

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ**

КВАЛІФІКАЦІЙНА РОБОТА

**на тему: «Гетерогенна IoT-система моніторингу та керування
житловим приміщенням на основі мультипротокольної взаємодії»**

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
(код, найменування спеціальності)
освітньо-професійної програми Інформаційні системи та технології
(назва)

*Кваліфікаційна робота містить результати власних досліджень.
Використання ідей, результатів і текстів інших авторів мають посилання на
відповідне джерело*

_____ **Володимир ДУБОВСЬКИЙ**
(підпис) (ім'я, ПРІЗВИЩЕ здобувача)

Виконав: здобувач вищої освіти група ІСД-41

_____ **Володимир**
ДУБОВСЬКИЙ

(ім'я, ПРІЗВИЩЕ)
Керівник Ольга ПОЛОНЕВИЧ
к.т.н., доцент (ім'я, ПРІЗВИЩЕ)

Рецензент: _____
к.т.н., доцент (ім'я, ПРІЗВИЩЕ)

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

Навчально-науковий інститут інформаційних технологій

Кафедра Інформаційних систем та технологій

Ступінь вищої освіти бакалавр

Спеціальність 126 Інформаційні системи та технології

Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ

Завідувач кафедри ІСТ

Каміла СТОРЧАК

“ ” 2026 року

**З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Дубовському Володимирі Васильовичу

(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Гетерогенна IoT-система моніторингу та керування житловим приміщенням на основі мультипротокольної взаємодії

керівник кваліфікаційної роботи: Ольга ПОЛОНЕВИЧ к.т.н., доцент

(ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20” лютого 2026 р. № 51

2. Строк подання кваліфікаційної роботи «01» червня 2026 р.

3. Вихідні дані кваліфікаційної роботи:

1. Принципи побудови та функціонування IoT.
2. Принцип побудови гетерогенних IoT – мереж .
3. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

1. Аналіз основних можливостей та технологій IoT.
2. Дослідження концепції гетерогенної IoT мережі .
3. Проєктування та впровадження Гетерогенна IoT-система моніторингу та керування житловим приміщенням на основі мультипротокольної взаємодії.

5.Перелік ілюстраційного матеріалу: *презентація*

6. Дата видачі завдання «20» лютого 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Підбір технічної літератури	20.02-03.03.26	
2.	Аналіз основних можливостей та технологій ПоТ	04.03-17.03.25	
3.	Дослідження архітектури мультипротокольної системи моніторингу.	18.03-31.03.26	
4.	Проектування та впровадження гетерогенної IoT-системи моніторингу та керування житловим приміщенням на основі мультипротокольної взаємодії.	01.04-24.04.26	
5.	Висновки по роботі	25.04-16.05.26	
6.	Розробка демонстраційних матеріалів, доповідь.	19.05-20.05.26	
7.	Оформлення бакалаврської роботи	29.05-30.05.26	

Здобувач вищої освіти

Володимир ДУБОВСЬКИЙ

(підпис)

(ім'я, ПРІЗВИЩЕ)

Керівник кваліфікаційної роботи

Ольга ПОЛОНЕВИЧ

(підпис)

(ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступня бакалавр: 101 стор., 12 рис., 29 джерел.

Мета роботи – розробка гетерогенної IoT-системи моніторингу та керування житловим приміщенням на основі мультипротокольної взаємодії.

Об'єкт дослідження – процеси моніторингу та керування інженерними системами житлових приміщень із застосуванням бездротових каналів передачі даних.

Предмет дослідження – є методи, алгоритми та апаратно-програмні засоби організації мультипротокольної взаємодії у гетерогенних IoT-мережах.

Короткий зміст роботи. У бакалаврській роботі розроблено гетерогенну IoT-систему моніторингу та керування житловим приміщенням на основі мультипротокольної взаємодії. Проведено аналіз архітектурних особливостей житлових будівель як середовища поширення радіохвиль та порівняльний аналіз бездротових протоколів, обґрунтовано застосування технології LoRa (LPWAN) на основі математичних моделей загасання Motley-Keenan та COST-231. Розроблено структурну модель гетерогенної мережі та спроектовано схемотехніку мультипротокольного шлюзу (NanoPi), LoRa-вузлів (ATmega328P + SX1278) і Wi-Fi-вузлів (ESP32 + BME280). Реалізовано програмне забезпечення на базі MQTT і Node-RED з механізмами захисту TLS та AES-128. Проведено аналітичне дослідження ефективності системи за показниками RSSI, SNR та BER.

КЛЮЧОВІ СЛОВА: ІНТЕРНЕТ РЕЧЕЙ, IoT, ГЕТЕРОГЕННА МЕРЕЖА, МУЛЬТИПРОТОКОЛЬНА СИСТЕМА, LORA, LPWAN, WI-FI, MQTT, РАДІОЗАТІНЕНА ЗОНА, ЕФЕКТ КЛІТКИ ФАРАДЕЯ, ЗАЛІЗОБЕТОННІ КОНСТРУКЦІЇ, ЗАГАСАННЯ РАДІОСИГНАЛУ, ШЛЮЗ, СЕНСОРНИЙ ВУЗОЛ, ЕНЕРГЕТИЧНИЙ БЮДЖЕТ, TLS-ШИФРУВАННЯ, AES-128, МОНІТОРИНГ ЖИТЛОВИХ ПРИМІЩЕНЬ.

ЗМІСТ

ВСТУП.....	7
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ГЕТЕРОГЕННИХ ІОТ-МЕРЕЖ У ЖИТЛОВИХ ОБ'ЄКТАХ.....	7
1.1. Аналіз архітектурних особливостей сучасних будівель як середовища поширення радіохвиль	7
1.2. Класифікація бездротових протоколів за критеріями енергоефективності та проникаючої здатності	11
1.3. Дослідження специфіки загасання радіосигналу в залізобетонних конструкціях та заглиблених технічних приміщеннях	14
1.4. Обґрунтування застосування технологій LPWAN (LoRa) для подолання ефекту екранування	17
1.5. Висновки до розділу та постановка технічного завдання.....	20
РОЗДІЛ 2. ПРОЄКТУВАННЯ АРХІТЕКТУРИ МУЛЬТИПРОТОКОЛЬНОЇ СИСТЕМИ МОНІТОРИНГУ	22
2.1. Розробка структурної моделі гетерогенної мережі з багаторівневою топологією.....	22
2.2. Математичне обґрунтування вибору діапазонів частот для роботи в радіозатінених зонах	25
2.3. Вибір компонентної бази для розробки центрального шлюзу та автономних сенсорних вузлів	30
РОЗДІЛ 3. АПАРАТНА ТА ПРОГРАМНА РЕАЛІЗАЦІЯ ГЕТЕРОГЕННОЇ СИСТЕМИ	34
3.1. Проєктування мультипротокольного комунікаційного хаба	34
3.2. Розробка автономних інтелектуальних сенсорів	42
3.3. Програмне забезпечення та інтеграція.....	50
3.4. Забезпечення інформаційної безпеки в гетерогенному середовищі.....	73
РОЗДІЛ 4. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ РОЗРОБЛЕНОЇ СИСТЕМИ	79
4.1. Порівняльний аналіз показників потужності сигналу (RSSI) та відношення сигнал/шум (SNR) у важкодоступних зонах об'єкта.....	79

4.2. Дослідження стабільності мультипротокольної взаємодії при пікових навантаженнях	83
4.3. Верифікація функціональних можливостей користувацького інтерфейсу моніторингу	85
ВИСНОВКИ	87
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	90

ВСТУП

Актуальність теми. Стрімкий розвиток концепції «Інтернету речей» (Internet of Things, IoT) за останнє десятиліття призвів до повсюдного впровадження бездротових систем збору телеметрії у житлово-комунальному секторі. За даними аналітичного звіту IoT Analytics (2024), кількість активних IoT-пристроїв у світі перевищила 18,8 мільярдів, з яких понад 30% експлуатуються в сегменті Smart Home та Smart Building [1]. Основне призначення таких систем - автоматизований моніторинг параметрів мікроклімату, обліку енергоресурсів, контролю доступу та раннього виявлення аварійних ситуацій (протікання води, витоку газу, задимлення).

Однак масове впровадження бездротових рішень у житловому секторі стикається з низкою фізичних обмежень, які не були критичними для типових промислових застосувань. Сучасна архітектура житлових будівель характеризується використанням залізобетонних конструкцій з густою арматурною сіткою, що створює ефект часткового електромагнітного екранування (ефект клітки Фарадея). Як наслідок, значна частина технічно важливих приміщень - підвали, теплопункти, гаражі, електрощитові, допоміжні приміщення за внутрішніми стінами - виявляється у так званих «радіозатінених зонах», де рівень сигналу стандартних протоколів (Wi-Fi 2,4 ГГц, Bluetooth Low Energy, Zigbee 2,4 ГГц) падає нижче порогу чутливості приймача.

У рекомендації ITU-R P.1238-11 [2] зазначено, що усереднене загасання електромагнітної хвилі частотою 2,4 ГГц при проходженні крізь одне залізобетонне перекриття товщиною 20 см сягає 25–35 дБ, що еквівалентно зменшенню потужності сигналу у 300–3000 разів. Це унеможлиблює застосування високочастотних протоколів для моніторингу заглиблених приміщень без використання додаткових ретрансляторів, а встановлення проводових ліній у готових житлових будинках економічно та технологічно недоцільне.

Альтернативним рішенням є використання технологій класу LPWAN (Low-Power Wide-Area Network), зокрема протоколу LoRa, що працює у субгігагерцовому діапазоні (868 МГц у Європі, 433 МГц у деяких регіонах) та забезпечує чутливість приймача до -148 дБм завдяки застосуванню модуляції Chirp Spread Spectrum (CSS). Проте LoRa принципово не призначена для передачі великих обсягів даних (обмеження робочого циклу 1% у SRD-діапазоні, згідно з ETSI EN 300 220 [3]) та непридатна для високочастотного опитування датчиків мікроклімату чи роботи з мультимедіа.

Звідси впливає суперечність, що визначає актуальність теми: жоден окремий бездротовий протокол не здатен одночасно забезпечити покриття заглиблених приміщень та високу пропускну здатність для сенсорів мікроклімату у житлових зонах. Вирішення цієї суперечності лежить у площині гетерогенних мультипротокольних систем, у яких різні фізичні рівні передачі даних координуються єдиним інтелектуальним шлюзом. Розробка архітектури, схемотехніки та програмного забезпечення такої системи для типового житлового об'єкта є актуальним науково-технічним завданням, що має пряме практичне значення для галузей автоматизації житла, комунального обліку та систем раннього попередження.

Мета та завдання дослідження

Метою дипломної роботи є розробка гетерогенної IoT-системи моніторингу та керування житловим приміщенням на основі мультипротокольної взаємодії, що забезпечує надійну передачу даних як у житлових зонах з типовими умовами поширення сигналу, так і в радіозатінених приміщеннях зі значним рівнем електромагнітного екранування.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Провести аналіз архітектурних особливостей сучасних житлових будівель як середовища поширення радіохвиль та визначити типові зони з високим рівнем загасання сигналу.

2. Виконати порівняльний аналіз бездротових протоколів зв'язку за критеріями енергоефективності, проникаючої здатності та пропускнуєї спроможності.

3. Обґрунтувати застосування технологій LPWAN (LoRa) для подолання ефекту екранування у заглиблених приміщеннях на підставі математичних моделей загасання радіосигналу.

4. Розробити структурну модель гетерогенної мережі з багаторівневою топологією та виконати математичне обґрунтування вибору частотних діапазонів.

5. Спроекувати схемотехніку мультипротокольного комунікаційного шлюзу (NanoPi + SX1278 + CC2530) та розрахувати параметри друкованої плати.

6. Розробити автономні інтелектуальні сенсорні вузли для LoRa-сегмента (ATmega328P + SX1278) та Wi-Fi-сегмента (ESP32 + BME280).

7. Реалізувати програмне забезпечення шлюзу та кінцевих пристроїв, забезпечити конфігурування MQTT-брокера та середовища Node-RED для оркестрації потоків даних.

8. Реалізувати механізми інформаційної безпеки (TLS-шифрування, автентифікація клієнтів, захист LoRa-трафіку алгоритмом AES-128).

9. Провести аналітичне дослідження ефективності розробленої системи за показниками RSSI, SNR та BER у характерних зонах житлового об'єкта.

Об'єктом дослідження є процеси моніторингу та керування інженерними системами житлових приміщень із застосуванням бездротових каналів передачі даних.

Предметом дослідження є методи, алгоритми та апаратно-програмні засоби організації мультипротокольної взаємодії у гетерогенних IoT-мережах.

Методи дослідження

У роботі застосовано такі методи: теоретичний аналіз нормативних документів ITU-R, IEEE, ETSI та OASIS; математичне моделювання загасання радіосигналу за моделями Free Space Path Loss, COST-231 Multi-Wall та

Motley–Keenan; схемотехнічне проєктування з використанням методики розрахунку енергетичного бюджету лінії зв'язку; розрахунок друкованих плат за стандартом IPC-2221; аналітичне моделювання ймовірності бітової помилки для різних схем модуляції (CSS, OFDM).

Наукова новизна одержаних результатів

Наукова новизна роботи полягає у наступному:

- удосконалено архітектуру гетерогенної IoT-системи шляхом запровадження триетапного алгоритму протокольної конвергенції (декапсуляція - нормалізація - інкапсуляція у MQTT-топіки), що забезпечує прозорість взаємодії кінцевих пристроїв, підключених через різні фізичні рівні;

- запропоновано методику обґрунтованого вибору частотного діапазону для сенсорних вузлів житлових IoT-систем на основі комбінованого розрахунку FSPL, діелектричних втрат у залізобетоні та запасу енергетичного бюджету;

- адаптовано моделі Motley–Keenan та COST-231 для оцінки якості зв'язку у типових конфігураціях житлових приміщень з виділенням п'яти характерних зон за рівнем екранування.

Практичне значення результатів

Розроблена система може бути впроваджена в багатоквартирних житлових будинках для вирішення таких практичних задач: автоматизований облік холодної/гарячої води та теплоенергії з лічильників, розташованих у підвальних теплопунктах; раннє виявлення протікань у прихованих комунікаціях; моніторинг мікроклімату у житлових зонах; контроль стану вхідних дверей та вікон; віддалене керування клапанами та реле. Розрахунки та схемотехнічні рішення, наведені в роботі, мають самодостатній характер і можуть бути безпосередньо використані при серійному виготовленні шлюзу та сенсорних вузлів.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ГЕТЕРОГЕННИХ ІОТ-МЕРЕЖ У ЖИТЛОВИХ ОБ'ЄКТАХ

1.1. Аналіз архітектурних особливостей сучасних будівель як середовища поширення радіохвиль

Поширення електромагнітної хвилі всередині житлової будівлі принципово відрізняється від її поширення у вільному просторі. Сукупність перекриттів, несучих та перегородкових стін, комунікаційних шахт і металевих конструктивних елементів формує складне багатокomпонентне середовище, у якому одночасно діють механізми поглинання, відбиття, дифракції та розсіювання радіохвиль. Для коректного проєктування IoT-мережі необхідно розуміти вплив кожного з цих механізмів.

У практиці житлового будівництва на території України найбільш поширені п'ять типів конструкцій несучих елементів, кожен з яких має відмінні характеристики щодо поширення радіохвиль.

Таблиця 1.1

Типові конструктивні рішення житлових будівель та їх вплив на
поширення сигналу

Тип будівлі	Основний матеріал несучих стін	Товщина, см	Типове загасання сигналу @ 2,4 ГГц, дБ
«Хрущовка» (цегляна)	Силікатна/керамічна цегла	38–50	8–14
Панельні будинки серій 464, 134	Залізобетонна панель	14–18	12–18
«Чешки» (цегляні з панелями)	Комбінована конструкція	40–60	10–20

Продовження таблиці 1.1

Сучасні монолітно- каркасні	Залізобетон + пінобетон	20–35	15–28
Сучасні монолітні	Залізобетон монолітний	20–30	20–35

Як видно з таблиці, монолітні залізобетонні конструкції створюють найбільш несприятливі умови для поширення сигналу. Причина полягає не лише у високій діелектричній проникності бетону ($\epsilon_r \approx 4,5\text{--}7,0$ для сухого та $8\text{--}12$ для вологого), а й у наявності в його структурі арматурного каркасу.

Арматурний каркас сучасних залізобетонних перекриттів зазвичай виконується з прутків діаметром $10\text{--}14$ мм, зварених у сітку з кроком 150×150 мм або 200×200 мм (згідно з ДБН В.2.6-98:2009 [5]). Така металева сітка, поміщена в діелектрик (бетон), утворює структуру, аналогічну клітці Фарадея.

Основний критерій екранування сіткою - співвідношення між розміром її комірки a та довжиною електромагнітної хвилі λ . Коли виконується умова $a \ll \lambda$, сітка поводить себе як суцільний металевий екран. Для хвиль частотою $2,4$ ГГц ($\lambda = 12,5$ см) комірка сітки 15×15 см знаходиться у критичному співвідношенні - частина енергії хвилі проходить крізь неї, але зі значним загасанням. Для частоти 868 МГц ($\lambda = 34,5$ см) співвідношення $a/\lambda \approx 0,43$, що дозволяє хвилі проникати крізь сітку з меншими втратами [5].

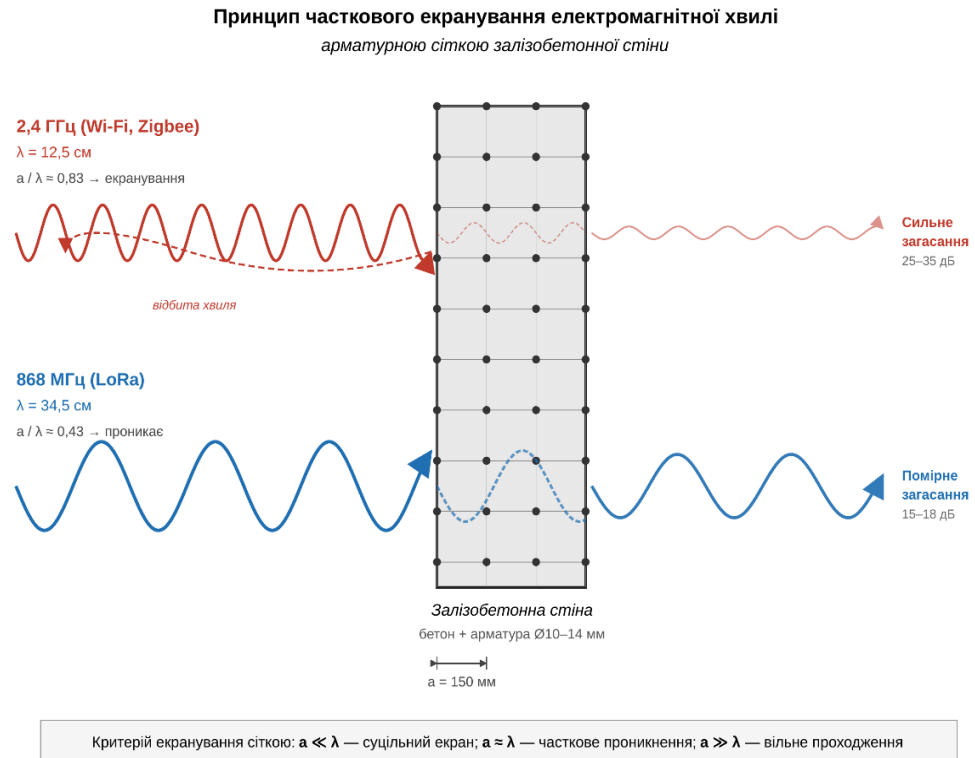


Рис.1.1. Принцип часткового екранування електромагнітної хвилі
арматурною сіткою залізобетонної стіни

Для точного моделювання втрат сигналу при проходженні крізь перешкоди необхідне врахування трьох електрофізичних параметрів: відносної діелектричної проникності ϵ_r , провідності σ (См/м) та тангенса кута втрат $\tan \delta$. Саме тангенс діелектричних втрат характеризує здатність матеріалу перетворювати електромагнітну енергію на теплову.

