

## **Тема 13.** Технології та протоколи передачі даних на короткі відстані в IoT мережах

### **Технологія Z-Wave**

Z-Wave — це безпроводова радіотехнологія з низьким енергоспоживанням. Z-Wave працює в діапазоні частот до 1 ГГц та оптимізована для передавання простих команд для управління з досить малими затримками (зміна гучності телевізору, виключення/включення побутової техніки, зміна яркості екрану тощо).

Вибір частот був зроблений не випадково. Для того, щоб зменшити кількість перешкод від інших технологій, якими вже користуються багато людей, наприклад Wi-Fi сильно навантажений на частоті 2,4 ГГц і тому вже зараз в нашій країні переходять на частоту 5 ГГц.

Технологія Z-Wave - ключ до того, щоб мати повний контроль над вашою домашньою безпекою і енергією, з мінімальними клопотами.

За допомогою технології Z-Wave можливо мати свою власну домашню систему автоматизації, програмувати всі основні елементи будинку, такі як освітлення, нагрівання, готування, охолодження і навіть вашу домашню безпеку.

Переваги не закінчуються цим, хоча це - складна система, вона дуже проста у використанні, а також вона ще є енергозберігаючою та економить наш дорогоцінний час.

Система працює за допомогою дистанційного керування і використовує радіохвилі малої потужності. Ця сіткоподібна мережа покриває всі області будинку, оскільки радіохвилі можуть проходити через стіни, поверхи та меблі, роблячи можливість з'єднання надійним майже на 100%.

Z - Wave Alliance підтриманий корпорацією Intel, яка зробила стратегічні інвестиції в компанію Zensys, технологію безпроводових комірчастих мереж Z, що розробила, - Wave. Z-Wave, є системою управління цифровим будинком, побудовану на базі mesh- мережі з дуплексним безпроводовим радіозв'язком FSK. Пропускна спроможність 40 кбіт/с. Відстань: близько 30 метрів на

“відкритому повітрі”, в приміщенні зменшується залежно від будівельних матеріалів і т.д. Z - Wave використовує 900МГц ISM смугу частот, 908.42МГц в США і 68.42МГц в Європі. Було прийнято рішення відмовитися від роботи на частоті 2,4ГГц, оскільки сигнал 908/868ГГц поширюється приблизно в 2,5 рази далі, чим еквівалентний 2.4ГГц сигнал. Це дозволяє Z - Wave радіо потребляти менше енергії, чим порівнянні безпроводові пристрої, працюючі в смузі 2.4ГГц. Окрім цього смуга 2.4ГГц занадто завантажена, приміром Wi - Fi мережами.

В порівнянні з конкурентами, Z - wave пристрої виділяються максимальною простотою і низькою вартістю. Максимальне число вузлів мережі (232) явно недостатньо для промислового застосування, проте, цілком вистачає для домашніх користувачів. Типовий Z - Wave чіп містить:

- Радіо трансівер,
- 32 кб flash пам'яті, включаючи Z - Wave протокол і додатки,
- Системні інтерфейси, включаючи цифрові і аналогові інтерфейси для приєднання зовнішніх пристроїв, таких як сенсори,
- 3des двигок для забезпечення конфіденційності і аутентифікації,
- Тріак контроллер, щоб зменшити вартість додатків, що вимикають світло.

### **Технологія NFC**

Технологія NFC (Near Field Communication) - створена компаніями такими, як Sony та NXP Semiconductors - являє собою комбінування наявних безконтактних технологій зв'язку та радіочастотної ідентифікації.

Технологія NFC призначена для обміну різною інформацією, наприклад, картинками, музичними файлами, номерами телефонів, або ключами цифрової авторизації між двома розташованими близько один до одного пристроями з підтримкою NFC. Це можуть бути смарт-картка, будь-які портативні пристрої, а також зчитувальні пристрої RFID. Дана технологія може використовуватися в якості ключу доступу до даних або служб (електричний замок, або безготівкова оплата).

На відміну від усіх інших технологій безконтактного зв'язку, які можуть передавати дані тільки від активного пристрою до пасивного, NFC може здійснювати обмін інформації між двома активними пристроями.

NFC використовується для взаємодії з пристроями радіочастотної ідентифікації RFID. Для забезпечення сумісності між картами RFID та мобільним телефоном різних виробників виконується перевірка цифрового протоколу і проводиться вимірювання всіх важливих властивостей радіочастотного сигналу: тимчасових характеристик, чутливості та амплітуди приймача в активному режимі, частоти несучої амплітуди сигналу.

