

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Автоматики і комп'ютеризованих технологій
(повна назва)

Кафедра Комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки
(повна назва)

АТЕСТАЦІЙНА РОБОТА

Пояснювальна записка

другий (магістерський)

(рівень вищої освіти)

Автоматизація проектування шлюзу для мережі пристроїв за технологією IoT
(тема)

Виконав: студент 2 курсу, гр. КІТПВм-19-1
Коцюба А.О.
(прізвище, ініціали)

Спеціальність 151 Автоматизація та комп'ютерно-інтегровані технології освітньої програми
Комп'ютерно-інтегровані технологічні процеси та виробництво

(код і повна назва напрямку)

Тип програми освітньо-професійна

(повна назва освітньої програми)

Керівник проф. Нефьодов Л.І.

(посада, прізвище, ініціали)

Допускається до захисту
зав. кафедри

(підпис)

Невлюдов І.Ш.

(прізвище,
ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет	Автоматики і комп'ютеризованих технологій
Кафедра	Комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки
Рівень вищої освіти	другий (магістерський)
Спеціальність	151 Автоматизація та комп'ютерно-інтегровані технології
Тип програми	освітньо-професійний
Освітня програма	Комп'ютерно-інтегровані технологічні процеси та виробництва

(код і повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____

(підпис)

«_____» 20 ____ р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові _____

Коцюбі Андрію Олександровичу

(прізвище, ім'я, по батькові)

1. Тема роботи Автоматизація проектування шлюзу для мережі пристроїв за технологією IoT

затверджена наказом по університету від 02.11.2020 р. № 1511 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 10.12.2020 р.

3. Вихідні дані до роботи

3.1 Об'єкт дослідження – промисловий інтернет речей

3.2 Предмет дослідження – процес обміну повідомленнями в мережі інтелектуальних пристроїв

3.3 Зв'язок з пристроями IoT за допомогою модуля LoRa

3.4 Основа шлюзу – Raspberry Pi

4. Перелік питань, що потрібно опрацювати в роботі

4.1 Вступ

4.2 Огляд літератури за темою атестаційної роботи

4.3 Математичні методи оцінки пропускну здатності шлюзу IoT мережі

4.4 Моделювання та вибір оптимальних параметрів роботи шлюзу IoT

4.5 Експериментальні дослідження

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Демонстраційний матеріал представлений у форматі презентації PowerPoint (*.ppt) – 17 с. формату А4

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування Розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	Дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Провести аналіз завдання	05.10.2020	Виконано
2	Провести огляд літературі за темою роботи	11.10.2020	Виконано
3	Провести аналіз існуючих рішень	17.10.2020	Виконано
4	Провести моделювання та підбір компонентів	6.11.2020	Виконано
5	Провести проведення експерименту	25.11.2020	Виконано
6	Оформлення атестаційної роботи	05.12.2020	Виконано
7	Подання роботи в ЕК	07.12.2020	Виконано

Дата видачі завдання __02__ __11__ 2020 р.

Студент _____
(підпис)

Керівник роботи _____
(підпис)

проф. Нефьодов Л.І.
(посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 96 с., 11 табл., 35 рис., 2 дод., 21 джерел.

ІОТ, LORAWAN, RESTFUL, ІНТЕРНЕТ РЕЧЕЙ, МОДЕЛЮВАННЯ,
ШЛЮЗ, ПРОМИСЛОВІСТЬ.

Об'єкт дослідження – процес обміну повідомленнями в мережі інтелектуальних пристроїв.

Предмет дослідження – промисловий інтернет речей.

Мета магістерської роботи – розробка методики вибору оптимального режиму роботи апаратного забезпечення для організації взаємодії між компонентами бездротової мережі промислового Інтернету речей.

Методи дослідження – математичні методи розрахунку, емпіричний метод спостереження, експеримент, аналіз даних.

В роботі проведено аналіз існуючих типів мереж промислового інтернету речей, та їх областей застосування. Розглянуто особливості комунікаційних можливостей шлюзів. Було проведено моделювання та вибір оптимальних параметрів роботи шлюзу IoT, за допомогою інструментів LoRa Modem Calculator, Channel Activity Detection було виявлено, що параметри описані у третьому розділі найбільше відповідають вимогам розробляемого макету.

Побудований IoT пристрій на модулі SX-1278, в отриманих результатів були досягнути задані значення конфігурації модуля LoRa, що відповідають оптимальному режиму прийому/передавання даних які були отримані в розділі моделювання.

Результати магістерської атестаційної роботи висвітлені в збірнику студентських наукових статей ADED-2020 [1].

ABSTRACT

Explanatory note: 92 pages, 11 tables, 35 figures, 2 appendix, 21 sources.

IOT, LORAWAN, RESTFUL, INTERNET OF THINGS, SIMULATION
GATEWAY, INDUSTRY.

The object of research is the IoT gateway.

The subject of research is the process of exchanging messages in a network of intelligent devices.

The purpose of the master's thesis is to develop hardware and software for the organization of interaction between the components of the wireless network of the industrial Internet of Things.

Research methods - mathematical methods of calculation, empirical method of observation, experiment, data analysis.

The paper analyzes the existing types of industrial Internet of Things, and their areas of application. Features of communication possibilities of gateways are considered. Modeling and selection of optimal parameters of the IoT gateway was performed, using the tools LoRa Modem Calculator, Channel Activity Detection it was found that the parameters described in the third section best meet the requirements of the developed layout. The IoT device on the SX-1278 module is constructed, in the received results the set values of a configuration of the LoRa module corresponding to an optimum mode of reception / data transmission which were received in the simulation section were reached.

The results of the master's certification work are covered in the collection of student scientific articles ADED-2020 [1].

ЗМІСТ

Перелік скорочень	8
Вступ.....	9
1 Огляд літератури за темою атестаційної роботи.....	11
1.1 Класифікація бездротових мереж в залежності від об'єму інформації, що передається	11
1.2 Порівняння протоколів обміну повідомленнями в мережі інтелектуальних пристроїв	13
1.3 Аналіз функціонального призначення шлюзу ІОТ пристроїв.....	21
1.4 Висновки по розділу	27
2 Математичні методи оцінки пропускної здатності шлюзу іот мережі	28
2.1 Аналіз архітектури промислової мережі інтелектуальних пристроїв	28
2.2 Опис методики розрахунку часу передавання пакету в мережі LoRaWAN.....	30
3 Моделювання та вибір оптимальних параметрів роботи шлюзу ІоТ	39
3.1 Опис принципу організації обміну повідомленнями за допомогою модулів LoRa.....	39
3.3 Результати моделювання та вибір оптимальних параметрів.....	50
3.4 Висновки по розділу	63
4 Експериментальні дослідження	65
4.1 Розробка структурної схеми макету.....	65
4.2 Результати експерименту	72
4.3 Висновки за розділом	82
5 Охорона праці	83
5.1 Аналіз умов праці на робочому місці	83

5.2 Промислова безпека в лабораторії	83
5.3 Виробнича санітарія в лабораторії	84
5.4 Пожежна безпека лабораторії	86
Висновки	87
Перелік джерел посилань	90
Додаток А Текст підпрограми виведення поточних значень налаштування модуля LoRa.....	93
Додаток б Демонстраційний матеріал	97

ПЕРЕЛІК СКОРОЧЕНЬ

ІТ – інформаційні технології;

ОТ – операційні технології;

АМQR – протокол кадрування та передачі;

CoAP – протокол, який використовує шаблон спілкування запит-відповідь;

IoT (Internet of things) – концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека;

LoRa (Long Range) – протокол широкополосної мережі низької потужності (LoRaWAN), розроблений Semtech та заснований на методах модуляції розширеного спектру, отриманих із технології розширення спектру чірпінгу.

ВСТУП

IoT-пристрої дозволяють в режимі реального часу спостерігати за роботою виробничих ліній, виявляти проблеми, отримувати інформацію про необхідні профілактичні заходи та обслуговуванні. Щоб об'єднані в мережу пристрої працювали ефективно і генерували потрібну для аналітики інформацію, підприємство повинно забезпечити зв'язаність своїх операцій і машин. Тобто операційні технології (OT) повинні функціонувати узгоджено з інформаційними (IT), а обладнання повинно бути підключено до людиномашинного інтерфейсу, щоб фахівці могли працювати з інформацією.

В промисловості використовується різноманітне обладнання, яке потребує окремі канали зв'язку для обміну інформацією. В залежності від типу обладнання та сфери застосовування мережею передається різний об'єм даних. В залежності від типу мережі використовуються певне обладнання. В мережах з високим навантаженням та великим об'ємами даних використовуються шлюзи, роутери, маршрутизатори.

Шлюзи в мережах IoT забезпечують підключення пристроїв і аналітику даних, що надходять до пристроїв IoT, які в як правило не мають цих можливостей. Будь-шлюз може використовувати IoT модулі для виконання аналізу або попередньої обробки перед передачею повідомлень від підлеглих пристроїв в центр Інтернету речей.

Таким чином, розробка шлюзу для мережі пристроїв за технологією IoT є актуальною задачею для сучасного виробництва. Об'єкт дослідження – процес обміну повідомленнями в мережі інтелектуальних пристроїв.

Предмет дослідження – промисловий інтернет речей.

Мета магістерської роботи – розробка методики вибору оптимального режиму роботи апаратного забезпечення для організації взаємодії між компонентами бездротової мережі промислового Інтернету речей.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

- дослідити існуючі протоколи обміну повідомленнями в мережі інтелектуальних пристроїв;
- виконати аналіз функціонального призначення шлюзу IoT пристроїв;
- обрати апаратну платформу для реалізації шлюзу Інтернету речей;
- розробити архітектуру взаємодій між компонентами промислової мережі та алгоритм управління засобами організації зв'язку;
- розробити дослідний зразок;
- провести експериментальне дослідження сумісного використання шлюзу та учбових макетів промислового обладнання;
- оформити магістерську атестаційну роботу згідно ДСТУ 3008:2015 [2], а також з методичними вказівками з розробки й оформлення магістерської атестаційної роботи другого (магістерського) рівня вищої освіти галузі знань 15 «Автоматизація та приладобудування» за спеціальністю 151 «Автоматизація та комп'ютерно-інтегровані технології» [3].

1 ОГЛЯД ЛІТЕРАТУРИ ЗА ТЕМОЮ АТЕСТАЦІЙНОЇ РОБОТИ

1.1 Класифікація бездротових мереж в залежності від об'єму інформації, що передається

В промисловості використовується різноманітне обладнання, яке потребує окремі канали зв'язку для обміну інформацією. В залежності від типу обладнання та сфери застосовування, мережею передається різний об'єм даних [4]. В таблиці 1.1 наведено приклади використання бездротових мереж різними програмними засобами.

Таблиця 1.1 – Класифікація бездротових мереж за типом повідомлень, що передаються

Тип повідомлення, що передається	Об'єм інформації, що передається	Приклад застосування
1. Потік даних, потоківідео	Великий (Мегабайти)	Управління технологічним обладнанням в реальному часі, моніторинг стану технологічного процесу, інтелектуальні системи відеоспостереження

Кінець таблиці 1.1

Тип повідомлення, що передається	Об'єм інформації, що передається	Приклад застосування
2. JSONповідомлення, текстові дані	Середній (Кілобайти)	Охоронні системи, система розумного будинку
3. Фрагменти кадру повідомлення, стан обладнання.	Малий (байти)	Системи обліку споживаних енергоресурсів, системи охоронної сигналізації, система розумного будинку

Як можна бачити з таблиці 1.1 за типом повідомлень, що передаються, можна виділити три типи мереж, що використовуються в промисловості.

Перший тип мережі – передаються великі потоки даних. Це може бути потоки відео, безперервні потоки даних, що отримані від промислового обладнання, телеметрія. Такі мережі використовуються в управлінні технологічним обладнанням в реальному часі, моніторинг стану технологічного процесу, інтелектуальні системи відеоспостереження.

Другий тип мережі – передаються текстові повідомлення, так звані JSON-повідомлення в яких міститься інформація, що отримана в процесі роботи промислового обладнання. Зазвичай, об'єм такої інформації складає декілька кілобайт даних. Такі мережі використовуються в інтелектуальних охоронних системах, система розумного будинку, промисловій автоматизації в разі виконання функції віддаленого налаштування обладнання.

Третій тип мережі – передаються дуже короткі повідомлення. Об'єм даних становить кілька байт інформації. Наприклад, це може бути команда ввімкнення освітлення, або відключення датчика, що спрацював. Такі мережі

використовуються в системі обліку споживаних енергоресурсів, системі охоронної сигналізації, системі розумного будинку.

1.2 Порівняння протоколів обміну повідомленнями в мережі інтелектуальних пристроїв

1.2.1 Протокол CoAP

Перший, та найбільш популярний протокол CoAP – це протокол, який використовує шаблон спілкування запит-відповідь. Це спеціалізований протокол веб-передачі для використання в пристроях з обмеженими вузлами та обмеженими (наприклад, малопотужними) мережами. Вузли часто мають 8бітові мікроконтролери з невеликою кількістю ПЗУ та оперативної пам'яті. Мережі, в яких використовується цей протокол є малопотужними бездротовими середовищами передачі даних, які часто мають високу частоту помилок пакетів і типову пропускну здатність 10 с Кбіт/с. Протокол призначений для додатків, що працюють без втручання людини, наприклад, при передаванні даних від машини до машини. Застосуванням таких мереж як правило є інтелектуальна енергетика та автоматизація будівель [5].

Протокол CoAP забезпечує модель взаємодії запит/відповідь між кінцевими точками додатків, підтримує вбудоване виявлення служб та ресурсів, а також включає ключові концепції Інтернету, такі як URI та типи носіїв Інтернету. CoAP розроблений для легкої взаємодії з HTTP та для інтеграції інтелектуальних пристроїв з Інтернетом. Також, даний протокол відповідає таким спеціальним вимогам, як підтримка багатоадресна передача інформації, дуже низькі накладні витрати на впровадження та простота використання для вбудованих систем.

1.2.2 Протокол AMQP

Розширений протокол черги повідомлень (AMQP), як і MQTT, використовує шаблон спілкування «публікація-передплата» [6]. AMQP – це протокол кадрування та передачі. Термін «кадр» означає, що він забезпечує структуру для двійкових потоків даних, які протікають в будь-якому напрямку мережевого з'єднання. Структура повідомлення забезпечує розмежування для окремих блоків даних, які називаються кадрами, для обміну між підключеними сторонами. Можливості передачі гарантують, що обидві сторони, що спілкуються, можуть налагодити спільне розуміння того, коли кадри повинні бути передані, а коли передача вважатиметься завершеною.

Протокол може бути використаний для симетричного однорангового зв'язку, для взаємодії з посередниками повідомлень, які підтримують черги та публікують дані, або підписуються на зміни цих даних.

На рисунку 1.1 показано приклад, коли запит від клієнту А не підтверджено.



Рисунок 1.1 – Приклад, коли запит від клієнту А не підтверджено

На рисунку 1.2 показано, як реалізовано випадок, коли запит від клієнту підтверджується.

Протокол AMQP 1.0 [6] розроблений таким чином, щоб його можна було розширювати, додаючи додаткові специфікації для покращення його можливостей. Наприклад, для організації зв'язку через існуючу інфраструктуру HTTPS використовується технологія WebSockets, але для налаштування з'єднання через TCP протокол AMQP може бути досить складним, тому використовується специфікація з'єднання, що визначає, як підключати AMQP через WebSockets.



Рисунок 1.2 – Випадок, коли запит від клієнту підтверджується

Для взаємодії з інфраструктурою обміну повідомленнями у спосіб запит-відповідь для цілей управління або для забезпечення розширених функціональних можливостей, специфікація управління AMQP визначає необхідні базові примітиви взаємодії.

Для інтеграції моделі авторизації, специфікація забезпечення безпеки протоколу AMQP визначає, як пов'язувати та поновлювати маркери авторизації, які пов'язані із посиланнями.

Приклад запиту в форматі протоколу AMQP показано на рисунку 1.3.

```
{  
  "headerMapping": {  
    "amqp.application.property:to": "{{ header:reply-to }}"  
  }  
}
```

Рисунок 1.3 – Приклад запиту в форматі протоколу AMQP

З наведеного прикладу можна побачити заголовок та тіло самого запиту, що передається.

1.2.3 Протокол STOMP

STOMP – це фреймовий протокол за зразком HTTP [7]. Кадр складається з команди, набору необов’язкових заголовків та необов’язкового тіла. STOMP заснований на тексті, але також дозволяє передавати двійкові повідомлення. Кодування за замовчуванням для STOMP – UTF-8, але воно підтримує специфікацію альтернативних кодувань для тіл повідомлень.

Сервер STOMP змодельований як набір пунктів призначення, куди можна надсилати повідомлення. Протокол STOMP розглядає місця призначення як непрозорі рядки, а їх синтаксис залежить від реалізації сервера. Крім того, STOMP не визначає, якою має бути семантика доставки пунктів призначення. Семантика доставки, або “обміну повідомленнями”, може змінюватися від сервера до сервера і навіть від пункту до пункту призначення. Це дозволяє серверам проявляти творчість із семантикою, яку вони можуть підтримувати за допомогою STOMP.

Клієнт STOMP – це користувальницький агент, який може діяти у двох (можливо, одночасному) режимах:

- як виробник інформації, надсилаючи повідомлення до місця призначення на сервері через кадр SEND;
- як споживач інформації, надсилаючи кадр SUBSCRIBE для даного пункту призначення та отримуючи повідомлення від сервера як кадри MESSAGE.

STOMP розроблений як полегшений протокол, який легко реалізувати як на клієнтській, так і на серверній частині широким колом мов. Це, зокрема, означає, що існує не так багато обмежень на архітектуру серверів, і багато функцій, таких як іменування призначення та семантика надійності, специфічні для реалізації.

1.2.4 Протокол MQTT

MQTT – це один із найбільш часто використовуваних протоколів, що засовується в IoT [8]. MQTT дозволяє обмеженим ресурсами пристроям IoT надсилати або публікувати інформацію про певну подію на сервер, який функціонує як посередник повідомлень MQTT. Далі, брокер передає інформацію тим клієнтам, які раніше підписалися на ту, або іншу тему. Для оператора така тема виглядає, як ієрархічний шлях до файлу. Клієнти можуть підписатися на певний рівень ієрархії теми або використовувати спеціальний символ, щоб підписатись на кілька рівнів.

MQTT не залежить від формату даних, що передається. Повідомлення може містити будь-який тип даних, тому і видавці, і передплатники повинні розуміти і погоджувати формат даних. Можна надсилати текстові повідомлення, дані зображення, звукові дані, зашифровані дані, двійкові дані, об'єкти або практично будь-яку іншу структуру в повідомленні. В IoT

текстові і двійкові дані є найбільш поширеними типами даних в повідомленнях.

MQTT також є асиметричним протоколом, тоді як HTTP – це несиметричний протокол [9]. Наприклад, один пристрій повинен зв'язуватися з другим пристроєм. Асиметричний протокол між пристроями вимагає, щоб протокол використовувала тільки одна сторона, проте вся інформація, необхідна для повторного складання пакетів, повинна міститися в заголовку фрагментації, надісланому першому пристрою. В асиметричних системах є один ведучий і один ведений пристрій. У симетричному протоколі обидва пристрої можуть брати на себе роль ведучого або веденого.

MQTT може зберігати повідомлення в брокера необмежено довго. Цей режим роботи управляється прапором при нормальній передачі повідомлення. Збережене на сервері повідомлення відправляється будь-якому клієнту, який підписується на цю тематичну гілку MQTT. Повідомлення негайновідправляється новому клієнту. Це дозволяє новому клієнтові отримати статус або сигнал з теми, на яку він недавно підписався, без очікування. Як правило, якщо клієнт, підписується на тему, то він може очікувати години або навіть дні, перш ніж клієнт опублікує нові дані.

На рисунку 1.4 показано приклад взаємодії пристроїв за допомогою протоколу MQTT.