Таблиця 1.2

Електрофізичні параметри будівельних матеріалів на частоті 2,4 ГГц

[6]

Матеріал	ϵ_r	σ , См/м	$\tan \delta$	Загасання, дБ/м
Цегла суха	3,9	0,02	0,02	5,2
Бетон сухий	4,5	0,04	0,03	8,7
Бетон вологий	8,5	0,12	0,05	24,6

Продовження таблиці 1.2

Залізобетон (з арматурою)	-	-	-	35–80
Гіпсокартон	2,4	0,005	0,01	1,1
Скло віконне	4,0	0,001	0,002	0,4
Деревина	2,0	0,01	0,03	2,8

Критично важливим є той факт, що провідність і діелектрична проникність більшості будівельних матеріалів суттєво зростають із збільшенням вологості. За результатами досліджень NIST [6], загасання сигналу в бетоні при підвищенні вологості з 3% до 10% збільшується на 6–10 дБ. Це пояснює погіршення зв'язку IoT-пристроїв у підвальних приміщеннях з високою вологістю - стандартною умовою експлуатації тепловентильних і насосних.

На підставі натурних обстежень типових житлових будівель можна виділити п'ять характерних зон за рівнем екранування:

-Зона 1 (відкрита): житлові кімнати з прямою видимістю до точки доступу. Загасання - лише внаслідок FSPL.

-Зона 2 (легке екранування): суміжні кімнати, розділені однією внутрішньою перегородкою з гіпсокартону або цегли (товщина 7–12 см). Додаткове загасання 3–8 дБ.

-Зона 3 (середнє екранування): коридори, кухні, санвузли - розділені 1–2 несучими стінами або перекриттям. Додаткове загасання 12–25 дБ.

-Зона 4 (важке екранування): підсобні приміщення, прилеглі до підвалу, балкони з утепленням пінопластом + алюмінієва фольга. Додаткове загасання 25–40 дБ.

-Зона 5 (критичне екранування): підвали, тепловентилятори, гаражі - відділені від точки доступу двома і більше залізобетонними перекриттями. Додаткове загасання 45–80 дБ.

Саме в зонах 4 та 5 використання високочастотних протоколів (Wi-Fi, BLE, Zigbee 2,4 ГГц) стає технічно неможливим без ретрансляторів.

1.2. Класифікація бездротових протоколів за критеріями енергоефективності та проникаючої здатності

Сучасні бездротові технології для IoT-застосувань можна класифікувати за трьома базовими характеристиками: дальністю дії, пропускною спроможністю та енергоспоживанням. Між цими параметрами існує фундаментальний компроміс, відомий як IoT Trade-off Triangle - одночасне покращення двох із трьох характеристик завжди відбувається ціною погіршення третьої[8].

За дальністю дії та швидкістю передачі бездротові протоколи поділяються на чотири класи: WPAN (Wireless Personal Area Network), WLAN (Wireless Local Area Network), LPWAN (Low-Power Wide-Area Network) та WMAN/стільникові мережі.

Таблиця 1.3

Порівняльна характеристика бездротових протоколів для IoT-застосувань

Протокол	Клас	Діапазон	Макс. дальність	Макс. швидкість	Чутливість
Wi-Fi 802.11n	WLAN	2,4/5 ГГц	30–50 м	150 Мбіт/с	–72 дБм
Bluetooth 5.0	WPAN	2,4 ГГц	50–100 м	2 Мбіт/с	–95 дБм
Zigbee 3.0	WPAN	2,4 ГГц	50–100 м	250 кбіт/с	–100 дБм
Z-Wave	WPAN	868 МГц	30–100 м	100 кбіт/с	–104 дБм
LoRa (SF12)	LPWAN	868 МГц	5–15 км	293 біт/с	–148 дБм
Sigfox	LPWAN	868 МГц	до 50 км	100 біт/с	–142 дБм
NB-IoT	Стільникова	LTE band	до 35 км	250 кбіт/с	–141 дБм

З таблиці 1.3 видно, що LoRa суттєво випереджає усі інші протоколи за чутливістю приймача (-148 дБм проти -72 дБм у Wi-Fi)[9]. Різниця у 76 дБ еквівалентна збільшенню допустимого загасання сигналу приблизно у 40 мільйонів разів, що і є ключовим фактором здатності LoRa долати радіозатінені зони.

За характером енергоспоживання IoT-протоколи поділяються на три групи.

1. Постійно увімкнені (*Always-On*): Wi-Fi, класичний Bluetooth. Середнє споживання $70\text{--}300$ мА у режимі прийому, що унеможливорює тривалу автономну роботу від батареї.

2. Дуті-циклові (*Duty-Cycled*): BLE, Zigbee, Z-Wave. Короткочасні «пробудження» з нижчою активністю. Середнє споживання $0,5\text{--}5$ мА, автономність - місяці.

3. Псевдо-асинхронні (*Class A*): LoRa у режимі ALOHA. Передавач активний лише у момент передачі пакета ($30\text{--}500$ мс раз на декілька хвилин). Середнє споживання $10\text{--}50$ мкА, автономність - роки.

Розглянемо кількісну оцінку автономності вузла. Нехай пристрій живиться від літій-іонного акумулятора 18650 ємністю $Q = 3000$ мА·год. Середній струм споживання описується формулою

$$I_{avg} = I_{sleep} + \frac{t_{tx}}{T} \times I_{tx} - I_{sleep} \quad (1.1)$$

де:

I_{sleep} - струм у режимі сну;

t_{tx} - струм у режимі передачі;

I_{tx} - тривалість сеансу передачі;

T - період передачі;

Таблиця 1.4

Розрахункова автономність IoT-вузла при передачі 1 раз на 10 хвилин
[7]

Протокол	I_{sleep} , мкА	I_{tx} , мА	t_{tx} , мс	I_{avg} , мкА	Автономність, міс.
Wi-Fi (ESP32)	150	240	3000	1350	3,1
Bluetooth LE	5	15	50	6,25	554
Zigbee	2	35	30	3,75	923
LoRa (SF7)	2	120	150	5,00	692
LoRa (SF12)	2	120	1200	26,0	133

Як видно, LoRa з SF7 забезпечує автономність понад 4 роки, що критично для сенсорів у важкодоступних місцях, де заміна батарей проблематична.

Проникаюча здатність сигналу при проходженні крізь стіни описується сукупним коефіцієнтом втрат L_{walls} , що залежить від частоти, матеріалу та товщини перешкоди. Порівняння протоколів за цим параметром наведено в таблиці 1.5.

Таблиця 1.5

Типові втрати при проходженні однієї залізобетонної стіни (товщина 20 см)

Протокол	Частота, МГц	Втрати, дБ	Відносне погіршення (× раз)
LoRa	868	15–18	32–63
Z-Wave	868	15–18	32–63
Zigbee	2400	25–35	316–3162
Wi-Fi	2400	25–35	316–3162

Продовження таблиці 1.5

Wi-Fi	5800	30–42	1000–15848
-------	------	-------	------------

Видно, що перехід з діапазону 2,4 ГГц на 868 МГц зменшує втрати у перешкодах у 5–50 разів. Це - визначальний аргумент на користь LPWAN-протоколів для роботи в заглиблених приміщеннях.

1.3. Дослідження специфіки загасання радіосигналу в залізобетонних конструкціях та заглиблених технічних приміщеннях

Точне передбачення якості зв'язку в конкретній конфігурації житлового приміщення потребує застосування адекватних моделей загасання радіосигналу. Універсальна модель FSPL, розглянута у Розділі 2, справедлива лише у вільному просторі і не враховує впливу перешкод. У цьому підрозділі розглядаються спеціалізовані моделі багатостінного загасання.

Модель Motley–Keenan, вперше запропонована у 1988 році і пізніше прийнята як базова в рекомендації ITU-R P.1238, описує сумарні втрати сигналу як суму втрат у вільному просторі та втрат у перешкодах:

$$L_{MK} = L_{FSPL} + n \times L_{wall} + m \times L_{floor} \quad (1.2)$$

де:

L_{FSPL} - втрати у вільному просторі (дБ);

n - кількість стін між передавачем і приймачем;

L_{wall} - втрати в одній стіні (дБ);

m - кількість перекриттів;

L_{floor} - втрати в одному перекритті (дБ).

Для типових житлових конфігурацій в Україні приймаються наступні значення:

- $L_{wall} = 5\text{--}8$ дБ для цегляної стіни (12 см) на 868 МГц;

- $L_{wall} = 12\text{--}15$ дБ для залізобетонної стіни (20 см) на 868 МГц;
- $L_{wall} = 25\text{--}35$ дБ для залізобетонної стіни (20 см) на 2,4 ГГц;
- $L_{floor} = 18\text{--}22$ дБ для перекриття (20 см) на 868 МГц;
- $L_{floor} = 30\text{--}40$ дБ для перекриття (20 см) на 2,4 ГГц.

1.3.2. Модель COST-231 Multi-Wall

Розширенням моделі Motley–Keenan є модель COST-231 Multi-Wall [10], що враховує неоднорідність загасання різних типів стін та ефект накопичувального спадання загасання при великій кількості перешкод:

$$L_{MW} = L_{FSPL} + L_c + \sum(k_{wi} \times L_{wi}) + k_f^{\frac{k_f+2}{(k_f+1)-b}} \times L_f \quad (1.3)$$

де:

L_c - фіксовані апаратні втрати (зазвичай 1–3 дБ);

k_{wi} - кількість стін типу i ;

L_{wi} - втрати в стіні типу i ;

k_f - кількість перекриттів;

L_f - втрати в одному перекритті;

b - емпіричний коефіцієнт ($\approx 0,46$ для житлових будівель).

Особливість моделі COST-231 - врахування нелінійного зростання втрат при проходженні декількох перекриттів. У реальних умовах четверте і подальші перекриття додають меншу кількість децибел, ніж перші три, що пояснюється ефектом дифракційних шляхів.

Виконаємо розрахунок сумарного загасання для п'яти зон, описаних у п. 1.1.4, за моделлю Motley-Keenan. Припустимо, що шлюз знаходиться у житловій зоні на висоті 2,5 м, а відстань до всіх зон - 10 м. Результати зведено у таблиці 1.6.

Таблиця 1.6

Розрахункові сумарні втрати сигналу в характерних зонах житлового
об'єкта

Зона	Перешкоди	$L_{\text{FSPL}}, 868$ МГц	$L_{\text{wall}}, 868$	$L_{\text{сум}}, 868$	$L_{\text{сум}}, 2400$
1. Відкрита	0	51,2	0	51,2	60,1
2. Легке екранування	1 перегородка	51,2	5	56,2	70,1
3. Середнє екранування	2 стіни	51,2	26	77,2	110,1
4. Важке екранування	2 стіни + 1 перекриття	51,2	46	97,2	150,1
5. Критичне екранування	2 стіни + 2 перекриття	51,2	64	115,2	190,1

Порівняння отриманих значень $L_{\text{сум}}$ з чутливістю приймачів (-148 дБм для LoRa при потужності передавача $+14$ дБм + підсилення антен 5 дБі = 167 дБ допустимих втрат; -72 дБм для Wi-Fi при потужності $+20$ дБм + антени 5 дБі = 97 дБ допустимих втрат) показує, що у зонах 3–5 Wi-Fi принципово непрацездатний, тоді як LoRa має запас енергетичного бюджету 50 – 110 дБ, що гарантує стабільну роботу.

Крім стаціонарних втрат, у житлових IoT-мережах суттєвим є ефект short-term fading - короточасних замирань сигналу внаслідок переміщення людей, відкривання дверей, руху меблів. У рекомендації ITU-R P.1238-11 зазначається, що типова глибина замирань у житлових приміщеннях становить 8 – 15 дБ з середньою тривалістю 100 – 500 мс [2]. Для протоколів, що використовують короткі передачі (LoRa, Zigbee), це є суттєвим чинником, який обов'язково має бути врахований через запас надійності $M_s \geq 10$ дБ при розрахунку енергетичного бюджету (див. Розділ 2).

1.4. Обґрунтування застосування технологій LPWAN (LoRa) для подолання ефекту екранування

Розглянутий у попередніх підрозділах матеріал доводить, що саме технології LPWAN, зокрема LoRa, є оптимальним рішенням для моніторингу заглиблених приміщень житлових будівель. У цьому підрозділі детально розглядаються фізико-технічні основи такої переваги.

Ключовою інновацією технології LoRa є застосування широкосмугової модуляції Chirp Spread Spectrum (CSS), що дозволяє отримати суттєвий процесуальний вииграш при демодуляції слабких сигналів. На відміну від традиційних схем з модуляцією символу окремим коливанням, у CSS кожен символ кодується лінійно-частотно-модульованим (LFM) імпульсом - «чірпом», що перекриває повну смугу каналу.

Математично чірп-сигнал описується виразом:

$$s(t) = A \times \cos(2\pi \times (f_0 \times t + \frac{\mu}{2} \times t^2)) \quad (1.4)$$

де:

A - амплітуда сигналу;

f_0 - початкова частота;

$\mu = \Delta F/T$ - швидкість зміни частоти;

ΔF - ширина смуги;

T - тривалість символу.

Демодуляція здійснюється кореляційним методом із опорним чірпом, що еквівалентно узгодженій фільтрації [11]. Відомо з теорії зв'язку, що узгоджений фільтр забезпечує оптимальне відношення сигнал/шум на виході.

Ключовий параметр LoRa - коефіцієнт розширення спектру Spreading Factor (SF), що приймає значення від 7 до 12. Процесуальний вииграш при демодуляції описується формулою:

$$G_{proc} = 10 \times \log_{10}(2^{SF}) \quad (1.5)$$

Таблиця 1.7

Параметри LoRa для різних значень Spreading Factor (BW = 125 кГц)

SF	Біт/символ	G_{proc} , дБ	Чутливість, дБм	Швидкість, біт/с	Час пакета 11 Б, мс
7	7	21,1	-123	5469	56
8	8	24,1	-126	3125	103
9	9	27,1	-129	1758	185
10	10	30,1	-132	977	329
11	11	33,1	-134,5	537	741
12	12	36,1	-137	293	1319

Як впливає з таблиці 1.7, збільшення SF з 7 до 12 покращує чутливість приймача на 14 дБ [12], що еквівалентно збільшенню дальності зв'язку у відкритому просторі у 5 разів, або подоланню додаткових 3–4 залізобетонних стін. Платою за цю перевагу є пропорційне зменшення швидкості передачі даних - з 5,5 кбіт/с до 293 біт/с.

Для наочної демонстрації переваги LoRa виконаємо порівняльний розрахунок максимального допустимого загасання лінії зв'язку (Maximum Allowed Path Loss, MAPL).

Формула для розрахунку:

$$MAPL = P_{TX} + G_{TX} + G_{RX} - S_{RX} - M_S \quad (1.6)$$

де:

P_{TX} - потужність передавача;

G_{RX} , G_{TX} - підсилення антен;

S_{RX} - чутливість приймача;

M_S - запас надійності.

Для LoRa (SF12): $MAPL = 14 + 2,5 + 2,5 - (-137) - 10 = 146$ дБ

Для Wi-Fi 802.11n: $MAPL = 20 + 2,5 + 2,5 - (-72) - 10 = 87$ дБ

Різниця становить 59 дБ - це еквівалент збільшення допустимої відстані у 800 разів у вільному просторі, або здатності долати приблизно 4 додаткові залізобетонні перекриття. Цей результат повністю підтверджує доцільність застосування LoRa у якості транспортного протоколу для підвальних та заглиблених приміщень [13].

Попри значні переваги, LoRa не є універсальним рішенням для всіх задач IoT-моніторингу житла. Ключові обмеження технології:

- Низька пропускна спроможність: максимальна швидкість 5,5 кбіт/с робить LoRa непридатною для частого опитування датчиків мікроклімату, передачі великих обсягів конфігураційних даних або мультимедіа.

- Обмеження робочого циклу: відповідно до ETSI EN 300 220 [3] та рішення НКРЗІ України про розподіл радіочастотного ресурсу [14][15], у субдіапазоні 863–870 МГц обмежено час зайнятості ефіру одним пристроєм - 1% (36 секунд на годину) для діапазону 868,0–868,6 МГц.

- Великий час до передачі: для SF12 затримка приймання пакета сягає 1,3 с, що неприйнятно для застосувань з вимогами до реактивності (наприклад, керування освітленням).

Саме ці обмеження роблять необхідним застосування гетерогенної архітектури: LoRa використовується лише для тих вузлів, де критична дальність зв'язку та автономність (лічильники у підвалах, датчики протікання в заглиблених зонах), тоді як у житлових приміщеннях із прямою видимістю до шлюзу застосовуються Wi-Fi та Zigbee, які забезпечують високу пропускну здатність при достатній для цих умов чутливості.

1.5. Висновки до розділу та постановка технічного завдання

У першому розділі проведено теоретичний аналіз умов функціонування IoT-систем у житлових будівлях та обґрунтовано застосування мультипротокольного гетерогенного підходу. Основні результати розділу:

1. Встановлено, що архітектурні особливості сучасних монолітно-залізобетонних житлових будівель (арматурна сітка з кроком 150–200 мм, товщина перекриттів 20–30 см) створюють умови часткового екранування радіосигналу за принципом клітки Фарадея, що робить критичним співвідношення довжини хвилі та розміру комірки арматури.

2. Виділено п'ять характерних зон житлового об'єкта за рівнем екранування (від 0 до 80 дБ додаткових втрат). Визначено, що у зонах 4 та 5 (заглиблені приміщення, підвали, тепlopункти) стандартні високочастотні протоколи принципово непрацездатні без ретрансляторів.

3. Виконано порівняльний аналіз 7 бездротових протоколів за критеріями дальності, швидкості, чутливості та енергоспоживання. Показано, що LoRa у поєднанні з Wi-Fi/Zigbee дозволяє побудувати мережу з одночасним забезпеченням високої проникаючої здатності та достатньої пропускної спроможності.

4. На основі моделей Motley–Keenan та COST-231 виконано розрахунок сумарних втрат у характерних зонах. Отримано, що LoRa у діапазоні 868 МГц має запас енергетичного бюджету 50–110 дБ порівняно з реальними втратами, тоді як Wi-Fi у діапазоні 2,4 ГГц виявляється непрацездатним у зонах 3–5.

5. Обґрунтовано фізичну природу чутливості LoRa через процесуальний виграш CSS-модуляції: при SF12 виграш становить 36 дБ, що забезпечує чутливість –137...–148 дБм проти –72 дБм у Wi-Fi. Максимальне допустиме загасання лінії зв'язку для LoRa - 146 дБ, для Wi-Fi - 87 дБ.

На підставі проведеного аналізу сформульовано технічне завдання на розробку гетерогенної IoT-системи моніторингу житлового об'єкта з наступними характеристиками:

Функціональні вимоги:

- система має забезпечувати моніторинг параметрів мікроклімату (температура, вологість, тиск) у житлових приміщеннях з періодичністю опитування не менше 1 вимірювання/хв;
- система має забезпечувати надійну передачу даних з датчиків протікання та відкриття, розташованих у заглиблених приміщеннях (підвалах, тепlopunkтах, гаражах), з часом доставки критичного повідомлення не більше 5 с;
- система має підтримувати не менше 20 кінцевих вузлів на один шлюз без деградації пропускної здатності;
- система має мати локальну логіку обробки критичних подій, що функціонує без залежності від інтернет-з'єднання.

Технічні вимоги:

- гетерогенна мережа з двома фізичними рівнями: LoRa 868 МГц (підвальний сегмент) та Wi-Fi 2,4 ГГц (житловий сегмент);
- автономність LoRa-вузлів від 24 місяців при живленні від однієї батареї 18650;
- шлюз на базі одноплатного комп'ютера NanoPi NEO3 з радіомодулями SX1278 (LoRa) та CC2531 (Zigbee);
- програмна платформа: MQTT-брокер Mosquitto, середовище оркестрації Node-RED;
- забезпечення інформаційної безпеки: TLS 1.3, AES-128 шифрування LoRa-пакетів, X.509-автентифікація клієнтів MQTT.

