НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет електроніки
(повна назва інституту/факультету)

Кафедра акустичних та мультимедійних електронних систем
(повна назва кафедри)

«На правах рукопису»
УДК 621.396.1

«До захисту допущено»

Завідувач кафедри
_____ - С.А. Найда
(ініціали, прізвище)

“7” грудня 2020 р.

Магістерська дисертація

зі спеціальності 171 «Електроніка»
(код і назва)

на тему: «Дослідження сенсорної мережі з використанням технології LoRa»

Виконав: студент II курсу, групи ДВ-92мп
(шифр групи)

Мавдрик Андрій Анатолійович _____
(прізвище, ім’я, по батькові) (підпис)

Керівник доцент, к.т.н. Попович П.В. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____
(науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент доцент кафедри ЕІ, к.т.н., доц. Попов А.О. _____
(посада,науковий ступінь,вчене звання,науковий ступінь,прізвище,ініціали) (підпис)

Засвідчую, що у цьому дипломному проекті немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет електроніки

Кафедра акустичних та мультимедійних електронних систем

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність 171 «Електроніка» («Електронні системи мультимедіа та засоби Інтернету речей»)

ЗАТВЕРДЖУЮ
Завідувач кафедри
С.А. Найда
(ініціали, прізвище)
« 7 » грудня 2020 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Мавдрику АндріюАнатолійовичу
(прізвище, ім'я, по батькові)

1 Тема роботи «Дослідження сенсорної мережі з використанням технології LoRa»
керівник роботи Попович Павло Васильович, доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «5» листопада 2020 р. № 3241-с

2 Строк подання студентом дисертації 07 грудня 2020 р.
3. Об'єкт дослідження технологія LoRa.

4. Предмет дослідження (Вихідні дані – для магістерської дисертації за освітньо-професійною програмою) створення сенсорних мереж в рамках IoT за технологією LoRa.

5. Перелік завдань, які потрібно розробити: розглянути концепцію сенсорних мереж і технології, що використовуються в системах Інтернету речей, дослідити технічні характеристики технології LoRa, проаналізувати можливості технології для її використання, змоделювати мережу покриття частини міста для використання технології LoRa.

6. Перелік графічного (ілюстративного) матеріалу 12-14 слайдів презентації: характеристика роботи, формулювання завдання роботи, загальні характеристики понять Інтернету речей та сенсорної мережі, безпроводові технології для створення мережі IoT, технологія LoRa, основні параметри технології LoRa, розрахунок основних параметрів мережі та моделювання в програмному середовищі Atoll мережі LoRa, висновки.

7. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

8. Дата видачі завдання 2 жовтня 2019 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Написання першого розділу	20.03.2020	виконано
2	Написання другого розділу	12.06.2020	виконано
3	Написання третього розділу	22.10.2020	виконано
4	Написання четвертого розділу	06.11.2020	виконано
	Написання п’ятого розділу	20.11.2020	виконано
5	Підготовка матеріалів до друку та оформлення пояснювальної записки	01.12.2020	виконано
6	Підготовка та оформлення презентації для доповіді	04.12.2020	виконано

Студент _____ А. А. Мавдрик
(підпис) (ініціали, прізвище)

Керівник роботи _____ П. В. Попович
(підпис) (ініціали, прізвище)

УДК 621.396.1

РЕФЕРАТ

Мавдрик А.А. Дослідження сенсорної мережі з використанням технології LoRa: магістерська дис.: 171 Електроніка. Київ, КПІ ім. Ігоря Сікорського, 2020, 129 с.

Ключові слова: інтернет речей, безпроводовий протокол, технологія LPWAN, LoRa, сенсорна мережа, LoRaWAN.

Актуальність роботи. Зі стрімким розвитком Інтернету речей та популяризацією концепції «розумного міста» кількість підключених до мережі пристроїв з кожним днем невпинно зростає. За прогнозами Ericsson до 2021 р. кількість підключень сягатиме 28 мільярдів. При цьому близько півтора мільярда пристроїв, підключених до глобальної мережі, будуть представляти категорію споживчої електроніки і смарт-автомобілів.

