконалює стандарти шифрування для здійснення обміну даними між вузлами, а також задає нові процедури підключення нових пристрої до мережі розумного будинку за допомогою QR-кодів [5, 6].

Z-Wave працює в діапазоні 800-900 МГц. Відмінна риса цих частот – здатність долати перешкоди, в тому числі перекриття і стіни. Також характерною є мала кількість перешкод на цих частотах.

Недоліком Z-Wave є те, що на законодавчому рівні у різних країнах для роботи пристроїв малого радіусу дії виділено різні частотні діапазони. Наприклад, для Європи, Китаю інших країн Азії – це 868,42 МГц. А в США і Мексиці ці частоти зайняті технологією GSM, тому Z-Wave там працює на

частоті 908, 42 МГц. Тому при придбанні пристроїв необхідно попередньо вияснити для використання в якій країні він був виготовлений [6].

1.2.3 Безпровідна мережа ZigBee

ZigBee є головним конкурентом Z-Wave в сегменті комунікаційних мереж для автоматизації і систем моніторингу [1, 7]. ZigBee, як і Z-Wave – це мережевий стандарт оптимізований для віддаленого моніторингу та управління розумним будинком та IoT і характеризується низьким споживанням енергії. Обидва стандарти використовують пористі mesh-мережі і мають схожий функціонал. На перший погляд, з точки зору можливостей, ці стандарти здаються однаковими, але при більш детальному аналізі між ZigBee і Z-Wave проявляються принципові відмінності.

Набір протоколів ZigBee (рис. 1.4) визначає тільки мережевий, транспортний і прикладний рівні моделі OSI [2, 7]. Він побудований на основі стандарту IEEE 802.15.4, котрий визначає реалізацію нижніх рівнів бездротової мережі, орієнтованої на кінцеві пристрої. Стандарт IEEE 802.15.4 підтримується декількома постачальниками чіпів і використовується не тільки для ZigBee, але і багатьма іншими протоколами. В якості робочого діапазону цей стандарт визначає частоти 2,4 ГГц у всьому світі, 915 МГц в Америки і Австралії і 868 МГц у Європі [1].

Принциповою є відмінність і схеми комунікації, так Z-Wave використовує маршрутизацію повідомлень від джерела, а ZigBee від адресата. Тому, в реалізації такої mesh-мережі на основі протоколу ZigBee бере участь три класи пристроїв: координатор (формує і координує роботу мережі), маршрутизатор (є основним елементом для трансляції та динамічної маршрутизації пакетів) і кінцеві пристрої (рис. 1.5). Таким чином, ZigBee технічно не тотожний за принципом організації мережі з Z-Wave, але він також здатний забезпечити самовідновлення мережі і може перенаправити пакети даних, щоб забезпечити їх доставки, у разі втрати зв’язку із одним з вузлів мережі [7].

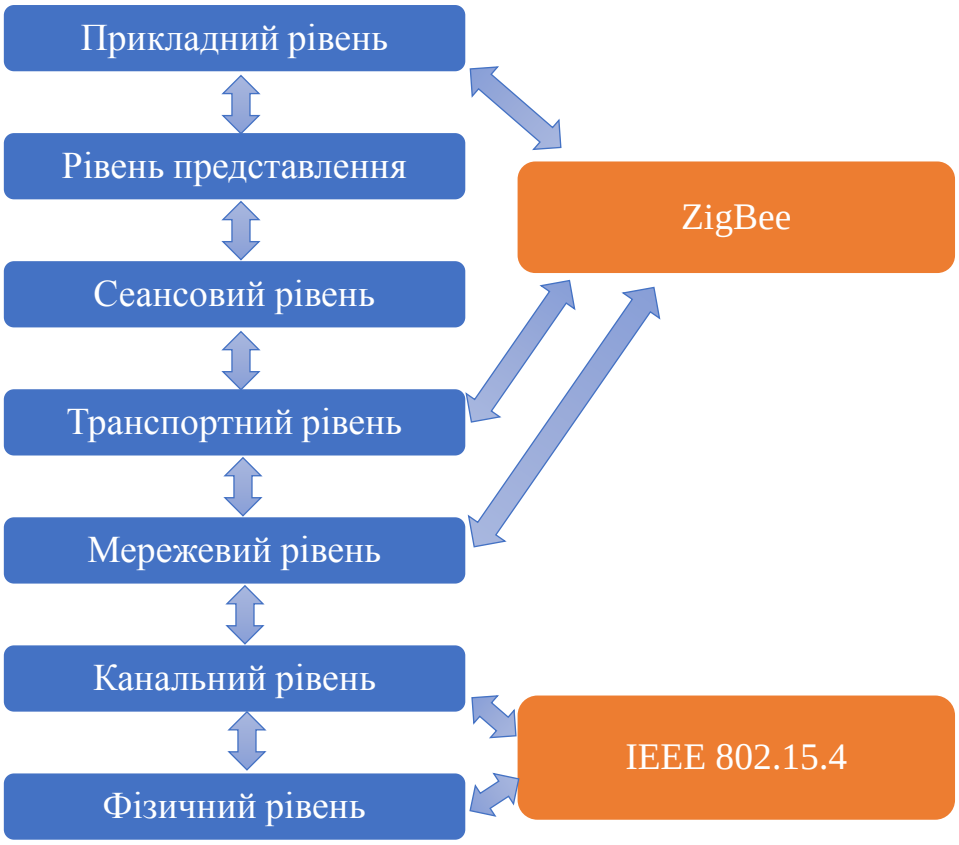


Рис 1.4 – Протокол ZigBee в моделі OSI. Адаптовано з роботи [7]