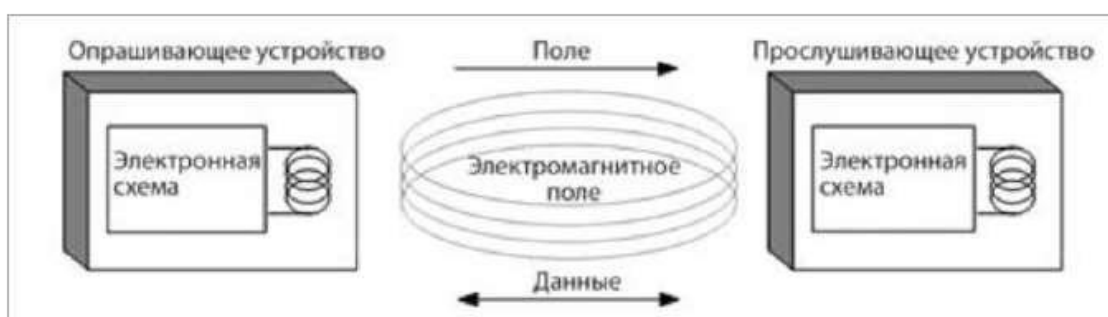


Рисунок 13.1 – Взаємодія пристроїв

При передачі інформації від активного пристрою до пасивного пристрою використовується амплітудна маніпуляція ASK. При обміні обидва пристрої рівноправні.

Кожен пристрій має власне джерело живлення, тому сигнал несної відключається відразу після закінчення передачі.

За рахунок індуктивного зв'язку між опитуваним і прослуховуючим пристроями пасивний пристрій впливає на активне. Зміна імпедансу прослуховуючого пристрою викликає зміну амплітуди або фази напруги на антені опитуваного пристрою. Після цього відбувається з'єднання двох пристроїв та передача даних. Як тільки ми роз'єднуємо два пристрої більш, ніж на 20 см розривається електромагнітний зв'язок і перестають передаватися дані автоматично.

В дійсності NFC можна вважати, по суті, продовженням вже досить відомої технології радіочастотної ідентифікації RFID. Як відомо, RFID повсюдно використовується в безконтактних картах і мітках. Однак NFC може не тільки зчитувати інформацію з будь-яких пасивних електронних міток, але і здатна забезпечувати двосторонній безпроводовий зв'язок між пристроями.

## **RFID**

RFID (Radio Frequency IDentification) – метод автоматичної ідентифікації об'єктів, в якому за допомогою радіосигналів зчитуються або записуються дані, що зберігаються в так званих транспондерах, або RFID – мітках.

Будь-яка RFID - система складається із зчитувального пристрою (зчитувач, рідер) та транспондери (він же RFID - мітка, іноді також називають RFID-тег).

Більшість RFID-міток складається з двох частин.

Перша – інтегральна схема для обробки та зберігання інформації, демодулювання та модулювання радіочастотного сигналу і деяких інших функцій.

Друга - антена для прийому і передачі сигналу. А також для роботи цих міток потрібне програмне забезпечення — програми, за допомогою яких здійснюється аналіз та збір інформації, одержуваної із RFID-міток.

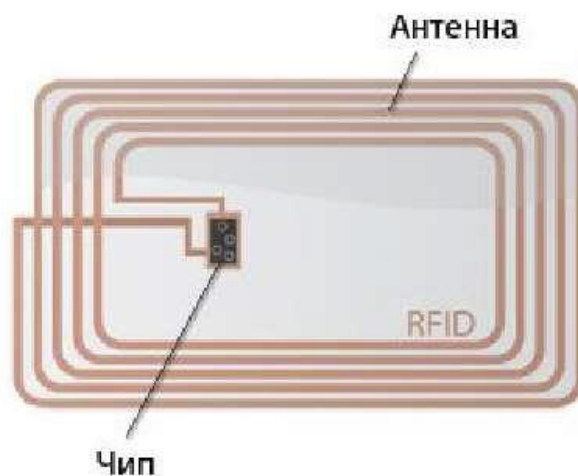


Рисунок 13.2 – Будова RFID-мітки

Мітки бувають двох видів активні та пасивні. Активні мітки мають власне джерело живлення, тому вони можуть самі посилати сигнал і зчитуватися з досить великої відстані. Пасивні мітки не мають власного джерела енергії і активізуються, тільки після того, коли надходить сигнал до пристрою зчитування і тоді передають записану в них інформацію.