Стає очевидним, що звичайних технологій мобільного зв’язку недостатньо для подальшого розвитку IoT мережі через невелику ємність та зону покриття, а також досить високу вартість терміналів. До того ж пристрої можуть знаходитись у важкодоступних місцях, що вимагає їх високої автономності та достатнього рівня сигналу в точці приймання. Це створює потребу впровадження нових технологій безпроводового зв’язку [1].

Для вирішення цієї проблеми була розроблена технологія IoT, яка отримала назву LoRa. Ця технологія, перш за все, відрізняється низьким рівнем енергоспоживання. Її основним призначенням є застосування у M2M додатках. LoRa надає компанії, що працює в сфері телекомунікацій, величезний вибір можливостей. Так, застосування цього стандарту дає змогу значно збільшити дохідності операторів від одного користувача. У цьому випадку, LoRa займе свою нішу в галузі, в якій вимагається мінімальне енергоспоживання та забезпечення безперебійного передавання даних [2].

Мета і завдання дослідження. *Метою* роботи є дослідження реалізації сенсорної мережі з використанням технологої LoRa. Для досягнення поставленої мети необхідно виконати такі *завдання*:

- розглянути концепцію сенсорних мереж і технології, що використовуються в системах Інтернету речей;
- дослідити технічні характеристики технології LoRa;
- проаналізувати можливості технології для її використання;
- змоделювати мережу покриття частини міста для використання технології LoRa;

Об'єкт дослідження - безпроводова телекомунікаційна технологія LoRa.

Предмет дослідження – створення сенсорних мереж в рамках IoT за технологією LoRa.

Методи дослідження – критичний аналіз технології LoRa та інших безпроводових технологій IoT, використання програмного забезпечення Atoll для моделювання мережі за технологією LoRa.

Наукова новизна одержаних результатів. Удосконалено застосування технології LoRa для створення сенсорних мереж IoT, що дає можливість реалізувати такі складові як транспортна, медична, адміністративна, що вимагають мінімальних затримок та невисокої швидкості передачі даних (близько 10 кбіт/с).

Практичне значення одержаних результатів. Запропоновано сценарії застосування технології LoRa у великих містах та мегаполісах в Україні на основі вже існуючих стільникових мереж LTE та встановленого обладнання на частоті 900 МГц, що вже використовується операторами. Розраховано параметри мережі та проведено її моделювання в програмному середовищі Atoll на території 4,5 км^2 [2].

Практичним результатом роботи є те, що отримано модель покриття сенсорної мережі та здобуто знання про її впровадження в системах Інтернету

речей. Результати проведеної роботи можуть бути використані для вибору для проектування сенсорних мереж для Інтернету речей на певній території.

SUMMARY

Graduate work: 129 pages, 41 figures, 22 tables, 1 application, 24 sources.

Key words: Internet of Things, wireless protocol, LPWAN technology, LoRa, sensor network, LoRaWAN.

With the rapid development of the Internet of Things and the popularization of the concept of "smart city", the number of devices connected to the network is constantly growing. Ericsson estimates that by 2021 the number of connections will reach 28 billion. At the same time about one and a half billion devices connected to the global network will represent the category of consumer electronics and smart cars.

It is becoming clear that conventional mobile technologies are not enough for the further development of the IoT network due to the small capacity and coverage area, as well as the relatively high cost of terminals. In addition, devices may be located in hard-to-reach places, which requires their high autonomy and a sufficient level of signal at the point of reception. This creates the need for new wireless technologies.