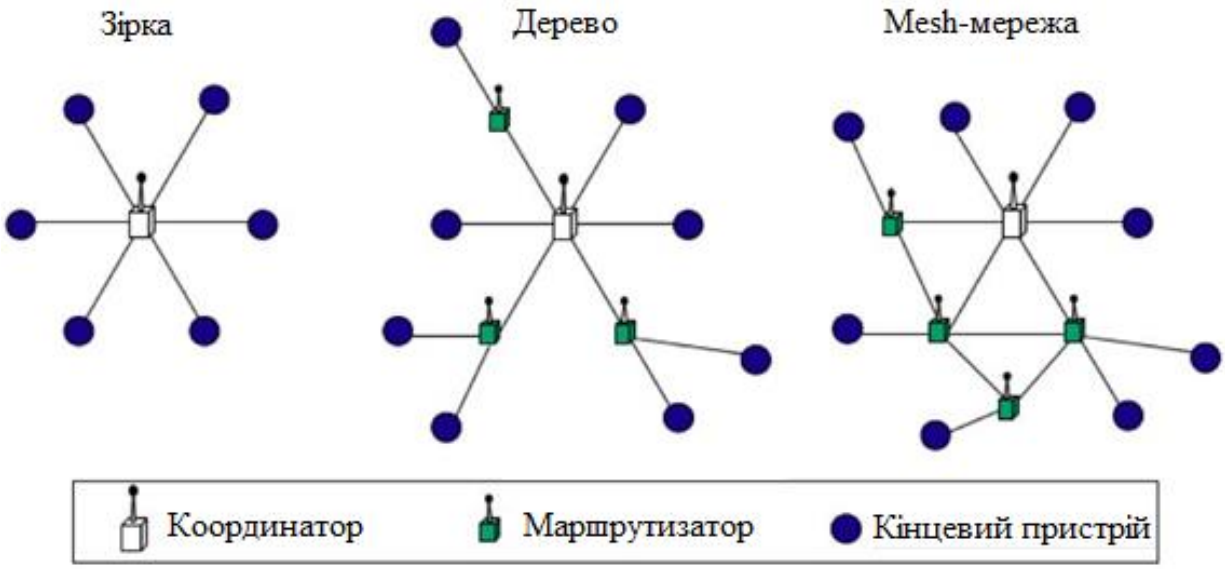


Рис 1.5 – Топологія ZigBee мережі. Адаптовано з роботи [7]

ZigBee – це відкритий стандарт безпровідного зв'язку, що зручно для розробників і виробників. Це дозволяє більш гнучко обирати необхідний функціонал та з меншими витратами представляти загалу нові пристрої (у зв’язку з відсутністю обов’язкової сертифікації). Саме тому ZigBee розповсюджений на корпоративному ринку, зокрема, комунальні підприємства забезпечують підтримку цього протоколу в лічильниках електроенергії і води, щоб удосконалити можливості моніторингу, контролю та управління споживання послуг для своїх користувачів. ZigBee має гарну масштабованість, він здатний комунікувати у межах однієї мережі до 65 тисяч окремих компонентів, та може реалізовувати покриття великої за площею охоплення системи, незважаючи на відносно малу відстань передачі даних окремими модулями (10-20 м) [1, 7].

До недоліків ZigBee слід віднести те, що ця технологія погано справляється з ситуаціями, коли в зоні дії мережі існують перешкоди, від інших пристроїв, оскільки є одноканальним рішенням, а частота 2,4 ГГц, спільно використовується протоколом Wi-Fi і Bluetooth. Покращення ситуації очікувати не слід, оскільки завантаженість частотного діапазону 2,4 ГГц з кожним роком лише збільшується. Також ненайкраще впливає для ZigBee той факт, що стандарт мережевий стандарт IEEE 802.15.4 має обмеження для швидкість передачі даних, а саме до 250 Кбіт / с.

Стосовно безпеки, ZigBee реалізує ряд заходів для забезпечення достатнього захисту пакетів даних, котрі передаються між окремими пристроями. В мережі застосовується 128-бітний алгоритмом AES для шифрування даних і безпечного підключення пристроїв, тому проблеми безпеки з мережами ZigBee не пов’язані з протоколом, а носять суб’єктивний характер.

Також недоліком ZigBee є той факт, що пристрої різних виробників не можуть комунікувати один з одним безпосередньо. Великі компанії створюють пропрієтарні ZigBee-рішення, здатні обмінюватися даними тільки з іншими пристроями цього брендом. Існують цілі ізольовані екосистеми

ZigBee різних брендів: Xiaomi, Philips Hue, IKEA. Саме в поганій взаємодії і є основний недолік ZigBee [1, 7].

1.2.4 Безпровідні мережі на основі Bluetooth

Насьогодні Bluetooth є основною технологією обміну даними в персональних обчислювальних мережах (смартфони, ПК) і для підключення різних периферійних пристроїв (гарнітури, бездротові клавіатури, миші, принтери і т.д.). Перший крок в сторону Інтернету речей було зроблено в 2010 році, з випуском версії Bluetooth 4.0, що включає в себе версію з низьким енергоспоживанням Bluetooth Smart. Ця технологія була розроблена з орієнтацією на нове покоління розумних пристроїв, багато з яких живиться від батарейок і вимагають більшої енергоефективності [8].

Як і Z-Wave, Bluetooth охоплює усі рівні моделі OSI – від фізичного до прикладного [2, 8]. Bluetooth Low Energy, як і інші стандарти зв'язку з низьким енергоспоживанням і низькою пропускною здатністю, орієнтований на передачу даних невеликими пакетами, тому пристрої Bluetooth Low Energy з'єднуються один з одним тільки при необхідності відправки або отримання даних.

Перевага Bluetooth Low Energy є те, що вона орієнтован на низьке енергоспоживання і швидкістю передачі даних досягає 1 Мбіт / с Чим швидше швидкість, тим більше інформації можна передати за одиницю часу, а це означає, що передавач Bluetooth швидше звільнить радіоефір, зменшуючи тим самим ймовірність виникнення перешкод, що важливо при роботі в діапазоні частот 2,4 ГГц [9].

Завдяки підтримці сплячих вузлів (пристрої, які проводять більшу частину часу неактивні, періодично прокидаються на короткий час для швидкого виконання свого завдання) Bluetooth Smart забезпечує хороший термін роботи в автономному режимі від батареї.