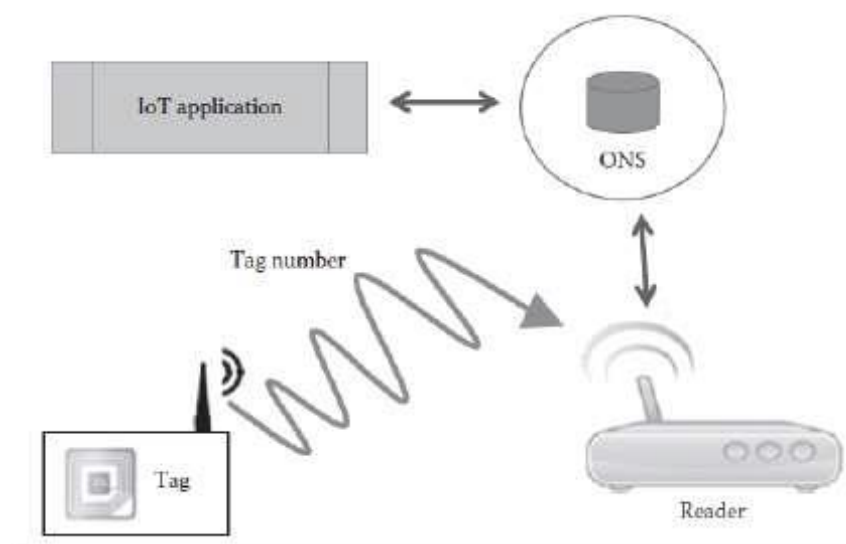


Рисунок 13.3 – Компоненти RFID системи

Тег RFID має дві основні компоненти: електронний мікросхеми для зберігання ідентичності об'єкта та антени, що дозволяє чіпу спілкуватися з системою читання тегів. Зв'язок між тегом і читачем тегів відбувається за допомогою радіохвиль. Два основних компоненти системи RFID:

- радіоприймач;
- читач тегів.

RFID-мітки можуть використовуватися для управління товарними запасами або відстеження часу на спортивних змаганнях. Магнітні мітки не замінюють штрих-коди, а їх доповнюють можливістю дистанційного зчитування. Мітками можуть маркувати велику рогату худобу для запису інформації про проходження ветеринарного огляду. Рішення для транспорту допомагають ідентифікувати автомобіль, навіть якщо вона рухається на великій швидкості. Деякі авіалінії користуються мітками для ефективного відстеження

великих потоків багажу. Також RFID вбудовується у біометричні паспорти, кредитні картки для безпечного доступу в захищені області.

Деякі мітки можуть бути прочитані на відстані декількох метрів від прямої видимості пристрою зчитування. Більшість міток представляють собою звичайний текстовий запис та штрих-код в якості доповнення для прямого зчитування у випадках несправності радіочастотної електроніки.

Електронний код продукту (EPC) - це унікальний ідентифікатор, що зберігається в тезі RFID, що допомагає ідентифікувати та відслідковувати елементи в сценарії керування ланцюжком постачання. EPCglobal – це організація, що розробила EPC, а EPCglobal також готує та підтримує стандарти, пов'язані з RFID та EPC. RFID може бути використана як ключова технологія для пристроїв IoT з наступних причин:

- Відкритість;
- Масштабованість;
- Надійність;
- Підтримка ідентифікаторів об'єктів та відкриття сервісів.

### **Bluetooth Low Energy**

Безпроводова технологія з низьким енергоспоживанням Bluetooth (BLE) – це частина специфікації Bluetooth, яка починається з покоління Bluetooth 4.0 і на даний момент закінчується Bluetooth 5.0.

Пристрої, що використовують BLE, споживають менше енергії, ніж інші версії Bluetooth - пристрої попередніх поколінь. У багатьох випадках пристрої зможуть працювати більше року на одній невеличкій батарейці типу таблетка без підзарядки. Завдяки цьому, можна буде використовувати датчики невеликих розмірів, які будуть постійно працювати та взаємодіяти з іншими пристроями.