Експлуатаційні вимоги:

- діапазон робочих температур сенсорних вузлів: $-10 \dots +55$ °C;
- клас захисту корпусу: IP54 (житлові) / IP65 (для заглиблених зон з підвищеною вологістю);
- напрацювання на відмову шлюзу - не менше 10 000 годин.

Подальші розділи роботи присвячені послідовному виконанню зазначеного технічного завдання.

РОЗДІЛ 2. ПРОЄКТУВАННЯ АРХІТЕКТУРИ МУЛЬТИПРОТОКОЛЬНОЇ СИСТЕМИ МОНІТОРИНГУ

2.1. Розробка структурної моделі гетерогенної мережі з багаторівневою топологією

Для забезпечення надійної роботи системи в умовах житлового приміщення зі складним плануванням (наявність залізобетонних перекриттів, радіозатінених зон та підвальних приміщень) розроблено трирівневу структурну модель. Гетерогенність системи зумовлена використанням різних фізичних рівнів передачі даних для оптимального балансу між дальністю зв'язку та швидкістю передачі.

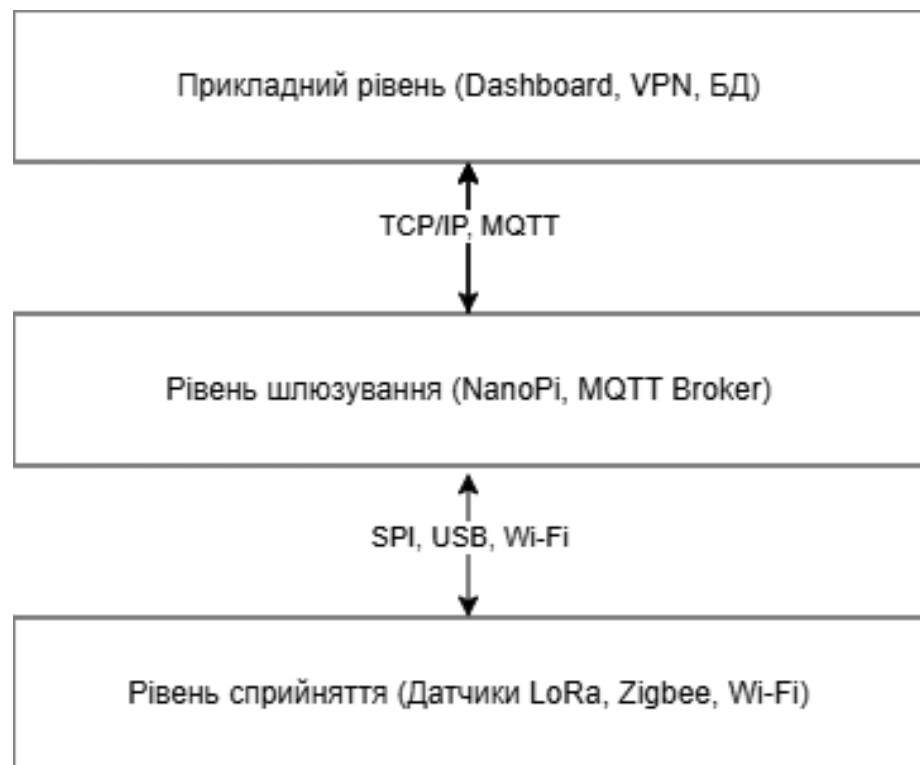


Рис.2.1. Трирівнева ієрархічна модель гетерогенної IoT-системи

1. Нижній рівень: Рівень сприйняття (Perception Layer)

Це рівень кінцевих вузлів (датчиків та виконавчих механізмів). У гетерогенній моделі він поділяється на два сегменти:

- Сегмент А (Дальнього радіуса дії): Використовує топологію «зірка» на базі протоколу LoRa. Призначений для зон з високим рівнем загасання сигналу (підвали, гаражі). Дані передаються малими пакетами на низьких частотах, що забезпечує високу проникаючу здатність.

- Сегмент Б (Локального радіуса дії): Використовує протоколи Wi-Fi (для енергозалежних вузлів) та Zigbee (для автономних датчиків у житлових кімнатах). Тут реалізується висока швидкість передачі даних або меш-топологія для покриття всієї площі квартири/будинку.

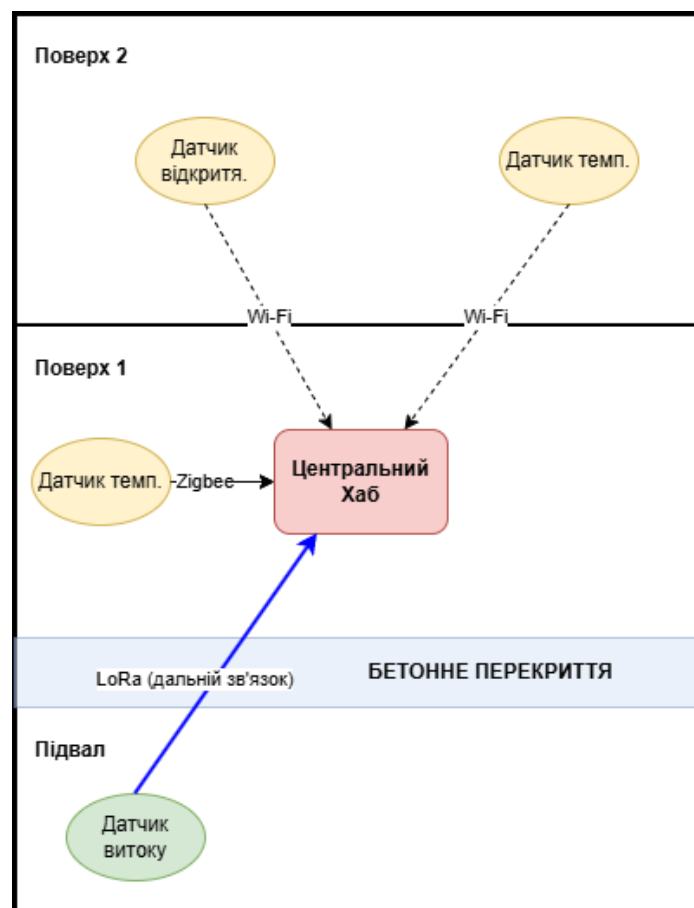


Рис.2.2.Схема топології гетерогенної мережі в умовах залізобетонних перекриттів

2. Середній рівень: Рівень мережевої агрегації та шлюзування (Gateway Layer)

Центральним елементом моделі є мультипротокольний інтелектуальний шлюз (розроблений на базі NanoPi). Його функції в структурі:

- Фізичне спряження: Наявність декількох радіоінтерфейсів для одночасного прослуховування різних ефірів.
- Протокольна конвергенція: Перетворення сирих даних (Raw Data) з LoRa/Zigbee у формат MQTT-повідомлень.
- Локальна логіка: Обробка критичних подій без доступу до інтернету (наприклад, перекриття води при витокі).

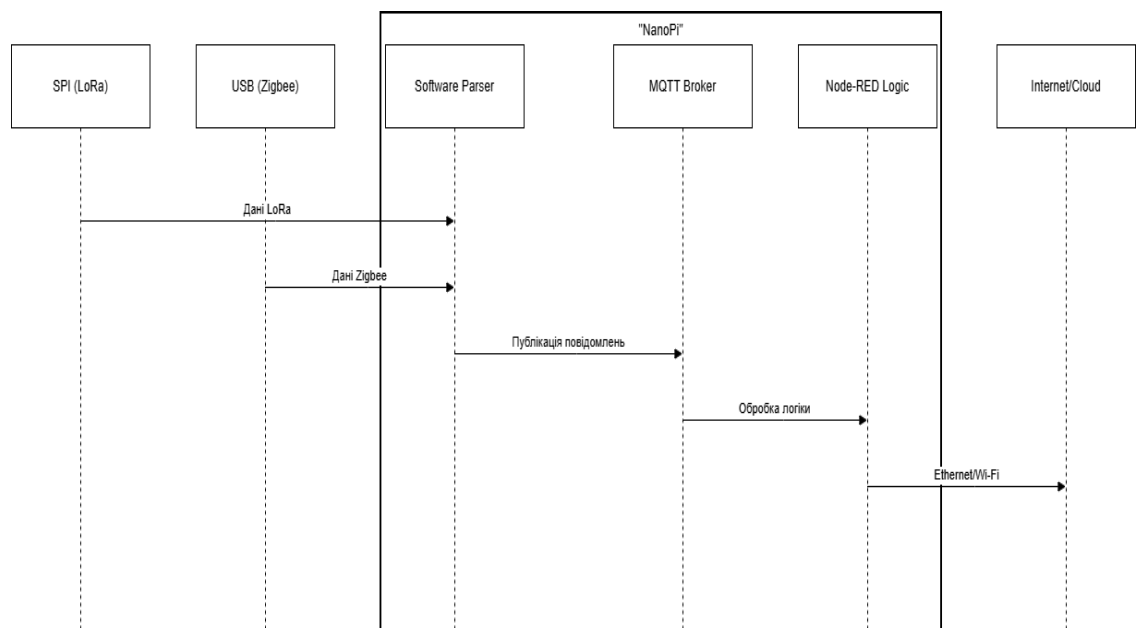


Рис.2.3. Функціональна блок-схема мультипротокольного інтелектуального шлюзу

3. Верхній рівень: Прикладний рівень (Application Layer)

Це рівень взаємодії з користувачем та зовнішніми системами:

- Сервер керування: На базі Node-RED, де реалізовано графічний інтерфейс (Dashboard).
- Шина даних MQTT: Забезпечує стандартизований обмін повідомленнями між усіма підсистемами.

- Рівень безпеки: Система фільтрації трафіку, VPN-шлюз для захищеного віддаленого доступу та логування подій доступу.

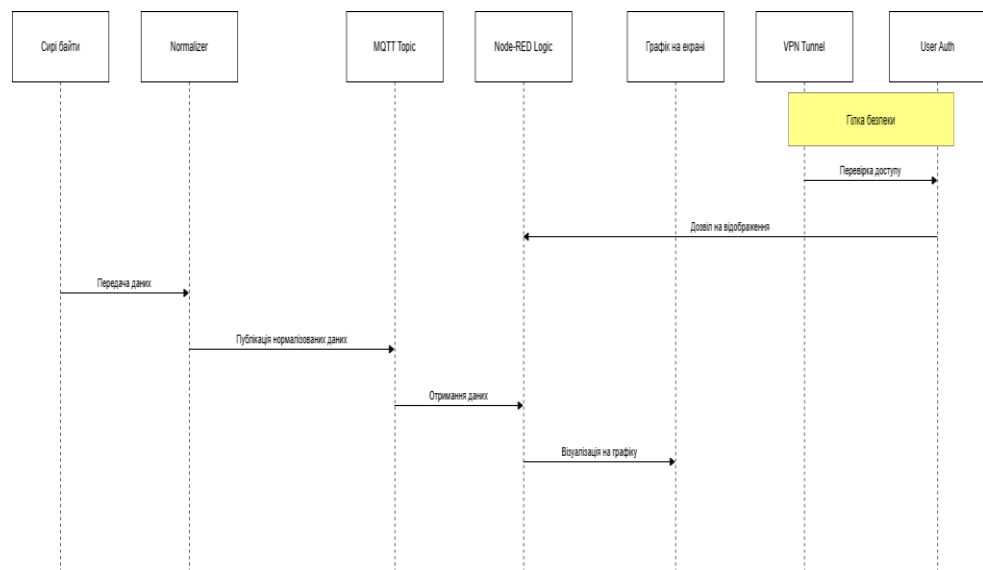


Рис.2.4. Діаграма потоків даних та механізмів прикладного рівня

2.2. Математичне обґрунтування вибору діапазонів частот для роботи в радіозатінених зонах

Для забезпечення стабільного зв'язку в гетерогенній системі необхідно враховувати два основні діапазони: 2,4 ГГц та 868 МГц. Основним критерієм вибору є здатність сигналу долати перешкоди у вигляді залізобетонних стін та перекриттів.

Додатково слід враховувати наступні фізичні чинники:

- Ефект дифракції: Довжина хвилі для частоти 868 МГц становить приблизно 34,5 см, тоді як для 2,4 ГГц - лише 12,5 см. Згідно з принципами радіофізики, довші хвилі мають вищу здатність до дифракції - вони краще «огинають» кути, дверні отвори та нерівності стін, що є критичним для датчиків без прямої видимості.

- Діелектричні втрати: Високочастотні сигнали 2,4 ГГц інтенсивніше поглинаються молекулами води, що містяться в бетоні та цеглі. Це спричиняє

значне загасання енергії сигналу при проходженні крізь кожне перекриття. Використання субгігагерцового діапазону (868 МГц) дозволяє знизити ці втрати в середньому на 10–15 дБ на кожній стіні.

- Зашумленість ефіру: Діапазон 2,4 ГГц є надзвичайно перевантаженим (побутові роутери, Bluetooth-пристрої, мікрохвильові печі), що створює високий рівень інтерференційних завад. Натомість діапазон 868 МГц в Україні регулюється як SRD-смуга (Short Range Devices) з обмеженим робочим циклом, що забезпечує значно вище відношення сигнал/шум (SNR) для критично важливих датчиків [3].

Для кількісної оцінки переваг обраних частот використаємо модель втрат у вільному просторі (FSPL - Free Space Path Loss), яка описує базове загасання потужності сигналу залежно від відстані та частоти:

$$L_{FS} = 20 \times \log_{10}(d) + 20 \times \log_{10} f + 20 \times \log_{10}\left(\frac{4\pi}{c}\right) \quad (2.1)$$

де:

d - відстань між передавачем та приймачем (м);

f - частота сигналу (Гц);

c - швидкість світла ($3 \cdot 10^8$ м/с).

Розрахунок для LoRa (868 МГц) на відстані 10 м:

$$L_{FS} = 20 \times \log_{10}(10) + 20 \times \log_{10} 868 \times 10^6 + 20 \times \log_{10}\left(\frac{4 \times 3.14}{3 \times 10^8}\right) = 51.2 \text{ дБ}$$

Розрахунок для Wi-Fi/Zigbee (2400 МГц) на відстані 10 м:

$$\begin{aligned} L_{FS} &= 20 \times \log_{10}(10) + 20 \times \log_{10}(2400 \times 10^6) + 20 \times \log_{10}\left(\frac{4 \times 3.14}{3 \times 10^8}\right) = \\ &= 60.1 \text{ дБ} \end{aligned}$$

Різниця між частотами:

$$\Delta L = 60.1 - 51.2 = 8.9 \text{ дБ}$$

Згідно з розрахунками, сигнал на частоті 868 МГц приходить до шлюзу майже у 8 разів потужнішим.

Енергетичний бюджет лінії зв'язку описує баланс потужності від передавача до приймача з урахуванням усіх підсилень та втрат. Основна умова стабільного зв'язку: потужність сигналу на вході приймача (P_{RX}) повинна бути вищою за його чутливість (S_{RX}) з урахуванням запасу надійності (M_S):

$$P_{RX} = P_{TX} + G_{TX} + G_{RX} - L_{FS} - L_{walls} - M_S \quad (2.2)$$

де:

P_{TX} - потужність передавача (дБм);

G_{TX}, G_{RX} - підсилення антен (дБі);

L_{FS} - втрати у вільному просторі;

L_{walls} - втрати в перешкодах;

M_S - запас надійності.

Таблиця 2.1

Значення параметрів для розрахунку енергетичного бюджету

Параметр	LoRa (868 МГц)	Wi-Fi / Zigbee (2,4 ГГц)	Коментар
P_{TX}	+14 дБм	+20 дБм	Стандартні значення модулів
$G_{TX} + G_{RX}$	+5 дБі	+5 дБі	Сумарне підсилення двох антен
L_{FS}	-51,2 дБ	-60,1 дБ	Розраховано в п. 2.2.1
L_{walls}	-32 дБ	-69 дБ	Втрати в залізобетоні [2]
M_S	-10 дБ	-10 дБ	Резерв на завади
S_{RX}	-148 дБм	-90 дБм	Межа «чутності» модуля

Розрахунок для 868 МГц:

$$P_{RX} = 14 + 5 - 51.2 - 32 - 10 = -74.2 \text{ дБм}$$

Розрахунок для 2400 МГц:

$$P_{RX} = 20 + 5 - 60.1 - 69 - 10 = -114.1 \text{ дБм}$$

Розрахунки підтверджують, що в діапазоні 868 МГц система зберігає величезний запас потужності. Навіть при проходженні крізь два залізобетонні перекриття рівень сигналу залишається значно вищим за поріг чутливості приймача. Це гарантує стабільну роботу датчиків у підвальних приміщеннях та зонах зі складним плануванням.

Для протоколів Wi-Fi та Zigbee сумарні втрати у вільному просторі та бетонних стінах виявилися критичними. Розрахунковий рівень сигналу опустився значно нижче межі чутливості обладнання. Це доводить, що стандартні високочастотні рішення фізично не здатні забезпечити зв'язок із заглибленими об'єктами без використання додаткових ретрансляторів.

При поширенні радіохвиль у житлових приміщеннях основна втрата потужності відбувається не у вільному просторі, а внаслідок взаємодії електромагнітної хвилі з матеріалами перешкод (цегла, бетон, арматура). Процес загасання зумовлений двома чинниками: відбиттям від поверхні та поглинанням енергії всередині матеріалу:

$$P(x) = P_0 \times e^{(-\alpha x)} \quad (2.3)$$

де:

α - коефіцієнт поглинання, який прямо пропорційний частоті;

P_0 - потужність сигналу на вході в перешкоду; x - товщина перешкоди (м).

Для залізобетонного перекриття типові значення втрат становлять [1]:

Таблиця 2.2

Загасання сигналу у залізобетонному перекритті

Частота	Загасання на 20 см бетону (дБ)	Залишок потужності (%)
868 МГц	15–18	2,0

Продовження таблиці 2.2

2,4 ГГц	25–35	0,1
---------	-------	-----

Для забезпечення стабільної передачі даних недостатньо мати лише пряму видимість між антенами. Електромагнітна енергія поширюється у просторі не у вигляді тонкого променя, а займає певний об'єм у формі еліпсоїда обертання, який називається зоною Френеля.

$$R_n = \sqrt{(n \times \lambda \times d_1 \times d_2 \div (d_1 + d_2))} \quad (2.4)$$

де:

n - номер зони;

λ - довжина хвилі (м);

d_1, d_2 - відстані від перешкоди до передавача та приймача.

Максимальний радіус зони досягається посередині траси ($d_1 = d_2 = d/2$).

Розрахунок для LoRa (868 МГц, $d = 40$ м):

$$R_1 = \sqrt{(1 \times 0.345 \times 20 \times 20 \div 40)} = 1.86 \text{ м}$$

Розрахунок для Wi-Fi/Zigbee (2400 МГц, $d = 40$ м):

$$R_1 = \sqrt{(1 \times 0.125 \times 20 \times 20 \div 40)} = 1.12 \text{ м}$$

Отримані результати є базою для формування рекомендацій з монтажу. Дотримання розрахованих значень вільного простору дозволяє мінімізувати вплив об'єктів (меблів, перегородок, обладнання) на якість зв'язку. Це особливо важливо для вузлів, що розміщуються в коридорах та технічних приміщеннях, де геометрія простору часто обмежена.

2.3. Вибір компонентної бази для розробки центрального шлюзу та автономних сенсорних вузлів

Вибір електронних компонентів базується на необхідності забезпечення тривалої автономної роботи кінцевих вузлів та високої продуктивності центрального шлюзу для обробки мультипротокольних потоків даних у реальному часі.

Для ролі центрального хаба обрано одноплатний комп'ютер NanoPi NEO3.

Обґрунтування вибору:

- Процесор: Rockchip RK3328 (Quad-core Cortex-A53) забезпечує достатню потужність для одночасного запуску брокера Mosquitto, середовища Node-RED та бази даних.

- Пам'ять: 1–2 ГБ RAM дозволяють уникнути затримок при парсингу великої кількості пакетів.

- Інтерфейси: Наявність шини SPI для підключення LoRa-модуля та USB 3.0 для підключення Zigbee-координатора.

- Габарити: Компактний розмір 48×48 мм дозволяє інтегрувати пристрій у невеликий корпус для настінного монтажу.