Крім того, Bluetooth Smart має цікаву функцію, якої немає у інших

технологій – маячки (beacons) (рис. 1.6). Використовуючи функцію визначення близькості Bluetooth, маячки можуть змусити інші пристрої виконувати певні дії, коли вони знаходиться поруч з ними. Маячки дозволяють впровадити широкий спектр унікальних додатків: від push-повідомлень на основі визначення місця розташування до точного позиціонування [9].

Рис 1.6 – Маячки Bluetooth, реалізовані у вигляді окремих пристроїв. Адаптовано з роботи [9]

З усіх технологій бездротового зв'язку, що використовуються в IoT, лише Bluetooth і Wi-Fi підтримуються практично всіма смартфонами, планшетами та ноутбуками. Але, крім того, що Wi-Fi не підходить для переважної більшості додатків Інтернету речей, він до того ж направляє всі повідомлення через центральну точку доступу, тоді як Bluetooth забезпечує прямий зв'язок між пристроями. Така топологія значно спрощує додавання нових пристроїв в існуючу мережу. За допомогою Bluetooth вся процедура може бути гранично спрощена, інтуїтивно зрозуміла і безпечна.

Bluetooth використовує той же діапазон 2,4 ГГц, що і багато інших радіотехнології (рис. 1.7). Незважаючи на те, що Bluetooth забезпечений інструментарієм для протидії перешкодам (наприклад, технологією адаптивної зміни частоти, що дозволяє уникати найбільш завантажених каналів), використання смуги частот 2, 4 ГГц – це мінус технології, адже, крім наявності перешкод, сигнал на цій частоті загасає набагато швидше, ніж на частотах менше 1 ГГц. З цієї ж причини радіус дії технології Bluetooth Low Energy розрахований на відстань до 10 метрів [1, 9].

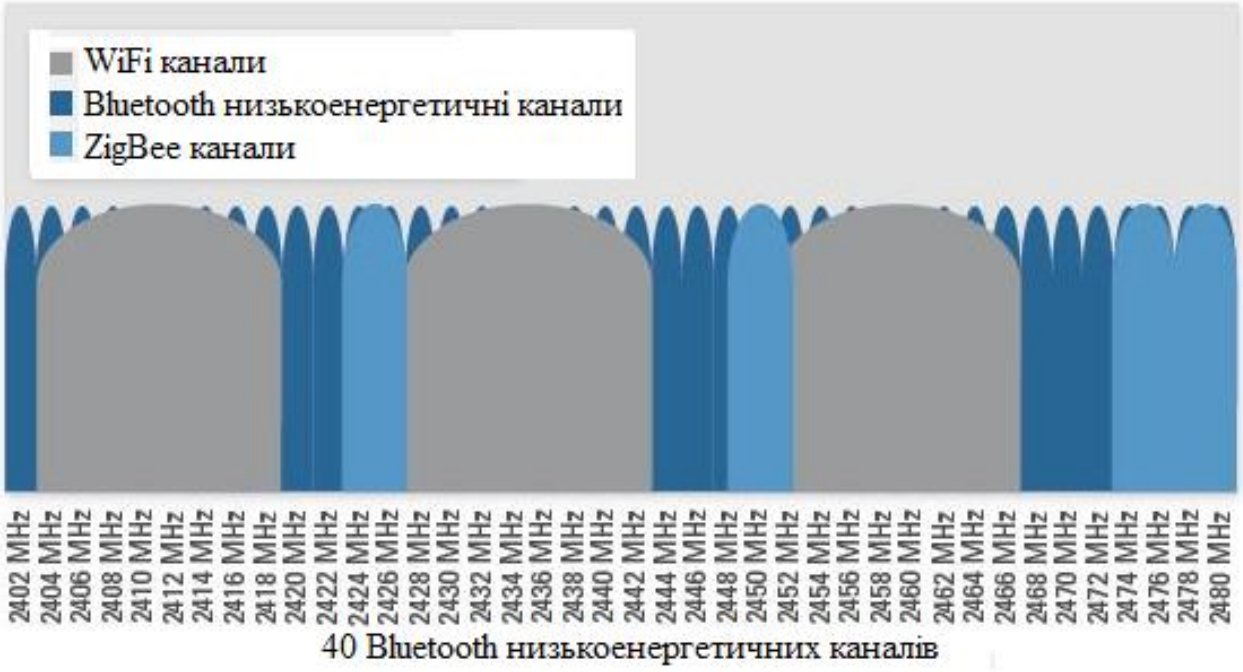


Рис 1.7 – Завантаженість діапазону частот 2,4 ГГц. Адаптовано з роботи [8]

Bluetooth Smart спроектований для підтримки відносно простих мереж з топологією «зірка», а вона погано підходить для створення динамічного, гнучкою і надійною середовища, тому всі найпопулярніші протоколи в категорії з низькою пропускною здатністю (Z-Wave і ZigBee) маршрутизують повідомлення через пористі мережі. Саме з цих причин Bluetooth Low Energy не здатний стати основою для реалізації повноцінних проектів домашньої автоматизації і розподілених систем моніторингу [9].

1.3 Порівняння безпровідних технологій для побудови безпровідних мереж моніторингу

Кожна із розглянутих вище технологій, незважаючи на усі обмеження, займає свою унікальну нішу на ринку IoT, і добре підходить для реалізації певного класу мереж у залежності від поставлених перед ними задач. У таблиці 1.1 в узагальненому вигляді наведено основні переваги і недоліки безпровідних мереж Wi-Fi, Bluetooth, Z-Wave і ZigBee.