1.2.5 Обґрунтування обирання протоколу

Треба зазначити, що альтернативою машинного протоколу є, так званий, RESTful-протокол, який не був представлений в наведеному аналізі. У моделі RESTful сервер володіє станом ресурсу, але стан не передається в повідомленні від клієнта на сервер. RESTful використовує HTTP-методи, такі як GET, PUT, POST і DELETE для розміщення запитів по універсальному

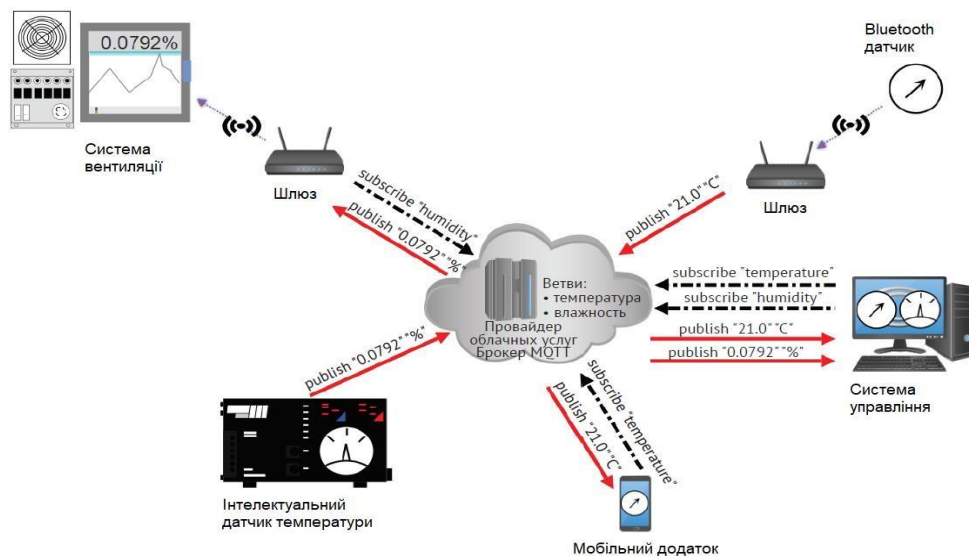


Рисунок 1.4 – Приклад взаємодії пристроїв за допомогою протоколу MQTT

ідентифікатором ресурсу (URI) [9]. У цій архітектурі не потрібно брокер або посередник. Оскільки вони засновані на стеку HTTP, вони користуються більшістю вбудованих сервісів, таких як безпека HTTPS. Проекти RESTful типові для клієнт-серверних архітектур. Клієнти ініціюють доступ до ресурсів через синхронні шаблони запиту-відповіді. Крім того, вони самі несуть відповідальність за помилки, навіть якщо сервер не відповідає на запити.

Розглянемо для прикладу рисунок 1.5 на якому показана діаграма взаємодії пристроїв IoT в традиційному варіанті «публікація-передплата» в порівнянні з сервісом RESTful.

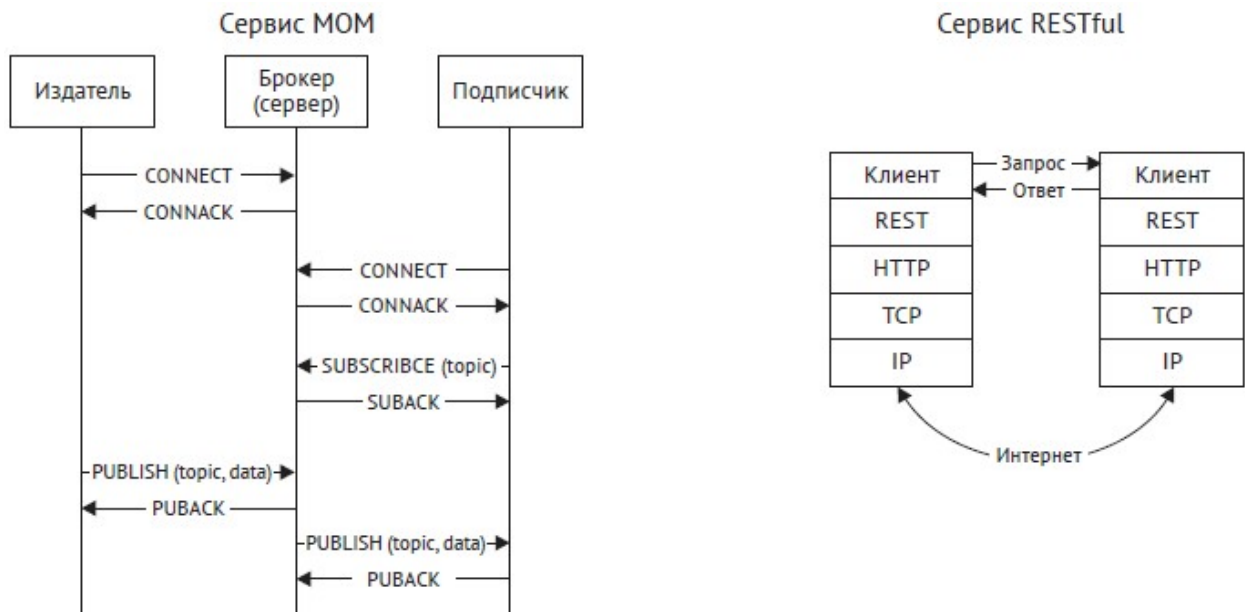


Рисунок 1.5 – Порівняння протоколів IoT

На рисунку 1.5 зліва показано приклад обміну повідомленнями (на основі MQTT), який використовує брокерський сервер, видавців і передплатників подій. Декілька клієнтів можуть виступати в ролі видавців повідомлень, в той же час, вони можуть бути й передплатниками, інформація може зберігатися або не зберігати в черзі для швидкого відновлення.

Справа на рисунку 1.5 показано приклад протоколу RESTful, де архітектура побудована на HTTP і використовує HTTP-принципи для зв'язку клієнт з сервером.

Після виконання аналізу існуючих протоколів для організації обміну повідомленнями в мережі інтелектуальних пристроїв можна обрати один варіант, який задовольняє нашим вимогам:

- наявність інструментів для розгортання серверу в лабораторних умовах;
- можливість роботи з простими пакетами даних в мережах з невеликим обсягом інформації, що передається;
- простий в реалізації;

– наявність бібліотек та приладів для Arduino, або STM32 в широкому доступі.

Більшості з цих вимог задовольняють практично всі розглянуті протоколи, але останній пункт дав змогу виділити лідера серед претендентів.

Таким виявився протокол MQTT. Даний протокол дуже широко використовується для підключення контролерів Arduino до мережі IoT пристроїв. В вільному доступі є бібліотеки на мові програмування C для використання в нашому проекті.

Для роботи з обраним протоколом є сервер Mosquitto, який виступає брокером MQTT з відкритим кодом та має наступні переваги:

- простий в реалізації;
- дуже легкий і ефективний з точки зору пропускну здатності;
- не залежить від платформи реалізації;
- постійно відстежує сеанс зв'язку;
- є рішення безпеки даних, що передаються.

1.3 Аналіз функціонального призначення шлюзу IoT пристроїв

1.3.1 Призначення шлюзів в мережах IoT пристроїв

Шлюзи в мережах IoT забезпечують підключення пристроїв і аналітику даних, що надходять до пристроїв IoT, які в як правило не мають цих можливостей [10].

Існує три шаблону використання пристрою IoT в якості шлюзу: прозорість, перетворення протоколу і перетворення посвідчення.

Основна відмінність між шаблонами полягає в тому, що прозорий шлюз передає повідомлення між підлеглими пристроями і центром Інтернету речей, не вимагаючи додаткової обробки. Однак перетворення протоколу і

перетворення фрагментів підтвердження вимагає обробки цих даних шлюзом для забезпечення взаємодії між пристроями.

Будь-шлюз може використовувати IoT модулі для виконання аналізу або попередньої обробки перед передачею повідомлень від підлеглих пристроїв в центр Інтернету речей.

1.3.2 Прозорий шаблон

У шаблоні прозорого шлюзу пристрою, які теоретично можуть підключатися до центру Інтернету речей, можуть підключатися до пристрою шлюзу. Підлеглі пристрої мають власні сертифікати Центру Інтернету речей і використовують будь-який з протоколів MQTT, AMQP або HTTP. Шлюз просто забезпечує взаємодію між пристроями і Центром Інтернету речей.

На рисунку 1.6 показано принцип роботи шлюзу в форматі «Прозорий шаблон».

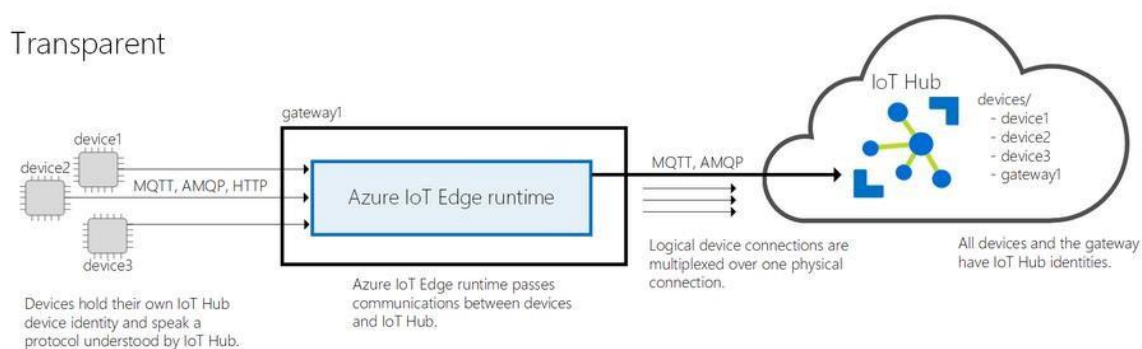


Рисунок 1.6 – Принцип роботи шлюзу в форматі «Прозорий шаблон»

Пристрої і користувачі, які взаємодіють з ними через центр Інтернету речей, не знають, що шлюз обробляють їх зв'язок. Відсутність обізнаності означає, що шлюз вважається прозорим.

1.3.3 Шаблон перетворення протоколу

Шлюз перетворення протоколів також називається непрозорим шлюзом на відміну від шаблону прозорого шлюзу. У цьому шаблоні пристрої, які не підтримують MQTT, AMQP або HTTP, можуть використовувати пристрій шлюзу для відправки даних в центр Інтернету речей від їх імені.

Шлюз розуміє протокол, який використовується підлеглими пристроями, і є єдиним пристроєм з посвідченням в Центрі Інтернету речей.

Вся інформація виглядає так, ніби вона надходить з одного пристрою, шлюзу.

Підлеглі пристрої повинні вбудовувати в повідомлення додаткову ідентифікаційну інформацію, якщо хмарним додатком потрібно аналізувати дані для кожного пристрою окремо. Крім того, примітиви Центру Інтернету речей, такі як двійники і методи, доступні тільки для пристроїв шлюзу (для підлеглих пристроїв вони недоступні).

На рисунку 1.7 показано принцип роботи шлюзу в форматі «Перетворення протоколу».

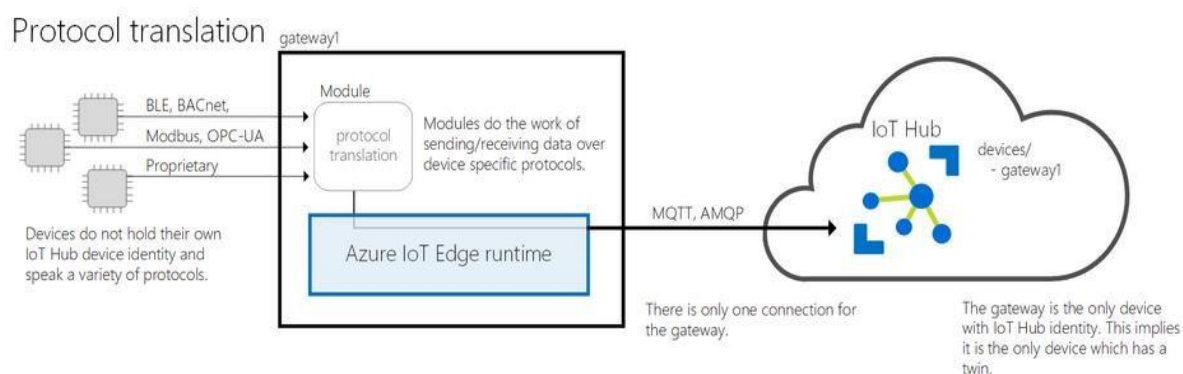


Рисунок 1.7 – Принцип роботи шлюзу в форматі «Перетворення протоколу»

1.3.4 Шаблон трансляції посвідчень

У шаблоні шлюзу перетворення посвідчень пристрої, які не можуть підключитися до центру Інтернету речей, можуть підключатися до пристрою шлюзу. Шлюз надає посвідчення Центру Інтернету речей і забезпечує перетворення протоколу від імені підлеглих пристроїв. Шлюз розпізнає протокол, який використовується підлеглими пристроями, надає посвідчення і перетворює примітиви центру Інтернету речей. Підлеглі пристрої відображаються в центрі Інтернету речей як пристрої першого класу з двійниками і методами.

На рисунку 1.8 показано принцип роботи шлюзу в форматі «Трансляції посвідчень».

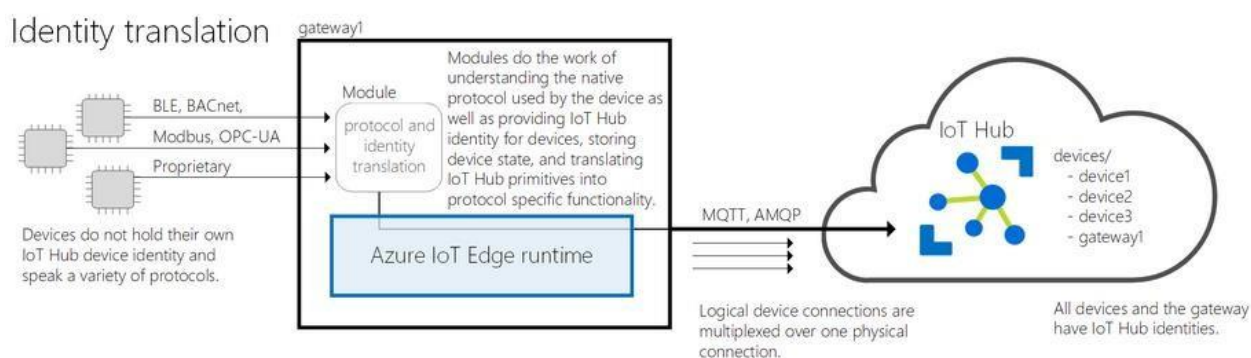


Рисунок 1.8 – Принцип роботи шлюзу в форматі «Трансляції посвідчень»

Для цього шаблону потрібні модулі користувача або сторонні модулі, які часто відносяться до обладнання, що використовується, або протоколу.

1.3.5 Приклади використання

Розглянуті варіанти реалізації шлюзу надають такі переваги:

— аналітика на прикордонному рівні. Служби штучного інтелекту використовуються локально для обробки даних, що надходять від

нижчестоящих пристроїв. В даному випадку дані телеметрії не відправляються відразу на сервер, а спочатку оброблюються;

- ізоляція підлеглого пристрою. Пристрій шлюзу може забезпечити всім підлеглим пристроям безпеку в Інтернеті. Воно може знаходитися між мережею інтелектуальних пристроїв без можливості підключення і ІТмережею, яка забезпечує доступ до Інтернету;

- мультиплексування підключення. Всі пристрої, що підключаються до Серверу Інтернету речей через шлюз IoT, будуть використовувати такі самі параметри базового підключення;

- згладжування трафіку – пристрій IoT буде автоматично виконувати необхідну затримку передачі даних, якщо Центр Інтернету речей регулює трафік, при цьому повідомлення зберігаються локально. Ця перевага робить рішення стійким до пік трафіку;

- автономна підтримка. Пристрій шлюзу зберігає повідомлення та оновлення двійника, які не можуть бути доставлені в центр Інтернету речей.

Шлюз, який виконує перетворення протоколу, може підтримувати існуючі пристрої і нові пристрої, обмежені ресурсами. Багато існуючих пристроїв виробляють дані, які можуть надати бізнес-аналітику, однак вони не були розроблені з урахуванням можливості підключення до хмари. Непрозорі шлюзи дозволяють розблокувати ці дані і використовувати їх в рішенні IoT.

Шлюз, який перетворює посвідчення, надає переваги перетворення протоколу і додатково дозволяє повністю управляти підлеглими пристроями з хмари. Всі пристрої мережі Інтернету речей відображаються в Центрі Інтернету речей незалежно від протоколу, який використовується.

На рисунку 1.9 показано принцип підключення шлюзу PoT типу SmartLink HW-DP для поєднання промислової мережі з хмарним сервером.

Шлюз IoT підключається до застарілих мереж, забезпечуючи підключення існуючого промислового обладнання до Індустрії 4.0.

Підключати можна пристрої PROFIBUS та HART до HART IP, OPC UA, MQTT та FDT / DTM.

SmartLink HW-DP забезпечує незалежний від PLC доступ до мереж PROFIBUS DP. Це забезпечує управління промисловим обладнанням для пристроїв автоматизації із використанням стандартних галузевих інструментів та дозволяє використовувати HART IP як стандартизований формат передавання даних. SmartLink HW-DP – це компактний інструмент, який можна інтегрувати до вже існуючих технологічних установок. Таким чином, це забезпечує підключення хмарних обчислювальних серверів до нових та існуючих мереж PROFIBUS DP.

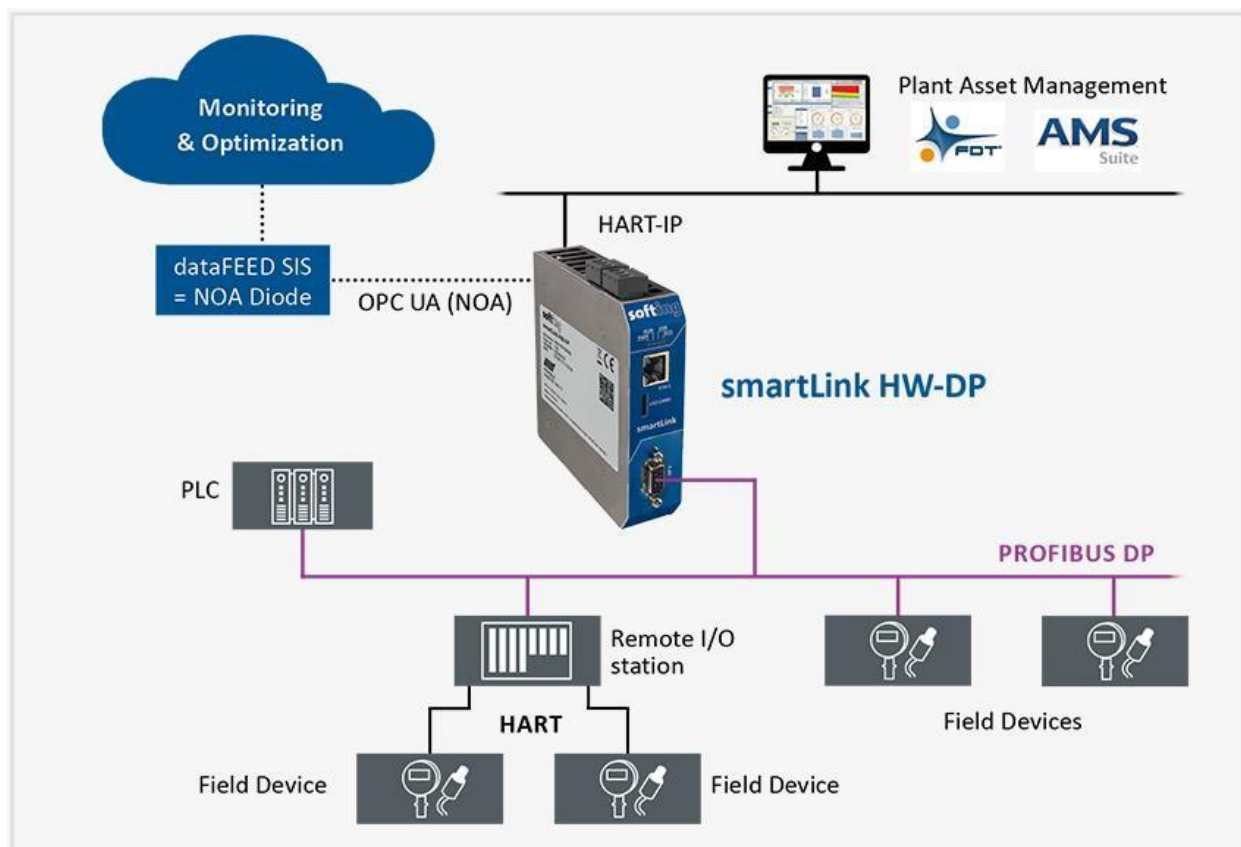


Рисунок 1.9 – Принцип підключення шлюзу IoT типу SmartLink HW-DP для поєднання промислової мережі з хмарним сервером

1.4 Висновки по розділу

Провівши аналіз технологій поєднання існуючого промислового обладнання з новими сучасними технологіями хмарних обчислень визначені основні компоненти для побудови мережі інтелектуальних пристроїв за концепцією Індустрії 4.0.