To solve this problem, IoT technology was developed, which was called LoRa. This technology, above all, has a low level of energy consumption. Its main purpose is to be used in M2M applications. LoRa provides telecommunications companies with a huge range of opportunities. Yes, the application of this standard allows to significantly increase the profitability of operators from one user. In this case, LoRa will occupy its niche in the industry, which requires minimal energy consumption and uninterrupted data transmission.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ, ОДИНИЦЬ ТА СКОРОЧЕНЬ 10
ВСТУП 12
1 БЕЗПРОВОДОВІ СЕНСОРНІ МЕРЕЖІ ТА ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ 13
1.1 Поняття Інтернету речей (IoT) 13
1.2 Безпроводові сенсорні мережі для Інтернету речей 18
1.2.1 Сенсорні вузли 19
1.2.2 Технології мережі доступу 19
1.3 Безпроводові технологі для IoT 21
1.3.1 Супутникові мережі 21
1.3.2 Wi-Fi 22
1.3.3 Bluetooth 24
1.3.4 ZigBee 25
1.3.5 RFID 28
1.3.6 NFC 29
2 ТЕХНОЛОГІЯ LORA ТА LORAWAN 32
2.1 Фізичний рівень LoRa 32
2.2 Рівень MAC LoRaWaN 35
2.2.1 Фізичний рівень (PHY Layer) 38
2.2.2 MAC рівень 40
2.2.3 Підтвердження отримання повідомлень 44
2.2.4 Адаптивна швидкість передачі (Adaptive Data Rate - ADR) 46
2.2.5 Основні константи стека протоколів LoRaWAN 47
2.2.6 Команди MAC рівня 48
2.3 Топологія LoRaWAN 50
2.4 Переваги та недоліки технології LoRa 52
3 ДОСЛІДЖЕННЯ ПАРАМЕТРІВ МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІЇ LORA 56

3.1 Основні параметри технології LoRa та зв'язок між ними 59
3.2 Методика оцінювання впливу параметрів фізичного інтерфейсу LoRa на надійність мережі 76
3.2.1 Безпека в мережах LoRa 77
3.2.2 Активація кінцевих пристроїв 79
3.3 Особливості роботи пристроїв Class-B 82
3.3.1 Передача даних в каналі "вниз" 82
3.3.2 Формат кадру Ping в DL каналі (при роботі в режимі класу "B") 85
3.3.3 Синхронізація тимчасового інтервалу в DL каналі для пристроїв класу "B" 87
3.3.4 Випадковий вибір слота 89
3.3.5 Частотні канали DL для індивідуальної і групової передачі 91
3.4 Особливості роботи пристроїв Class-C 92
3.4.1 Групова передача повідомлень для пристроїв класу C 93
4 ОСОБЛИВОСТІ ФОРМУВАННЯ РАДІОПОКРИТТЯ ТА ЄМНОСТІ МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІ LORA 96
4.1 Особливості радіопокриття LoRa 96
4.1.1 Розрахунок параметрів 96
4.1.2 Моделювання мережі 99
4.2 Особливості формування ємності мережі LoRa 101
5 СТАРТАП-ПРОЕКТ 113
5.1 Основні відомості про проект 113
5.2 Технологічний аудит ідеї стартап-проекту 115
5.3 Аналіз можливостей ринку для запуску проекту 115
ВИСНОВКИ 119
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ 122
Додаток А 125

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ, ОДИНИЦЬ ТА СКОРОЧЕНЬ

AES	–	Advanced Encryption Standard (алгоритм блочного шифрування);
AppSKey	–	Application Security Key(ключ шифрування програми);
DL	–	Downlink (лінія вниз);
DR	-	Data Rate (швидкість передавання);
GSM	–	Global System for Mobile Communications;
IEEE	–	Institute of Electrical and Electronics Engineers (інститут інженерів з електротехніки і електроніки);
IOT	–	Internet of Things (Інтернет речей);
IPv6	–	Internet Protocol version 6 (Інтернет протокол версії 6);
LPWAN	–	Low-power Wide-area Network (енергоефективна мережа далекого радіусу дії);
LTE	–	Long Term Evolution (довгостроковий розвиток);
M2M	–	Machine-to-Machine (машино-машинна взаємодія);
NB-IoT	–	Narrow-Band Internet of Things (вузькосмуговий Інтернет речей);
NFC	–	Near Field Communication (Зв'язок на невеликих відстанях);
NwkSKey	–	Network Security Key (ключ шифрування мережі);
OFDM	–	Orthogonal Frequency-Division Multiplexing (мультиплексування з ортогональним частотним розділенням каналів);
OFDMA	–	Orthogonal Frequency-Division Multiple Access (множинний доступ з ортогональним частотним розділенням каналів);
OTAA	–	Over The Air Activasion (активація по повітрю);
P2P	–	Peer-To-Peer (рівний до рівного);
QPSK	–	Quadrate Phase Shift Keying (квадратурна фазова маніпуляція);
RF	–	Radio Frequency (радіочастота)