Таблиця 1.1

Переваги і недоліки безпровідних мереж. Адаптовано з роботи [1, 4, 5, 7, 8]

Безпровідний протокол	Переваги	Недоліки
Wi-Fi	1. Широко поширений в комп'ютерах і мобільних пристроях; 2. Забезпечує високу швидкість передачі даних 3. Має достатній радіус дії.	1. Високе енергоспоживання; 2. Мережева топологія «зірка» не гарантує відмовостійкості мережі 3. Сумісність пристроїв різних виробників погана, оскільки прикладний рівень OSI не стандартизований; 4. Складний процес додавання пристроїв в мережу.
Z-Wave	1. Лідер за поширеністю; 2. Висока відмовостійкість і масштабованість завдяки комірчастої топології мережі; 3. Високий рівень безпеки; 4. Низький рівень енергоспоживання; 5. Взаємна сумісність пристроїв Z-Wave різних виробників; 6. Захищеність від впливу перешкод.	1.У різних країнах для Z-Wave використовуються різні частоти;

Продовження таблиці 1.1

ZigBee	1. Поширена технологія; 2. Висока відмовостійкість і масштабованість завдяки комірчастій топології мережі; 3. Низький рівень споживання енергії.	1. Використовує діапазон 2,4 ГГц, де є багато перешкод; 2. Погана сумісність між пристроями ZigBee різних виробників; 3. Проблеми з безпекою через недотримання виробниками вимог сертифікації
Bluetooth	1. Висока швидкість передачі даних; 2. Помірне енергоспоживання, у порівнянні з Wi-Fi; 3. Хороша сумісність – охоплені всі рівні моделі OSI.	1. Погана перешкодозахищеність у діапазоні частот 2,4 ГГц; 2. Не використовується топологія пористих мереж; 3. Малий радіус дії (до 10 м); 4. Топологія "зірка" не дозволяє розширювати мережу за допомогою ретрансляторів.

РОЗДІЛ 2
АРХІТЕКТУРА БЕЗПРОВІДНИХ МЕРЕЖ НА ОСНОВІ МІКРОКОНТРОЛЕРІВ ТА IoT КОМПОНЕНТІВ

2.1 Огляд систем з мікроконтролером Arduino та ZigBee

Серед розглянутих у першому розділі безпровідних протоколів і технологій досить легко прослідковується дві технології, які добре підходять для побудови розподілених систем моніторингу – Z-Wave та ZigBee. Обидві технології розроблялись для побудови IoT систем, широко розповсюджені та мають велику кількість датчиків і керуючих пристроїв з підтримкою цих протоколів [1, 9]. Також обидві технології забезпечують хорошу автономність і масштабованість систем при хорошій безпеці системи. Однак при розробці не стандартизованих систем моніторингу із використанням модулів різних виробників більш прийнятним є використання модулів ZigBee, оскільки вони мають відкриту програмну архітектуру і дозволяють розробнику гнучко настроювати як роботу окремих складових, так і системи загалом. Також важливим аспектом є економічна складова кінцевого проекту, а використання модулів ZigBee дозволяє зменшити вартість кінцевого проекту внаслідок того, що ці модулі мають меншу вартість у порівнянні із Z-Wave модулями аналогічної функціональності [10, 11].

Побудова систем моніторингу і керування зазвичай виконується із застосуванням центрального вузла обробки даних, яким може виступати комп’ютер, або мікроконтролерна платформа. Розглянемо просту систему, котра забезпечує комунікацію двох пристроїв із використанням мікроконтролерів та забезпечує передачу даних по протоколу ZigBee. Як контролер використаємо плату Arduino а засобом комунікації виступатиме модуль Xbee, який підтримує протокол ZigBee [12-14].

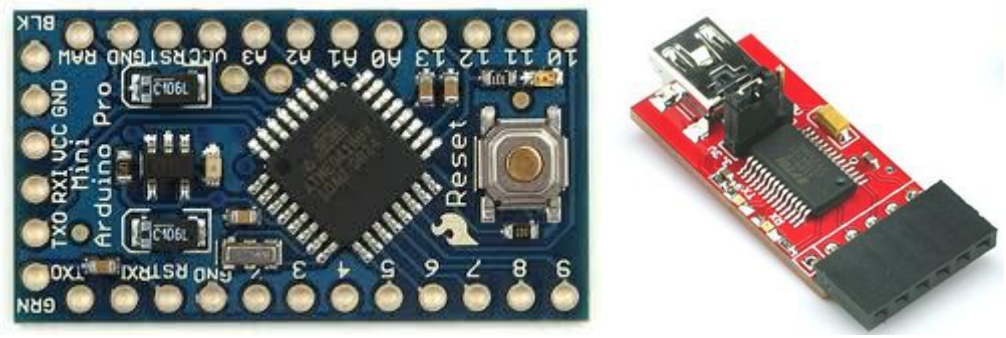
Xbee представляє собою бездротовий прийомо-передатчик, який працює за протоколом ZigBee і може формувати мережі PAN (персональні мережі).

Вони використовуються у різних галузях промисловості, науки, медицини, тощо [12].

Модулі Xbee**,** незважаючи на те, що використовують складний протокол Zigbee на основі пакетних даних для взаємодії між собою, можуть спілкуватися з іншими пристроями, використовуючи послідовний протокол зв'язку, а отже, вони широко використовуються в базових платах мікроконтролера. Розглянемо методику комунікації двох мікроконтролерів, використовуючи два модулі Xbee, один з яких передає дані, а інший отримує, а керування системою здійснюється за допомогою плати Arduino [12, 13].

Плата Arduino побудована на мікроконтролері AVR і має всі необхідні схеми для запуску вбудованого мікроконтролера AVR. Arduino може взаємодіяти з іншими пристроями за допомогою системи цифрового вводу-виводу, послідовного порту, порту I2C, SPI тощо [14]. Будь-яка плата на основі мікроконтролера AVR, яка відповідає стандартній схемі Arduino і прошивається за допомогою завантажувача Arduino, може називатися платою Arduino. Arduino IDE проста у використанні, і кожен, хто має базові знання програмування на мові C++, може швидко освоїти роботу з нею.