Проведено порівняння протоколів обміну повідомленнями в мережі інтелектуальних пристроїв та виявлені переваги та недоліки основних претендентів на використання в якості інструменту передавання даних на хмарний сервер. Таким протоколом виявився MQTT та сервер Mosquitto.

Для побудови шлюзу в якості платформи будемо використовувати одноплатний комп'ютер Raspberry PI з операційною системою Linux в якості базової операційної системи.

В наступному розділі роботи необхідно розробити архітектуру промислової мережі та принцип організації взаємодії в IoT мережі.

2 МАТЕМАТИЧНІ МЕТОДИ ОЦІНКИ ПРОПУСКНОЇ ЗДАТНОСТІ ШЛЮЗУ ІОТ МЕРЕЖІ

2.1 Аналіз архітектури промислової мережі інтелектуальних пристроїв

Мережа IoT (Internet of Things, українською «Інтернет речей») – екосистема різноманітних, не пов'язаних між собою пристроїв, які не втручаються в роботу один одного і існують для збору та передачі великого спектру даних [11]. Головною умовою для їхнього успішного функціонування є єдиний протокол передачі даних. Найвідомішими IoT протоколами у світі можна назвати Bluetooth, Wifi, Zigbee, MQTT, NFC, DDS, LTE та LoRaWAN.

LoRaWAN – один з найпопулярніших стандартів передачі даних в мережах широкого радіусу дії з низьким рівнем енергоспоживання пристроїв (Low Power Wide Area Network, LPWAN). Його популяризацією займається міжнародна некомерційна організація LoRa Alliance, ключову роль в якій грають французька компанія Semtech, IBM і Cisco. Вони стоять біля самих витоків появи протоколу LoRaWAN.

Стандарт LoRaWAN є відкритим. Одним з головних його переваг є висококонкурентний ринок постачальників обладнання та сумісність пристроїв від різних виробників (до сервера можна підключити базові станції декількох брендів, а в мережу – увімкнути пристрої відразу декількох вендорів).

На рисунку 2.1 показано принцип організації взаємодії в IoT мережі. У мережі LoRaWAN кінцеві пристрої (радіомодулі) направляють дані на концентратор (шлюз, базова станція). Від базової станції по швидкісному

каналу пакети даних передаються на сервер, який, в свою чергу, віддає конкретний тип даних відповідному серверу додатків [11].

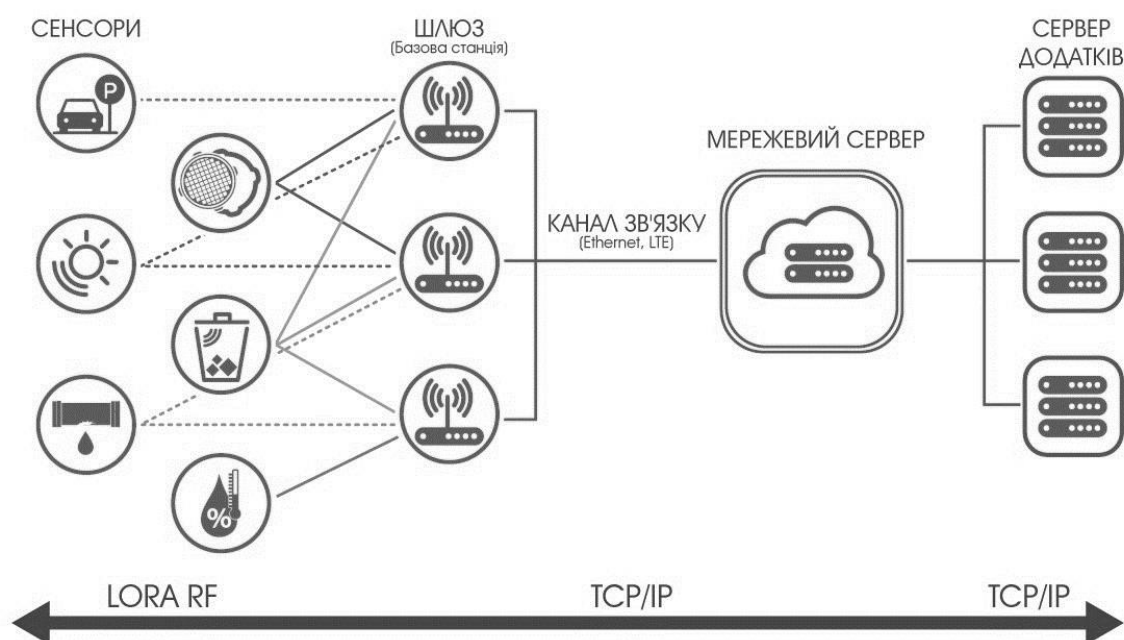


Рисунок 2.1 – Принцип організації взаємодії в IoT мережі

У LoRa виділяють 3 класи пристроїв за енергоспоживанням:

- А-клас – найекономніший. Пристрої цього класу живляться від батареї декілька років, що досягається за рахунок активності пристрою тільки під час передачі даних за програмованим розкладом;
- С-клас, навпаки, постійно знаходиться у стані прийому. Саме тому в пристроїв класу С не передбачається живлення від батарейок;
- В-клас, більшу частину часу В-клас, як і А-клас, перебуває в режимі енергозбереження, але при цьому має деякі можливості для взаємодії з сервером, що притаманні для С-класу.

LoRaWAN використовує неліцензовану частину радіочастотного спектру в діапазоні 868,0 МГц – 868,6 МГц (в Україні). Стандарт передбачає

наявність базових станцій і абонентських пристроїв, які, за умови автономного живлення, більшу частину часу перебувають в режимі збереження енергії. Пристрої «прокидаються» лише для обміну даними з сервером.

2.2 Опис методики розрахунку часу передавання пакету в мережі LoRaWAN

Одна з головних задач при проектуванні шлюзу промислової мережі – це оптимізація часу передавання пакетів від сенсорів до мережевого сенсору та отримання зворотної відповіді.

Кожен пакет, що передається по $n_{preamble}$ мережі LoRaWAN, включає в себе преамбулу і блок даних фізичного рівня. Кількість символів в преамбулі є конфігурованим в діапазоні 0...65535.

Кількість символів в блоці даних фізичного рівня визначається наступною формулою (2.1) [12]:

$$payloadSymbNb = 8 + \text{ceil} \left(\frac{8 \cdot PL - 4 \cdot SF + 28 + 16 \cdot CRC - 20 \cdot H}{4 \cdot (SF - 2 \cdot DE)} \right) \cdot (CR + 4) \quad , (2.1)$$

де $PL = 12 + FRM$ – кількість байт корисних даних в блоці фізичного рівня (PHYPayload);

FRM – кількість байт корисних даних на рівні додатку (FRMPayload);

SF – коефіцієнт розширення спектра;

$CRC = 1$, коли передача поля CRC блоку корисного навантаження включена і $CRC = 0$ – коли вимкнена;

$H = 0$, коли передача заголовка (PHDR + PHDR_CRC) включена і $H = 1$ – коли заголовок відсутній;

$DE = 1$, коли оптимізація для низьких швидкостей передачі включена і $DE = 0$ – коли вимкнена (для $SF = 11$ і $SF = 12$ оптимізація швидкостей передачі повинна бути включена);

$CR = 1..4$ – швидкість коду;

$ceil$ – операція округлення до найближчого більшого цілого числа.

Тривалість передачі преамбули можна визначити за формулою (2.2):

$$T_{preamble} = (n_{preamble} + 4,25) \cdot T_{sym}, \quad (2.2)$$

де $T_{sym} = \frac{2^{SF}}{W}$ – тривалість передачі одного символу;

W – смуга одного радіоканалу (125 кГц).

Тривалість передачі блоку даних фізичного рівня визначається за формулою (2.3):

$$T_{payload} = payloadSymNb \cdot T_{sym}. \quad (2.3)$$

Тривалість передачі всього пакету по мережі LoRaWAN визначається за формулою (2.4):

$$T_{packet} = T_{preamble} + T_{payload}, \quad (2.4)$$

В таблиці 2.1 наведена залежність тривалості передачі одного символу від коефіцієнту розширення спектра.

Таблиця 2.1 – Залежність тривалості передачі одного символу від коефіцієнту розширення спектра

SF	7	8	8	10	11	12
W, кГц	125	125	125	125	125	125
T _{sym} , мс	1,024	2,048	4,096	8,192	16,384	32,768

У таблиці 2.2 наведені результати розрахунку часу, необхідного для передачі одного UL-пакета (з корисним навантаженням 10 байт) між кінцевим пристроєм (EndNode) і сервером додатків (Application Server).

Таблиця 2.2 – Результати розрахунку часу, необхідного для передачі одного UL-пакета

Коефіцієнт розширення спектра	SF	7	8	9	10	11	12
Смуга радіоканалу	W, кГц	125	125	125	125	125	125
Тривалість передачі 1-го символу	T _{sym} , мс	1,024	2,048	4,096	8,192	16,384	32,768

Продовження таблиці 2.2

Кількість символів в преамбулі (6-65535)	<i>npreamble</i>	6	6	6	6	6	6
Корисні дані (FRMPayload)	<i>FRM, байт</i>	0	0	0	0	0	0
Фізичний блок даних (PHYPayload)	<i>PL, байт</i>	12	12	12	12	12	12
Прапор включення заголовка в пакет: 0 - включений, 1 - вимкнений	<i>H</i>	1	1	1	1	1	1
Прапор включення CRC в пакет: 1 - включений, 0 - вимкнено	<i>CRC</i>	1	1	1	1	1	1
Прапор включення оптимізації швидкостей: 1 - включена, 0 - виключена	<i>DE</i>	0	0	0	0	0	0

Кінець таблиці 2.2

Швидкість кодування: 1 - 4/5 2 - 4/6 3 - 4/7 - 4/8	CR	1	1	1	1	1	1
Кількість символів в блоці даних	$payloadSymNb$	28	23	23	18	23	18
Тривалість передачі преамбули	$T_{preamble}, мс$	10,50	20,99	41,98	83,97	167,94	335,87
Тривалість передачі блоку даних	$T_{payload}, мс$	28,67	47,10	94,21	147,46	294,91	589,82
Тривалість передачі всього пакету	$T_{packet}, мс$	39,17	68,10	136,19	231,42	462,85	925,70

Для підтвердження отримання пакету від кінцевого пристрою LoRaшлюз передає етикетки в DL-каналі.

У таблиці 2.3 наведені результати розрахунку часу, необхідного для передачі одного DL-пакета без поля FRMPayload.

Всі LoRaWAN пристрої класу "A", включаючи кінцеві пристрої, а також LoRa-шлюз, використовують довільний (не синхронізований) доступ до загального середовища передачі. При цьому тимчасові інтервали

відправки пакетів плануються кінцевими пристроями на основі власних потреб.

Таблиця 2.3 – Результати розрахунку часу, необхідного для передачі одного DL-пакета без поля FRMPayload

Коефіцієнт розширення спектра	SF	7	8	9	10	11	12
Смуга радіоканалу	W , кГц	125	125	125	125	125	125
Тривалість передачі 1-го символу	T_{sym} , мс	1,024	2,048	4,096	8,192	16,384	32,768
Кількість символів в преамбулі (6-65535)	$npreamble$	6	6	6	6	6	6
Корисні дані (FRMPayload)	FRM , байт	0	0	0	0	0	0
Фізичний блок даних (PHYPayload)	PL , байт	12	12	12	12	12	12
Прапор включення заголовка в пакет: 0 – включений, 1 – вимкнений	H	1	1	1	1	1	1

Продовження таблиці 2.3

Прапор включення CRC в пакет: 1 – включений, 0 – вимкнено	<i>CRC</i>	1	1	1	1	1	1
Прапор включення оптимізації швидкостей: 1 – включена, 0 – виключена	<i>DE</i>	0	0	0	0	0	0
Швидкість кодування: 1 – 4/5 2 – 4/6 3 – 4/7 4 – 4/8	<i>CR</i>	1	1	1	1	1	1
Кількість символів в блоці даних	<i>payloadSymNb</i>	28	23	23	18	23	18
Тривалість передачі преамбули	<i>T_{preamble}</i> , мс	10,50	20,99	41,98	83,97	167,94	335,87
Тривалість передачі блоку даних	<i>T_{payload}</i> , мс	28,67	47,10	94,21	147,46	294,91	589,82

Кінець таблиці 2.3

Тривалість передачі всього пакету	T_{packet} , мс	39,17	68,10	136,19	231,42	462,85	925,70
--	----------------------	-------	-------	--------	--------	--------	--------

Оцінка пропускної здатності системи [12] визначається при наступних припущеннях:

- призначені для користувача дані, призначені для передачі, надходять на термінали випадково, утворюючи пуассоновський потік;
- відкинуті через помилки передачі пакети передаються повторно, утворюючи також пуассоновський потік;
- всі пакети даних мають однакову довжину і передаються однаковий час;
- в мережі знаходиться нескінченне число віддалених терміналів (при цьому якщо якийсь термінал вже передає дані, це ніяк не впливає на ймовірність передачі даних іншими терміналами).

У цьому випадку ймовірність того, що за час передачі одного пакета T надійде ще k пакетів від всіх терміналів мережі визначається формулою Пуассона (2.5):

$$P_r(k) = \frac{G^k * e^{-G}}{k!}, \quad (2.5)$$

де G – інтенсивність надходження пакетів (або середнє число повідомлень для передачі, що з'явилося на всіх терміналах мережі за час T).

Колізія не виникне, якщо на інтервалі передачі повідомлення, а також на одному попередньому інтервалі не з'являться ще пакети для передачі від

інших кінцевих пристроїв мережі ($k = 0$). Отже, ймовірність успішної передачі становить:

$$P = e^{-2G}.$$

Середнє число успішно переданих за час T пакетів, тобто пропускна здатність мережі, становить:

$$S = G \cdot P = G \cdot e^{-2G}.$$

2.3 Висновки по розділу

В результаті виконання даного розділу магістерської атестаційної роботи проаналізовані вимоги до архітектури побудови мережі бездротових пристроїв за технологією IoT. Для поєднання з сенсорами мережі запропоновано використовувати модеми LoRaWAN для побудови а також LoRa-шлюза.

Наведено математичне обґрунтування методу розрахунку пропускної здатності шлюзу та показано, що максимальне значення пропускної здатності мережі досягається при інтенсивності надходження пакетів G дорівнює 0,5 і становить 0,184 (при цьому ймовірність втрати пакетів через колізію – P_{Loss} складе 63 %) [11]. Наведено методику розрахунку інтенсивності отримання пакетів та ймовірності втрати пакетів через колізії P_{Loss} .

3 МОДЕЛЮВАННЯ ТА ВИБІР ОПТИМАЛЬНИХ ПАРАМЕТРІВ РОБОТИ ШЛЮЗУ ІОТ

3.1 Опис принципу організації обміну повідомленнями за допомогою модулів LoRa

Для моделювання роботи шлюзу необхідно визначитися з принципом передачі пакетів. Від зміни параметрів модуля, що відповідають за режими передачі та прийому залежить загальний час передачі та споживана потужність. Змінюючи ці параметри можна обрати оптимальний режим роботи модуля LoRa для вирішення поставленої задачі та настроїти модуль на мінімальний рівень споживаної енергії, що забезпечить максимальний час роботи пристрою від автономного живлення.

Для організації обміну повідомленнями на фізичному рівні забезпечується передача блоків даних між кінцевим пристроєм (End Node) і шлюзом LoRa (Gateway).

На стороні передавального пристрою виконуються такі послідовні дії:

- прийом блоку даних від верхнього апаратного рівня (PHYPayload);
- формування фізичного заголовка пакета (PHDR + PHDR_CRC);
- кодування фізичного заголовка пакета (PHDR + PHDR_CRC) з фіксованою швидкістю 4/8;
- обчислення контрольної суми блоку корисних даних PHYPayload (CRC);
- кодування блоку корисних даних (PHYPayload + CRC) з попередньо встановленою швидкістю CR;
- передача по радіоканалу преамбули;
- модуляція і передача по радіоканалу фізичного блоку даних.

На стороні приймального пристрою виконується:

- виявлення преамбули і визначення початку фізичного блоку даних;
- демодуляція сигналу;
- декодування фізичного заголовка пакета (PHDR + PHDR_CRC) і перевірка його контрольної суми;
- декодування блоку корисних даних (PHYPayload + CRC) і перевірка його контрольної суми;
- підтвердження прийнятих даних (для відповідних типів повідомлень);
- передача даних на верхній рівень модуля для подальшого використання кінцевими пристроями.

Загальний вигляд пакету LoRa показано на рисунку 3.1 та складається з трьох елементів:

- преамбула;
- необов'язковий заголовок;
- корисне навантаження даних.

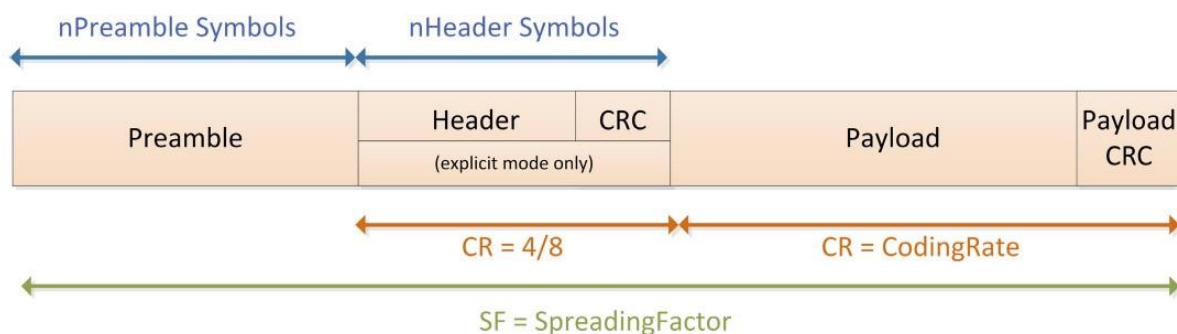


Рисунок 3.1 – Структура пакету даних пакета Lora

Преамбула використовується для синхронізації приймача з потоком вхідних даних. За замовчуванням пакет налаштований на послідовність 12 символів. Це програмована змінна, тому довжина преамбули може бути збільшена, наприклад, з метою зменшення робочого циклу приймача в

інтенсивних програмах прийому. Мінімальної довжини вистачає для будьякого спілкування. Довжину преамбули, що передається, можна змінити, встановивши регістр PreambleLength від 6 до 65535, отримуючи загальну довжину преамбули від $6 + 4$ до $65535 + 4$ символів. Це дозволяє передавати майже довільно довгу послідовність преамбули.

Далі ми будемо моделювати різні варіанти побудови пакету даних з метою визначення оптимального формату для конкретної задачі.

Приймач здійснює процес виявлення преамбули, який періодично перезапускається. З цієї причини довжина преамбули повинна бути налаштована ідентично довжині преамбули передавача. Якщо довжина преамбули невідома або може змінюватися, максимальна довжина преамбули повинна бути запрограмована на стороні приймача.

Залежно від обраного режиму роботи модуля Lora доступні два типи заголовків:

- explicit mode;
- implicit mode.