RFID – Radio-frequency identification (радіочастотна ідентифікація);

UL – Uplink (лінія вгору);

WIFI – Wireless Fidelity (безпроводова точність);

WLAN – Wireless local area network (безпроводова локальна мережа);

WSN – Wireless sensor network (безпроводова сенсорна мережа);

ВСТУП

Інтернет речей - один з головних технологічних трендів. Якщо пояснювати зовсім просто, це об'єднання різних пристроїв, від холодильника до заводу, в єдину мережу практично без участі людини. Мова не про комп'ютери та смартфони, а взагалі про все: медицині, фінансах, армії, торгівлі і навіть видобутку нафти. Все це може працювати автоматично, у своїй «екосистемі». Аналітики називають це «новою промисловою революцією», яка вже йде, і оцінюють цей ринок в трильйони доларів. І для підключення всіх цих пристроїв в єдину мережу потрібна надійна технологія, наприклад, LoRa.

Модуляція LoRa визначає фізичний рівень передачі даних, в той час як LoRaWAN ™ це відкритий протокол для мереж з високою ємністю (до 1 000 000 пристроїв в одній мережі) з великим радіусом дії і низьким енергоспоживанням, який LoRa Alliance стандартизував для глобальних мереж з низьким енергоспоживанням (Low Power Wide Area Networks, LPWAN). LoRaWAN мережа організована як мережа типу зірка і включає різні класи (A, B і C) вузлів для оптимізації компромісу між швидкістю доставки інформації і терміном роботи при живленні від батареї.

Протокол забезпечує двосторонній зв'язок з шифруванням для всіх класів пристроїв. Архітектура протоколу розроблялася в тому числі і для того, щоб легко знайти мобільні об'єкти для відстеження пересувань - найбільш швидкозростаючим напрямком додатків інтернету речей (Internet of Things, IoT).

LoRaWAN розробляється з можливістю застосування в загальнонаціональних мережах великих операторів зв'язку і LoRa Alliance стандартизує LoRaWAN з урахуванням сумісності і взаємодії з глобальними операторами зв'язку.

1 БЕЗПРОВОДОВІ СЕНСОРНІ МЕРЕЖІ ТА ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Поняття Інтернету речей (IoT)

Інтернет речей, або IoT, - це система взаємопов’язаних обчислювальних пристроїв, механічних та цифрових машин, об’єктів, тварин чи людей, які забезпечуються унікальними ідентифікаторами (UID) та можливістю передавати дані через мережу, не вимагаючи взаємодії людини з людиною або людини з комп’ютером.

«Річчю» в Інтернеті речей може бути людина з імплантатом монітора серця, сільськогосподарська тварина з транспондером біочіпа, автомобіль, який має вбудовані датчики, що сповіщають водія про низький тиск в шинах або будь-який інший природний або штучний об'єкт, якому може бути присвоєна адреса Інтернет-протоколу (IP) який здатний передавати дані через мережу [3].

Все частіше організації в різних галузях використовують IoT для ефективнішої роботи, кращого розуміння клієнтів для надання розширеного обслуговування споживачів, вдосконалення процесу прийняття рішень та збільшення вартості бізнесу.

Інтернет речей базується на традиційних телекомунікаційних мережах та інших носіях інформації. IoT є розширенням звичайного Інтернету. Кінцевий пристрій Інтернету - комп'ютер (ПК, сервер) виконує всі види програм. Інтернет - це не що інше, як обробка даних і передавання їх між комп'ютером і мережею.