У цьому прикладі ми будемо використовувати плату Arduino pro-mini (рис. 2.1 а)



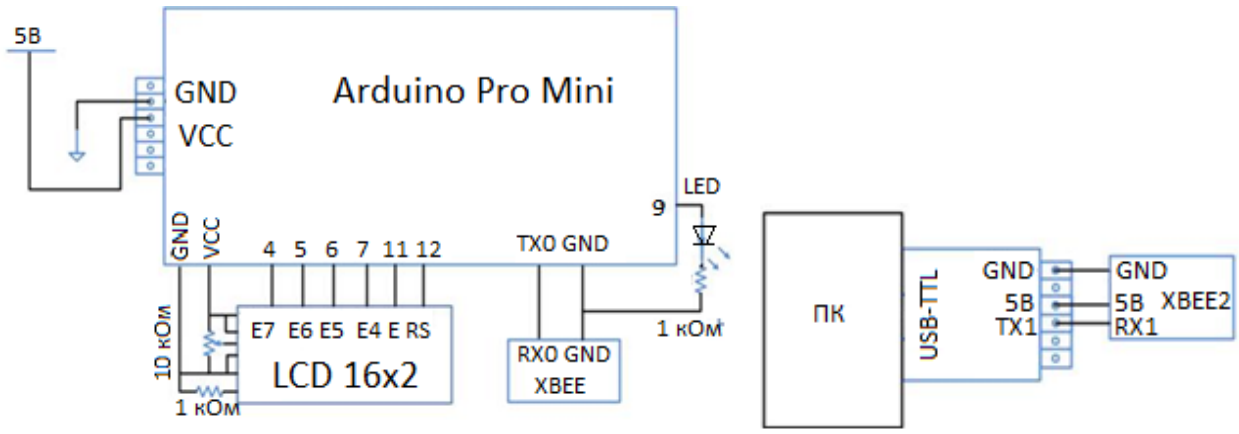
а б

Рис. 2.1 – Зовнішній вигляд плати Arduino Pro-Mini (а) та перетворювача USB – TTL (б)

Оскільки плата arduino pro-mini не має схеми для взаємодії з послідовним або USB-портом ПК, то для її підключення до потрібна зовнішня плата перетворювача USB в TTL (рис. 2.1 б). Це обладнання допомагає в програмуванні плати Arduino, а також у послідовному зв'язку з USB-портом.

На рисунку 2.2 показано модуль серії Xbee S1. Оскільки модулі Xbee можуть взаємодіяти за допомогою протоколу послідовного зв'язку з іншими пристроями, їх можна підключити до мікроконтролера, використовуючи мінімум чотири виводи, джерело живлення, заземленнята дві лінії UART для прийому і передічі даних (Rx та Tx). Модулі Xbee мають 20 контактів, призначення кожного із яких представлене у таблиці 2.1.

Рис. 2.2 – Зовнішній вигляд модуля Xbee S1



а б

Рис. 2.3 – Схема підключення модуля Xbee до контролера Arduino (а) та перетворювача інтерфейсів USB – TTL (б). Адаптовано з роботи [12]

Таблиця 2.1

Призначення виводів модуля Xbee S1. Адаптовано з роботи [12]

№ піна	**Призначення**
1	Живлення
2	Вихід даних UART
3	Вхід даних UART
4	Не використовується
5	Скидання модуля (Reset)
6	Індикатор потужності сигналу
7	ШІМ-вихід 1
8	Не використовується
9	Лінія управління режимом сну DTR / цифровий вхід 8
10	Земля (GND)
11	Аналоговий вхід 4 або цифровий вхід / вихід 4
12	цифровий вхід / вихід 7
13	Індикатор стану модуля
14	Вхід опорної напруги напруги для аналогових входів
15	Аналоговий вхід 5 або вхід / вихід 5
16	Аналоговий вхід 6 або вхід / вихід 6
17	Аналоговий вхід 3 або вхід / вихід 3
18	Аналоговий вхід 2 або вхід / вихід 2
19	Аналоговий вхід 1 або вхід / вихід 1
20	Аналоговий вхід 0 або вхід / вихід 0

Розглянемо схему підключення для комунікації модуля Xbee та контролера Arduino (рис. 2.3 а) і з перетворювачем USB – TTL (рис. 2.3 б). Вивод №2 – UART Data Out підключений до виводу Rx1 плати Arduino pro mini, а контакт №3 – UART Data In до виводу Tx0. Код, написаний для взаємодії з Xbee використовує функції послідовного стандартної бібліотеки Arduino «Serial.h». Функція Serial.begin(), дозволяє ініціалізувати послідовний порт із заданою швидкістю передачі даних, Serial.write() і Serial.print() використовуються для передачі даних до послідовного порту, а Serial.available() та Serial.read() для перевірки заповненості буфера даних і зчитування з послідовного порту відповідно.

Після написання мікрокоду для контролера Arduino, його слід завантажити у плату. По завершенні цієї процедури буде закінчено усі підготовчі процедури для встановлення зв’язку між двома контролерами із використання протоколу ZigBee. При включенні двох контролерів Arduino, Xbee, підключений до неї автоматично встановлює зв'язок з іншим Xbee, який підключений до послідовного порту ПК. Після подачі живлення на платі Arduino постійно надсилається пакет даних до модуля Xbee з невеликою затримкою, і ці дані відображаються у вікні монітора послідовного порту ПК, де підключений інший модуль Xbee. Другу плату Xbee можна підключити до ПК за допомогою тієї ж плати перетворювача USB в TTL, яка була використана для програмування плати Arduino (рис. 2.3 б).