Тип заголовка вибирається бітом ImplicitHeaderModeOn, який знаходиться у реєстрі RegModemConfig1. На рисунку 3.1 показано приклад пакету даних в режимі explicit mode

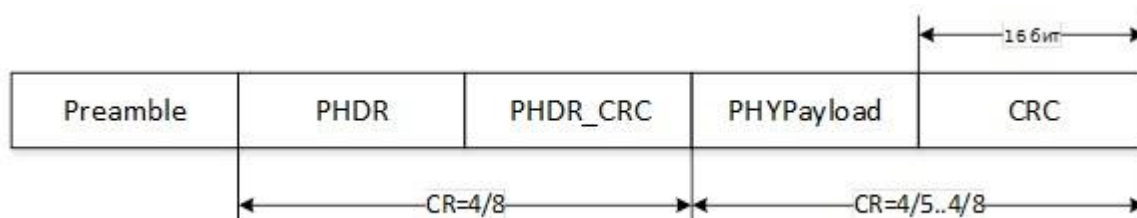


Рисунок 3.1 – Формат повідомлення explicit mode

На рисунку 3.1 Preamble – це преамбула, яка використовується для синхронізації приймача з вхідним потоком і визначення початку фізичного блоку даних. Довжина преамбули для SX1278 є програмованою величиною.

PHDR – фізичний заголовок пакета. Присутній тільки при використанні явного режиму (explicit mode) і містить:

- довжина поля даних (Payload) в байтах;
- частота виправлення кодів помилок;
- наявність додаткового 16-бітового CRC для поля даних.

У певних сценаріях, коли поле даних, швидкість кодування та наявність CRC фіксовані або відомі заздалегідь, може бути вигідно зменшити час передачі, викликаючи неявний режим заголовка. У цьому режимі заголовок видаляється з пакета. У цьому випадку довжина поля даних, швидкість кодування помилок і наявність CRC корисного навантаження повинні бути налаштовані вручну з обох сторін радіолінії.

PHDR_CRC – контрольна сума поля PHDR.

PHYPayload – корисне навантаження (блок даних, отриманий від рівня MAC або переданий на рівень MAC).

CRC – контрольна сума поля PHYPayload (опціональне поле).

При цьому заголовок PHDR кодується надлишковим кодом з фіксованою швидкістю 4/8; корисне навантаження - з програмованої швидкістю. На рисунку 3.2 показано приклад пакету даних в режимі implicit mode (неявний режим заголовка).

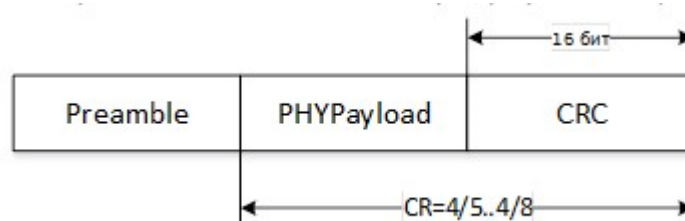


Рисунок 3.2 – Формат повідомлення implicit mode

При використанні неявного режиму (implicit mode) фізичний заголовок пакета не передається і пристрої працюють з попередньо встановленими параметрами.

На рисунку 3.3 показано випадок, коли поле контрольна сума (CRC) відсутнє.

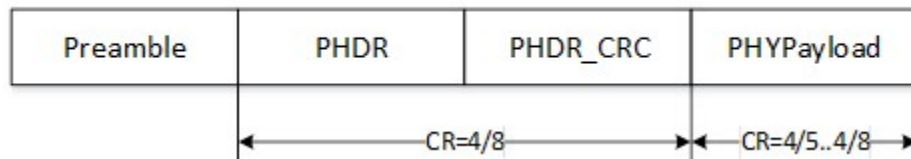


Рисунок 3.3 – Формат повідомлення з відсутнім полем CRC

Принцип функціонування детектора преамбули заснований на використанні узгодженого фільтра (СФ), чия імпульсна характеристика комплексно пов'язана з CSS радіосигналом в частотній області і має дзеркальне відображення його в часі [13]:

$$h(t) = A_1 \cdot \cos \left(\omega_n \cdot (T_{sym} - t) - \frac{\mu}{2} \cdot (T_{sym} - t)^2 \right), 0 \leq t < T_{sym} \quad (3.1)$$

де $T_{sym} = 2SF/BW$ – тривалість радіосигналу;

$\mu = \frac{BW}{T_{sym}}$ – швидкість зміни частоти радіосигналу;

t – час передавання одиниці даних;

ω_n – частота радіосигналу.

На рисунку 3.4 показано приклад передавання пакету даних на рівні модуляції.

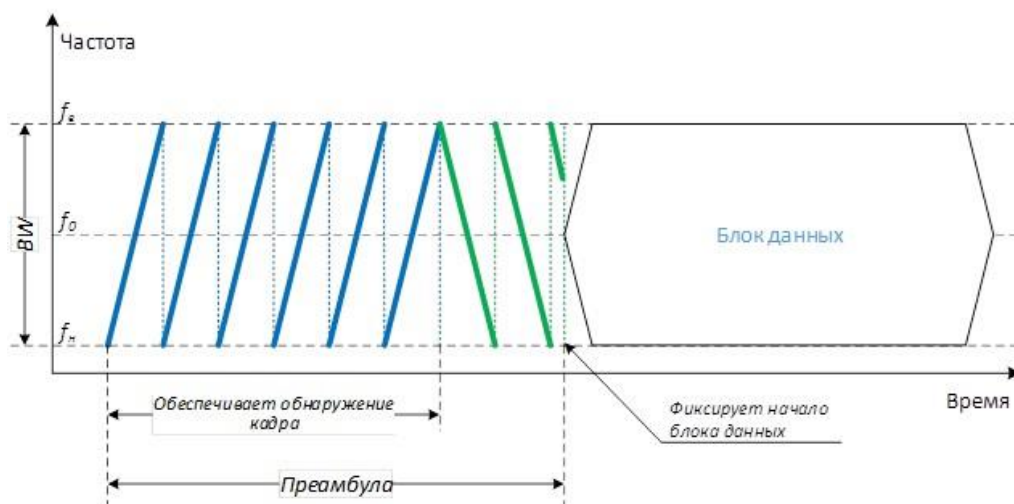


Рисунок 3.4 – Принцип передавання пакету даних

Технологія LoRa використовує асинхронний режим прийому-передачі при якому передавач може почати генерацію радіосигналу в будь-який момент часу [13]. В даному випадку існує механізм, що забезпечує синхронізацію приймача по сигналу від передавача. В якості такого механізму використовується преамбула, що передує кожному сеансу зв'язку. Преамбула включає в себе послідовність символів, що дозволяють приймачу виявити активність передавача, визначити використовуваний передавачем коефіцієнт розширення спектра (SF) і виконати символне синхронізацію. Тривалість преамбули є конфігурується величиною і повинна бути не менше, ніж

$$T1 + 2 \cdot T2, \quad (3.2)$$

де $T1$ – визначає максимальний час знаходження приймача в стані "сну" (Sleep);

$T2$ – визначає час пошуку приймачем преамбули.

Принцип передачі символів інформації блоку даних фізичного рівня за допомогою широкосмугового радіосигналу LoRa полягає в частотному зсуві

$$e^{j \cdot \Delta \omega \cdot k \cdot t}$$

відносно опорного сигналу

$$e^{j \cdot (\omega_H \cdot t + \mu \cdot t^2)},$$

де $k = 0, 1, 2, \dots, 2SF$ – інформаційний символ, розмірністю SF біт.

Таким чином, функція $x(t)$ запишеться наступним чином:

$$x(t) = \begin{cases} A_0 \cdot \cos \left(\omega_H \cdot t + \Delta \omega \cdot k \cdot t + \frac{\mu}{2} \cdot t^2 \right), & 0 \leq t < T_0 \\ A_0 \cdot \cos \left(\omega_H \cdot t + \Delta \omega \cdot k \cdot t - BW \cdot t + \frac{\mu}{2} \cdot t^2 \right), & T_0 \leq t < T_{sym} \end{cases} \quad (3.3)$$

де BW – ширина спектра радіосигналу; $k = 0, 1, 2, \dots, 2SF$ – інформаційний символ, розмірністю SF біт;

$T_{sym} = 2SF/BW$ – тривалість радіосигналу;

$\mu = \frac{BW}{T_{sym}}$ – швидкість зміни частоти радіосигналу;

t – час передавання одиниці даних;

ω_H – частота радіосигналу.

Приклад залежності частоти радіосигналу від часу для кадру даних показаний показано на рисунку 3.5.

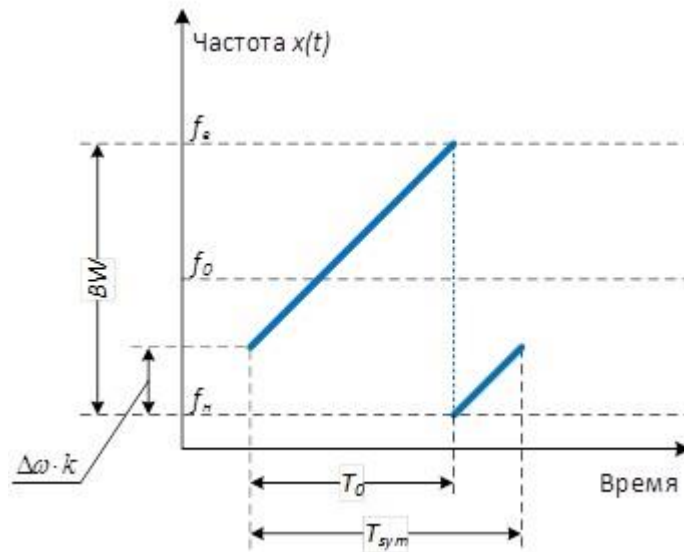


Рисунок 3.6 – Приклад залежності частоти радіосигналу від часу для кадру даних

3.2 Опис протоколу передачі даних в мережі IoT пристроїв

Для прикладу будемо розглядати випадок обміну повідомленнями між пристроями розумного будинку та шлюзом бездротової мережі. За допомогою технології IoT можна контролювати роботу модуля контролю за споживанням електроенергії, датчиком температури та розумним світильником.

Для обміну даними між пристроями розумного будинку пропонується використовувати наступний протокол обміну даними. Структура протоколу представлена на рисунку 3.6.

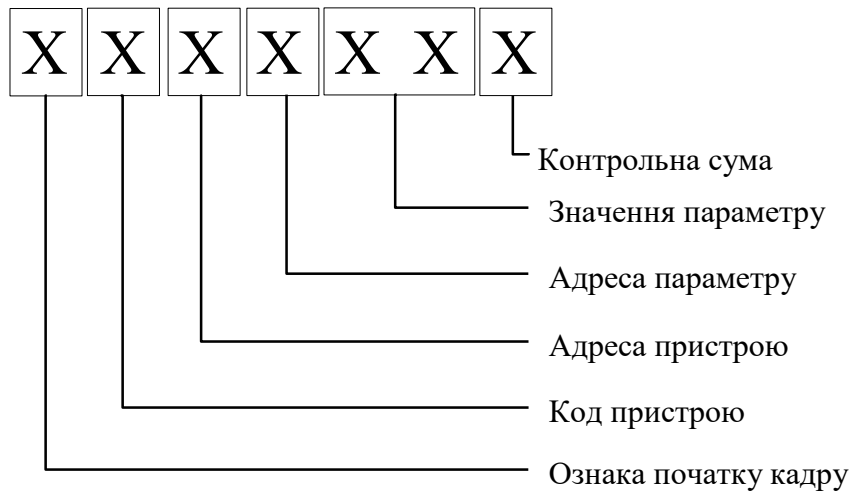


Рисунок 3.6 – Структура поля даних в протоколі обміну даними

Стартовий байт визначає тип обміну інформацією. Можливі варіанти стартового байту представлені в таблиці 3.1.

Таблиця 3.1 – Стартовий байт протоколу обміну даними

Стартовий байт	Значення
S	Контроль стану інтелектуального пристрою
P	Зчитування поточних параметрів пристрою
C	Управління пристроєм. Зміна параметрів

В режимі контролю відбувається контроль підключення і справності пристрою. Пристрій повинен надіслати повідомлення в якому буде міститися відповідь, що дублює надісланий запит.

В режимі зчитування поточних параметрів від пристрою до шлюзу повинні надійти поточні значення вимірюваних величин, або значення встановленої раніш величини.

В режимі управління в запиті надсилаються нові значення параметрів, що потрібно встановити на кінцевому пристрої.

У таблиці 3.2 наведені значення параметра «Код пристрою», і якому пристрою цей параметр відповідає.

Таблиця 3.2 – Параметри «Код пристрою»

Код пристрою	Пристрій
01	Контролер освітлення
02	Модуль контролю витрат електроенергії
03	Датчик температури

Параметр «Адреса пристрою» необхідний для можливості розрізняти пристрої, встановлених в різних приміщеннях будівлі. Значення байту «Адреса параметру» вказує в яку комірку пам'яті на кінцевому пристрої необхідно записати передане значення.

Розглянемо приклад процес обміну даними між шлюзом та модулем управління освітленням. Обмін даними починається з команди контролю, яка перевіряє, чи працює підключений пристрій, і запитує поточні значення його параметрів. В даному конкретному випадку команда має вигляд, представлений на рисунку 3.7.

S	01	03	00	00	00	CR
---	----	----	----	----	----	----

Рисунок 3.7 – Команда контролю стану модуля управління освітленням

Перший символ «S» означає, що відбувається контроль справності і запит поточних параметрів пристрою. Другий байт «01» означає, що здійснюється запит параметрів модуля управління освітленням. Третій байт «03» – це номер пристрою в межах об’єкту. Четвертий байт встановлено в «00» тому що при перевірці стану пристрою до нього не передаються параметри і тому не треба вказувати адрес комірки

Наступні два байти дорівнюють «00 00», що свідчить про команду контролю.

В кінці поля даних передається байт контрольної суми «CR» для перевірки правильності передачі команди.

Після отримання запиту модуль управління освітленням формує таку відповідь (рисунок 3.8).

P	01	03	00	00	00	CR
---	----	----	----	----	----	----

Рисунок 3.8 – Відповідь пристрою на команду від шлюзу

Перший символ «P» показує, що це відповідь містить параметри. Далі йдуть код пристрою «01» та адреса пристрою «03». Далі йдуть нульові байти тому що відповідь не передбачає передачу параметрів.

Для зчитування поточних даних з пристрою управління освітленням від шлюзу формується команда виду:

P 01 03 01 00 00 CR

Перший символ вказує на запит параметрів. Байт «01» вказує комірку, з якої потрібно прочитати дані. Відповідь очікується в такому форматі:

P 01 03 01 00 55 CR

Відповідь практично повністю повторює запит за винятком байтів даних. Як можна бачити в них міститься поточне значення 55h, що при перетворенні в десятинне значення буде дорівнювати 125. Тобто освітлення включене не на повну потужність.

3.3 Результати моделювання та вибір оптимальних параметрів

Виконаємо моделювання роботи за допомогою програмного засобу LoRa Modem Calculator від фірми Semtech. Зовнішній вигляд інструменту показано на рисунку 3.9.

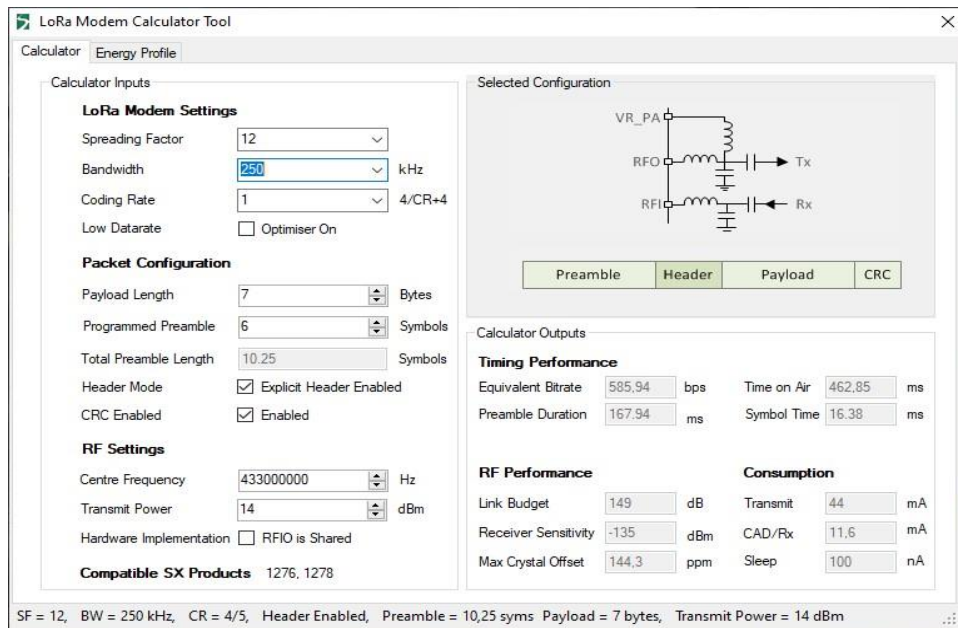


Рисунок 3.9 – Програмні засіб LoRa Modem Calculator

Як можна бачити з інтерфейсу програми, вхідними умовами для моделювання є наступні параметри:

- довжина поля даних;
- довжина поля преамбули;
- ширина спектра радіосигналу BW;
- коефіцієнт розповсюдження (фактор розширення спектра);
- частотний діапазон;
- потужність передатчика; – формат пакету даних.

В результаті моделювання нам потрібно визначити наступні умови експлуатації:

- час, що необхідно для передавання пакету даних;
- швидкість передачі даних;
- чутливість приймача;
- потужність, що необхідна для передачі даних;
- термін роботи від автономного джерела живлення.

Початкові умови, що є незмінними:

- інтервал передавання = 1 с. ;
- ємність батареї = 1000 мАч;
- напруга живлення = 3,3 В;
- робоча частота = 433 МГц.

Розмір Payload може змінюватись в межах 7 – 3 байти. Виконаємо моделювання роботи пристрою для цих параметрів. Результати моделювання занесені в таблицю 3.3.

Таблиця 3.3 – Результати моделювання роботи модуля прийому /передачі даних при різних розмірах поля Payload

Payload, байт	7	6	5	4	3
SF = 12, BW = 125 кГц, CR = 4/5, Header Enabled, Preamble = 10,25 симв., Payload = 7 байт, TR Power = 14 дБ					
Час в ефірі, мс	925,7	761,86	761,86	761,86	761,86
Час передачі симв, мс	32,77	32,77	32,77	32,77	32,77
Споживаний струм при передаванні, мА	44	44	44	44	44
Чутливість приймача, дБ	-138	-138	-138	-138	-138
Орієнтований час роботи від батареї, діб	80,54	80,54	80,54	80,54	80,54
CAD, мс	61,1	61,1	61,1	61,1	61,1

На русинку 3.10 показано результат моделювання в програмі LoRa Modem Calculator для режиму роботи Periodic Receiver.

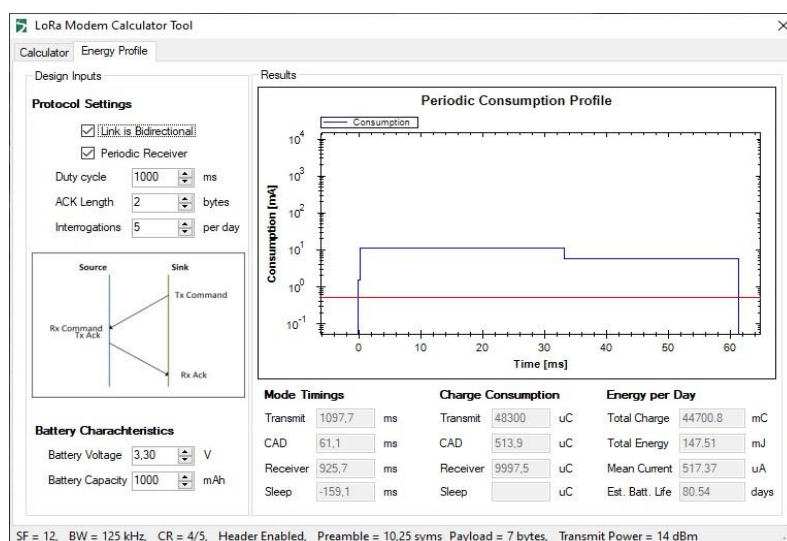


Рисунок 3.10 – Результат моделювання в програмі LoRa Modem Calculator для режиму роботи Periodic Receiver

На рисунку 3.11 показано результат моделювання в програмі LoRa Modem Calculator для режиму роботи Periodic Transmitter.