Основними рівнями BLE є:

- Додаток – реалізує корисну для кінцевого користувача логіку роботи.
- Основний пристрій, або хост – надає верхні рівні стеку протоколів Bluetooth.

- Контролер – займається нижніми рівнями стеку протоколів Bluetooth.
- Рівень додатків – найвищий рівень стеку протоколів. Рівень хосту містить такі підрівні:
  - GAP (Generic Access Profile) – профіль загального доступу;
  - GATT (Generic Attribute Profile) – профіль загальних атрибутів;
  - ATT (Attribute Protocol) – протокол атрибутів;
  - SM (Security Manager) – менеджер безпеки;
  - L2CAP (Logical Link Control and Adaptation Protocol) – протокол логічного з'єднання та адаптації;
  - HCI (Host Controller Interface) – інтерфейс хост-контролеру, на стороні хосту.

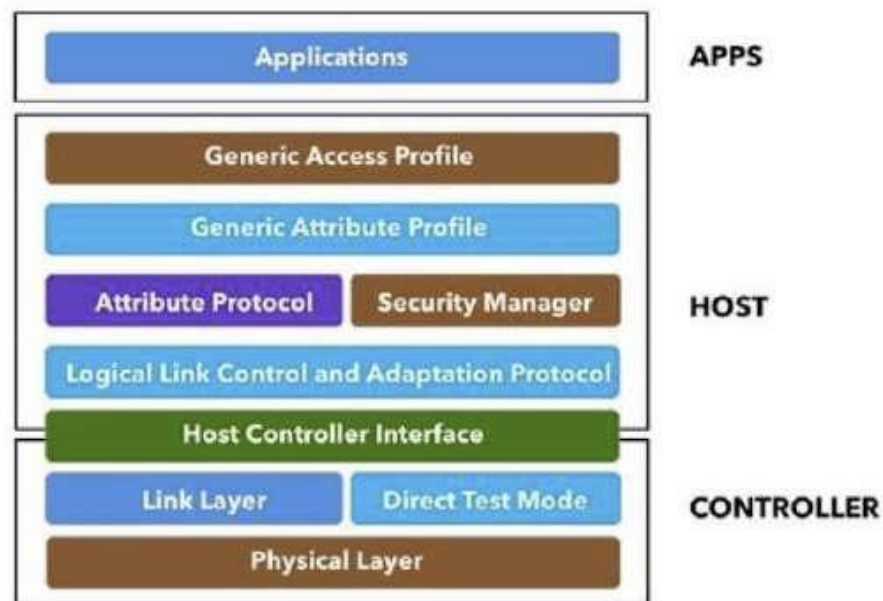


Рисунок 13.4 – Архітектура BLE

BLE призначений для тих пристроїв, які мають невеликі розміри, тобто для пристроїв, у яких важлива компактність і куди не можна встановити повноцінний акумулятор, або батарею великого об'єму. Bluetooth LE споживає в 10-20 разів менше енергії і цілком здатний передавати дані в 50 і більше разів швидше та на відстані більше 100 метрів, ніж класичні Bluetooth рішення.

Крім перерахованих вище переваг, BLE має високу безпеку, надійність, низьку затримку при підключенні та низьку споживчу потужність. Є ще одна важлива особливість даного стандарту, вона полягає в адаптивності переналаштування частоти, тобто відбувається захист від помилок при передачі сигналу, BLE швидко змінює свою робочу частоту, вибираючи найбільш оптимальну для усунення перешкод, проблем переповнення і для зниження інтерференції.

Специфікація Bluetooth 5.0 була створена, з орієнтацією на Інтернет речей. Це остаточно показало, що стандарт прагне "захопити" ринок пристроїв.

В порівнянні з попередньою версією 4.0 була підвищена швидкість передачі даних майже до швидкостей HSPA і LTE ранніх версій, при цьому енергоспоживання залишилося в колишніх показниках.

Важливим показником для побудови мереж Інтернету речей як раз є енергоефективність. В даний момент дана специфікація є мало поширеною через те що вона з'явилася нещодавно. Bluetooth 5 як і всі попередні версії має зворотну сумісність. Цілком можливо, через декілька років кожний мобільний пристрій буде підтримувати 5 версію цього стандарту, що є найважливішою перевагою цієї технології над іншими.