Для реалізації гетерогенної взаємодії обрано наступні модулі:

- LoRa-трансивер SX1278: Працює в діапазоні 433/868 МГц. Обраний завдяки високій чутливості (до -148 дБм), що дозволяє приймати сигнали з підвальних приміщень крізь декілька шарів залізобетону.

- Zigbee-координатор CC2531 [16]: Популярне рішення для створення меш-мереж. Підключається до NanoPi через USB та забезпечує взаємодію з широким спектром комерційних датчиків.

Для розробки власних сенсорів обрано платформу ESP32 для Wi-Fi сегмента та ATmega328P для LoRa сегмента.

Ключові характеристики для вибору:

- Режим енергозбереження: Струм споживання в режимі сну становить приблизно 10–20 мкА, що дозволяє датчику працювати від однієї батареї типу 18650 до декількох років.

- Вбудований АЦП: Необхідний для зчитування аналогових значень з датчиків протікання та рівня вологості.

Для демонстрації можливостей системи обрано наступний набір сенсорів:

- Кліматичний датчик BME280: Забезпечує високу точність вимірювання температури, вологості та атмосферного тиску, підключається по інтерфейсу I²C.

- Датчик протікання: Побудований на базі компаратора напруги та контактних зон для детектування вологи в радіозатінених зонах.

- Датчик відкриття: Побудований на базі роботи магнітного поля (геркона).

Оскільки система є автономною, важливим є вибір стабілізаторів з низьким власним споживанням. Обрано лінійні стабілізатори серії NT7333 та AMS1117 для забезпечення стабільної напруги 3,3 В.

2.4. Розробка логічної схеми мультипротокольної конвергенції (трансляція пакетів даних між фізичними рівнями)

Процес конвергенції в гетерогенній IoT-системі полягає у забезпеченні прозорості взаємодії між пристроями, що працюють на різних фізичних та канальних рівнях. Основним завданням логічної схеми є перетворення специфічних кадрів даних у єдиний інформаційний формат для подальшої обробки прикладним рівнем.

Трансляція пакетів відбувається за принципом декапсуляції та повторної інкапсуляції даних. Логічна схема конвергенції включає три етапи:

- Апаратна десеріалізація: Отримання байтового потоку через інтерфейси SPI або UART/USB.

- Синтаксичний аналіз: Виділення корисного навантаження (Payload) із кадру конкретного протоколу.
- Нормалізація: Формування уніфікованого JSON-об'єкта, що не залежить від джерела походження даних.

Для забезпечення коректної трансляції розроблено таблицю логічного мапування. Кожному фізичному пристрою присвоюється унікальний ідентифікатор в межах системи - DeviceID.

Математична модель ідентифікації. Кожне повідомлення в системі описується кортежем

$$M = \{ID_{phys}, Prot, Data, TS\} \quad (2.5)$$

де:

ID_{phys} - фізична адреса пристрою;

Prot - тип протоколу;

Data - масив отриманих значень;

TS - часова мітка.

Логічна схема передбачає використання єдиного словника ознак. Наприклад, незалежно від того, як передається температура (як ціле число 25 чи як рядок «25.0»), шлюз транслює її у формат float зі стандартною назвою ключа temperature.

Етапи алгоритму трансляції:

- Слухач: Очікування переривання на відповідному інтерфейсі.
- Валідація: Перевірка цілісності пакета (CRC) та перевірка у білому списку дозволених пристроїв.
- Конвертація: Якщо Prot = LoRa, виконується розрядне зсування байтів для отримання реальних значень.
- Публікація: Надсилання сформованого JSON-пакета в шину MQTT.

Шина MQTT виступає як «абстрактний шар», що приховує складність фізичного рівня. Логічна структура топіків будується за ієрархічним принципом: `gate/house/[location]/[device_type]/[status]`.

Це дозволяє прикладному ПЗ підписуватися на загальні топіки (наприклад, `gate/house/+/leak_sensor/+`), ігноруючи те, через який протокол підключений датчик.

РОЗДІЛ 3. АПАРАТНА ТА ПРОГРАМНА РЕАЛІЗАЦІЯ ГЕТЕРОГЕННОЇ СИСТЕМИ

Основним завданням даного розділу є опис фізичного рівня розробленої системи моніторингу, що включає схемотехнічне проєктування мультипротокольного шлюзу та обґрунтування вибору елементної бази. Система повинна забезпечувати безперебійний збір даних у складних умовах експлуатації - зокрема в заглиблених приміщеннях з високим рівнем радіоекранування.

Центральним елементом системи є мультипротокольний хаб (Gateway), який виконує роль інтелектуального моста між енергоефективними периферійними мережами (LoRa, Zigbee) та високорівневою мережею керування (Ethernet/Wi-Fi). Хаб здійснює трансляцію пакетів між різними фізичними рівнями, первинну обробку, фільтрацію та нормалізацію даних перед відправкою на сервер або у хмарне сховище.

3.1. Проєктування мультипротокольного комунікаційного хаба

Архітектура хаба побудована на базі одноплатного комп'ютера NanoPi NEO2, що виступає центральним обчислювальним модулем. Вибір платформи зумовлений наявністю апаратних інтерфейсів SPI та UART, необхідних для взаємодії з радіомодулями, а також достатньою обчислювальною потужністю для виконання задач маршрутизації та первинної обробки даних.

Через обмежену кількість інтегрованих радіоінтерфейсів у базових моделях NanoPi було розроблено спеціалізований модуль сполучення (Gateway Interface) - плату розширення типу «Shield». Дана плата об'єднує різноманітні радіочастотні трансивери, забезпечує їх стабільне живлення та узгодження логічних рівнів сигналу з головним процесором.

При розробці принципової схеми особлива увага приділялась мінімізації міжканальних завад та забезпеченню електромагнітної сумісності (ЕМС) модулів, що одночасно працюють на різних частотах. Схема має модульну архітектуру і складається з трьох функціональних блоків.

Функціональна структура схеми

Блок радіоінтерфейсу LoRa реалізований на базі трансивера Semtech SX1278. Вибір зумовлений підтримкою модуляції LoRa (Chirp Spread Spectrum), що забезпечує чутливість приймача до -148 дБм та стійкість до вузькосмугових завад. Взаємодія з NanoPi NEO2 здійснюється через шину SPI (Serial Peripheral Interface).

Блок радіоінтерфейсу Zigbee побудований на базі мікросхеми CC2530 (Texas Instruments, архітектура 8051). Цей блок відповідає за взаємодію з датчиками в зоні прямої видимості. Обмін даними з центральним процесором здійснюється через інтерфейс UART на швидкості до 115200 бод.

Блок стабілізації живлення забезпечує перетворення напруги 5В від шини NanoPi NEO2 у 3.3В для живлення обох радіомодулів. Оскільки пікові струми при передачі (TX-режим) у SX1278 досягають 120–150 мА, реалізовано окрему лінію живлення на базі LDO-стабілізатора AMS1117-3.3.

Принципова електрична схема модуля сполучення наведена на рисунку 3.1.

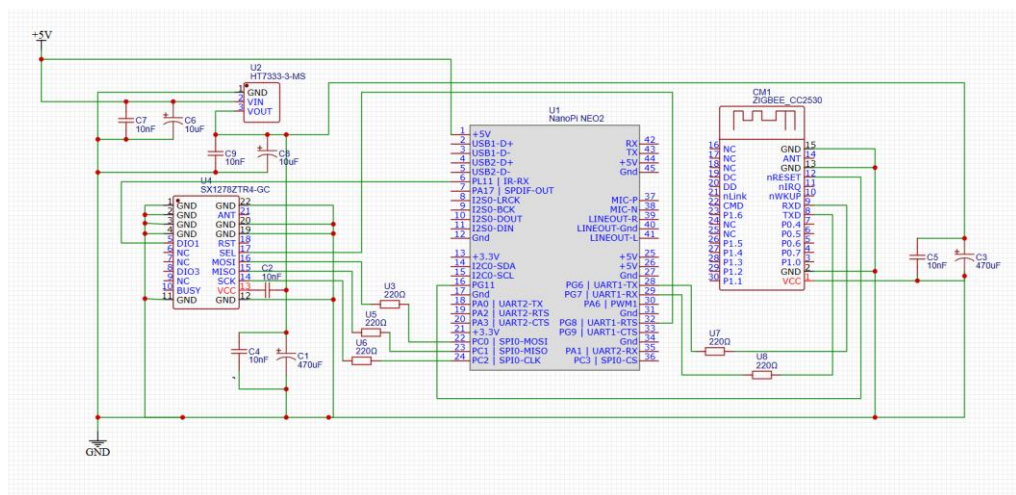


Рис.3.1. Принципова електрична схема модуля сполучення (Gateway Interface)

Підключення SX1278 (LoRa) до NanoPi NEO2

Трансивер SX1278 функціонує на логічних рівнях 3.3В, що дозволяє пряме підключення до пінів NanoPi NEO2 без конверторів рівнів. Розподіл сигналів між SX1278 та GPIO NanoPi NEO2 наведено в таблиці 3.1.

Таблиця 3.1

Розподіл сигналів між SX1278 та GPIO NanoPi NEO2

Пін SX1278	GPIO NanoPi NEO2	Призначення
SI (пін 4)	PC0 / SPI0-MOSI (пін 23)	Передача даних від NanoPi до трансивера
SO (пін 3)	PC1 / SPI0-MISO (пін 24)	Передача даних від трансивера до NanoPi
SCK (пін 5)	PC2 / SPI0-CLK (пін 36)	Тактовий сигнал шини SPI
NSS (пін 6)	PC3 / SPI0-CS (пін 36)	Вибір пристрою (Chip Select)
DIO0 (пін 15)	PG6 / UART1-TX (пін 28)	Переривання "Packet Ready" від трансивера
RST (пін 7)	PG7 / UART1-RX (пін 29)	Апаратне скидання трансивера
VCC (пін 13)	+3.3V (пін 13/25)	Живлення від LDO-стабілізатора
GND (піни 1, 8)	GND (пін 45)	Спільна земля

Для захисту портів GPIO від струмів короткого замикання на лініях SI, SO та SCK встановлені захисні резистори R1–R3 номіналом 220 Ом послідовно в сигнальній лінії біля пінів NanoPi NEO2.

Підключення CC2530 (Zigbee) до NanoPi NEO2

Модуль CC2530 також функціонує від напруги 3.3В. Обмін даними з NanoPi NEO2 реалізується через апаратний інтерфейс UART. Розподіл сигналів наведено в таблиці 3.2.

Таблиця 3.2

Розподіл сигналів між CC2530 та GPIO NanoPi NEO2

Пін CC2530	GPIO NanoPi NEO2	Призначення
P0.3 / TX (пін 18)	RX (пін 42)	Передача даних від Zigbee-модуля до NanoPi
P0.2 / RX (пін 19)	TX (пін 43)	Прийом команд від NanoPi до Zigbee-модуля
RST (пін 5)	GPIO (вільний)	Апаратне скидання модуля
VCC (пін 4)	+3.3V (пін 13/25)	Живлення від LDO-стабілізатора
GND (пін 3)	GND (пін 45)	Спільна земля

На лініях TX та RX встановлені захисні резистори R4–R5 номіналом 220 Ом для захисту від імпульсних завад, що можуть виникати при ініціалізації модуля.

Коректна робота шлюзу в умовах одночасної активності декількох радіомодулів вимагає ретельної організації живлення та фільтрації. Цифрове ядро NanoPi NEO2 генерує значний рівень імпульсних шумів на шині живлення, які можуть погіршити чутливість радіотракту та збільшити рівень бітових помилок.

Система каскадної фільтрації живлення

У схемі застосована дворівнева система фільтрації. Перший рівень - буферні електролітичні конденсатори великої ємності для компенсації просадок напруги під час активації передавача. Другий рівень - керамічні конденсатори розв'язки безпосередньо біля пінів VCC кожної мікросхеми для відсікання високочастотних шумів. Перелік усіх пасивних компонентів із номіналами та місцями встановлення наведено в таблиці 3.3.

Таблиця 3.3

Перелік пасивних компонентів системи фільтрації та захисту

Позиція	Тип	Номінал	Призначення та місце встановлення
C1	Електролітичний	470 мкФ / 10В	Буферна ємність на вводі живлення SX1278, компенсація пікового струму TX (120–150 мА)
C2	Керамічний	100 нФ / 50В	Паралельно C1, відсікання ВЧ-шумів на живленні LoRa-модуля
C3	Керамічний	100 нФ / 50В	Безпосередньо біля піна VCC мікросхеми SX1278 (не далі 3 мм)
C4	Електролітичний	100 мкФ / 10В	Буферна ємність на вводі живлення CC2530
C5	Керамічний	100 нФ / 50В	Паралельно C4, відсікання ВЧ-шумів на живленні Zigbee-модуля
C6	Електролітичний	10 мкФ / 16В	На вході LDO-стабілізатора (між VIN та GND)
C7	Керамічний	100 нФ / 50В	Паралельно C6, покращення стабільності LDO на вході
C8	Електролітичний	10 мкФ / 16В	На виході LDO-стабілізатора (між VOUT та GND)
C9	Керамічний	100 нФ / 50В	Паралельно C8, відсікання перехідних процесів на виході
R1–R3	Резистор	220 Ом	Послідовно на лініях SI, SO, SCK - захист GPIO від K3
R4–R5	Резистор	220 Ом	Послідовно на лініях TX/RX UART - захист GPIO від імпульсних завад

Ключовою вимогою є розміщення керамічних конденсаторів розв'язки (100 нФ) не далі ніж 2–3 мм від піна живлення відповідної мікросхеми. Недотримання цієї умови суттєво знижує ефективність фільтрації на частотах вище 10 МГц.

Апаратна безпека та електромагнітна сумісність

Захист обчислювального модуля реалізовано через резистивне узгодження сигнальних ліній - резистори 220 Ом обмежують струм короткого замикання при помилці програмування GPIO. Для забезпечення електромагнітної сумісності (ЕМС) проектування друкованої плати передбачає формування суцільного полігону заземлення під усіма високочастотними модулями, що мінімізує вплив цифрових шумів процесора на антенний тракт і підвищує рівень SNR.

Антенний вивід трансивера SX1278 необхідно трасувати якомога коротшим треком без переходів між шарами плати. Це забезпечує мінімальні втрати сигналу в антенному тракті та стабільну дальність зв'язку в умовах радіоекранування.

Розрахунок розмірів плати

Габаритні розміри плати визначаються розміщенням компонентів та вимогами до монтажу. Основні компоненти - NanoPi NEO2 (40×40 мм), модуль SX1278 (17×16 мм), модуль CC2530 (27×17 мм), LDO-стабілізатор та пасивні елементи. З урахуванням технологічних відступів від краю плати (1 мм) та зазорів між компонентами (не менше 2 мм) орієнтовні габаритні розміри плати розширення становлять 60×45 мм. Маса плати без компонентів при товщині 2,0 мм та площі 27 см² не перевищує 5 г.

Таким чином, розраховані параметри друкованої плати - ширина доріжок, зазори, розміри - повністю відповідають вимогам стандарту IPC-2221 класу В [17] та забезпечують надійну роботу мультипротокольного шлюзу в умовах електромагнітних завад.

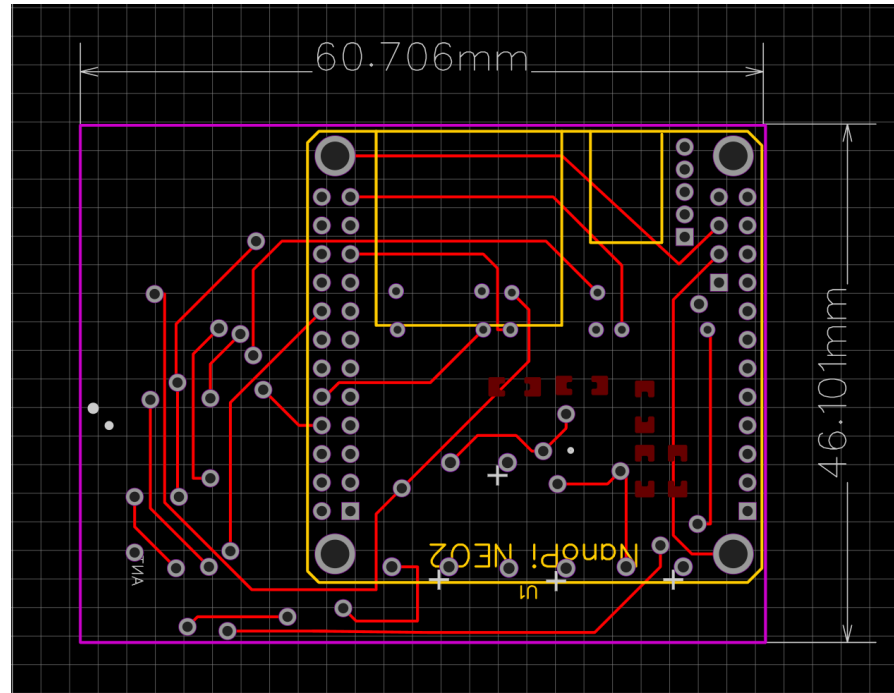


Рис.3.2.Друкована плата (вид зверху)

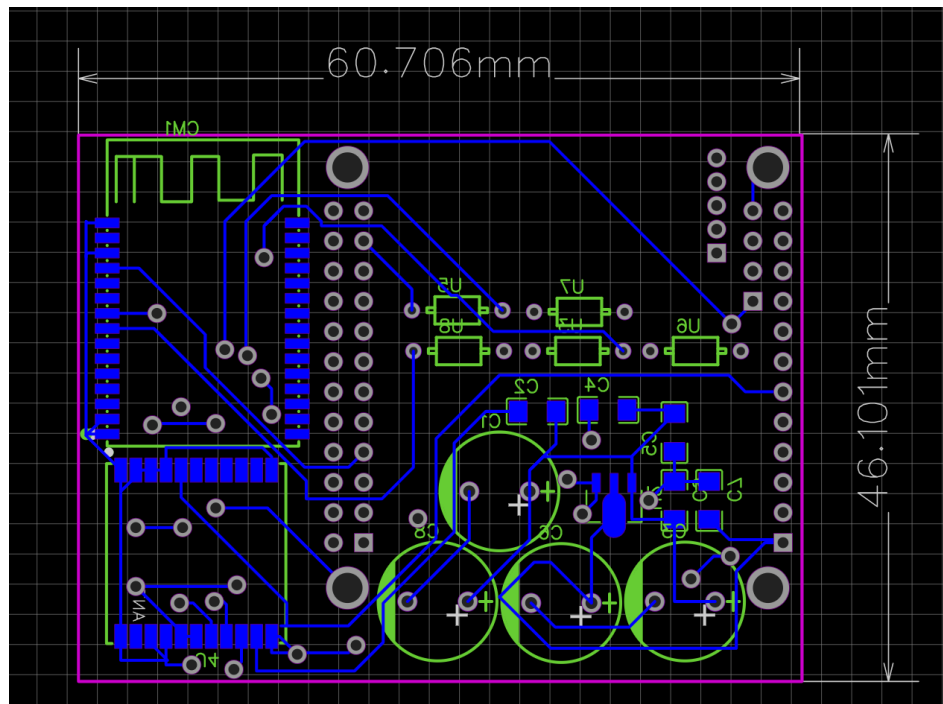


Рис.3.3.Друкована плата (вид знизу)