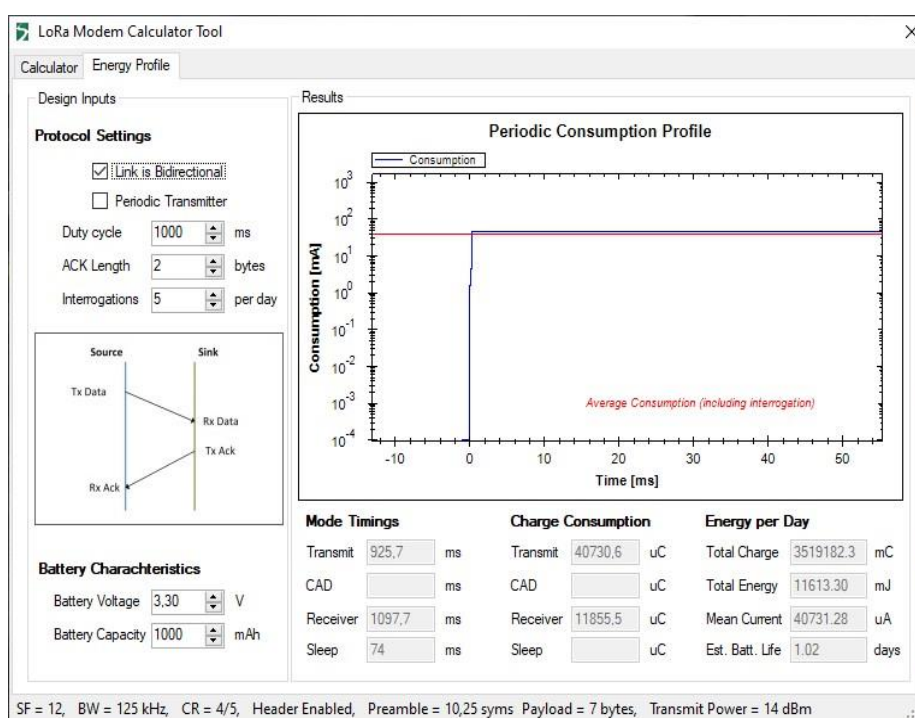


Рисунок 3.11 – Результат моделювання в програмі LoRa Modem Calculator для режиму роботи Periodic Transmitter

Виходячи з аналізу протоколу обміну даними можна зробити висновок, що для зниження споживаної потужності та зменшення часу в ефірі можна зробити змінну довжину кадру. Наприклад, для контролю наявності пристрою потрібно лише 4 байти (прибрати з протоколу порожні поля даних та адресу комірки). Як можна бачили з таблиці 3.3 при зменшенні довжини поля даних ми зменшуємо час знаходження в ефірі з 925,7 мс до 761,86 мс. При цьому споживаний струм не зменшується. Таким чином, потрібно знайти інші параметри, що дадуть нам можливість подовжити час автономної роботи.

Іншим параметром, яким можна змінювати споживані властивості модуля є наявність, або відсутність полів заголовку та контрольної суми. Визначено вплив цих параметрів для двох значень розміру поля даних: 7 та 4 байти.

Результати моделювання роботи модуля прийому/передачі даних при різних розмірах кадру представлені в таблиці 3.4

Таблиця 3.4 – Результати моделювання роботи модуля прийому/передачі даних при різних розмірах кадру

Payload, байт	7	7	7	4	4	4
Header Enabled	Так	Ні	Ні	Так	Ні	Ні
CRC Enabled	Так	Так	Ні	Так	Так	Ні
SF = 12, BW = 125 кГц, CR = 4/5, Header Enabled, Preamble = 10,25 симв., Payload = 7 байт, TR Power = 14 дБ						
Час в ефірі, мс	925,7	761,86	761,86	761,86	761,86	598,02
Час передачі симв, мс	32,77	32,77	32,77	32,77	32,77	32,77

Кінець таблиці 3.4

Споживаний при передаванні, мА	44	44	44	44	44	44
Чутливість приймача, дБ	-138	-138	-138	-138	-138	-138
Орієнтований час роботи від батареї, діб	80,54 1,02	80,6 1,24	80,6 1,24	80,54 1,24	80,6 1,24	80,6 1,58
CAD, мс	61,1	61,1	61,1	61,1	61,1	61,1

Виходячи з результатів моделювання можна бачити, що при відключенні одного з полів Header або CRC вдалось трохи збільшити автономний час роботи від батареї з 80,54 до 80,6 діб.

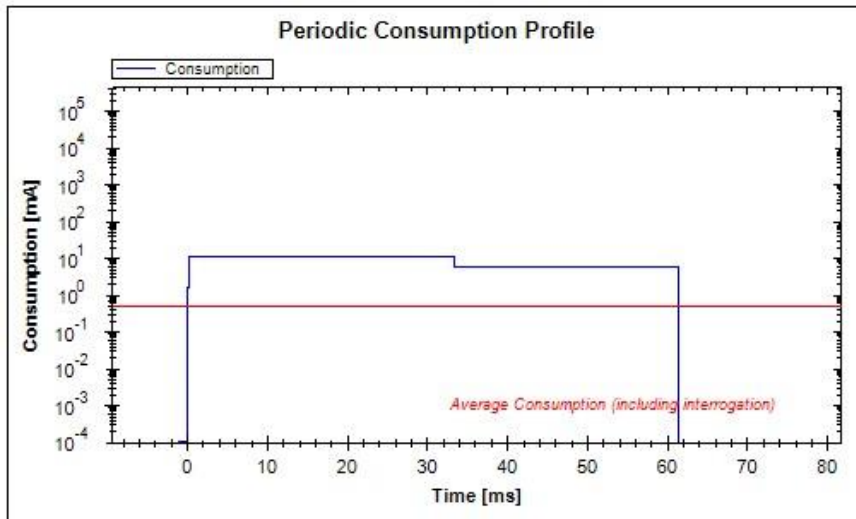
Для передавача при відключенні зазначених полів кадру вдалось збільшити час автономної роботи з 1,02 до 1,24 доби, та з 1,24 до 1,58 відповідно для 7 та 4 байт даних. Таким чином, приріст часу роботи передавача від батареї становить більше 20 %.

Відключивши відразу два поля ми також зменшили загальний час знаходження в ефірі до 598,02 мс.

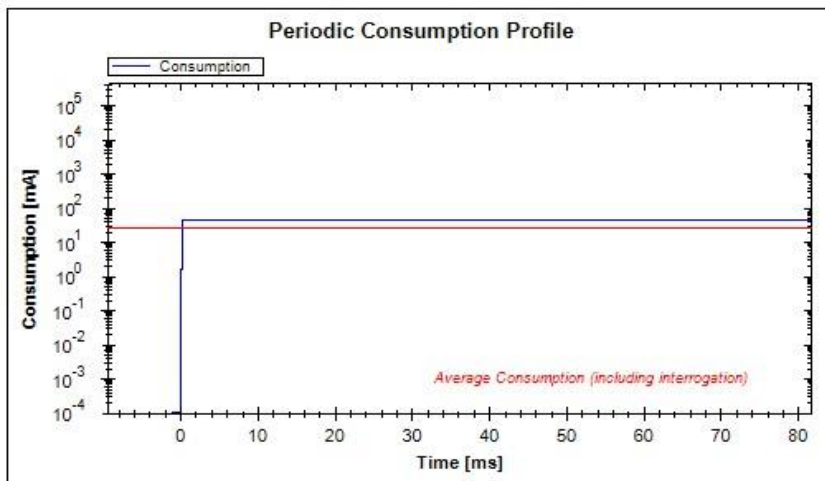
Щоб визначити, чи присутній сигнал чи ні, замість використання індикатора потужності прийнятого сигналу (RSSI) в системі LoRa для ідентифікації присутності сигналу використовується комбінована адаптивна система виявлення активності каналу (Channel Activity Detection, CAD).

Вона може розрізняти шум і корисний сигнал LoRa. Процес функціонування цієї системи вимагає двох символів. Якщо система виявила сигнал, то переривання по CAD_Detected дасть підтвердження, і в цьому випадку, щоб отримати корисні дані, пристрій залишиться в режимі прийому.

На рисунку 3.12 показано результат моделювання роботи Channel Activity Detection.



а) результат моделювання для приймача



б) результат моделювання для передавача

Рисунок 3.12 – Результат моделювання роботи Channel Activity Detection

За результатами експерименту можна бачити, що зміна параметру CR призводить до збільшення потрібного часу на передачу інформації і, відповідно, до зменшення часу автономної роботи модуля.

Ще одним висновком є те, що для значенню параметру $CR = 4/7$, та $CR = 4/8$ ми виходимо за кордони заданого значення інтервалу передавання – 1000 мс. При вказаних значеннях параметру CR час знаходження в ефірі повинен становити 1057 мс та 1122 мс. Це суперечить початковим умовам і ми не можемо використовувати наведені параметри. Таким чином, для практичного використання залишаються два значення параметру CR - $4/5$ та $4/6$.

Розглянуті параметри властиві для організації максимально можливої дальності передавання сигналу. Запатентована технологія організації зв'язку використовує свій спосіб модуляції, який має назву «чірп» - нелінійна модуляція при якій частота сигналу лінійно зростає від початкової частоти f_0 до кінцевої f_1 [14]. За стандартом LoRa кодування здійснюється шляхом циклічного зсуву чірпа щодо кадру часу. Параметрами сигналу в LoRa є SF (Spreading factor) і Bandwidth (BW) - ширина смуги передачі. Параметр SF задається зумовленими значеннями SF7 - SF12, де 7 найшвидший, а 12 - найповільніший режим. На рисунку 3.13 показано приклад різних швидкостей передачі даних при різних значення SF.

Самий повільний сигнал відповідає найбільшій дальності передавання. Якщо дальність не є ти критерієм якого треба досягти при проектуванні пристрою, то за документацією до модулю SX-1278 можна суттєво знизити споживану потужність змінюючи параметри SF та BW.

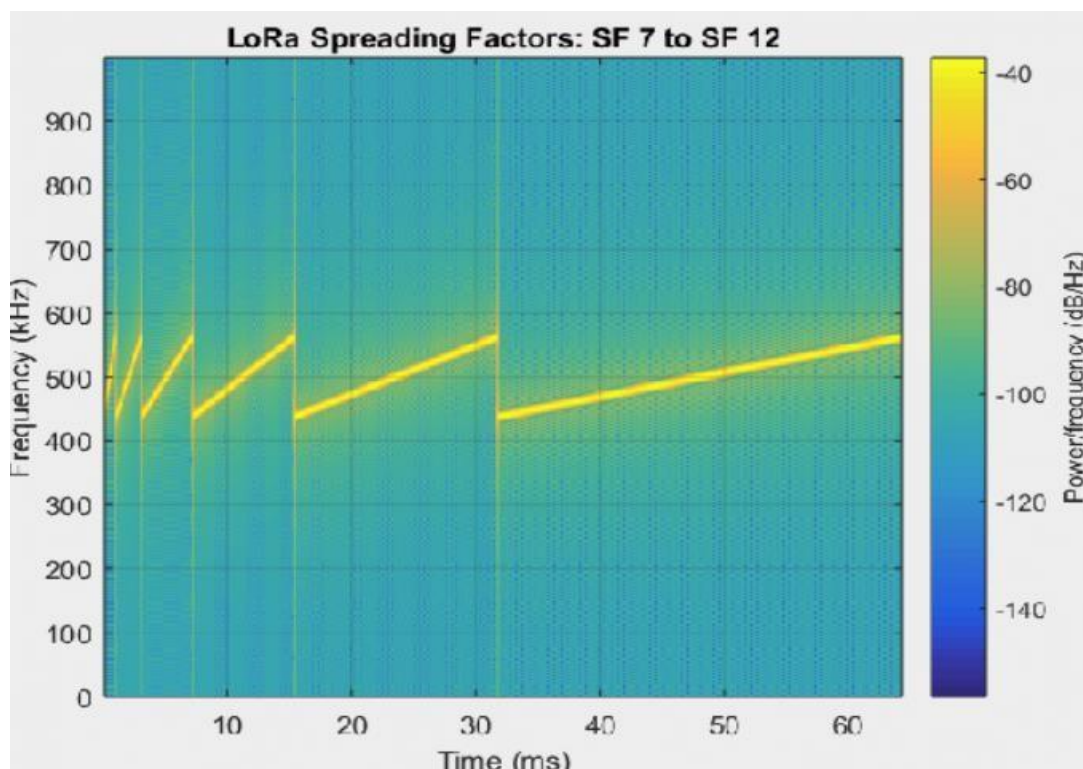


Рисунок 3.13 – Приклад різних швидкостей передачі даних при різних значення SF

Виконаємо моделювання таких ситуацій за допомогою інструменту LoRa Modem Calculator. Параметр BW буде змінюватись в наступних межах: 125 кГц, 250 кГц та 500 кГц. Результати моделювання занесені в таблицю 3.6

Таблиця 3.6 – Результати моделювання роботи модуля прийому /передачі даних при різних значеннях параметру CR

BW, кГц	125	250	500
SF = 12, CR = 4/5, Header Enabled, Preamble = 10,25 симв., Payload = 7 байт, TR Power = 14 дБ			
Час в ефірі, мс	925,7	462,85	231,42
Час передачі симв, мс	32,7	16,38	8,19

Кінець таблиці 3.6

Споживаний передаванні, мА	44	44	44
Чутливість приймача, дБ	-138	-135	-132
Орієнтований час роботи від батареї, діб	80,54 1,02	110,76 2,05	124,96 4,09
CAD, мс	61,1	44,6	36,3

Як можна бачити, розширення полоси пропускання значно впливає на скорочення часу передачі даних та приводить к зростанню загального часу автономної роботи. При максимальному значенні параметра $BW = 500$ кГц, час автономної роботи зріс в чотири рази для режиму передавання даних, та 70 % в режимі прийому.

Наступне моделювання проведемо для різних значення Spreading factor.

Будемо змінювати всі можливі значення цього параметру ($SF = \{6, 7, 8, 9, 10, 11, 12\}$). Результати моделювання роботи представлені в таблиці 3.7.

Визначивши значення параметрів при яких досягається максимальна енергоефективність виконаємо моделювання такої ситуації за допомогою LoRa Modem Calculator.

Моделювання виконаємо для двох значень розміру поля Payload (7 та 4 байти).

Таблиця 3.7 – Результати моделювання роботи пристрою SX-1278 для різних значень параметру SF

SF	12	11	10	9	8	7	6
BW = 125 кГц, CR = 4/5, Header Enabled, Preamble = 10,25 симв., Payload = 7 байт, TR Power = 14 дБ							
Час в ефірі, мс	925,7	462,8	231,42	115,7	68,1	34,05	17,02
Час передачі симв, мс	32,7	16,38	8,19	4,10	2,05	1,02	0,51
Споживаний струм при передаванні, мА	44	44	44	44	44	44	44
Чутливість приймача, дБ	-138	-135,5	-133	-130	-127	-124	-119
Орієнтований час роботи від батареї, діб	80,54	164,12	332,21	663,20	1288	2376	4041
	1,02	2,05	4,09	8,18	13,90	27,80	55,57
CAD, мс	61,1	29,5	14,3	7	3,5	1,8	1

Для моделювання передачі пакету довжиною 7 байт будемо використовувати такі параметри:

- Spreading factor = 6;
- розмір поля даних Payload = 7;
- поле заголовка відсутнє;
- поле контрольної суми відсутнє;
- тип кодування (CR) = 4/5.

Результати моделювання покажемо для трьох значень ширини полоси пропускання 125 кГц, 250 кГц та 500 кГц.

Результати моделювання показані в таблиці 3.8.

Таблиця 3.8 – Результати моделювання для оптимальних значень параметрів модуля LoRa

BW, кГц	125	250	500
SF = 6, CR = 4/5, Header Disable, CRC Disable, Preamble = 10,25 симв., Payload = 7 байт, TR Power = 14 дБ			
Час в ефірі, мс	14,46	7,23	3,62
Час передачі симв, мс	0,51	0,26	0,13
Споживаний струм при передаванні, мА	44	44	44
Чутливість приймача, дБ	-119	-116	-113
Орієнтований час роботи від батареї, діб	4041,37 65,39	6269 130,64	8321,94 260,66
CAD, мс	1	0,6	0,4

Для моделювання передачі пакету довжиною 4 байти будемо використовувати такі параметри:

- Spreading factor = 6;
- розмір поля даних Payload = 4;
- поле заголовка відсутнє;
- поле контрольної суми відсутнє;
- тип кодування (CR) = 4/5.

Результати моделювання покажемо для трьох значень ширини полоси пропускання 125, 250 та 500 кГц.

Результати моделювання показані в таблиці 3.9.

Таблиця 3.9 – Результати моделювання для оптимальних значень параметрів модуля LoRa

BW, кГц	125	250	500
SF = 6, CR = 4/5, Header Disable, CRC Disable, Preamble = 10,25 симв., Payload = 4 байт, TR Power = 14 дБ			
Час в ефірі, мс	11,9	5,95	2,98
Час передачі симв, мс	0,51	0,26	0,13
Споживаний струм при передаванні, мА	44	44	44
Чутливість приймача, дБ	-119	-116	-113
Орієнтований час роботи від батареї, діб	4041,37	6269	8321,94
	79,44	158,65	316,40
CAD, мс	1	0,6	0,4

Для встановленого нами обмеження в цикл передавання даних на рівні 1000 мс час передавання повинен бути 10 мс.

3.4 Висновки по розділу

В результаті виконання третього розділу магістерської атестаційної роботи проведено моделювання та вибір оптимальних параметрів роботи шлюзу IoT, за допомогою інструментів LoRa Modem Calculator, Channel Activity Detection.

Результати моделювання показали, що умові в знаходженні в ефірі до 1 % часу активного циклу для розміру поля даних розмір поля даних Payload = 7 або 4 відповідають такі параметри:

- Spreading factor = 6;
- BW \geq 250 кГц;
- поле заголовка відсутнє;
- поле контрольної суми відсутнє;
- тип кодування (CR) = 4/5.

4 ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

4.1 Розробка структурної схеми макету

Для перевірки запропонованої методики визначення пропускної здатності шлюзу та тестування його роботи необхідно зібрати тестовий макет.

На рисунку 4.1 показана структурна схема макету.