Вихідний код для контролера Arduino, котрий реалізовує описані вище функції виглядає наступним чином [11, 12]:

```
#include <LiquidCrystal.h>
// ініціалізуємо бібліотеку номерами контактів
інтерфейсу

LiquidCrystal lcd(12, 11, 7, 6, 5, 4);
// називаємо вихід №9 ім’ям «led»
int led = 9;

void setup()
```

```
{
  // налаштовуємо кількість стовпців і рядків на
рідкокристалічному дисплеї
  lcd.begin(16, 2);
  lcd.print("ENGINEERS GARAGE");
  lcd.setCursor(0, 1);
  lcd.print(" XBEE INTERFACE ");

  // initialize the led pin as an output.
  pinMode(led, OUTPUT);
  // start serial port at 9600 bps
  Serial.begin(9600);
  // чекаємо, поки послідовний порт не буде готовий
  delay(100);
// відпраляємо дані один раз
  Serial.print("  XBEE Demo");
}

void loop()
{
  // безперервно надсилаємо цей рядок до іншого Xbee
    Serial.println("hello world");
    // блимаємо світлодіодом
    digitalWrite(led, HIGH);
    delay(1000);
    digitalWrite(led, LOW);
    delay(1000);
}
```

2.2 Розробка архітектури розподіленої безпровідної системи моніторингу

Розглянемо приклад розробки системи моніторингу в розрізі наповнення житлового приміщення системою датчиків і керуючих пристроїв підключених до безпровідної мережі.

Для стабільної роботи екосистеми розумного будинку, необхідна надійна, здатна до самовідновлення і проста в розгортанні бездротова мережа, причому, у більшості випадків, висока пропускна здатність не має істотного значення, більш важливим фактором є те, що обладнання, яке працює в такий мережі, має працювати автономно протягом тривалого часу [13, 15]. Також,

бажано, щоб пристрої працювали за одним із стандартних протоколів безпровідного зв'язку. Зважаючи на поставлені вимоги, можна зробити висновок, що Zigbee повністю відповідає всім цим умовам [16]: завдяки mesh топології вона забезпечує самовідновлення і гарантовану доставку пакетів, має криптографічний захист і, нарешті, має високу автономність роботи. Тим більше найбільша кількість пристроїв бюджетного і середнього цінового сегменту підтримують протокол Zigbee, а також їх підтримують зручні програмні додатки керування екосистемою інтернету речей, наприклад, Xiaomi MiHome.

Розглянемо необхідний набір датчиків і керуючих пристроїв, які можуть бути використані в розумному будинку. Для того, щоб мати можливість взаємодіяти з ZigBee пристроями, необхідний шлюз [15] – пристрій який підтримує два інтерфейси: ZigBee і Wi-Fi для підключення до домашньої мережі і основне його призначення – трансляція пакетів між ZigBee і Wi-Fi інтерфейсами. Одним зі шлюзів, які можна використати є Mi/Mijia V3, крім свого основного функціоналу він може виконувати роль LED світильника, онлайн радіо, дверного дзвінка і будильника. Такий шлюз підтримує роботу з системою керування MiHome та великою кількістю пристроїв, і, насьогодні, є найбільш популярним у рішеннях IoT, котрі використовують протокол ZigBee.

Датчики розумного будинку підключаються безпосередньо до шлюзу, а максимальна їх кількість – 30 пристроїв, але підключення може відбуватись до декількох шлюзів у рамках однієї мережі [13]. Кожен з шлюзів, які знаходяться в різних точках будинку, управляє пулом датчиків розташованих в безпосередній близькості від нього. Варто зазначити, що другий шлюз не продовжує покриття першого, а працює як самостійний пристрій зі своїми датчиками. Датчики керовані різними шлюзами можуть без проблем взаємодіяти один з одним.

За протоколом ZigBee працюють датчики здебільшого ті, які не мають стаціонарного джерела живлення від. Крім них, в системі Xiaomi MiHome, по протоколу ZigBee працюють всі типи настінних вимикачів, вбудовані розетки,

привід для штор, розумний дверний замок та ін.. Датчики можна умовно розділити на два типи – сигнальний і виконавчий. До сигнальних відносяться ті, які є умовами сценаріїв і вони не передбачають віддаленого управління. Розглянемо такі датчики [16]:

–бездротові кнопки – наприклад mijia та Aqara підтримують три дії (один клік, подвійний клік та тривале натискання);

–датчик руху – може використовуватись у сценаріях увімкнення освітлення та сигналізації;

–куб-контролер – багатофункціональний датчик, за допомогою якого можна керувати величезною кількістю параметрів, ним підтримуються такі умови, як поворот на 90 і 180 градусів, тряска, удар, зсув, обертання;

–датчик відкриття – складається із датчика на основі геркону і магніту, одна його частина прикріплюється на двері чи вікно, а інша на стіну. Застосувується у системах сигналізації і як блокуючий тригер для інших систем (наприклад системи обігріву);

–датчик протікання води – застосовується для сценаріїв крану автоматичного перекривання води, у разі виявлення протікання;

–датчики газу та диму – фіксують присутність в атмосфері газу. Існують датчики, котрі зпрацьовують на різні гази, проте найбільш необхідними в будинку будуть датчик чадного газу та метану (природній газ);

–датчики температури і вологості – використовуються для задання параметрів мікроклімату у зв’язці з, наприклад, обігрівачами або зволожувачами повітря;

–розумні розетки – застосовуються для керування навантаженням і контролю енергоспоживання. Також є потужними ретрансляторами сигналу, оскільки мають стаціонарне живлення;

–Розумний дверний замок – використовується в різних сценаріях, починаючи з відкриття за відбитком пальця чи введенні коду до блокування доступу.