### **Wi-Fi HaLow**

Wi-Fi HaLow — це протокол безпроводової мережі, опублікований у 2017 році, як доповнення до стандарту бездротової мережі IEEE\_802.11. Цей протокол працює на непотребуючій ліцензування частоті 900 МГц, для забезпечення розширеного діапазону Wi-Fi мереж, порівняно зі звичайними мережами Wi-Fi, працюючими в діапазонах 2,4 ГГц і 5 ГГц. Його низьке енергоспоживання також є перевагою, таким, що дозволяє створювати великі групи станцій або датчиків, які взаємодіють щоб поширювати сигнали, підтримуючи концепцію інтернет-речей (Internet of Things, IoT). Низьке енергоспоживання протоколу конкурує з Bluetooth і має додаткову перевагу - вищі швидкості передачі даних і більш широкий діапазон покриття.(див. рис. 13.5).



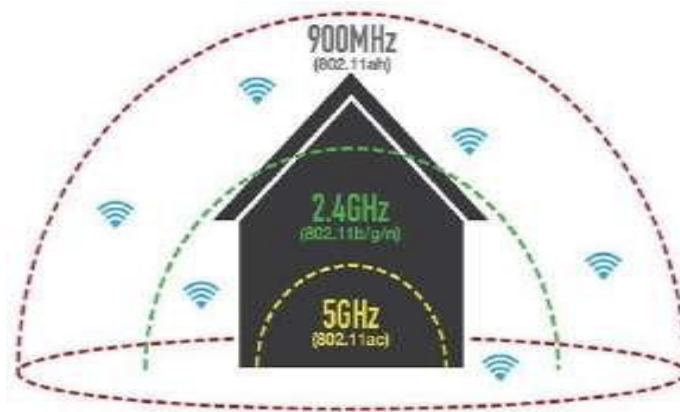


Рисунок 13.5 – Діапазон покриття Wi-Fi HaLow

Wi-Fi HaLow дозволить розширити можливості енергоефективного сценарію використання розумного будинку, автомобілів, а також в торгівлі, промисловості, сільському господарстві тощо.

Wi-Fi HaLow розширює Wi-Fi в діапазоні 900 МГц, даючи можливість з'єднання пристроїв малої потужності, таких як датчики та портативні комп'ютери. Wi-Fi HaLow успадкує позитивні якості попередніх протоколів, такі як надійний захист інформації, широку сумісність обладнання та простоту встановлення.

Пристрої з підтримкою Wi-Fi HaLow будуть також працювати у діапазонах 2,4 та 5 ГГц, що дасть можливість інтегрування в екосистему, яка на даний момент налічує більше 7 млрд пристроїв. Також Wi-Fi HaLow буде мати підтримку підключення по IP, це дозволить працювати з хмарами, що дуже важливо для IoT. Також буде можливість підключатися до одієї точки доступу близько 1000 пристроїв.

Таблиця 13.1 – Порівняльна характеристика технологій та протоколів передачі даних на короткі відстані в IoT

| Характеристики           | RFID   | NFC                    | BLE      | Z-Wave                | Wi-Fi HaLow        |
|--------------------------|--|------------------------|----------|-----------------------|--------------------|
| Смуга частот             | 6/13,5/433/863-870/902-928 МГц<br>2,4/5-27 ГГц | 13,56 МГц              | 2,4 ГГц  | 868/915 МГц           | Під діапазон 1 ГГц |
| Швидкість передачі даних | 500 кбіт/с                                     | 106/212/424/848 кбіт/с | 1 Мбіт/с | 9,6, 40 та 100 кбіт/с | До 4 мбіт/с        |

|                              |   |              |                              |             |                                  |
|------------------------------|---|--------------|------------------------------|-------------|----------------------------------|
| Радіус дії                   | 0,1-5 м                                 | 0,1 м        | 70 м                         | 100 м       | 100 – 1000 м                     |
| Пропускна здатність на канал | 10 МГц для 6 МГц<br>14 МГц для 13,5 МГц | Змінна       | 40 каналів з шириною в 2 МГц | 300-400 кГц | 1/2/4/8/16 МГц                   |
| Модуляція                    | -                                       | ASK,BPSK     | GFSK                         | FSK/GFSK    | BPSK, QPSK, 16-/64-/256-Qam,OFDM |
| Топологія                    | Point to Point<br>Point to Multipoint   | Peer to peer | Singl-Hop                    | Mesh        | Star                             |
| Безпека                      | Шифрування                              | Шифрування   | AES-128                      | AES-128     | WPA                              |