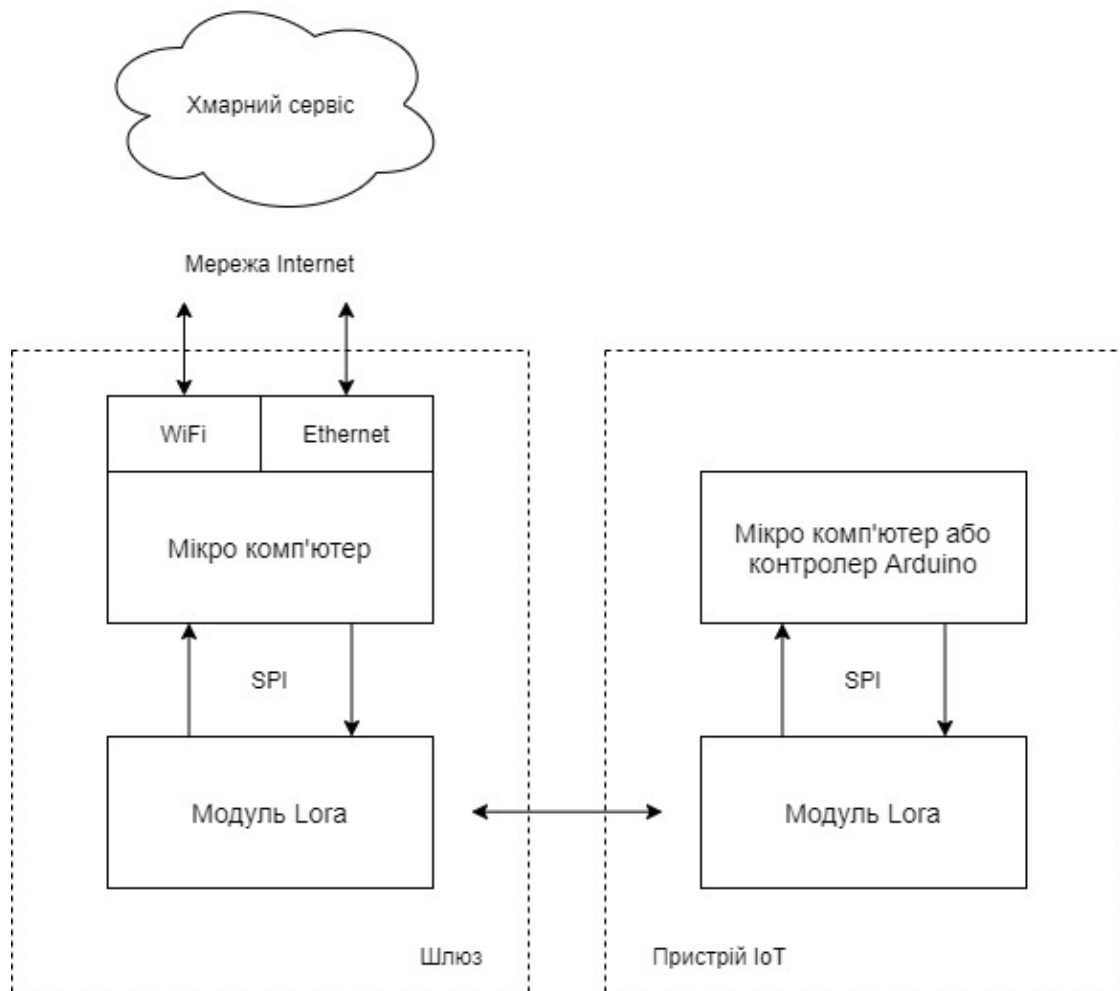


Рисунок 4.1 – Структурна схема макету

До складу макету повинні входити:

- мікрокомп'ютер з встановленою операційною системою;
- модуль Lora;
- тестовий модуль для емуляції роботи IoT пристроїв.

Операційна система на мікрокомп'ютері запускає процес опитування модуля Lora з метою отримання даних від пристроїв IoT, що знаходяться в радіусі дії шлюзу та зареєстровані на ньому.

В якості хмарного сервісу будемо використовувати ресурс <https://www.thethingsnetwork.org/>.

В якості модуля організації зв'язку на боці шлюзу будемо використовувати Raspberry Pi LoRa HAT на базі SX1268, що показано на рисунку 4.2.

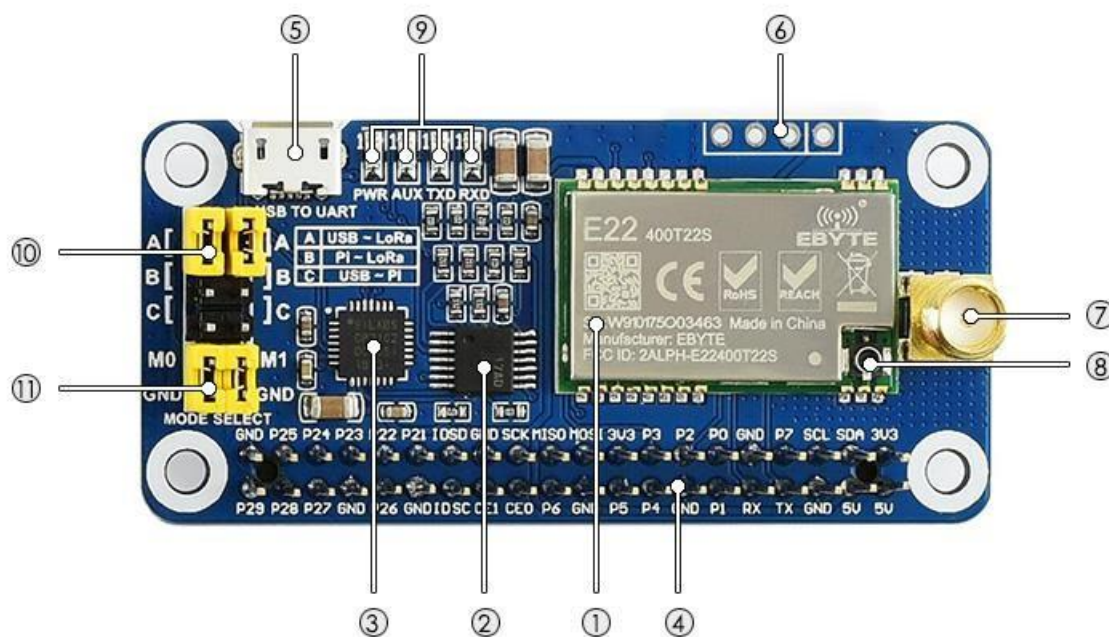


Рисунок 4.2 – Модуль Raspberry Pi LoRa HAT на базі SX1268

Даний модуль спеціально розроблений для проведення різних експериментів з мережею LoRaWAN та має доволі широкий набір компонентів, що інтегровані на плату:

- а) SX1268 LoRa модуль (1);
- б) 74HC125V: перетворювач рівня напруги (2);
- в) CP2102: конвертер USB TO UART (3);
- г) роз'єм Raspberry Pi GPIO: для з'єднання з Raspberry Pi (4);
- д) micro USB роз'єм USB TO UART порту (5);
- є) майданчики UART для підключення хост-плат, таких як STM32 /
- ж) Arduino (6);
- з) SMA антенний роз'єм (7);
- і) роз'єм антени IPEX (8); – індикатори (9):
 - 1) RXD / TXD: індикатор UART RX / TX;
 - 2) AUX: допоміжний індикатор;
 - 3) PWR: індикатор живлення; – UART вибір перемичок (10):
 - 4) А: управління модулем LoRa через USB TO UART;
 - 5) В: управління модулем LoRa через Raspberry Pi;
 - 6) С: доступ до Raspberry Pi через USB TO UART;
- к) перемички вибору режиму LoRa (11):
 - 1) замкнутий M0, замкнутий M1: режим передачі;
 - 2) замкнутий M0, розімкнутий M1: режим конфігурації;
 - 3) розімкнутий M0, замкнутий M1: режим WOR;
 - 4) розімкнутий M0, розімкнутий M1: режим глибокого сну.

Як можна бачити на платі є цілий набір можливостей для дослідження різних режимів експлуатації модуля (конфігурація, передачі даних та режим глибокого сну). Останній режим дуже корисний при побудові реальних пристроїв IoT де використовується батарейне живлення та потрібно економити енергію.

Даний модуль працює на частоті 433 МГц і дозволяє передавати дані до 5 км через послідовний порт. Завдяки використанню технології модуляції з розширеним спектром LoRa нового покоління максимальна дальність зв'язку модуля становить 5 км, а також підтримується автоматичне повторення передачі даних при виникненні помилок передачі.

Інші функції включають Wake on Radio, бездротову конфігурацію, визначення несучої, ключ зв'язку і так далі. У порівнянні зі звичайними модулями LoRa, SX1268 LoRa HAT забезпечує велику дальність зв'язку, більш високу швидкість, низьке споживання, кращу безпеку і захист від перешкод. Таким чином, даний модуль підходить для різних додатків, таких як промислове управління обладнанням, розумний будинок, збір даних і т. д.

Для підключення модуля LoRa HAT до Raspberry Pi будемо використовувати стандартний роз'єм 40PIN GPIO, який підтримують всі плати серії Raspberry Pi.

Завдяки вбудованому перетворювачу USB TO UART CP2102 можна підключити модуль до персонального комп'ютера для виконання задачі попередньої конфігурації мікросхеми SX1268.

Даний модуль можна підключити до контролерів Arduino або STM32 за допомогою інтерфейсу управління UART.

В платі використовується технологія модуляції з розширеним спектром LoRa, що має до 84 доступних каналів сигналу, велику дальність зв'язку, та підвищену стійкість до перешкод. Автоматичне багаторівневе повторення передачі, підходить для зв'язку на великих відстанях та дозволяє використовувати кілька мереж в одному регіоні. Завдяки підтримка технології LBT, можна, відстежуючи шум каналу сигналу перед передачею, значно покращити коефіцієнт успішності в екстремальних умовах передавання даних.

В модулі LoRa HAT підтримується технологія визначення потужності сигналу RSSI, що може використовуватись нами для оцінки якості сигналу, налаштування мережі, проведення експериментальних досліджень роботи шлюзу.

В модулі є можливість налаштувати закритий ключ зв'язку, що значно підвищує безпеку призначених для користувача даних через шлюз. Також є можливість налаштування параметрів бездротової мережі, відправляючи пакет бездротової команди або даних, віддалено через мережу Internet.

На рисунку 4.3 показано зовнішній вигляд зібраного макету шлюзу Lora WAN.



Рисунок 4.3 – Макет Lora WAN шлюзу

Для тестування роботи шлюзу потрібен ще один пристрій з модулем LoRa. Даний модуль буде моделювати роботу IoT пристрою та обмінюватись даними зі шлюзом.

Тестовий модуль розроблюється самостійно з використанням окремої мікро-передавача Ra-01 LoRa - SX1278 - 433 МГц.

Ra-01 – це функціонально закінчений модуль, що побудовано на мікросхемі SX1278. Для підключення к контролеру Arduino або мікрокомп'ютеру Raspberry PI використовується інтерфейс SPI.

Зовнішній вигляд модуля та призначення його контактів можна побачити на рисунку 4.4.

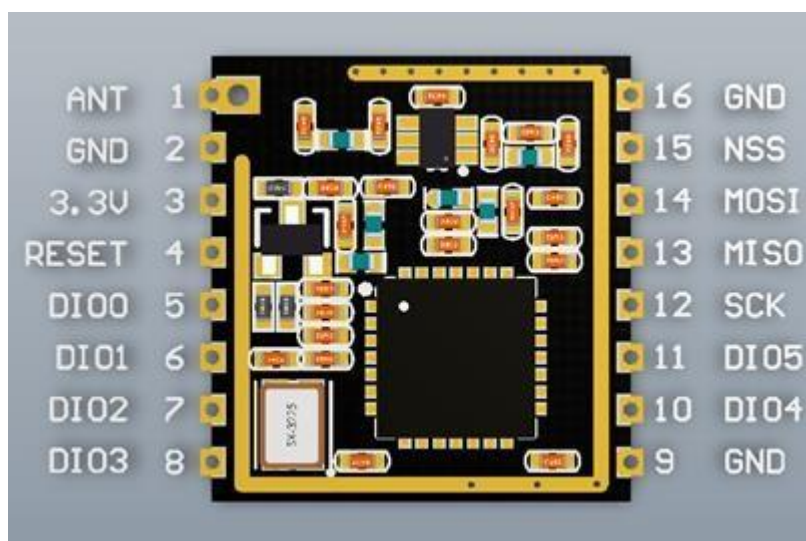


Рисунок 4.4 – Ra-01 LoRa - SX1278 - 433 МГц

Для управління роботою даного пристрою необхідно користуватись її структурної схемою, що показана на рисунку 4.5.

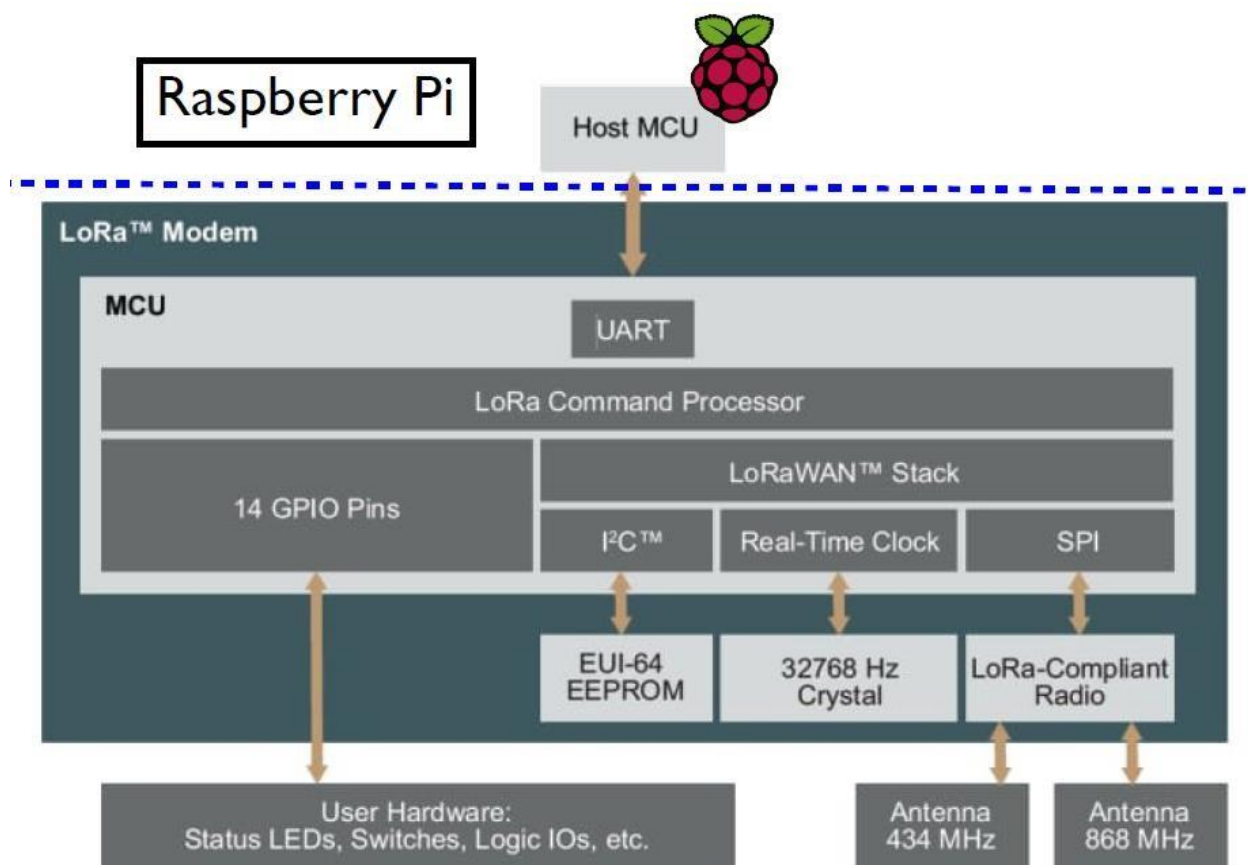


Рисунок 4.5 – Структурна схема модуля Ra-01

Як можна бачити з даного рисунку, деякі моделі модулів, наприклад, той що розташовано на платі LoRa HAT, мають можливість виконувати підключення до комп'ютера безпосередньо через послідовний інтерфейс RS232 за протоколом UART. В даному режимі можна виконувати конфігурування модуля та передавання текстових даних. В модулі Ra-01 піни для підключення за протоколом UART не виведені на зовнішні контакти. Доступними для підключення є контакти протоколу SPI.

На рисунку 4.6 показана функціональна схема мікросхеми SX-1278 яка є основою модуля Ra-01.

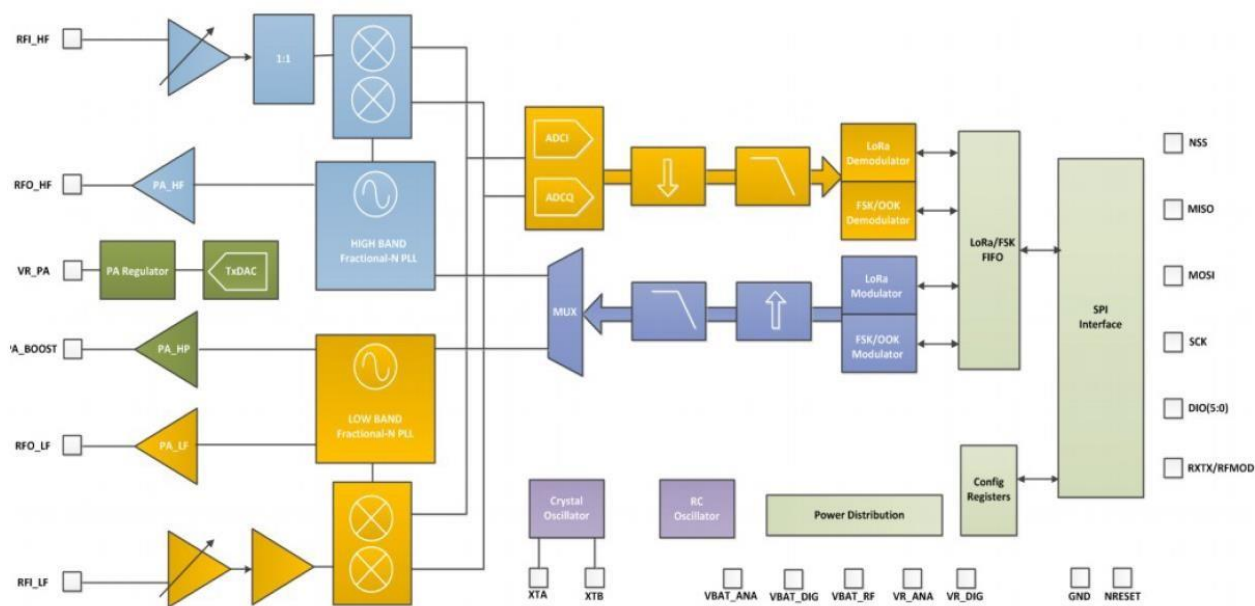


Рисунок 4.6 – Функціональна схема мікросхеми SX-1278

З наведеного рисунку можна побачити якими ресурсами можна управляти при виконанні конфігурації пристрою на етапі моделювання. Так, ми можемо програмно задавати робочу частоту в певному діапазоні, можемо змінювати номер каналу передачі даних, управляти потужністю передатчика, задавати можливість кодування інформації, що передається [17].

Для перевірки результатів моделювання, що виконували на попередньому етапі, виконаємо програмування та тестове підключення модулю, що моделює роботу IoT пристрою до шлюзу.

4.2 Результати експерименту

Експериментальне моделювання будемо проводити з IoT-пристроєм який побудований на модулі SX-1278. На рисунку 4.7 показано зовнішній вигляд тестового пристрою, який буде взаємодіяти зі шлюзом.