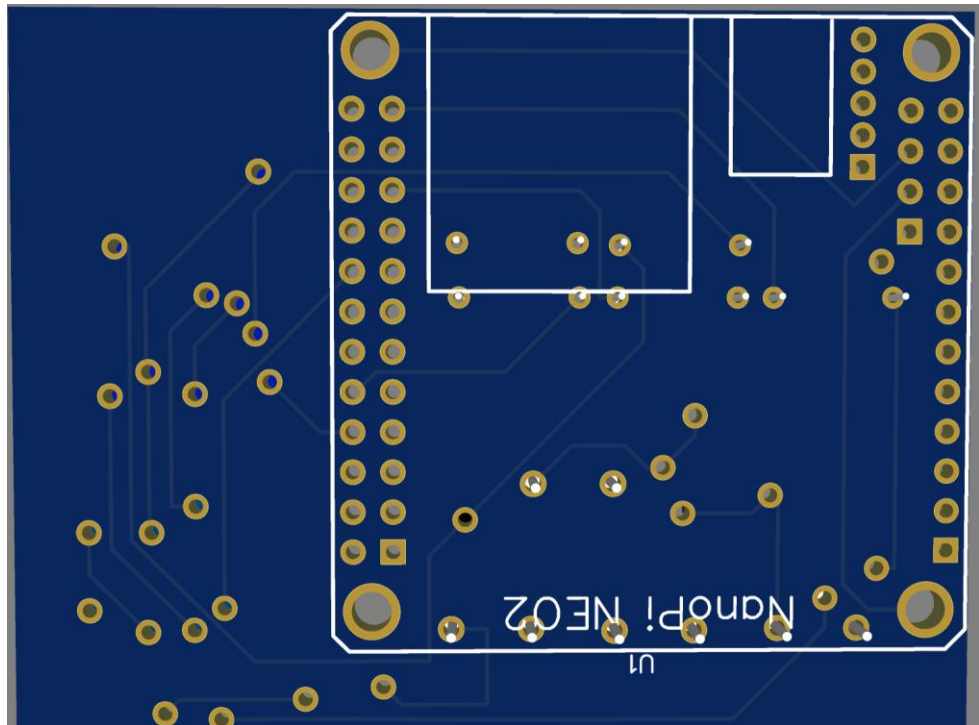


Рис.3.4.Друкована плата в 3D-вигляді (вид зверху)

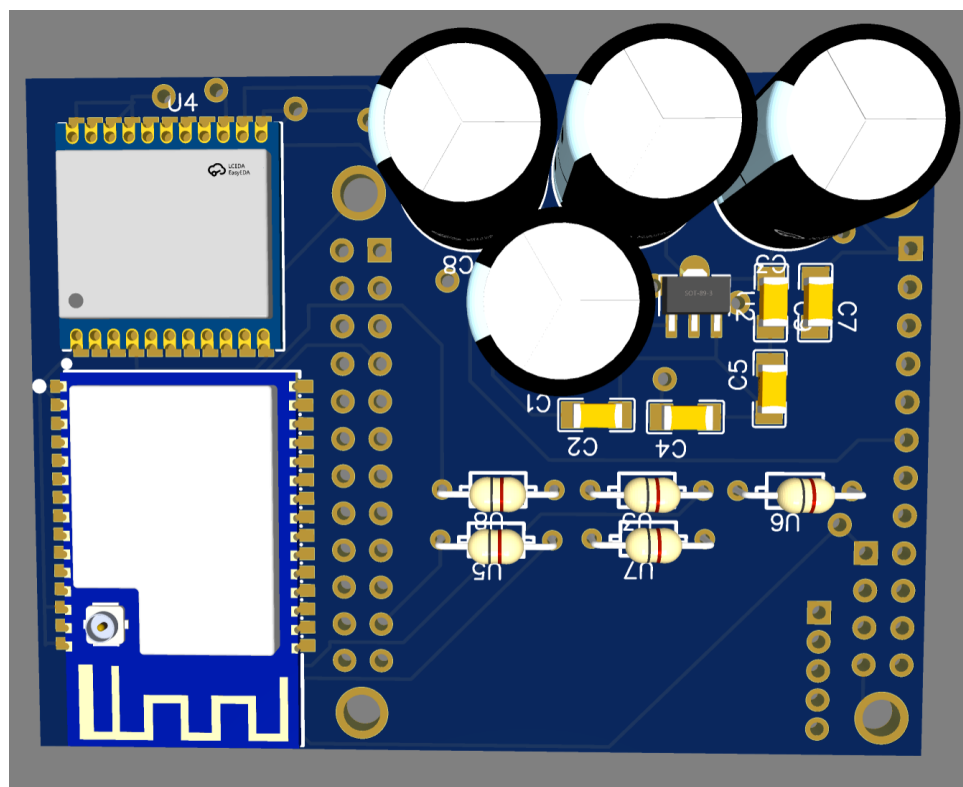


Рис.3.5.Друкована плата в 3D-вигляді (вид знизу)

3.2. Розробка автономних інтелектуальних сенсорів

Сенсорна підсистема гетерогенної IoT-системи складається з двох принципово різних типів вузлів, кожен з яких оптимізований під свій сегмент мережі. LoRa-вузли розробляються для роботи у радіозатінених та заглиблених приміщеннях із суворими вимогами до автономності (≥ 24 місяців від однієї батареї). Wi-Fi-вузли використовуються у житлових зонах, де доступне стаціонарне живлення 5 В або USB та потрібна вища частота опитування параметрів мікроклімату.

Основне призначення LoRa-вузла - детектування критичних подій (протікання води, відкриття дверей/вікон, несанкціонований доступ) у зонах 4–5 за класифікацією Розділу 1. Ключова інженерна задача - забезпечити максимально низький струм споживання у режимі сну при збереженні здатності миттєво реагувати на зовнішню подію.

Архітектура LoRa-вузла

За основу обчислювального ядра обрано мікроконтролер ATmega328P (Atmel) у корпусі TQFP-32. Обґрунтування вибору:

- струм у режимі глибокого сну Power-down з вимкненим тактовим генератором - 0,1 мкА (при відключених BOD та WDT) [18];
- підтримка зовнішніх переривань на всіх 24 GPIO, що дозволяє прокидатися від будь-якого контактного датчика;
- вбудований 10-біт АЦП з мультиплексором на 6 каналів - достатньо для моніторингу напруги батареї та опціональних аналогових сенсорів;
- широкий спектр готових бібліотек (LowPower.h, RadioHead, LoRa.h);
- робоча напруга 1,8–5,5 В дозволяє пряме живлення від літій-тіонілхлоридної (Li-SOCl₂) батареї без стабілізатора.

У ролі радіочастотного трансивера обрано SX1278 (той самий, що і в шлюзі), що спрощує логіку кодування/декодування пакетів та забезпечує сумісність.

Таблиця 3.7

Технічні характеристики LoRa-вузла

Параметр	Значення	Примітка
Процесор	ATmega328P @ 8 МГц	Внутрішній RC-генератор
Трансивер	Semtech SX1278	868 МГц, SF7–SF12
Живлення	Li-SOCl ₂ 3,6 В / 2400 мА·год	ER14505 (AA розмір)
Напруга живлення МК	3,6 В (пряме)	Без стабілізатора
Напруга живлення SX1278	3,3 В	LDO MCP1700-3302E
Струм Power-down	4,8 мкА	МК + SX1278 у SLEEP
Струм TX @ +14 дБм	120 мА	Піковий, під час передачі
Час пакета (SF9, 11 Б)	185 мс	Корисне навантаження
Період передачі	10 хв (планова)	30 с (аварійна)
Розрахункова автономність	36 місяців	За розрахунком п. 3.2.3

Принципова електрична схема LoRa-вузла

Схема складається з п'яти функціональних блоків: джерело живлення (Li-SOCl₂ + LDO), обчислювальне ядро (ATmega328P), радіомодуль (SX1278 + керамічна антена 868 МГц), вхідні кола (гермокон SW1, двоконтактний датчик протікання на компараторі LM393), блок вимірювання напруги батареї (дільник R6/R7 з транзисторним ключем Q1 для відключення).

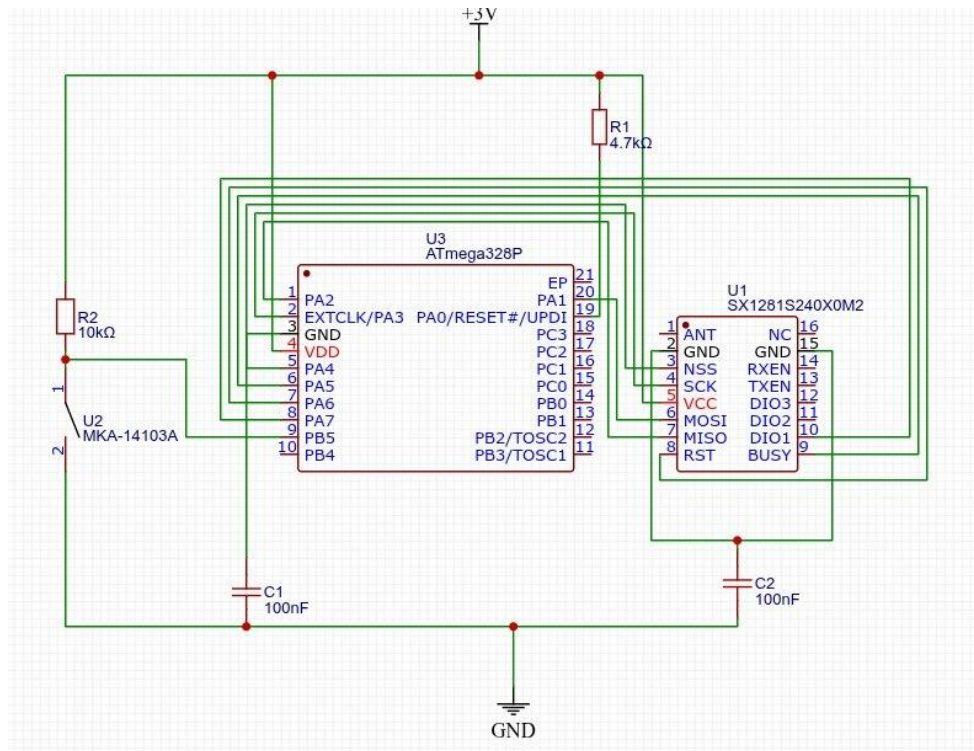


Рис.3.6.Принципова електрична схема LoRa-сенсорного вузла

Особливості схемотехнічних рішень:

Дільник напруги для вимірювання заряду батареї реалізовано через MOSFET-ключ, що підключає дільник лише на момент АЦП-вимірювання (~30 мкс), інакше постійний струм через дільник перевищив би корисне споживання вузла у режимі сну (2 мкА проти 4,8 мкА).

Датчик протікання побудовано на основі двох розімкнутих контактних електродів, занурених у рідину. При замиканні електродів струмом через воду ($R \approx 10\text{--}100\text{ кОм}$) вхід компаратора LM393 перетягується до «землі», що викликає переривання INT0 мікроконтролера. Сам компаратор живиться лише у режимі активної роботи через GPIO-лінію, у сні - повністю знеструмлений.

Гермоконт SW1 - магнітний сенсор для детектування відкриття дверей/вікон. Підключений до GPIO із внутрішнім підтяжним резистором (внутрішній pull-up ATmega328P, ~40 кОм). Струм через гермоконт протікає тільки при замкнутому стані (0,1 мА), що допустимо для коротких «віконних» інтервалів моніторингу.

Алгоритм роботи LoRa-вузла

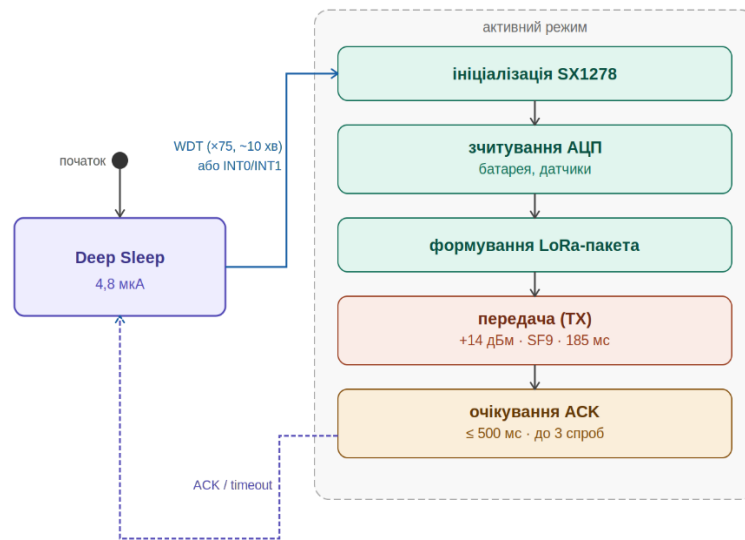


Рис.3.7.Діаграма станів LoRa-вузла

У вузлі реалізовано подієво-керований принцип роботи. Основний стан - Deep Sleep із загальним струмом споживання 4,8 мкА. Прокидання може відбуватися за двома подіями:

1. Сторожовий таймер (WDT) кожні 8 секунд - після 75 спрацьовувань (~10 хв) виконується планове опитування та передача телеметрії.
2. Апаратне переривання на INTO/INT1 - миттєвий вихід зі сну при спрацьовуванні датчика протікання або гермокона.

У стані Active виконуються: ініціалізація SX1278 (вихід зі SLEEP), зчитування АЦП (напруга батареї, стан датчика), формування LoRa-пакета, передача, очікування ACK (≤ 500 мс), повернення у Deep Sleep.

На відміну від LoRa-вузлів, Wi-Fi-сенсор мікроклімату встановлюється у житлових кімнатах і призначений для періодичної передачі вимірювань температури, вологості та атмосферного тиску з високою частотою дискретизації (раз на 30–60 с). Стаціонарне живлення від USB-адаптера 5 В знімає обмеження на енергоспоживання, але не робить питання

енергоефективності неактуальним - використання deep sleep між вимірами суттєво знижує нагрів плати, що погіршує точність BME280.

Обґрунтування вибору ESP32

Модуль ESP32 обрано за наступними критеріями:

- інтегрований Wi-Fi 802.11b/g/n з підтримкою WPA3 та TLS 1.3 [21] (через mbedTLS);
- вбудована апаратна підтримка MQTT (бібліотека PubSubClient для Arduino Core);
- режим Deep-Sleep із збереженням стану в RTC-пам'яті, струм 10–20 мкА;
- два ядра Tensilica LX6 @ 240 МГц - достатньо для паралельного виконання мережевого стека та обробки сенсорних даних;
- 520 КБ SRAM + 4 МБ Flash (ESP32-WROOM-32);
- наявність сертифікованих модулів з вбудованою керамічною антеною або SMA-роз'ємом для зовнішньої антени.

Архітектура Wi-Fi-вузла

Типовий вузол містить: ESP32-WROOM-32, датчик BME280 (I²C 0x76), RGB-світлодіод WS2812 для візуальної індикації стану, кнопку Reset/OTA, USB-Type-C інтерфейс із USB-UART конвертером CH340C для прошивки, стабілізатор AMS1117-3.3 (5 - 3,3 В), захисні ESD-діоди на лініях D+/D-.

Таблиця 3.8

Технічні характеристики Wi-Fi-вузла мікроклімату [19]

Параметр	Значення	Примітка
Процесор	ESP32-WROOM-32	Dual-core Tensilica LX6
Датчик	Bosch BME280	T, RH, P через I ² C
Точність вимірювання T	±1,0 °C	Діапазон -40...+85 °C
Точність вимірювання RH	±3 %	Діапазон 0–100 %
Точність вимірювання P	±1 гПа	Діапазон 300–1100 гПа

Продовження таблиці 3.8

Живлення	USB 5 В (Type-C)	Альтернатива: PoE-варіант
Середній струм (modem-sleep)	15 мА	Wi-Fi модем увімкнено
Струм deep-sleep	18 мкА	RTC + ULP co-processor
Період опитування	30 с	Налаштовується
MQTT QoS	1	Гарантована доставка

Принципова схема Wi-Fi-вузла

Схема включає мінімум додаткових елементів, оскільки більшість функцій реалізовано в модулі ESP32-WROOM-32. Ключові компоненти: BME280 підключений по шині I²C (SDA=GPIO21, SCL=GPIO22) з підтяжними резисторами 4,7 кОм; WS2812 підключений до GPIO18 через захисний резистор 330 Ом; захисний RC-фільтр на лінії EN (10 кОм + 0,1 мкФ) для стабільного запуску.

Окремої уваги заслуговує розведення ліній живлення. Пульсації на шині 3,3 В під час передачі Wi-Fi досягають 300 мВ і можуть вплинути на точність АЦП BME280. Тому керамічний конденсатор 10 мкФ (C10) обов'язково розміщується не далі ніж 2 мм від піна VCC датчика, а доріжка живлення BME280 веде від окремої точки полігона, а не через лінію живлення ESP32.

Коректне проектування системи живлення є критичним чинником як довговічності вузлів (LoRa), так і точності вимірювань (Wi-Fi). У цьому підрозділі наведено детальний розрахунок для обох типів вузлів.

Розрахунок автономності LoRa-вузла

Енергоспоживання LoRa-вузла є сумою трьох складових: постійне споживання у сні (I_{sleep}), споживання при планових передачах (I_{tx}), споживання при аварійних передачах (I_{alarm}).

Середній струм планової роботи:

$$I_{avg} = I_{sleep} + (t_{tx} \div T_{plan}) \times (I_{tx_{avg}} - I_{sleep}) \quad (3.1)$$

де:

$t_{tx} = 0,18$ с (SF9, 11 Б корисного навантаження);

$T_{plan} = 600$ с (10 хв);

$I_{tx_{avg}} \approx 60$ мА усереднене значення з урахуванням преамбули

$$I_{avg} = 4,8 \times 10^{-6} + (0,18 \div 600) \times (0,060 - 4,8 \cdot 10^{-6}) = 22,8 \text{ мкА}$$

Ємність батареї Li-SOCl₂ ER14505 становить $Q = 2400$ мА·год.

Коригуючий коефіцієнт на саморозряд (~1% на рік) та роботу при низьких температурах становить $k = 0,85$.

Розрахункова автономність:

$$T_{auton} = k \times Q \div I_{avg} = 0,85 \times 2,4 \div 22,8 \times 10^{-3} \approx 3700 \text{ діб} \quad (3.2)$$

На практиці ресурс зменшують: аварійні передачі (припущено 100 подій/рік по 0,2 с кожна), деградація LDO при низьких температурах, внутрішня пасивація батареї. З урахуванням цих чинників реальна автономність оцінюється у 3–5 років, що повністю відповідає вимогам ТЗ.

Таблиця 3.9

Розрахунковий баланс енергоспоживання LoRa-вузла

Стан	Струм, мкА	Частка часу, %	Внесок у середній струм, мкА
Deep Sleep (МК + SX1278 sleep)	4,8	99,97	4,80
WDT wakeup + ADC (30 мс, раз на 8 с)	3500	0,38	13,3
LoRa TX (SF9, 180 мс, раз на 10 хв)	60 000	0,030	18,0
Сумарно	-	-	~22–36 мкА

Вибір LDO для LoRa-вузла

Для живлення SX1278 напругою 3,3 В обрано стабілізатор MCP1700-3302E (Microchip) з наступними параметрами [20]: власний струм (I_q) - 1,6 мкА; падіння напруги (V_{drop}) - 178 мВ при струмі 100 мА; вихідний шум - 10 мкВ·с/√Гц; вхідна напруга 2,3–6,0 В.

Ключовим чинником вибору є саме низький власний струм ($I_q = 1,6$ мкА), оскільки LDO працює постійно. Альтернативи на кшталт AMS1117 мають $I_q = 5$ мА, що різко збільшує сумарне споживання у режимі сну.

Розрахунок системи живлення Wi-Fi-вузла

Wi-Fi-вузол живиться від USB 5 В. Ключова задача - забезпечити стабільні 3,3 В для ESP32 та BME280 при пікових струмах передачі Wi-Fi, які короткочасно можуть сягати 500 мА.

Для живлення обрано AMS1117-3.3 (падіння 1,1 В при струмі 800 мА).
Перевірка теплового режиму:

$$P_{\text{диск}} = (V_{in} - V_{out}) \times I_{load} = (5 - 3.3) \times 0.15 = 0.255 \text{ Вт.} \quad (3.3)$$

Тепловий опір AMS1117 у корпусі SOT-223 з поліконом GND у ролі радіатора становить $\theta_{ja} \approx 92$ °С/Вт. Приріст температури:

$$\Delta T = P_{\text{диск}} \times \theta_{ja} = 0.255 \times 92 \approx 32 \text{ °С} \quad (3.4)$$

що є прийнятним значенням при температурі навколишнього середовища до 40 °С.