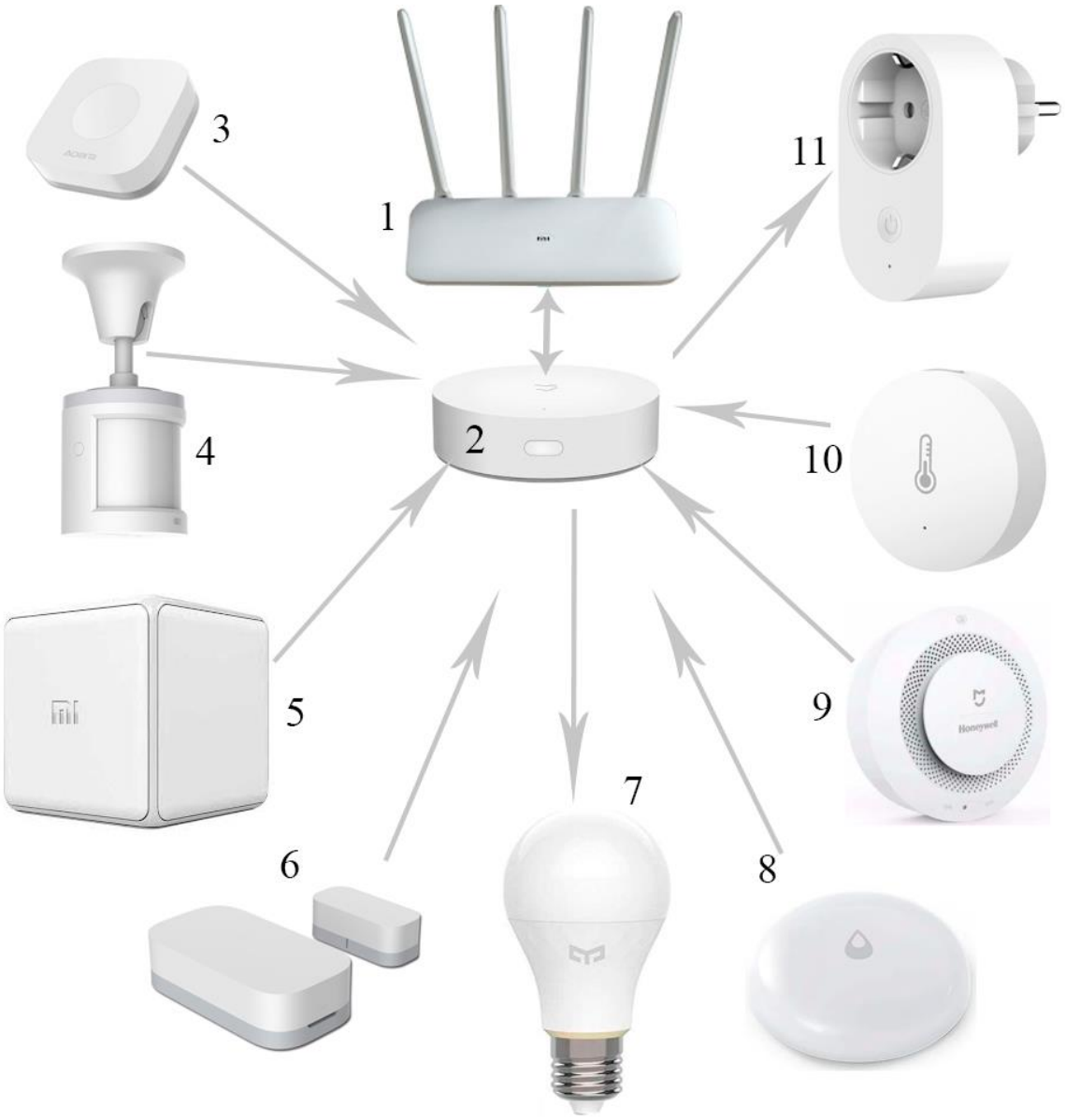


Рис. 2.4 – Архітектура системи розумний будинок, побудована на основі пристроїв Xiaomi з підтримкою протоколу ZigBee: 1 – Wi-Fi маршрутизатор; 2– ZigBee шлюз Mi/Mijia V3; 3 – бездротова кнопка; 4 – датчик руху; 5 – куб-контролер; 6 – датчик відкриття; 7 – розумна лампочка; 8 –датчик протікання рідини; 9 – датчик газу (диму); 10 – датчик температури та вологості; 11 – розумна розетка

Окрім цих датчиків у системах розумний будинок застосовуються і інші пристрої, інтегровані в екосистему. Насьогодні популярні системи керування IoT підтримують велику кількість розумних пристроїв різних категорій, від кліматичної і кухонної техніки до транспорту і систем енергоменеджменту.

Оскільки важливим параметром будь-якої розподіленої системи моніторингу і керування є універсальність і зручність використання, як засіб взаємодії з користувачем і настроювання системи доцільно обрати вільно розповсюджуваний мобільний додаток Xiaomi MiHome. Датчики та пристрої керування також доцільно обрати виробництва Xiaomi, оскільки вони гарантовано підтримуються системою керування будинком MiHome і мають одну з найнижчих вартостей, серед аналогів. Зобразимо графічно (рис. 2.4) можливу архітектуру системи розумний будинок і розглянемо доцільність застосування кожного елемента. Wi-Fi маршрутизатор (1) у системі забезпечує підключення mesh-мережі розумного будинку до мережі інтернет. Шлюз (2) служить центральним комунікатором усіх пристроїв ZigBee – отримує дані з датчиків, і посилає сигнали до пристроїв керування, а також служить для комутації протоколу ZigBee у Wi-Fi. Додаток MiHome дозволяє використовувати безпровідні кнопки (3) для багатьох операцій, так, ними модна керувати освітленням, розумними розетками та будь-якими пристроями, інтегрованими в екосистему розумного будинку – роботи-пилососи, чайники, кавоварки і т.д.. Куб-контролер (5) дозволяє реалізовувати усі функції, що і бездротова кнопка, та має ряд додаткових можливостей – він може розпізнавати велику кількість жестів, і, таким чином розширює області застосування, наприклад ним можна не лише вмикати і вимикати освітлення, а і змінювати його рівень. Датчик руху (4) може бути настроєний, як і кнопка на ряд дій, від вмикання світла, до керування опаленням чи кондиціонуванням. Датчики відкриття (6) у розумному будинку, здебільшого, застосовуються для сигналізації відкритого вікна, що служить блокуванням для увімкнення обігрівача або кондиціонера. Сенсор протікання (8) забезпечує сигналізацію про появу рідини, і, якщо в системі розумного будинку є аварійний розумний

клапан перекриття води, сигналу для його спрацювання. Як і датчик протікання, датчики диму та газу, по перше, повідомлять про нештатну ситуацію, по друге можуть увімкнути систему пожежогасіння. Кліматичний датчик (10) служить для передачі інформації про мікроклімат у приміщенні у додаток, а також застосовується для настройки автоматичного увімкнення кліматичних приладів. Розумна розетка (11) може бути застосована для підключення будь-яких пристроїв, живленням яких потрібно керувати програмно або віддалено (обігрівачі, зволожувачі повітря і т.д.) а також для забезпечення можливості їх аварійного відключення від мережі. Ще одним застосуванням розумної розетки є використання її як ретранслятора мережі, розширюючи таким чином покриття ZigBee, замість використання декількох шлюзів.