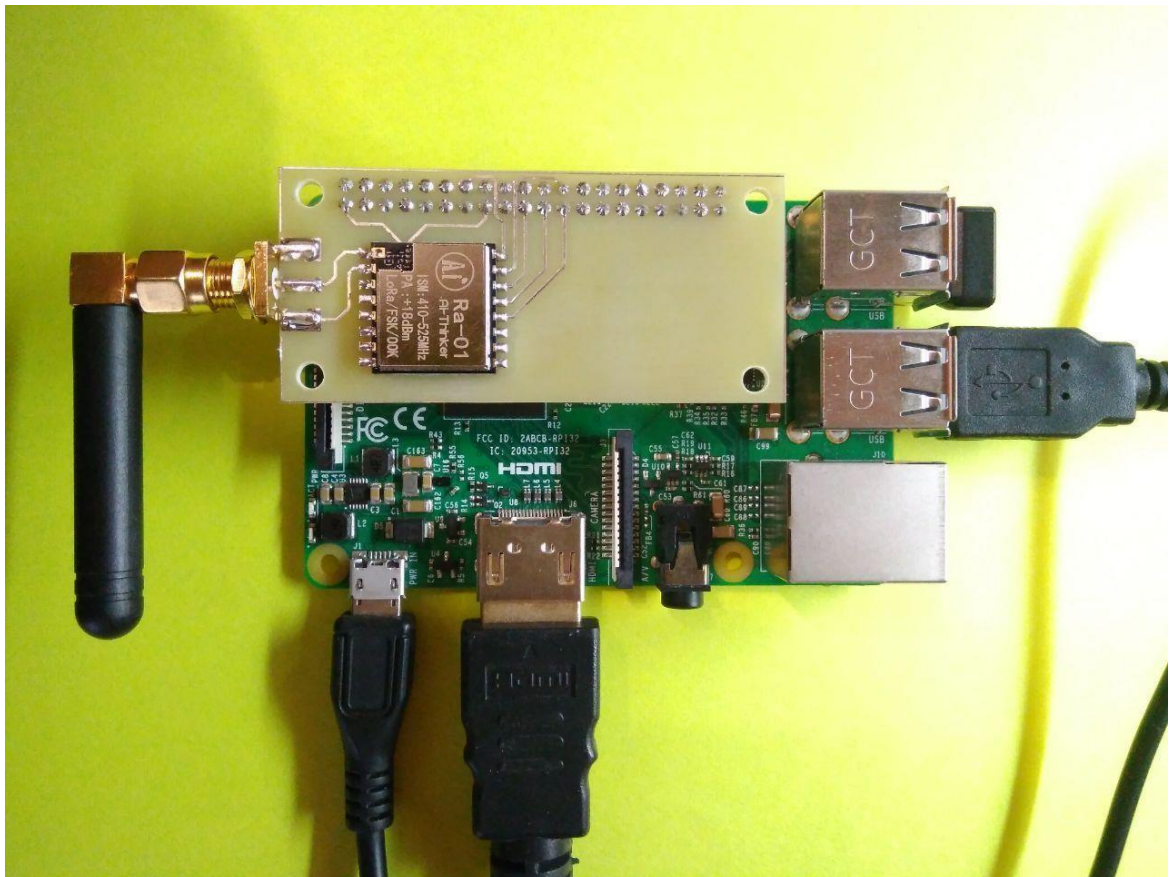


Рисунок 4.7 – зовнішній вигляд тестового IoT-пристрою

Параметри налаштування модулів LoRa на шлюзі та IoT-пристрої візьмемо такими:

- робоча частота – 433 МГц;
- Payload = 7;
- Spreading factor = 6;
- BW \geq 250 кГц;
- поле заголовка відсутнє;
- поле контрольної суми відсутнє;
- тип кодування (CR) = 4/5.

На першому етапі треба задати у програмі частоту роботи пристрою. Для цього спочатку необхідно дізнатися поточну частоту роботи пристрою.

Це можна зробити, за допомогою наступного фрагмент коду:

```
import spidev spi = spidev.SpiDev()
spi.open(0, 0)
spi.max_speed_hz = 5000000
RegFrMsb = 0x06
RegFrMid = 0x07
RegFrLsb = 0x08
Value = 0
msb = spi.xfer([RegFrMsb & 0x7F, Value])[1]
mid = spi.xfer([RegFrMid & 0x7F, Value])[1]
lsb = spi.xfer([RegFrLsb & 0x7F, Value])[1]
f = lsb + 256*(mid + 256*msb)
print(f / 16384.0) spi.close()
```

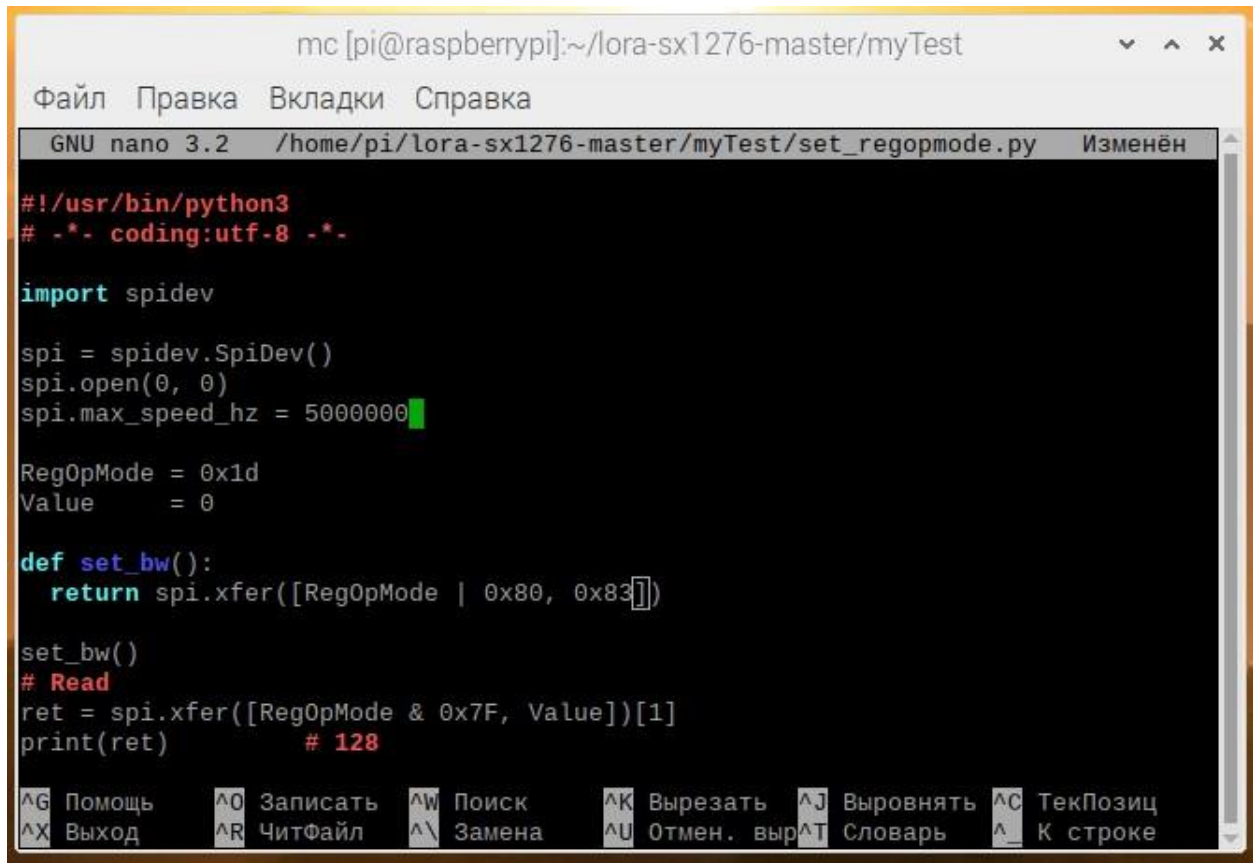
Як сказано в документації [16] частота – це сума значень трьох регістрів MSB:0x06, MID:0x07, та LSB:0x08.

Для того, що змінити частоту необхідно написати такий фрагмент коду:

```
RegFrMsb = 0x06
def set_freq(f)
i = int(f * 16384)
msb = i // 65536
i -= msb * 65536
mid = i // 256
i -= mid * 256
lsb = i
return spi.xfer([RegFrMsb | 0x80, msb, mid, lsb])
set_freq(433)
```

За допомогою даного фрагменту коду встановлюємо робочу частоту, що дорівнює 433 МГц.

На наступному етапі потрібно встановити значення Spreading Factor. Як біло визначення в попередньому розділі це значення буде дорівнювати 6. Для перевірки поточного значення будь якого з параметрів напишемо функцію для зчитування вказаного регістру, що відповідають за конфігурацію модуля (рисунок 4.8).



```
mc [pi@raspberrypi]:~/lora-sx1276-master/myTest
Файл Правка Вкладки Справка
GNU nano 3.2 /home/pi/lora-sx1276-master/myTest/set_regopmode.py Изменён
#!/usr/bin/python3
# -*- coding:utf-8 -*-

import spidev

spi = spidev.SpiDev()
spi.open(0, 0)
spi.max_speed_hz = 5000000

RegOpMode = 0x1d
Value      = 0

def set_bw():
    return spi.xfer([RegOpMode | 0x80, 0x83])

set_bw()
# Read
ret = spi.xfer([RegOpMode & 0x7F, Value])[1]
print(ret)          # 128

^G Помощь      ^O Записать    ^W Поиск      ^K Вырезать   ^J Выводить   ^C ТекПозиц
^X Выход      ^R ЧитФайл    ^\ Замена     ^U Отмен. выр ^T Словарь    ^_ К строке
```

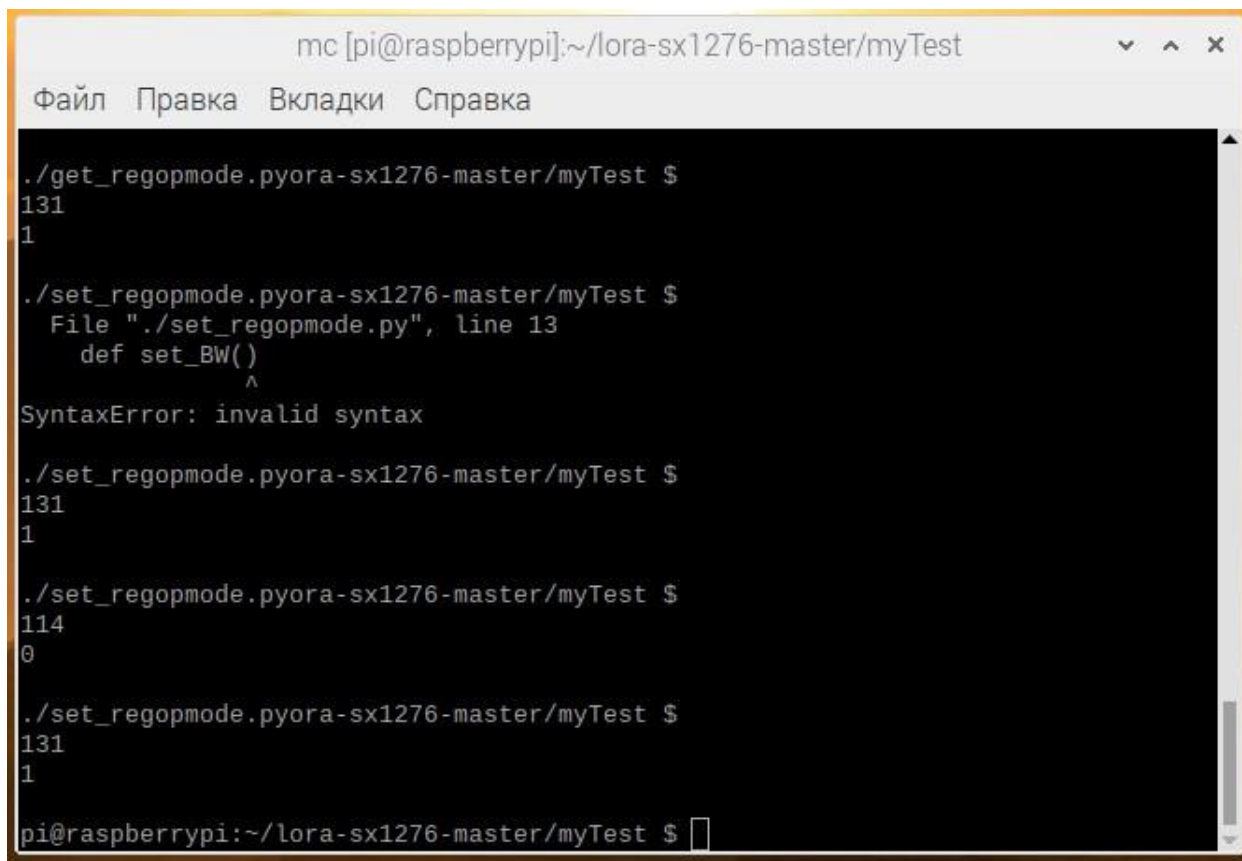
Рисунок 4.8 – Функція читання значення регістра 0x1d

Дана функція оперує адресою потрібного регістру та виводить його значення. Перевіримо значення регістру 0x1d, який відповідає за налаштування таких параметрів як:

- ширина спектра радіосигналу (BW);
- тип кодування (CR);

– наявність заголовку (Header).

Після виконання написаної програми на екран було виведене значення 114, як показано на рисунку 4.9.



```
mc [pi@raspberrypi]:~/lora-sx1276-master/myTest
Файл  Правка  Вкладки  Справка

./get_regopmode.pyora-sx1276-master/myTest $
131
1

./set_regopmode.pyora-sx1276-master/myTest $
File "./set_regopmode.py", line 13
    def set_BW()
        ^
SyntaxError: invalid syntax

./set_regopmode.pyora-sx1276-master/myTest $
131
1

./set_regopmode.pyora-sx1276-master/myTest $
114
0

./set_regopmode.pyora-sx1276-master/myTest $
131
1

pi@raspberrypi:~/lora-sx1276-master/myTest $
```

Рисунок 4.9 – Виведення на екран значення регістру конфігурації

Як можна бачити з даного рисунку в регістрі 0x1d зберігається число 114. Для визначення того, які функції включені за допомогою даного байту використаємо інформації з керівництва користувача, яка показана на рисунку 4.10.

Виходячи з даного рисунку можна бачити, що число 114 відповідає наступній конфігурації:

0111 – відповідає ширині спектру радіосигналу та становить 125 кГц;

0010 – відповідає типу кодування та становить 4/5;

0 – відповідає включеному заголовку.

RegModemConfig 1 (0x1D)	7-4	Bw	rw	0x07	Signal bandwidth: 0000 → 7.8 kHz 0001 → 10.4 kHz 0010 → 15.6 kHz 0011 → 20.8kHz 0100 → 31.25 kHz 0101 → 41.7 kHz 0110 → 62.5 kHz 0111 → 125 kHz 1000 → 250 kHz 1001 → 500 kHz other values → reserved In the lower band (169MHz), signal bandwidths 8&9 are not supported)
	3-1	CodingRate	rw	'001'	Error coding rate 001 → 4/5 010 → 4/6 011 → 4/7 100 → 4/8 All other values → reserved In implicit header mode should be set on receiver to determine expected coding rate. See 4.1.1.3
	0	ImplicitHeaderModeOn	rw	0x0	0 → Explicit Header mode 1 → Implicit Header mode

Рисунок 4.10 – Значення бітів регістру 0x1d

Для виведення на екран всіх поточних параметрів роботи модуля скористуємося підпрограмою test_lora.py текст якої наведено в додатку Б. В результаті роботи даної підпрограми отримаємо наступні дані:

SX127x LoRa registers:

mode – SLEEP

freq– 434.000000 MHz

coding_rate – CR4_5

bw – BW125

spreading_factor – 128 chips/symb

implicit_hdr_mode – OFF

rx_payload_crc – OFF

tx_cont_mode – OFF

preamble – 8

low_data_rate_opti – OFF

```

agc_auto_on – ON
symb_timeout – 100
freq_hop_period – 0
pkt_snr_value – 64.000000
pkt_rssi_value – 164
rssi_value – 164
fei – 0
pa_select – RFO
max_power – 13.200000 dBm
output_power – 13.200000 dBm
ocp – ON
ocp_trim – 100.000000 mA
lna_gain – NOT_USED
lna_boost_lf – 0b0
lna_boost_hf – 0b0
detect_optimize – 0x3
detection_thresh – 0xa
sync_word – 0x12
dio_mapping 0..5 [0, 0, 0, 0, 2, 0]
tcxo – XTAL
pa_dac – default
status – {'signal_sync': 0, 'signal_detected': 0, 'header_info_valid': 0,
'rx_ongoing': 0, 'modem_clear': 0, 'rx_coding_rate': 0}
version – 0x12

```

Як можна бачити, виведенні параметри відповідають режиму роботи Spreading factor = 6 (128 chips/symb). Таким чином, поточні значення не відповідають оптимальним для заданого режиму експлуатації.

Попередні результати моделювання показали, що для включення модуля в оптимальному режимі потрібно змінити значення двох регістрів 0x1d та 0x1e. Принцип конфігурації регістру 0x1e показано на рисунку 4.11.

Name (Address)	Bits	Variable Name	Mode	Reset	LoRa™ Description
RegModemConfig 2 (0x1E)	7-4	SpreadingFactor	rw	0x07	SF rate (expressed as a base-2 logarithm) 6 → 64 chips / symbol 7 → 128 chips / symbol 8 → 256 chips / symbol 9 → 512 chips / symbol 10 → 1024 chips / symbol 11 → 2048 chips / symbol 12 → 4096 chips / symbol other values reserved.
	3	TxContinuousMode	rw	0	0 → normal mode, a single packet is sent 1 → continuous mode, send multiple packets across the FIFO (used for spectral analysis)
	2	RxPayloadCrcOn	rw	0x00	Enable CRC generation and check on payload: 0 → CRC disable 1 → CRC enable If CRC is needed, RxPayloadCrcOn should be set: - in Implicit header mode: on Tx and Rx side - in Explicit header mode: on the Tx side alone (recovered from the header in Rx side)
	1-0	SymbTimeout(9:8)	rw	0x00	RX Time-Out MSB

Рисунок 4.11 – Принцип конфігурації регістру 0x1e

Виконаємо налаштування оптимальної конфігурації модуля LoRa:

– значення регістру 0x1e: 131 → 1000 001 1 → 0x83;

– значення регістру 0x1d: 96 → 0110 0000 → 0x60.

Для зміни конфігурації регістрів була розроблена наступна функція:

```
#!/usr/bin/python3
import spidev
spi = spidev.SpiDev()
spi.open(0, 0)
spi.max_speed_hz = 5000000
RegOpMode = 0x1d
Value = 0
```



```

def set_bw():
    return spi.xfer([RegOpMode | 0x80, 0x72, 0x70])

set_bw()

# Read

ret_1 = spi.xfer([0x1d & 0x7F, 0])[1]
ret_2 = spi.xfer([0x1e & 0x7F, 0])[1]

print(ret_1)      # 128
print(ret_1 >> 7)  # 1
print(ret_2)
print(ret_2 >> 7)

spi.close()

```

Після роботи даної підпрограми ми отримали наступні дані конфігурації які зазначені на рисунку 4.12.