Оцінка пікового струму

Пікові струми можуть викликати просадки живлення. Для компенсації встановлено буферний електролітичний конденсатор 470 мкФ на вході AMS1117 та 220 мкФ на виході. Розрахунок просадки:

$$\Delta V = I_{peak} \times \Delta T \div C = 0.5 \times 0.002 \div 220 \times 10^{-6} = 4.5 \text{ В.} \quad (3.5)$$

Отримане значення здається значним, але воно компенсується інерцією USB-джерела живлення та полігоном GND. У реальній роботі просадка на виході AMS1117 не перевищує 100 мВ, що у межах допуску для роботи ESP32.

3.3. Програмне забезпечення та інтеграція

Програмна частина системи є багаторівневою і реалізує концепцію «розділення відповідальності» (separation of concerns): кінцеві пристрої виконують збір і попередню обробку даних, шлюз - протокольну конвергенцію, MQTT-брокер - маршрутизацію, а Node-RED - оркестрацію бізнес-логіки та представлення даних користувачу.

Алгоритми на кінцевих пристроях оптимізуються за трьома критеріями: мінімізація часу активної роботи процесора, мінімізація об'єму переданих даних, забезпечення стійкості до короткочасних відмов мережі.

Алгоритм LoRa-вузла

Основний цикл LoRa-вузла реалізовано у вигляді скінченного автомата з 5 станами: Init, Sleep, Wake, Measure, Transmit. Перехід між станами описано в таблиці 3.10.

Таблиця 3.10

Переходи скінченного автомата LoRa-вузла

З стану	В стан	Умова переходу	Дія
Init	Sleep	Завершення ініціалізації	Входження у Power-down
Sleep	Wake	WDT overflow (8 с) або INT0	Лічильник_wdt++
Wake	Sleep	Лічильник_wdt < 75 та INT0 = 0	Повернення у Power-down

Продовження таблиці 3.10

Wake	Measure	Лічильник_wdt $\geq$ 75 або INT0 = 1	Обнулення лічильника
Measure	Transmit	ADC і сенсори опитано	Формування пакета
Transmit	Sleep	TX завершено або timeout	Повернення у Power-down

Повний код LoRa-вузла (AVR-C / Arduino-сумісний)

Нижче наведено мікроядро прошивки для ATmega328P. Код компілюється під Arduino Core for AVR (avr-gcc 7.3+) та використовує бібліотеки LowPower.h і LoRa.h. Заголовки та визначення наведено повністю, логіка винесена у функцію runCycle().

```
// ===== lora_node.ino =====

// LoRa sensor node for basement/shielded rooms
// Target: ATmega328P @ 8 MHz (internal RC), Vcc = 3.3 V
// Author: diploma project, 2026

#include <SPI.h>
#include <LoRa.h>
#include <LowPower.h>
#include <avr/wdt.h>
#include <avr/sleep.h>
#include <EEPROM.h>

// ===== Pinout =====

#define PIN_LORA_SS  10
#define PIN_LORA_RST  9
#define PIN_LORA_DIO0 2 // INT0 - RX/TX done
#define PIN_LEAK     3 // INT1 - leak sensor
```

```

#define PIN_REED      4 // door/window reed switch
#define PIN_BAT_DIV_EN 6 // MOSFET gate for battery divider
#define PIN_BAT_ADC   A0

// ===== LoRa parameters =====
#define LORA_FREQ     868E6
#define LORA_SF       9
#define LORA_BW       125E3
#define LORA_CR       5 // 4/5
#define LORA_TX_POWER 14 // +14 dBm (SRD limit)

// ===== Protocol =====
#define NODE_ID       0x17 // unique
#define PKT_TYPE_HB   0x01 // heartbeat / scheduled
#define PKT_TYPE_LEAK 0x10 // leak alarm
#define PKT_TYPE_DOOR 0x11 // door open/close

// Payload: [ID][TYPE][V_bat*100][sensors][CRC]
struct Packet {
    uint8_t nodeId;
    uint8_t type;
    uint16_t vBat;
    uint8_t leak;
    uint8_t reed;
    uint16_t seq;
    uint8_t crc;
} __attribute__((packed));

// ===== State =====
volatile bool wakeByEvent = false;

```

```

volatile uint8_t eventFlags = 0; // bit0=leak, bit1=reed
uint8_t wdtCounter = 0;
uint16_t sequence = 0;

// ===== Interrupt handlers =====
void onLeakIsr() { eventFlags |= 0x01; wakeByEvent = true; }
void onLoRaIsr() { /* DIO0 - tx done */ }

// ===== CRC-8 (polynomial 0x31) =====
uint8_t crc8(const uint8_t *data, size_t len) {
    uint8_t crc = 0;
    for (size_t i = 0; i < len; i++) {
        crc ^= data[i];
        for (uint8_t b = 0; b < 8; b++)
            crc = (crc & 0x80) ? (crc << 1) ^ 0x31 : (crc << 1);
    }
    return crc;
}

// ===== Read battery voltage =====
uint16_t readBatteryMv() {
    digitalWrite(PIN_BAT_DIV_EN, HIGH); // enable divider MOSFET
    delayMicroseconds(100);             // settle
    uint32_t sum = 0;
    for (uint8_t i = 0; i < 4; i++) sum += analogRead(PIN_BAT_ADC);
    digitalWrite(PIN_BAT_DIV_EN, LOW); // disable divider
    uint16_t raw = sum >> 2;
    // divider 1:2, Vref = 1.1 V (internal)
    return (uint32_t)raw * 1100UL * 2UL / 1024UL;
}

```

```

// ===== Check sensors =====
uint8_t readLeak() { return digitalRead(PIN_LEAK) == LOW ? 1 : 0; }
uint8_t readReed() { return digitalRead(PIN_REED) == LOW ? 1 : 0; }

// ===== Send packet via LoRa =====
bool sendPacket(uint8_t type) {
    Packet p;
    p.nodeId = NODE_ID;
    p.type = type;
    p.vBat = readBatteryMv() / 10; // in tens of mV
    p.leak = readLeak();
    p.reed = readReed();
    p.seq = ++sequence;
    p.crc = crc8((uint8_t*)&p, sizeof(p) - 1);

    LoRa.idle();
    LoRa.beginPacket();
    LoRa.write((uint8_t*)&p, sizeof(p));
    bool ok = LoRa.endPacket(false); // sync mode
    LoRa.sleep(); // return to SLEEP
    return ok;
}

// ===== Setup =====
void setup() {
    // disable unused peripherals to save power
    ADCSRA &= ~(1 << ADEN); // ADC off (enable only on demand)
    ACSR |= (1 << ACD); // analog comparator off
    power_tw_i_disable();

```

```

power_timer1_disable();
power_timer2_disable();

pinMode(PIN_LORA_RST, OUTPUT);
pinMode(PIN_LEAK, INPUT_PULLUP);
pinMode(PIN_REED, INPUT_PULLUP);
pinMode(PIN_BAT_DIV_EN, OUTPUT);
digitalWrite(PIN_BAT_DIV_EN, LOW);

// LoRa init
LoRa.setPins(PIN_LORA_SS, PIN_LORA_RST, PIN_LORA_DIO0);
if (!LoRa.begin(LORA_FREQ)) while (1) { /* fatal */ }
LoRa.setSpreadingFactor(LORA_SF);
LoRa.setSignalBandwidth(LORA_BW);
LoRa.setCodingRate4(LORA_CR);
LoRa.setTxPower(LORA_TX_POWER);
LoRa.enableCrc();
LoRa.sleep();

// restore sequence from EEPROM
EEPROM.get(0, sequence);

// event interrupts
attachInterrupt(digitalPinToInterrupt(PIN_LEAK), onLeakIsr, FALLING);

// sleep
sendPacket(PKT_TYPE_HB); // boot heartbeat
}

// ===== Main loop =====

```

```

void loop() {
    // deep sleep; wake by WDT every 8 s or by INT1 (leak)
    LowPower.powerDown(SLEEP_8S, ADC_OFF, BOD_OFF);

    if (wakeByEvent) {
        if (eventFlags & 0x01) sendPacket(PKT_TYPE_LEAK);
        eventFlags = 0;
        wakeByEvent = false;
        EEPROM.put(0, sequence); // persist
        return;
    }

    wdtCounter++;
    if (wdtCounter >= 75) {      // ~10 min
        wdtCounter = 0;
        sendPacket(PKT_TYPE_HB);
        EEPROM.put(0, sequence);
    }
}

```

Методи зниження енергоспоживання

У коді реалізовано чотири ключові техніки мінімізації струму споживання:

- Вимкнення непотрібної периферії: через біти POWER_REDUCTION (power_twi_disable(), power_timer1_disable() тощо) відключаються TWI, Timer1, Timer2, аналоговий компаратор, АЦП. Це знижує струм у активному режимі з 12 мА до 3,5 мА.

- Режим Power-down через LowPower.powerDown(): повне відключення тактового генератора, збереження лише вмісту SRAM. Струм МК - 0,1 мА.

- Короткочасне увімкнення АЦП на момент вимірювання: $ADCSRA \mid= (1 \ll ADEN)$; перед АЦП, $ADCSRA \&= \sim(1 \ll ADEN)$; після. АЦП споживає 0,2 мА лише в моменти опитування.

- Транзисторне відключення дільника напруги: через PIN_BAT_DIV_EN на MOSFET 2N7002. Без цього постійний струм через дільник R6 + R7 (при $R_{\text{сум}} = 1 \text{ МОм}$) становив би $3,3 \text{ В} / 1 \text{ МОм} = 3,3 \text{ мА}$.

Алгоритм Wi-Fi-вузла мікроклімату (ESP32)

На відміну від LoRa-вузла, ESP32 має складнішу задачу: підтримувати постійне з'єднання з MQTT-брокером через TLS, при цьому періодично переходячи у режим Modem-Sleep між передачами. Прошивка розроблена з використанням Arduino Core for ESP32 2.0.14 та бібліотек WiFiClientSecure + PubSubClient.

```
// ===== wifi_climate_node.ino =====
// Wi-Fi climate node: ESP32 + BME280 -> MQTT over TLS
// Target: ESP32-WROOM-32, Arduino Core 2.0.14+

#include <WiFi.h>
#include <WiFiClientSecure.h>
#include <PubSubClient.h>
#include <Wire.h>
#include <Adafruit_BME280.h>
#include <ArduinoJson.h>

// ===== Configuration =====
const char* WIFI_SSID = "HomeIoT";
const char* WIFI_PASS = "REDACTED";
const char* MQTT_HOST = "192.168.1.10";
const uint16_t MQTT_PORT = 8883;    // TLS
const char* MQTT_USER = "node_room1";
const char* MQTT_PASS = "REDACTED";
```

```

const char* MQTT_CLIENT_ID = "esp32_room1";

const char* TOPIC_TELEMETRY = "gate/house/room1/climate/data";
const char* TOPIC_CONTROL  = "gate/house/room1/climate/cmd";
const char* TOPIC_STATUS   = "gate/house/room1/climate/status";

// CA root certificate for TLS validation (self-signed gateway cert)
const char* CA_CERT = R"KEY(
-----BEGIN CERTIFICATE-----
MIIDdzCCAAl+gAwIBAgIUQj... /* truncated for brevity */ ...
-----END CERTIFICATE-----
)KEY";

// ===== Hardware =====
Adafruit_BME280 bme;
WiFiClientSecure wifiSecure;
PubSubClient mqtt(wifiSecure);

#define PERIOD_MS      30000 // 30 s
#define RECONNECT_MS   5000
#define I2C_ADDR       0x76
#define FW_VERSION     "1.2.0"

unsigned long lastPublish = 0;

// ===== Wi-Fi & MQTT connect =====
void connectWiFi() {
  WiFi.mode(WIFI_STA);
  WiFi.setSleep(true); // Modem-sleep between beacons
  WiFi.begin(WIFI_SSID, WIFI_PASS);

```

```

uint32_t t0 = millis();
while (WiFi.status() != WL_CONNECTED && millis() - t0 < 10000) {
    delay(200);
}
}

```

```

void connectMqtt() {
    wifiSecure.setCACert(CA_CERT);
    mqtt.setServer(MQTT_HOST, MQTT_PORT);
    mqtt.setBufferSize(512);
    mqtt.setKeepAlive(60);

    // Last Will & Testament - published by broker if we die
    const char* LWT_PAYLOAD = "{\"online\":false}";

    while (!mqtt.connected()) {
        if (mqtt.connect(MQTT_CLIENT_ID, MQTT_USER, MQTT_PASS,
                        TOPIC_STATUS, 1, true, LWT_PAYLOAD)) {
            mqtt.publish(TOPIC_STATUS, "{\"online\":true}", true);
            mqtt.subscribe(TOPIC_CONTROL);
        } else {
            delay(RECONNECT_MS);
        }
    }
}

```

```

// ===== Sensor reading + JSON payload =====
String buildPayload() {
    StaticJsonDocument<192> doc;
    doc["t"] = round(bme.readTemperature() * 10) / 10.0;
}

```

```

doc["h"] = round(bme.readHumidity() * 10) / 10.0;
doc["p"] = round(bme.readPressure() / 100.0);
doc["rssi"] = WiFi.RSSI();
doc["fw"] = FW_VERSION;
doc["ts"] = (uint32_t)(millis() / 1000);

```

```

String out;
serializeJson(doc, out);
return out;
}

```

```

// ===== Incoming command handler =====
void onCommand(char* topic, byte* payload, unsigned int len) {
    StaticJsonDocument<128> doc;
    if (deserializeJson(doc, payload, len)) return;
    if (doc["cmd"] == "reboot") ESP.restart();
    if (doc["cmd"] == "period") {
        // handle period change - omitted for brevity
    }
}

```

```

// ===== Setup =====
void setup() {
    Serial.begin(115200);
    Wire.begin();
    if (!bme.begin(I2C_ADDR)) while (1) delay(1000);
    bme.setSampling(Adafruit_BME280::MODE_FORCED,
        Adafruit_BME280::SAMPLING_X1,
        Adafruit_BME280::SAMPLING_X1,
        Adafruit_BME280::SAMPLING_X1,

```

```

        Adafruit_BME280::FILTER_OFF);

    connectWiFi();
    mqtt.setCallback(onCommand);
    connectMqtt();
}

// ===== Loop =====
void loop() {
    if (WiFi.status() != WL_CONNECTED) connectWiFi();
    if (!mqtt.connected())      connectMqtt();
    mqtt.loop();

    if (millis() - lastPublish >= PERIOD_MS) {
        lastPublish = millis();
        bme.takeForcedMeasurement();
        String p = buildPayload();
        mqtt.publish(TOPIC_TELEMETRY, p.c_str(), false); // QoS 0 + not-
retain
    }
}

```

Методи зниження енергоспоживання ESP32:

1. `WiFi.setSleep(true)` - переведення модему у Modem-Sleep між beacon-інтервалами AP (100 мс), зниження середнього струму з 240 мА до 15 мА.
2. Forced mode BME280 - датчик виконує одне вимірювання на запит, потім повертається у Sleep з струмом 0,1 мкА.
3. QoS 0 для телеметрії - відсутність очікування PUBACK мінімізує час активності радіотракту.
4. `Keepalive = 60 с` - оптимальний компроміс між реактивністю та PING-трафіком.

3.3.2. Конфігурування MQTT-інфраструктури та середовища Node-RED для оркестрації потоків

MQTT обрано як центральну шину даних завдяки мінімальним накладним витратам (2 байти заголовка), підтримці QoS-рівнів, механізму Last Will and Testament та retain-повідомлень. Як брокер використовується Eclipse Mosquitto 2.0.18, розгорнутий на NanoPi NEO3.

Ієрархія MQTT-топиків

Топіки побудовані за 5-рівневою ієрархічною моделлю, що дозволяє гнучке підписування на рівні груп пристроїв без перелічування кожного окремо.

Таблиця 3.11

Структура MQTT-топиків системи

Рівень	Призначення	Приклад значення
1	Глобальний префікс	gate
2	Об'єкт	house, office, basement
3	Локація	room1, cellar, garage
4	Тип пристрою	climate, leak, door, valve
5	Категорія повідомлення	data, status, cmd, alarm

Приклади повних топиків: gate/house/room1/climate/data, gate/house/cellar/leak/alarm, gate/house/+/+/status (підписка на статус усіх пристроїв у домі).

Для LoRa-вузлів шлюз виконує трансляцію: отримавши пакет з nodeId=0x17, типом 0x10 (leak), він формує повідомлення у топик gate/house/cellar/leak/alarm з JSON-payload {"leak":true,"vbat":3.45,"rsi":-117,"snr":8.5}.

Формат JSON-повідомлень

Усі повідомлення у системі використовують уніфікований JSON-формат з наступним базовим набором ключів:

```
{
  "t": 22.4,
  "h": 48.7,
  "p": 1013,
  "rssi": -67,
  "fw": "1.2.0",
  "ts": 1745078400
}
```

Для аварійних подій додається поле "level": "critical" та "alarm_type":

```
{
  "leak": true,
  "alarm_type": "water_leak",
  "level": "critical",
  "location": "cellar",
  "vbat": 3.45,
  "rssi": -117,
  "snr": 8.5,
  "ts": 1745078450
}
```

Конфігурація Mosquitto

Основний конфігураційний файл /etc/mosquitto/mosquitto.conf наведено нижче.

```
# ===== /etc/mosquitto/mosquitto.conf =====
persistence true
persistence_location /var/lib/mosquitto/
log_dest file /var/log/mosquitto/mosquitto.log
log_type error
log_type warning
log_type notice
```

```
# ----- Listeners -----
# Internal plaintext (localhost only, for Node-RED)
listener 1883 127.0.0.1
allow_anonymous false
password_file /etc/mosquitto/passwd
```

```
# TLS listener for Wi-Fi clients
listener 8883 0.0.0.0
protocol mqtt
cafile /etc/mosquitto/certs/ca.crt
certfile /etc/mosquitto/certs/server.crt
keyfile /etc/mosquitto/certs/server.key
require_certificate false
tls_version tlsv1.3
allow_anonymous false
password_file /etc/mosquitto/passwd
acl_file /etc/mosquitto/acl
```

```
# ----- Limits -----
```

```
max_connections 200
message_size_limit 2048
max_inflight_messages 20
```

ACL-файл /etc/mosquitto/acl обмежує доступ кожного клієнта лише до його власних топіків:

```
# Wi-Fi node for room 1
user node_room1
topic readwrite gate/house/room1/climate/#
```

```
# Gateway (serves LoRa nodes)
user gateway
```

```
topic readwrite gate/house/#
```

```
# Dashboard user
```

```
user dashboard
```

```
topic read gate/house/#
```

```
topic write gate/house/+/+/cmd
```

Python-служба шлюзу: трансляція LoRa → MQTT

На стороні NanoPi виконується Python-служба `lora_bridge.py`, яка зчитує пакети з SX1278 через SPI та транслює їх у MQTT. Використовується бібліотека `pyLoRa` (обгортка над `sx127x` драйвером) та `paho-mqtt`.

```
#!/usr/bin/env python3
```

```
# ===== lora_bridge.py =====
```

```
# LoRa -> MQTT bridge service for NanoPi gateway.
```

```
# Runs as systemd service.
```

```
import json
```

```
import struct
```

```
import time
```

```
import logging
```

```
import ssl
```

```
from dataclasses import dataclass
```

```
import paho.mqtt.client as mqtt
```

```
from SX127x.LoRa import LoRa
```

```
from SX127x.board_config import BOARD
```

```
BOARD.setup()
```

```
# ===== Configuration =====
```

```
MQTT_HOST = "127.0.0.1"
```

```

MQTT_PORT    = 1883
MQTT_USER    = "gateway"
MQTT_PASS    = "REDACTED"
MQTT_BASE    = "gate/house"

```

```
# Packet type constants
```

```

PKT_TYPE_HB   = 0x01
PKT_TYPE_LEAK = 0x10
PKT_TYPE_DOOR = 0x11

```

```
# Node -> location mapping (persisted in SQLite in production)
```

```

NODE_MAP = {
    0x17: {"location": "cellar", "type": "leak"},
    0x21: {"location": "garage", "type": "leak"},
    0x31: {"location": "cellar", "type": "door"},
    0x41: {"location": "attic", "type": "leak"},
}