Система керування розумним будинком Xiaomi MiHome дозволяє побудувати мережу на основі підтримуваних пристроїв та їх забезпечує легке настроювання. Оскільки система встановлюється на смартфон, то керування розумним будинком можна здійснювати звідки завгодно, головне мати доступ до інтернету. MiHome дозволяє настроїти сценарії взаємодії пристроїв між собою та реакцію на події, встановлювати розклад роботи окремих пристроїв і, що найголовніше, інформувати про все це за допомогою повідомлень на смартфоні.

ВИСНОВКИ

1. Показано, що розподілена безпровідна система віддаленого моніторингу фізичних величин може бути побудована із використанням мікроконтролерних платформ та системи датчиків і керуючих компонентів об’єднаних у мережу.

2. Встановлено, що для побудови безпровідних мереж може застосовуватись велика кількість протоколів, найбільш ефективними з яких будуть Wi-Fi, Bluetooth, Z-Wave та ZigBee. Кожен з цих протоколів має ряд переваг і недоліків, при застосування його в системах моніторингу.

3. Встановлено, що системи моніторингу побудовані на технологіях Wi-Fi і Bluetooth матимуть погану автономність роботи внаслідок низької енергоефективності. У той же час пристрої Z-Wave та ZigBee споживають мало енергії, проте характеризуються низькою швидкістю передачі даних.

4. Мережі Z-Wave і ZigBee здатні до самоорганізації і динамічної маршрутизації пакетів даних, що дозволяє розширити корисну площу охоплену безпровідними пристроями. Також у цих мережах застосовуються криптографічні механізми, які забезпечують високий ступінь захисту від несанкціонованого доступу.

5. Розглянуто приклад системи, яка встановлює комунікацію двох контролерів Arduino за протоколом ZigBee з використанням модулів безпровідного зв’язку підключених через шину UART.

6. Встановлено, що розподілена мережа може бути побудована на основі датчиків і керуючих пристроїв, що підтримують протокол ZigBee, а керування такою системою може здійснюватися додатком Xiaomi MiHome, встановленим на смартфоні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. S. Marksteiner, V. J. Exposito Jimenez, H. Vallant, H. Zeiner. An Overview of Wireless IoT Protocol Security in the Smart Home // 10th CMI Conference on Internet of Things Business Models, Users, and Networks, Copenhagen, 2017. – http://ieeexplore.ieee.org/document/8260940/
2. The OSI model explained and how to easily remember its 7 layers. Електронний ресурс. Режим доступу: https://www.networkworld.com/article/3239677/the-osi-model-explained-and-how-to-easily-remember-its-7-layers.html. Дата доступу: 14.11.2020.
3. Layers of OSI Model. Електронний ресурс. Режим доступу: https://www.geeksforgeeks.org/layers-of-osi-model/. Дата доступу: 14.11.2020.
4. Wi-Fi and the OSI model. Режим доступу: https://www.controleng.com/articles/wi-fi-and-the-osi-model/. Дата доступу: 14.11.2020.
5. Z-wave protocol stack. Режим доступу: https://www.rfwireless-world.com/Tutorials/z-wave-protocol-stack.html. Дата доступу: 14.11.2020.
6. Обзор протокола Z-Wave. Режим доступу: https://rus.z-wave.me/z-wave-knowledge-base/about-z-wave/z-wave-technical-overview. Дата доступу: 14.11.2020.
7. Z-Wave Vs. Zigbee. Режим доступу: https://www.link-labs.com/blog/z-wave-vs-zigbee. Дата доступу: 14.11.2020.
8. The Bluetooth Protocol Architecture. Режим доступу: https://www.tutorialspoint.com/the-bluetooth-protocol-architecture. Дата доступу: 14.11.2020.
9. Zigbee против Z-Wave / Bluetooth / Wi-Fi. Режим доступу: http://domosystems.com.ua/index.php?route=information/news&news_id=28. Дата доступу: 14.11.2020.

10. H. H. Hadwan, Y. P. Reddy. Smart Home Control by using Raspberry Pi & Arduino UNO // International Journal of Advanced Research in Computer and Communication Engineering. – 2016. – V. 5, № 4. – P. 283–288.
11. S. Wadhwani, U. Singh, P. Singh, S. Dwivedi. Smart Home Automation and Security System using Arduino and IOT // International Research Journal of Engineering and Technology. – 2018. – V.5, №2. – P. 1357 – 1359
12. How To Interface XBEE With Arduino. Електронний ресурс. Режим доступу: https://www.engineersgarage.com/arduino/how-to-interface-xbee-with-arduino-part-29-49/. Дата доступу: 14.11.2020.
13. Z. A. Jabbar, R.S. Kawitkar. Implementation of Smart Home Control by Using Low Cost Arduino & Android Design // International Journal of Advanced Research in Computer and Communication Engineering. – 2016. – V. 5, № 2. – P. 248–256.
14. Микроконтролери AVR. Електронний ресурс. Режим доступу: http://www.studmed.info/docs/document3940/content. Дата доступу: 14.11.2020.
15. Как работает умный дом. Режим доступу: https://www.ixbt.com/live/chome/kak-rabotaet-umnyy-dom-xiaomi-mijia---zigbee-ustroystva.html. Дата доступу: 11.12.2020.
16. Из чего собрать умный дом в 2020 году. Режим доступу: https://habr.com/ru/company/mvideo/blog/499706/ Дата доступу: 11.12.2020.