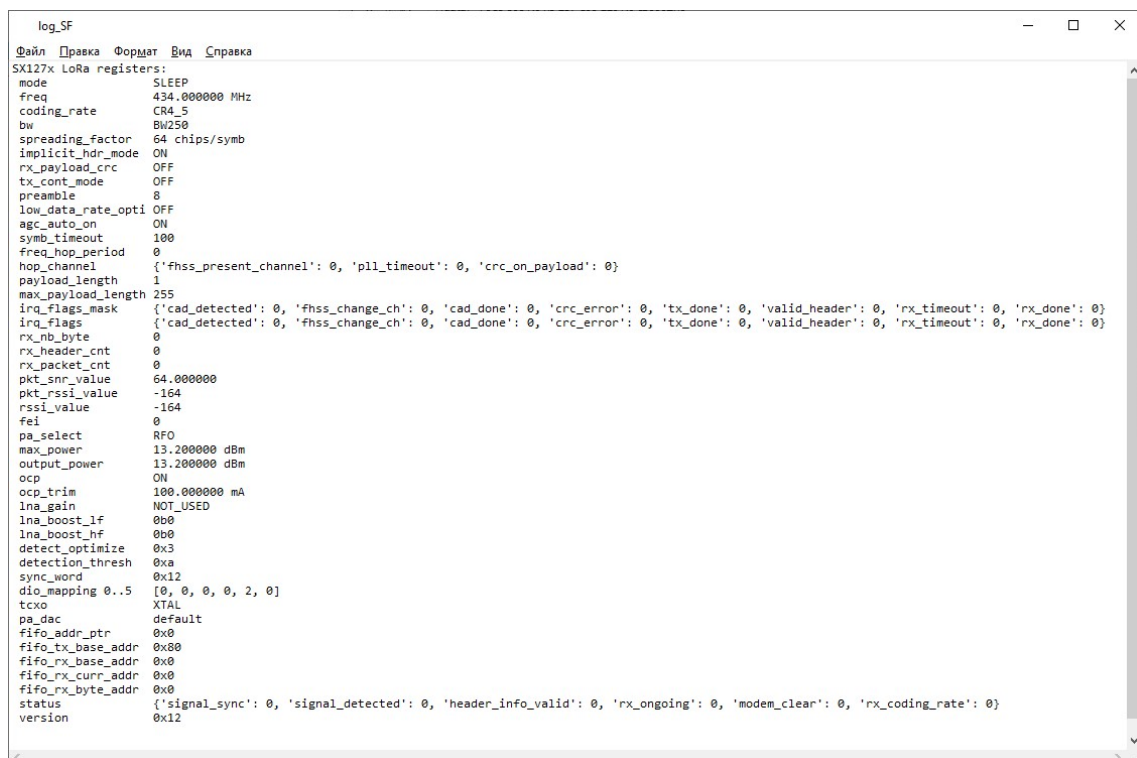
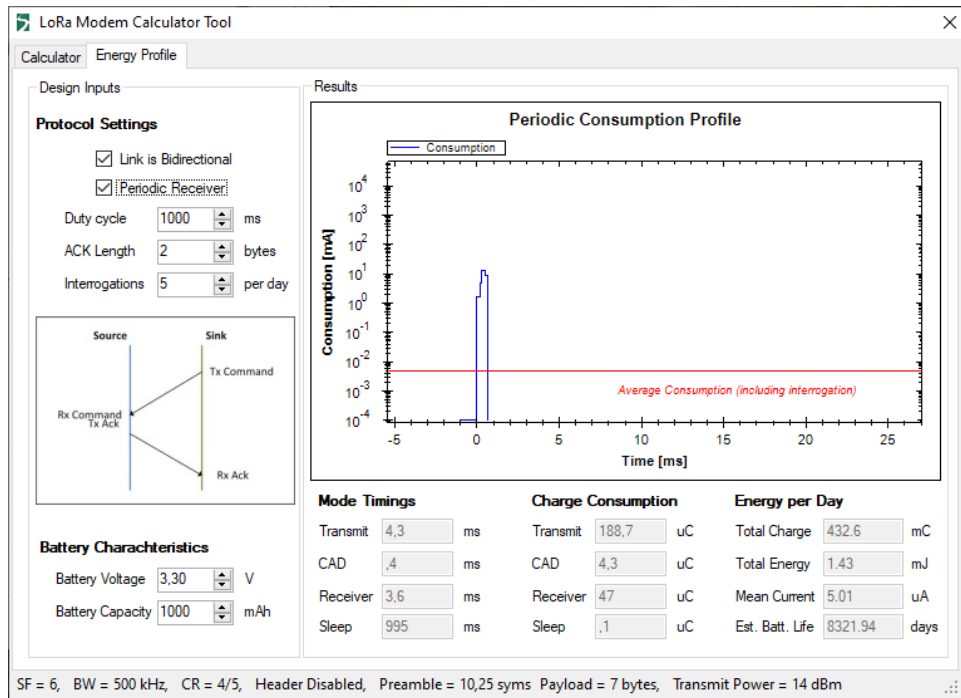


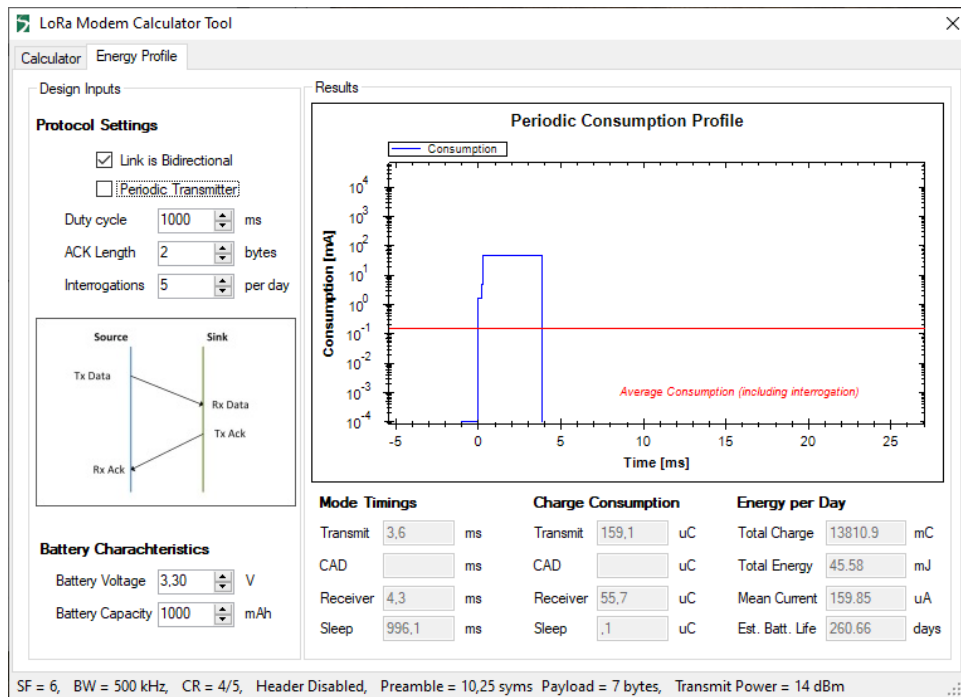
Рисунок 4.12 – Отримані результати оптимальної конфігурації модуля

LoRa

На рисунку 4.13 показано результат моделювання роботи шлюзу при використанні набору оптимальних параметрів.



а) результат моделювання для приймача



б) результат моделювання для передавача

Рисунок 4.13 – Результат моделювання роботи шлюзу при використанні вказаного набору оптимальних параметрів

4.3 Висновки за розділом

В результаті виконання четвертого розділу магістерської атестаційної роботи розроблена структурна схема макету до якого входять: мікрокомп'ютер з встановленою операційною системою; модуль Lora; тестовий модуль для емуляції роботи IoT пристроїв.

Проведено експериментальне дослідження роботи шлюзу, який побудовано на модулі SX-1278. На даному пристрої виконувалось моделювання роботи шлюзу з параметрами конфігурації, що отримані на етапі теоретичного моделювання.

Як можна бачити з рисунку 4.12 досягнуті задані режими роботи модуля LoRa, що відповідають оптимальному режиму прийому/передавання даних для заданих умов експлуатації.

В результаті моделювання та експериментальних досліджень отримані оптимальні параметри роботи шлюзу для заданих в попередньому розділі обмеженнях:

- Payload = 7 або 4 байти;
- Spreading factor = 6;
- BW \geq 250 кГц;
- поле заголовка відсутнє;
- поле контрольної суми відсутнє;
- тип кодування (CR) = 4/5.

Таким чином, нами розроблені методика та програмні скрипти для автоматизації визначення оптимальної конфігурації режимів роботи шлюзу IoT.

5 ОХОРОНА ПРАЦІ

5.1 Аналіз умов праці на робочому місці

Необхідні розміри для лабораторії, в якій проектується система, становить $10\text{ м} \times 6\text{ м} \times 3\text{ м}$. Робоче місце має складатися зі стола, стільця і персонального комп'ютера. У приміщенні працює 5 осіб. Площа приміщення 60 м^2 , об'єм – 180 м^3 . Згідно ДСанПіН 3.3.2.007-98 площа на одне робоче місце має становити не менше 6 м^2 , а об'єм – 20 м^3 . Для даного приміщення робоча площа і об'єм на одну людину відповідає нормам, так як в нашому випадку площа на одне робоче місце становить 8 м^2 , а об'єм – 25 м^3 .

Можна визначити перелік потенційно небезпечних і шкідливих виробничих факторів у приміщенні:

а) фізичні фактори: нестача природного світла, підвищене значення напруги в електричному ланцюзі, замикання, яке може статися через тіло людини, підвищена температура повітря робочої зони;

б) психофізіологічні фактори: розумове перенапруження, перенапруження зорових аналізаторів.

З перерахованих вище факторів, був обраний домінуючий фактор: підвищена температура повітря робочої зони.

5.2 Промислова безпека в лабораторії

Живлення комп'ютерів здійснюється від трифазної чотири провідної електричної мережі змінного струму з глухо заземленою нейтраллю, напругою 220/380 В, частотою 50 Гц.

Згідно НПАОП 40.1-1.21-98 лабораторію можна віднести до категорії без підвищеної небезпеки, так як в приміщенні відсутні чинники, які викликають підвищену або особливу небезпеку.

Для створення безпечних умов праці необхідно провести ряд організаційних і технічних заходів. Згідно НПАОП 40.1-1.32-01 для запобігання ураження людини електричним струмом у приміщенні застосовується система заземлення.

Відповідно до вимог НПАОП 0.00-4.12-05 проводиться вступний, первинний на робочому місці, повторний, цільовий та позаплановий інструктажі.

Зміст інструктажів відповідає вимогам НПАОП 0.00-4.12-05. Інструктаж зазначається у відповідних журналах з підписами інструктуємих.

5.3 Виробнича санітарія в лабораторії

Робота в лабораторії проводиться сидячи і не вимагає фізичної напруги. Тому вона відноситься до категорії Ia (легкі фізичні роботи, енерговитрати до 120 ккал/год.). З метою забезпечити комфортні умови для працівників відповідно до ДСН 3.3.6.042-99 в приміщенні встановлені наступні метеорологічні параметри:

а) для холодного періоду метеорологічні параметри забезпечуються опаленням приміщення:

- 1) температура повітря від 22 °С до 24 °С;
- 2) вологість повітря від 40 % до 60 %;
- 3) швидкість руху повітря оптимальна 0,1 м/с;

б) для теплого періоду року метеорологічні параметри забезпечуються кондиціонуванням повітря:

- 1) температура повітря від 23 °С до 25 °С;

2) вологість повітря від 40 % до 60 %;

3) швидкість руху повітря оптимальна 0,1 м/с.

Для освітлення робочих місць і приміщення в цілому застосовується як природне бічне освітлення, так і штучне освітлення.

Приміщення з ЕОМ повинні мати природне і штучне освітлення відповідно до ДБН Ст. 25-28-2006. Природне світло повинно проникати через бічні світлопройми, зорієнтовані, як правило, на північ чи північний схід, і забезпечувати коефіцієнт природної освітленості (КЕО) не нижче 1,5 %: $e^{IV} = 1,35$, де $e^{IV_{\text{норм}}}$ – нормоване значення КЕО для 4-го поясу світлового клімату.

Згідно ДСН 3.3.6.037-99 рівень шуму в лабораторії не перевищує 50 дБ.

Якщо обсяг приміщення, що припадає на одну людину, менше 20 м^3 , то кількість впускного повітря, необхідного для провітрювання, повинне бути не менш $G_I = 30 \text{ м}^3/\text{рік}$ на кожного працюючого; при об'ємі приміщення більше 20 м^3 на одного працюючого кількість приточного повітря для провітрювання, повинне бути не менш $G_I = 20 \text{ м}^3/\text{год.}$ на кожного працюючого.

Знаходимо об'єм приміщення, що припадає на одну людину:

$$V_1 = \frac{V}{n} = \frac{180}{7} = 25 \text{ м}^3 / \text{люд.}$$

Оскільки $V_1 > 20 \text{ м}^3/\text{люд.}$, то тоді норма подачі припливного повітря на 1 людину $G_I = 20 \text{ м}^3/\text{год.}$

Кількість припливного повітря з урахуванням чисельності робітників розраховується за формулою:

$$G = G_1 \cdot n = 20 \cdot 7 = 140 \text{ м}^3 / \text{люд.}$$

5.4 Пожежна безпека лабораторії

Розглянуте приміщення, згідно НАПБ Б. 03.002-2007, відноситься до категорії В – пожежонебезпечне. За ступенем вогнестійкості будівлі, згідно ДБН Ст. 1.1.7-2002 відноситься до 1-го ступеня вогнестійкості що відповідає класу пожежонебезпечності приміщення П-Па за НПАОП 40.1-1.21-97.

Пожежна безпека лабораторії забезпечується відповідно до ГОСТ 12.1.004-91 системою протипожежного захисту:

- встановлена автоматична пожежна сигналізація з димовими сповіщувачами ДІП-1, з розрахунку один сповіщувач на 20 м², але не менше 2 в одному приміщенні, враховуючи високу вартість обладнання, наявність прихованих комунікацій і специфіку загоряння ПК. Тобто на площу 60 м² необхідно три димових сповіщувача згідно ДБН Ст. 2.5-56-2010;

- розміщені 3 вуглекислотних вогнегасника ВВК-2 з розрахунку 1 вогнегасник на 3 ПК відповідно до НАПБ Б. 03.001-2004.

Організаційні заходи:

- проводиться інструктаж персоналу з техніки безпеки;
- розроблені заходи щодо дій адміністрації на випадок виникнення пожежі;
- схема евакуації при пожежі розміщена на видному місці.

У приміщенні 5 працюючих, тому згідно ДБН Ст. 1.1.7-2002 евакуацію під час пожежі можна проводити через робочий вихід. Додаткового евакуаційного виходу приміщення не має.

ВИСНОВКИ

В результаті виконання даної магістерської атестаційної роботи розроблена методика вибору оптимального режиму роботи апаратного забезпечення для організації взаємодії між компонентами бездротової мережі промислового Інтернету речей.

Методика вибору оптимального режиму роботи отримала розвиток у атестаційній роботі.

Проведено порівняння протоколів обміну повідомленнями в мережі інтелектуальних пристроїв та виявлені переваги та недоліки основних претендентів на використання в якості інструменту передавання даних на хмарний сервер. Таким протоколом виявився MQTT та сервер Mosquitto. Для побудови шлюзу в якості платформи використали одноплатний комп'ютер Raspberry PI з операційною системою Linux в якості базової операційної системи.

Проаналізовані вимоги до архітектури побудови мережі бездротових пристроїв за технологією IoT. Наведено математичне обґрунтування методу розрахунку пропускної здатності шлюзу.

В результаті виконання третього розділу магістерської атестаційної роботи проведено моделювання та вибір оптимальних параметрів роботи шлюзу IoT, за допомогою інструментів LoRa Modem Calculator, Channel Activity Detection.

Отримані наукові результати подальше використовувалися для настройки модуля:

- Spreading factor = 6;
- BW \geq 250 кГц;
- поле заголовка відсутнє;
- поле контрольної суми відсутнє;

– тип кодування (CR) = 4/5.

В результаті виконання четвертого розділу магістерської атестаційної роботи розроблена структурна схема макету до якого входять: мікрокомп'ютер з встановленою операційною системою; модуль Lora; тестовий модуль для емуляції роботи IoT пристроїв.

Проведено експериментальне дослідження роботи шлюзу проводили з IoT-пристроєм який побудовано на модулі SX-1278. На даному пристрої виконувались моделювання роботи шлюзу з параметрами конфігурації, що отримані на етапі теоретичного моделювання.

Як можна бачити з рисунку 4.12 були досягнуті задані режими роботи модуля LoRa, що відповідають оптимальному режиму прийому/передавання даних для заданих умов експлуатації.

В результаті моделювання та експериментальних досліджень отримані оптимальні параметри роботи шлюзу при заданих в попередньому розділі обмеженнях:

- Payload = 7 або 4 байти;
- Spreading factor = 6;
- BW \geq 250 кГц;
- поле заголовка відсутнє;
- поле контрольної суми відсутнє;
- тип кодування (CR) = 4/5.

Таким чином, нами розроблені методика та програмні скрипти для автоматизації визначення оптимальної конфігурації режимів роботи шлюзу IoT.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Коцюба А.О. Моделювання роботи мережі Iotawan для автоматизованої системи контролю та обліку електроенергії / Збірник студентських наукових статей «Automation and Developed of Electronic Devices» ADED-2020. – 2020. – № 1. – С. 74-79.

2. ДСТУ 3008-2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлення: Введ. 2015-22-06. – К.: Вид-во стандартів, 2016. – 26 с.

3. Методичні вказівки з «Розробки й оформлення магістерської атестаційної роботи» для студентів другого (магістерського) рівня вищої освіти галузі знань 15 Автоматизація та приладобудування за спеціальністю 151 Автоматизація та комп'ютерно-інтегровані технології освітні програми: «Автоматизоване управління технологічними процесами», «Комп'ютерноінтегровані технологічні процеси і виробництва», «Комп'ютеризовані та робототехнічні системи» / Упоряд. І.Ш. Невлюдов, В.В. Косенко, В.В. Євсєєв. – Харків: ХНУРЕ, 2019. – 55 с.

4. Бездротові технології [Електронний ресурс]. – Електрон. текстові дані. Режим доступу: https://uk.wikipedia.org/wiki/Бездротові_технології – 01.10.2020.

5. The Constrained Application Protocol (CoAP) [Електронний ресурс]. Електрон. текстові дані. – Режим доступу: <https://tools.ietf.org/html/rfc7252> – 20.10.2020 р.

6. AMQP 1.0 in Azure Service Bus and Event Hubs protocol guide [Електронний ресурс]. – Електрон. текстові дані. – Режим доступу: <https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-amqp-protocol-guide> – 21.10.2020 р. MQTT (MQ Telemetry Transport) [Електронний ресурс]. – Електрон. текстові дані. –

Режим доступу : <https://internetofthingsagenda.techtarget.com/definition/MQTT-MQ-Telemetry-Transport> – 20.10.2020 р.

7. STOMP Protocol Specification, Version 1.2 [Електронний ресурс]. – Електрон. текстові дані. – Режим доступу: <https://stomp.github.io/stompspecification-1.2.html>–21.10.2020р.

8. MQTT (MQ Telemetry Transport) [Електронний ресурс]. – Електрон. текстові дані. – Режим доступу : <https://internetofthingsagenda.techtarget.com/definition/MQTT-MQ-Telemetry-Transport> – 20.10.2020 р.

9. Архитектура интернета вещей / пер. с англ. М. А. Райтмана. - М.: ДМК Пресс, 2019. - 454 с.: ил.

10. Использование устройства IoT Edge в качестве шлюза [Електронний ресурс]. – Електрон. текстові дані. – Режим доступу: <https://docs.microsoft.com/ru-ru/azure/iot-edge/iot-edge-as-gateway> – 22.10.2020.

11. Особливості технології LoRaWAN [Електронний ресурс]. – Електронні текстові дані. – Режим доступу :https://iotji.io/osoblyvostilorawan/?gclid=Cj0KCQjw28T8BRDbARIsAEOMBcw8xpvff2xIG4ORdAd2KVkhEypF0fswOE7o1xSCFTUbch4vEefyg90aAhDnEALw_wcB – 22.10.2020 р.

12. Емкость сети LoRa [Електронний ресурс]. – Електрон. текстові дані. – Режим доступу: <https://itechinfo.ru/content/емкость-сети-lora> – 22.10.2020 р.

13. Обзор технологии Lora [Електронний ресурс]. – Електрон. текстові дані. – Режим доступу: <https://itechinfo.ru/content/обзор-технологии-lora> – 17.11.2020 р.

14. Модуляция и кодирование [Електронний ресурс]. – Електрон. текстові дані. – Режим доступу: <https://gist.github.com/Garrus007/d696715917626edd4ba19bb76e72e71a> – 17.11.2020 р.

15. Software Defined Radio – как это работает? Часть 7 [Електронний ресурс]. – Електрон. текстові дані. – Режим доступу: <https://habr.com/ru/post/454666/> – 18.11.2020 р.

16. SX1276/77/78/79 Керівництво користувача. [Електронний ресурс]. – Електрон. текстові дані. – Режим доступу: https://cdnshop.adafruit.com/product-files/3179/sx1276_77_78_79.pdf – 18.11.2020 р.

17. Novoselov, Sergii & Sychova, Oksana. Using Wireless Technology for Managing Distributed Industrial Automation Objects within the Concept of Industry // IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T – 2019 – P. 580-584.

18. Технічні засоби автоматизації: Підручник / І.Ш. Невлюдов, А.О. Андрусевич, О.І. Филипенко, Н.П. Демська, С.П. Новоселов. – Кривий Ріг : Криворізький коледж НАУ, 2019. – 366 с.

19. Невлюдов І. Ш. Людино-машинний інтерфейс в технічних засобах автоматизації: Навчальний посібник / І. Ш. Невлюдов, О. І. Филипенко, Б. О. Шостак. – Харків : «ХТМТ», 2019. – 244 с.

20. Основи наукових досліджень: Навч. посібник / І.Ш. Невлюдов, Ю.М. Олександров, А.О. Андрусевич, О.О. Чала. – Кривий Ріг: Криворізький коледж НАУ, 2019. – 396 с.

21. Конспект лекцій з дисципліни "Теорія автоматичного управління" для напряму підготовки 6.050202 «Автоматизація та комп'ютерно-інтегровані технології» [Електронний ресурс] / ХНУРЕ ; розроб. О. В. Токарева. - Харків, 2015. — 32 с.