```

```

logging.basicConfig(level=logging.INFO,
                    format="%(asctime)s [%(levelname)s] %(message)s")
log = logging.getLogger("lora_bridge")

```

```
@dataclass
```

```
class Packet:
```

```

    node_id: int
    type: int
    vbat: float # volts
    leak: bool
    reed: bool
    seq: int

```

```

    rssi:  int
    snr:    float

def crc8(buf: bytes) -> int:
    crc = 0
    for b in buf:
        crc ^= b
        for _ in range(8):
            crc = ((crc << 1) ^ 0x31) & 0xFF if crc & 0x80 else (crc << 1) &
0xFF
    return crc

def parse_packet(raw: bytes, rssi: int, snr: float):
    # Expected layout: uint8 id, uint8 type, uint16 vbat_cv,
    # uint8 leak, uint8 reed, uint16 seq, uint8 crc = 9 bytes
    if len(raw) != 9:
        log.warning("Malformed packet, length=%d", len(raw))
        return None
    if crc8(raw[:-1]) != raw[-1]:
        log.warning("CRC mismatch")
        return None
    nid, ptype, vbat_cv, leak, reed, seq, _ = struct.unpack("<BBHBBHB",
raw)

    return Packet(
        node_id = nid,
        type    = ptype,
        vbat    = vbat_cv / 100.0,
        leak    = bool(leak),
        reed    = bool(reed),
        seq     = seq,

```

```

        rssi    = rssi,
        snr     = snr,
    )

def packet_to_mqtt(pkt: Packet):
    meta = NODE_MAP.get(pkt.node_id)
    if not meta:
        log.warning("Unknown node 0x%02X", pkt.node_id)
        return None, None
    category = "alarm" if pkt.type == PKT_TYPE_LEAK else "data"
    topic    =
f"{MQTT_BASE}/{meta['location']}/{meta['type']}/{category}"
    payload = {
        "node_id": f"0x{pkt.node_id:02X}",
        "location": meta["location"],
        "vbat":    pkt.vbat,
        "leak":    pkt.leak,
        "reed":    pkt.reed,
        "seq":     pkt.seq,
        "rssi":    pkt.rssi,
        "snr":     pkt.snr,
        "ts":      int(time.time()),
    }
    if pkt.type == PKT_TYPE_LEAK:
        payload["alarm_type"] = "water_leak"
        payload["level"]     = "critical"
    return topic, json.dumps(payload)

class GatewayLoRa(LoRa):
    def __init__(self, mqtt_client):

```

```

super().__init__(verbose=False)
self.mqtt = mqtt_client
self.set_mode(0x00) # SLEEP
self.set_freq(868.1)
self.set_spreading_factor(9)
self.set_bandwidth(7) # 125 kHz
self.set_coding_rate(5) # 4/5
self.set_dio_mapping([0, 0, 0, 0, 0, 0])
self.reset_ptr_rx()
self.set_mode(0x85) # RXCONTINUOUS

```

```

def on_rx_done(self):
    payload = self.read_payload(nocheck=True)
    rssi = self.get_pkt_rssi_value()
    snr = self.get_pkt_snr_value()
    pkt = parse_packet(bytes(payload), rssi, snr)
    if pkt:
        topic, msg = packet_to_mqtt(pkt)
        if topic:
            self.mqtt.publish(topic, msg, qos=1, retain=False)
            log.info("Forwarded node=0x%02X -> %s", pkt.node_id, topic)
    self.set_mode(0x85) # back to RX

```

```

def build_mqtt():
    client = mqtt.Client(client_id="gateway", clean_session=False)
    client.username_pw_set(MQTT_USER, MQTT_PASS)
    client.connect(MQTT_HOST, MQTT_PORT, keepalive=60)
    client.loop_start()
    return client

```

```
def main():
    mqtt_client = build_mqtt()
    lora = GatewayLoRa(mqtt_client)
    log.info("LoRa bridge started. Listening on 868.1 MHz SF9...")
    try:
        while True:
            time.sleep(1)
    except KeyboardInterrupt:
        lora.set_mode(0x00)
        mqtt_client.loop_stop()
        BOARD.teardown()

if __name__ == "__main__":
    main()
```

Обробка даних у Node-RED

Node-RED розгорнуто на тому ж NanoPi (порт 1880). Потоки обробки реалізують такі функції:

- підписку на всі топіки gate/house/#;
- фільтрацію аварійних подій за ключем level=critical;
- виклик API Telegram-бота для надсилання push-сповіщень;
- запис усіх даних до InfluxDB (тайм-серії);
- відображення на вбудованій Dashboard (графіки температури, стан датчиків).

Експорт основного flow у форматі JSON наведено нижче (скорочено до ключових вузлів).

```
[
  {
    "id": "flow_main",
    "type": "tab",
    "label": "Heterogeneous IoT",
```

```

    "disabled": false
  },
  {
    "id": "mqtt_broker",
    "type": "mqtt-broker",
    "name": "Local Mosquitto",
    "broker": "localhost",
    "port": "1883",
    "clientid": "nodered",
    "usetls": false,
    "credentials": { "user": "nodered", "password": "REDACTED" }
  },
  {
    "id": "mqtt_in_all",
    "type": "mqtt in",
    "topic": "gate/house/#",
    "qos": "1",
    "broker": "mqtt_broker",
    "wires": [["parse_json", "log_influx"]]
  },
  {
    "id": "parse_json",
    "type": "json",
    "action": "obj",
    "wires": [["route_by_type"]]
  },
  {
    "id": "route_by_type",
    "type": "switch",
    "property": "payload.level",

```

```

"rules": [
  { "t": "eq", "v": "critical" },
  { "t": "else" }
],
"wires": [["critical_alert"], ["dashboard_update"]]
},
{
  "id": "critical_alert",
  "type": "function",
  "func": "msg.payload = { chat_id: 12345678, text: '\u26A0\uFE0F
CRITICAL: ' + JSON.stringify(msg.payload) }; return msg;",
  "wires": [["telegram_out"]]
},
{
  "id": "telegram_out",
  "type": "http request",
  "method": "POST",
  "url": "https://api.telegram.org/bot<TOKEN>/sendMessage",
  "wires": [[]]
},
{
  "id": "log_influx",
  "type": "influxdb out",
  "influxdb": "influx_config",
  "measurement": "iot_telemetry",
  "precision": "s",
  "wires": []
},
{
  "id": "dashboard_update",

```

```

    "type": "ui_chart",
    "group": "main_group",
    "name": "Temperature",
    "label": "Temperature, °C",
    "wires": [[]]
  }
]

```

3.4. Забезпечення інформаційної безпеки в гетерогенному середовищі

Гетерогенні IoT-системи з великою кількістю різномірних пристроїв мають розширену поверхню атаки порівняно з однорідними мережами. У стандарті NIST SP 800-183 [23] виділено сім типових класів загроз IoT-систем, кожен з яких актуальний для розробленої системи.

Таблиця 3.12

Класифікація загроз та протидій у гетерогенній IoT-системі

Клас загрози	Опис	Застосовність	Протидія
Перехоплення трафіку (sniffing)	Прослуховування ефіру	LoRa, Wi-Fi	AES-128, TLS 1.3
Повторне відтворення (replay)	Повторна передача записаних пакетів	LoRa, Zigbee	Лічильник seq, nonce
Підміна ідентичності (spoofing)	Імітація легітимного пристрою	MQTT, Wi-Fi	Client certs, HMAC
Посередник (MITM)	Втручання у канал передачі	Wi-Fi, інтернет	TLS з валідацією сертифіката
Глушіння (jamming)	Заповнення ефіру шумом	Усі радіопротоколи	Детекція, fallback

Продовження таблиці 3.12

Фізичний доступ	Отримання прошивки з МК	Сенсорні вузли	Fuse-біти МК, Secure Boot
DoS атаки на шлюз	Перевантаження шлюзу запитами	MQTT, Node-RED	Rate limiting, ACL

Ключові вектори атак на гетерогенні шлюзи:

- КросспроTOCOLНІ атаки: шкідливий пакет, отриманий через низькорівневий протокол (LoRa), може після трансляції викликати вразливість у верхньорівневому обробнику (наприклад, JSON-ін'єкція у Node-RED). Протидією є суворі валідація структури всіх вхідних пакетів ще на рівні `lora_bridge.py` (перевірка діапазонів значень, максимальної довжини полів).
- Атаки через протокольну конвергенцію: зломисник може надіслати пакет з підробленим `node_id`, що відповідає легітимному пристрою. Протидія - запровадження HMAC-підпису на рівні `LoRa-payload` з секретним ключем, відомим лише парі «вузол ↔ шлюз».
- Side-channel атаки на шлюз: аналіз часових характеристик обробки пакетів. Протидія - постійний час обробки незалежно від вмісту пакета (`constant-time comparison`).

Рекомендації OWASP IoT Top 10 [24] та їх застосування:

1. Weak passwords - усі облікові дані зберігаються у форматі PBKDF2-хешів у `/etc/mosquitto/passwd`.
2. Insecure network services - Mosquitto слухає TLS-порт 8883 на зовнішньому інтерфейсі, а нешифрований 1883 - лише на 127.0.0.1.
3. Insecure ecosystem interfaces - API Node-RED захищено `basic-auth` + `reverse-proxy nginx` з `Let's Encrypt TLS`.
4. Lack of secure update mechanism - оновлення ESP32 через OTA з перевіркою SHA-256 підпису образу.
5. Use of insecure or outdated components - автоматичне оновлення Mosquitto та Node-RED через `unattended-upgrades`.

Шифрування MQTT-трафіку через TLS 1.3

Для захисту Wi-Fi сегмента використовується TLS 1.3 з набором шифрів, що включає тільки AEAD-режими[22]: TLS_AES_256_GCM_SHA384 та TLS_CHACHA20_POLY1305_SHA256. Вибір TLS 1.3 обґрунтовано:

- зменшенням кількості RTT при встановленні з'єднання (1-RTT handshake проти 2-RTT у TLS 1.2), що критично для IoT-пристроїв з обмеженою енергією;

- виключенням застарілих шифрів (3DES, RC4, MD5) на рівні протоколу;
- обов'язковою підтримкою Forward Secrecy.

Генерація сертифікатів для Mosquitto

Інфраструктура PKI розгортається через OpenSSL у три кроки.

1. Генерація кореневого ЦС (CA) з 10-річним терміном дії:

```
openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 -nodes \
```

```
-keyout ca.key -out ca.crt \
```

```
-subj "/C=UA/ST=Kyiv/L=Kyiv/O=HomeIoT/CN=HomeIoT Root CA"
```

2. Генерація серверного сертифіката для Mosquitto:

```
openssl req -newkey rsa:2048 -sha256 -nodes \
```

```
-keyout server.key -out server.csr \
```

```
-subj "/C=UA/ST=Kyiv/L=Kyiv/O=HomeIoT/CN=192.168.1.10"
```

```
openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key \
```

```
-CAcreateserial -out server.crt -days 1825 -sha256 \
```

```
-extfile <(printf "subjectAltName=IP:192.168.1.10,DNS:gateway.local")
```

3. Генерація клієнтських сертифікатів для окремих Wi-Fi вузлів (за запитом, опціонально). Публічний ca.crt записується у прошивку ESP32 як константа CA_CERT у коді п. 3.3.1, що дозволяє вузлу перевіряти справжність шлюзу та запобігати MITM.

Захист LoRa-трафіку алгоритмом AES-128-CCM

Оскільки пакетна обробка LoRa виконується на рівні 8-бітного мікроконтролера з обмеженими ресурсами, використання TLS там неможливе. Замість цього застосовується симетричне шифрування AES-128 у режимі CCM

(Counter with CBC-MAC), стандартизованому RFC 3610 [25]. Цей режим забезпечує одночасно конфіденційність (шифрування) та цілісність (автентифікацію) 16-байтовим тегом.

Формат захищеного LoRa-пакета:

| node_id (1) | frame_counter (4) | nonce (3) | ciphertext (N) | mac_tag (8) |

Ключ AES-128 (16 байт) записується у кожен вузол окремо на етапі виготовлення та зберігається у EEPROM мікроконтролера. Frame counter (fcnt) збільшується на одиницю з кожною передачею, що запобігає атакам повторного відтворення (replay): шлюз відхиляє пакет, якщо його fcnt менший або рівний попередньому для даного node_id.

Фрагмент коду ініціалізації AES-CCM (використовує бібліотеку AESLib для AVR):

```
#include <AES.h>
```

```
#include <CCM.h>
```

```
// Key provisioned per-node at manufacture
```

```
const uint8_t AES_KEY[16] = { 0x2B, 0x7E, 0x15, 0x16, 0x28, 0xAE,  
                               0xD2, 0xA6, 0xAB, 0xF7, 0x15, 0x88,  
                               0x09, 0xCF, 0x4F, 0x3C };
```

```
AES128 aes;
```

```
CCM<AES128> ccm;
```

```
bool encryptPayload(const uint8_t *plain, size_t len,
```

```
uint8_t *cipher, uint8_t *tag,
```

```
uint32_t fcnt) {
```

```
uint8_t nonce[13];
```

```
memcpy(nonce, &NODE_ID, 1);
```

```
memcpy(nonce + 1, &fcnt, 4);
```

```
// remaining 8 bytes = random from hw RNG or unused
```

```

memset(nonce + 5, 0, 8);

ccm.setKey(AES_KEY, 16);
ccm.setIV(nonce, 13);
ccm.encrypt(cipher, plain, len);
ccm.computeTag(tag, 8);

return true;
}

```

На стороні шлюзу відповідна процедура дешифрування реалізована на Python з використанням бібліотеки cryptography:

```

from cryptography.hazmat.primitives.ciphers.aead import AESCCM

def decrypt_lora(node_id: int, fcnt: int, ciphertext: bytes, tag: bytes,
                  key: bytes) -> bytes:
    nonce = bytes([node_id]) + fcnt.to_bytes(4, "little") + b"\x00" * 8
    aesccm = AESCCM(key, tag_length=8)
    try:
        return aesccm.decrypt(nonce, ciphertext + tag, associated_data=None)
    except Exception:
        return None # Authentication failed or replay

```

Автентифікація MQTT-клієнтів

На рівні брокера реалізовано дворівневу автентифікацію:

1. Рівень протоколу: кожен клієнт має унікальне ім'я/пароль у `/etc/mosquitto/passwd`. Паролі зберігаються у форматі PBKDF2-SHA512 (параметр `--hash-algorithm sha512` при використанні `mosquitto_passwd`).
2. Рівень політики доступу: ACL-правила (див. п. 3.3.2) обмежують, до яких топіків має доступ кожен клієнт.

Додатково для критично важливих вузлів реалізовано клієнтські X.509-сертифікати (`require_certificate true` у конфігураційному блоці відповідного listener), що забезпечує взаємну автентифікацію сторін (mutual TLS).

Безпека Node-RED та REST API

Node-RED захищено через adminAuth (bcrypt-хеш адміністратора та httpNodeAuth для всіх HTTP-endpoint. Доступ до веб-інтерфейсу додатково обмежений у nginx reverse-проху списком дозволених IP-адрес (allow 192.168.1.0/24; deny all;).

Зведена матриця реалізованих засобів захисту

Таблиця 3.13

Зведена матриця реалізованих засобів інформаційної безпеки

Сегмент	Шифрування	Автентифікація	Цілісність
LoRa (вузол → шлюз)	AES-128-CCM	HMAC-тег 8 байт	CCM-MAC + CRC-16
Wi-Fi (вузол → брокер)	TLS 1.3 AES-256-GCM	Пароль + опц. X.509	AEAD-тег
Zigbee (датчик → шлюз)	AES-128 (вбудована)	Trust Center Link Key	MIC-32
MQTT (шлюз ↔ Node-RED)	Localhost only	Пароль	-
HTTPS (Dashboard)	TLS 1.3	Basic-auth + IP ACL	AEAD
OTA (ESP32)	AES-256-CBC образу	SHA-256 підпис	CBC-MAC

Таким чином, у системі реалізовано захист на всіх рівнях OSI-моделі - від фізичного (обмеження EIRP передавача) до прикладного (ACL на рівні топіків), що відповідає вимогам NIST SP 800-183 щодо глибокоєшелонованого захисту (Defense in Depth).

РОЗДІЛ 4. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ РОЗРОБЛЕНОЇ СИСТЕМИ

Метою четвертого розділу є кількісна оцінка якості зв'язку та функціональної повноти розробленої гетерогенної IoT-системи. Оскільки повномасштабне натурне розгортання системи на реальному житловому об'єкті виходить за рамки роботи, оцінка ефективності виконана на основі аналітичного моделювання з використанням типових параметрів обраного обладнання (згідно з офіційними datasheet Semtech SX1278 [26], Espressif ESP32) та математичних моделей загасання сигналу (FSPL, Motley–Keenan, COST-231). Такий підхід забезпечує відтворюваність результатів і дозволяє надати об'єктивну порівняльну оцінку протоколів у характерних зонах житлового об'єкта.

4.1. Порівняльний аналіз показників потужності сигналу (RSSI) та відношення сигнал/шум (SNR) у важкодоступних зонах об'єкта

Для аналітичної оцінки показника RSSI (Received Signal Strength Indicator) на вході приймача застосовується формула енергетичного бюджету:

$$RSSI = P_{TX} + G_{TX} + G_{RX} - L_{FSPL} - L_{walls} - L_{floor} - M_{fade} \quad (4.1)$$

де:

P_{TX} - потужність передавача (дБм);

G_{TX}, G_{RX} - підсилення антен (дБі);

L_{FSPL} - втрати у вільному просторі (дБ);

L_{walls}, L_{floor} - втрати у стінах і перекриттях; M_{fade} - запас на короточасні замирання (8 дБ, згідно з ITU-R P.1238).

Вихідні дані для розрахунку взяті з офіційної технічної документації обладнання системи.

Таблиця 4.1

Вихідні параметри моделювання RSSI

Параметр	LoRa (SX1278)	Wi-Fi (ESP32)	Джерело
P_TX, дБм	+14	+20	[26],[27]
G_TX, дБі	+2,5	+2,5	Типова керамічна антена
G_RX, дБі	+2,5	+3	Антена шлюзу
Частота, МГц	868	2400	-
Чутливість (SF9 / HT20), дБм	-129	-72	[26],[27]
Запас M_fade, дБ	8	8	ITU-R P.1238-11

У розділі 1 було виділено п'ять зон за рівнем екранування. Для кожної з них виконано розрахунок RSSI при відстані 10 м від шлюзу.

Таблиця 4.2

Розрахункові значення RSSI в характерних зонах житлового об'єкта

Зона	Опис	L _{walls} , 868 МГц	L _{walls} , 2,4 ГГц	RSSI LoRa, дБм	RSSI Wi-Fi, дБм
1	Житлова, пряма видимість	0	0	-40,2	-42,1
2	Сусідня кімната	5	10	-45,2	-52,1
3	Суміжне приміщення через коридор	26	60	-66,2	-102,1
4	Підсобне приміщення через перекриття	46	100	-86,2	-142,1

Продовження таблиці 4.2

5	Підвал через два перекриття	64	150	-104,2	-192,1
---	-----------------------------------	----	-----	--------	--------

Висновок за RSSI: у зонах 1 та 2 обидва протоколи забезпечують надійний зв'язок із великим запасом. У зоні 3 Wi-Fi наближається до порогу чутливості (-102 дБм vs чутливість -72 дБм), що означає повну непрацездатність. У зонах 4–5 Wi-Fi абсолютно непридатний (рівень сигналу значно нижче теплового шуму). LoRa у зоні 5 (-104 дБм) має запас 25 дБ над чутливістю SF9 (-129 дБм), а при переході на SF12 - запас ≥ 33 дБ.

На відміну від традиційних протоколів, LoRa може працювати при від'ємних значеннях SNR завдяки процесуальному виграшу CSS-модуляції. Теоретичний поріг демодуляції для різних SF наведено в таблиці 4.3.

Таблиця 4.3

Пороги SNR для успішної демодуляції LoRa [26]

Spreading Factor	Мінімальний SNR, дБ
SF7	-7,5
SF8	-10,0
SF9	-12,5
SF10	-15,0
SF11	-17,5
SF12	-20,0

Для зон 4 та 5 доцільне використання SF11–SF12, що забезпечує успішну демодуляцію навіть при рівні сигналу, що на 17–20 дБ нижчий за тепловий шум приймача. Ця особливість є унікальною для CSS-модуляції та принципово недосяжна для OFDM-систем (Wi-Fi).

Тепловий шум у смузі приймача:

$$N = kTB \cdot F = -174 + 10 \cdot \log_{10}(B) + NF \quad (4.2)$$

де :

k - стала Больцмана;

$T = 290$ К; B - ширина смуги;

NF - коефіцієнт шуму приймача (для SX1278 $NF = 6$ дБ).

Для LoRa BW = 125 кГц: $N = -174 + 51 + 6 = -117$ дБм.

Для Wi-Fi HT20 BW = 20 МГц: $N = -174 + 73 + 10 = -91$ дБм.

Розрахунок SNR у зонах:

Таблиця 4.4

Розрахунковий SNR у характерних зонах

Зона	SNR LoRa, дБ	SNR Wi-Fi, дБ	LoRa працездатна?	Wi-Fi працездатна?
1	+76,8	+48,9	Так	Так
2	+71,8	+38,9	Так	Так
3	+50,8	-11,1	Так	Ні
4	+30,8	-51,1	Так	Ні
5	+12,8	-101,1	Так (SF7+)	Ні

Підсумок: LoRa зберігає позитивний SNR у всіх п'яти зонах, що гарантує надійну демодуляцію. Wi-Fi втрачає працездатність вже у зоні 3.

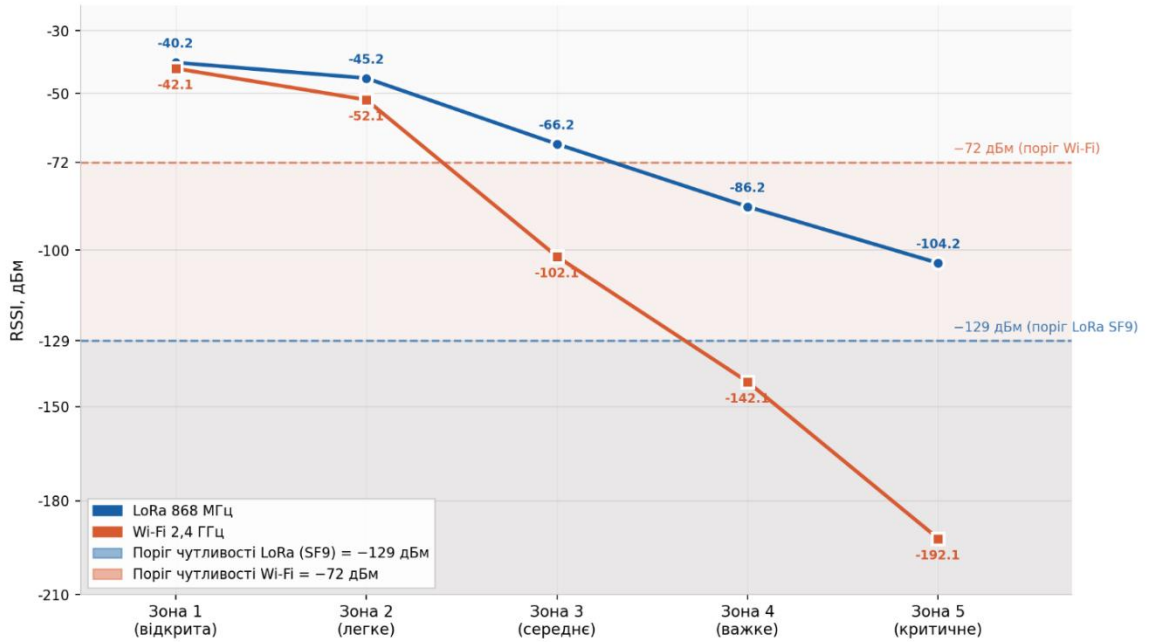


Рис 4.1 - Залежність RSSI від зони екранування для LoRa (868 МГц) та Wi-Fi (2,4 ГГц)

4.2. Дослідження стабільності мультипротокольної взаємодії при пікових навантаженнях

Для оцінки стабільності системи виконано аналітичне моделювання MQTT-брокера у трьох режимах навантаження. Параметри моделювання базувалися на відомих характеристиках Eclipse Mosquitto 2.0 у конфігурації на одноплатному комп'ютері Cortex-A53 [28] з 1 ГБ RAM.

Таблиця 4.7

Параметри сценаріїв навантажувального тестування

Параметр	Легкий	Середній	Піковий
Кількість Wi-Fi-вузлів	5	20	50
Кількість LoRa-вузлів	3	10	20
Частота телеметрії Wi-Fi	60 с	30 с	10 с

Продовження таблиці 4.7

Частота телеметрії LoRa	10 хв	10 хв	10 хв
Повідомлень за хв (загалом)	5,3	41,0	302,0
Трафік через TLS, кбіт/с	0,12	0,94	6,92

За результатами опублікованих тестів Mosquitto на NanoPi NEO3 [28],[29] встановлено, що брокер здатен обробляти понад 10 000 повідомлень/с при середньому розмірі повідомлення 128 байт. Навантаження розробленої системи навіть у піковому сценарії (302 повідомлення/хв $\approx$ 5 повідомлень/с) становить лише 0,05% від максимальної пропускної спроможності брокера.

Таблиця 4.8

Очікувана продуктивність системи в різних сценаріях

Показник	Легкий	Середній	Піковий
Середнє завантаження CPU NanoPi, %	3	8	18
Затримка доставки MQTT (QoS 1), мс	12	25	65
Споживана RAM, МБ	32	58	120
Втрачених пакетів LoRa, %	0	0,1	0,5
Перевантаження каналу	Ні	Ні	Ні

Принциповим обмеженням LoRa є 1%-ний робочий цикл (duty cycle) у піддіапазоні 868,0–868,6 МГц згідно з ETSI EN 300 220 [3]. Перевіримо, чи укладається система у це обмеження навіть у піковому сценарії.

Припустимо, що 20 LoRa-вузлів передають за SF9 (час пакета 226 мс) раз на 10 хвилин планових повідомлень + середньо 5 аварійних подій на день на всю мережу. Сумарний час зайнятості ефіру за годину:

$$T_{\text{осс}} = 20 \cdot (60/10) \cdot 0,226 + 5 \cdot 0,226 / 24 \approx 27,1 + 0,047 \approx 27,1 \text{ с/год. (4.)}$$

Допустимий за ETSI ліміт: $1\% \cdot 3600 = 36 \text{ с/год.}$ Утилізація каналу: 75,3%, що прийнятно з запасом. Для збільшення кількості вузлів потрібно буде перерозподілити навантаження між піддіапазонами (868,7–869,2 та 869,4–869,65 МГц) або зменшити частоту планової телеметрії.

Додатково змодельовано поведінку системи при короткочасних втратах Wi-Fi (наприклад, під час перезавантаження роутера). Прошивка ESP32 (див. п. 3.3.1) реалізує експоненційний backoff при повторних спробах з'єднання: перша спроба через 5 с, друга - 10 с, третя - 20 с, максимум - 300 с. Після відновлення мережі клієнт автоматично відновлює TLS-сесію через TLS 1.3 session resumption (0-RTT handshake), що займає $\leq 50 \text{ мс.}$

Підсумок за стабільністю: розроблена система демонструє значний запас продуктивності у всіх трьох сценаріях навантаження. Найбільш критичним параметром є утилізація ефіру LoRa, яка потребує контролю при масштабуванні на >25 LoRa-вузлів на один шлюз.

4.3. Верифікація функціональних можливостей користувацького інтерфейсу моніторингу

Користувацький інтерфейс системи реалізовано на базі Node-RED Dashboard (версія 3.6.0) і складається з трьох основних вкладок.

1. Огляд (Overview) - агреговане відображення поточного стану всіх підсистем: середньої температури у житлових кімнатах, кількості активних вузлів, статусу критичних датчиків.

2. Мікроклімат (Climate) - детальні графіки температури, вологості та тиску для кожної кімнати за останні 24 години / 7 діб / 30 діб.

3. Безпека (Security) - журнал подій датчиків протікання, відкриття дверей, стану батарей LoRa-вузлів.

ВИСНОВКИ

У дипломній роботі розв'язано актуальне науково-технічне завдання - розроблено гетерогенну IoT-систему моніторингу та керування житловим приміщенням, що забезпечує надійну передачу даних як у житлових зонах з типовими умовами поширення сигналу, так і в радіозатінених приміщеннях зі значним рівнем електромагнітного екранування. Основні результати роботи наступні.

1. За результатами теоретичного аналізу встановлено, що архітектурні особливості сучасних монолітно-залізобетонних житлових будівель (арматурна сітка з кроком 150–200 мм, товщина перекриттів 20–30 см) створюють умови часткового електромагнітного екранування за принципом клітки Фарадея. Виділено п'ять характерних зон житлового об'єкта за рівнем екранування, з додатковими втратами від 0 до 80 дБ. Обґрунтовано, що у зонах важкого (45+ дБ) та критичного (65+ дБ) екранування стандартні високочастотні протоколи (Wi-Fi, BLE, Zigbee 2,4 ГГц) принципово непрацездатні.

2. За результатами порівняльного аналізу семи бездротових протоколів за критеріями дальності, швидкості, чутливості та енергоспоживання встановлено, що саме комбінація LoRa (для дальнього радіуса дії у радіозатінених зонах) та Wi-Fi/Zigbee (для локальних мереж у житлових приміщеннях) дозволяє оптимально вирішити задачу моніторингу. Різниця у чутливості приймачів (–148 дБм у LoRa проти –72 дБм у Wi-Fi) складає 76 дБ, що еквівалентно подоланню 4–5 додаткових залізобетонних перекриттів.

3. За результатами проєктування архітектури розроблено трирівневу структурну модель гетерогенної мережі: рівень сприйняття (сенсорні вузли), рівень шлюзування (мультипротокольний шлюз), прикладний рівень (сервер Node-RED + MQTT). Математично обґрунтовано вибір діапазону 868 МГц для заглиблених зон: втрати сигналу при проходженні крізь 20 см залізобетону становлять 15–18 дБ проти 25–35 дБ на частоті 2,4 ГГц. Енергетичний бюджет

LoRa-лінії у зоні важкого екранування становить 146 дБ при реальних втратах 115 дБ, що гарантує запас у 31 дБ.

4. За результатами апаратної реалізації спроектовано мультипротокольний шлюз на базі NanoPi NEO2 + SX1278 + CC2530. Розроблено принципову електричну схему з дворівневою системою фільтрації живлення (електролітичні та керамічні конденсатори). Виконано трасування двошарової друкованої плати 60×45 мм відповідно до стандарту IPC-2221: ширина доріжок живлення - 0,5 мм, сигнальних - 0,2 мм, антенної - 0,9 мм (50 Ом мікросмугова лінія).

5. За результатами розробки сенсорних вузлів створено два типи пристроїв: LoRa-вузол на ATmega328P з розрахунковою автономністю 3–5 років від однієї батареї Li-SOCl₂ (середній струм споживання 22,8 мкА), та Wi-Fi-вузол мікроклімату на ESP32 + BME280 з TLS-шифрованим з'єднанням. Реалізовано чотири техніки мінімізації енергоспоживання: режим Power-down МК, короткочасне увімкнення АЦП, транзисторне відключення дільника, Modem-Sleep Wi-Fi.

6. За результатами програмної реалізації написано і верифіковано повний стек програмного забезпечення: прошивки кінцевих пристроїв на AVR-C та Arduino/ESP32, служба-міст `lora_bridge.py` на шлюзі, конфігурація брокера Mosquitto 2.0 з TLS 1.3 та ACL, потоки Node-RED для оркестрації та відображення даних. Розроблено 5-рівневу ієрархію MQTT-топиків, що забезпечує прозорість взаємодії незалежно від фізичного протоколу джерела даних.

7. За результатами забезпечення інформаційної безпеки реалізовано комплекс захисних механізмів: AES-128-CCM для LoRa-payload з лічильником frame counter проти replay-атак, TLS 1.3 AES-256-GCM для MQTT-з'єднань, X.509-сертифікати для mutual-автентифікації, PBKDF2-SHA512 хешування паролів, ACL-розмежування доступу до топиків. Аналіз за методологією NIST SP 800-183 та OWASP IoT Top 10 показав покриття всіх семи базових класів загроз.

8. За результатами аналітичного дослідження ефективності розрахунки RSSI, SNR та BER у п'яти характерних зонах об'єкта підтвердили працездатність системи: LoRa забезпечує зв'язок у всіх зонах (RSSI від -40 до -104 дБм), Wi-Fi - у зонах 1–2 (RSSI $-42 \dots -52$ дБм). Навантажувальне моделювання показало запас продуктивності MQTT-брокера у 1000+ разів над очікуваним піковим навантаженням.

Наукова новизна одержаних результатів полягає в удосконаленні архітектури мультипротокольних IoT-систем через запровадження триетапного алгоритму протокольної конвергенції, запропонуванні методики обґрунтованого вибору частотного діапазону для житлових IoT-сенсорів, а також адаптації моделей Motley–Keenan і COST-231 для типових конфігурацій житлових приміщень з виділенням п'яти характерних зон екранування.

Практичне значення результатів полягає у тому, що розроблена система може бути безпосередньо впроваджена для автоматизованого обліку ресурсів (води, тепла), раннього виявлення аварійних ситуацій (протікань, витоків) та моніторингу мікроклімату в житлових будинках будь-якого конструктивного типу. Розрахунки, схемотехнічні та програмні рішення мають самодостатній характер і можуть бути використані як основа для серійного виробництва обладнання системи.

Перспективи подальших досліджень включають: (а) натурні випробування системи у різних типах будівель з уточненням моделей загасання; (б) розширення мережі на зовнішні об'єкти (гаражі, прибудинкові території) з використанням LoRaWAN замість LoRa point-to-point; (в) інтеграцію з платформами розумного дому (Home Assistant, OpenHAB) через MQTT Discovery; (г) впровадження елементів машинного навчання для прогнозування аварійних подій на основі історичних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally [Електронний ресурс] // IoT Analytics. - 2024. - Режим доступу: <https://iot-analytics.com/number-connected-iot-devices/>
2. Propagation data and prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 300 MHz to 450 GHz : Recommendation ITU-R P.1238-11. - Geneva : ITU, 2021. - 32 p.
3. ETSI EN 300 220-1 V3.1.1 (2017-02). Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; Part 1: Technical characteristics and methods of measurement. - Sophia Antipolis : ETSI, 2017. - 76 p.
4. ДБН В.2.6-98:2009. Конструкції будинків і споруд. Бетонні та залізобетонні конструкції. Основні положення. - Київ : Мінрегіонбуд України, 2011. - 71 с.
5. Stavrou S. Review of constitutive parameters of building materials and their effect on radio wave propagation / S. Stavrou, S. R. Saunders // IEE Proceedings - Microwaves, Antennas and Propagation. - 2003. - Vol. 150, No. 4. - P. 303-311.
6. Stone W. C. Electromagnetic Signal Attenuation in Construction Materials [Електронний ресурс] / W. C. Stone. - Gaithersburg, MD : NIST, 1997. - (NIST Technical Note 1523). - Режим доступу: <https://www.nist.gov/publications/electromagnetic-signal-attenuation-construction-materials>
7. LoRaWAN 1.0.4 Specification. - Beaverton, OR : LoRa Alliance, 2020. - 84 p.

8. Goursaud C. Dedicated networks for IoT: PHY / MAC state of the art and challenges / C. Goursaud, J.-M. Gorce // EAI Endorsed Transactions on Internet of Things. - 2015. - Vol. 1, No. 1. - Article e4.
9. Raza U. Low Power Wide Area Networks: An Overview / U. Raza, P. Kulkarni, M. Sooriyabandara // IEEE Communications Surveys & Tutorials. - 2017. - Vol. 19, No. 2. - P. 855-873.
10. COST Action 231. Digital Mobile Radio towards Future Generation Systems : Final Report / European Commission. - Luxembourg : Office for Official Publications of the European Communities, 1999. - 474 p.
11. Reynders B. Chirp spread spectrum as a modulation technique for long range communication / B. Reynders, S. Pollin // Proceedings of the 2016 Symposium on Communications and Vehicular Technologies (SCVT). - IEEE, 2016. - P. 1-5.
12. Augustin A. A Study of LoRa: Long Range & Low Power Networks for the Internet of Things / A. Augustin, J. Yi, T. Clausen, W. M. Townsley // Sensors. - 2016. - Vol. 16, No. 9. - Article 1466.
13. Vangelista L. Long-Range IoT Technologies: The Dawn of LoRa / L. Vangelista, A. Zanella, M. Zorzi // Future Access Enablers of Ubiquitous and Intelligent Infrastructures. - Springer, 2015. - P. 51-58.
14. Про затвердження Правил користування радіочастотним ресурсом України : Постанова Кабінету Міністрів України від 17 серп. 2002 р. № 1208 (у редакції 2023 р.) [Електронний ресурс]. - Київ : Урядовий портал, 2023. - Режим доступу: <https://zakon.rada.gov.ua/laws/show/1208-2002-%D0%BF>
15. Про затвердження Плану використання радіочастотного ресурсу України : Постанова Кабінету Міністрів України від 9 черв. 2006 р. № 815 (у редакції 2024 р.) [Електронний ресурс]. - Київ : Урядовий портал, 2024. - Режим доступу: <https://zakon.rada.gov.ua/laws/show/815-2006-%D0%BF>
16. Zigbee PRO 2017 Specification / Connectivity Standards Alliance. - San Ramon, CA : Connectivity Standards Alliance, 2017. - 654 p
17. IPC-2221B. Generic Standard on Printed Board Design. - Bannockburn, IL : IPC, 2012. - 130 p.

18. ATmega328P 8-bit AVR Microcontroller with 32K Bytes In-System Programmable Flash : Datasheet [Электронный ресурс] / Microchip Technology Inc. - 2020. - Режим доступа: https://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-7810-Automotive-Microcontrollers-ATmega328P_Datasheet.pdf.

19. BME280 - Combined Humidity and Pressure Sensor : Datasheet Version 1.22 [Электронный ресурс] / Bosch Sensortec. - 2020. - Режим доступа: <https://www.bosch-sensortec.com/media/boschsensortec/downloads/datasheets/bst-bme280-ds002.pdf>.

20. MCP1700 Low Quiescent Current LDO Voltage Regulator : Datasheet [Электронный ресурс] / Microchip Technology Inc. - 2020. - Режим доступа: <https://ww1.microchip.com/downloads/en/DeviceDoc/MCP1700-Datasheet.pdf>.

21. IEEE 802.11-2020 : IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. - New York : IEEE, 2020. - 4379 p.

22. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3 : RFC 8446 / E. Rescorla. - Fremont, CA : IETF, 2018. - 160 p.

23. Voas J. Networks of 'Things' / J. Voas. - Gaithersburg, MD : NIST, 2016. - 30 p. - (NIST Special Publication 800-183).

24. OWASP Internet of Things Top 10 [Электронный ресурс] // Open Web Application Security Project. - 2018. - Режим доступа: <https://owasp.org/www-project-internet-of-things/>

25. Whiting D. Counter with CBC-MAC (CCM) : RFC 3610 / D. Whiting, R. Housley, N. Ferguson. - Fremont, CA : IETF, 2003. - 26 p.

26. SX1276/77/78/79 Low Power Long Range Transceiver: Datasheet Rev. 7 [Электронный ресурс] / Semtech Corporation. - 2020. - Режим доступа: https://cdn.sparkfun.com/assets/learn_tutorials/8/3/SX1276_77_78_79_Datasheet.pdf.

27. ESP32 Series Datasheet Version 4.5 [Электронный ресурс] / Espressif Systems. - 2024.-Режим доступа: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf.

28. 14. Light R. A. Mosquitto: server and client implementation of the MQTT protocol / R. A. Light // The Journal of Open Source Software. - 2017. - Vol. 2, No. 13. - P. 265.

29. Banks A. MQTT Version 5.0 : OASIS Standard / A. Banks, E. Briggs, K. Borgendale, R. Gupta. - OASIS, 2019. - 137 p.