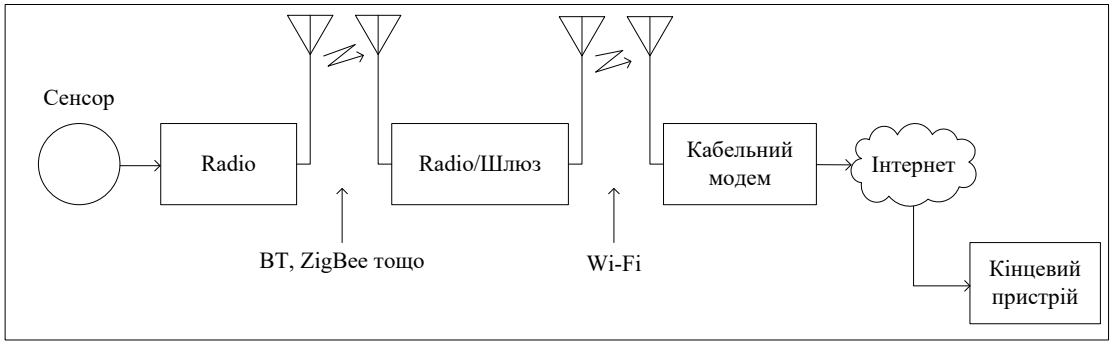

Рисунок 1.1 - Сценарії бездротового з'єднання для IoT

На рис. 1.1 показано, як виглядає IoT у бездротовому з'єднанні. Крім того, в IoT використовуються шість важливих стандартів протоколу бездротового зв'язку для того, щоб відповідати різним вимогам у створенні IoT [4].

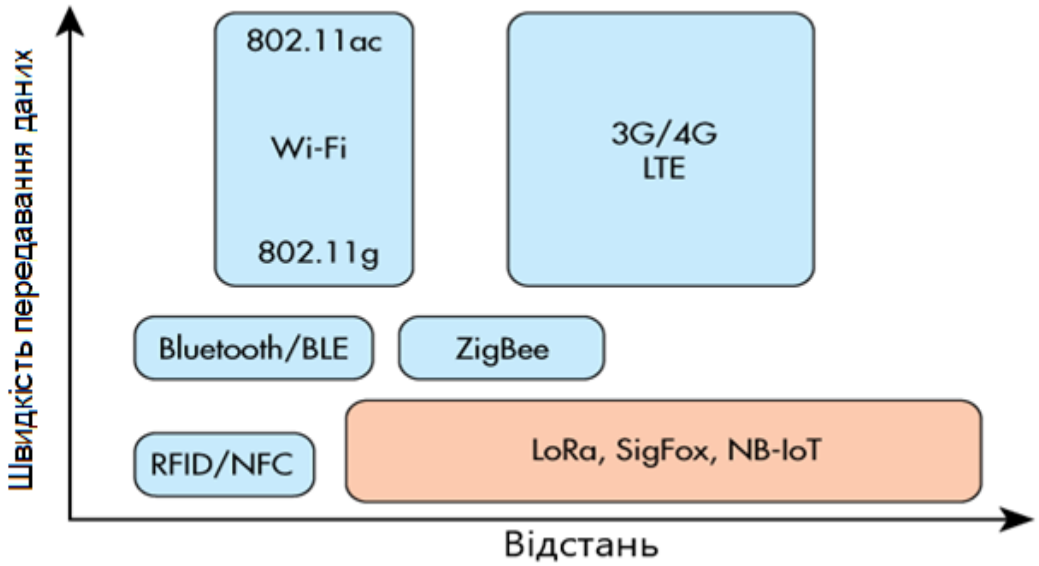

Рисунок 1.2 - Місце технологій IoT у сімействі безпроводових стандартів

Екосистема IoT складається з розумних пристроїв з підтримкою Інтернету, які використовують вбудовані системи, такі як процесори, датчики та

комунікаційне обладнання, для збору, надсилання та дій з даними, які вони отримують із свого середовища. Пристрої IoT обмінюються даними датчиків, які вони збирають, підключаючись до шлюзу IoT або іншого крайового пристрою, де дані або надсилаються в хмару для їх аналізу або локального аналізу. Іноді ці пристрої взаємодіють з іншими пов'язаними пристроями та діють на основі інформації, яку вони отримують один від одного. Пристрої виконують більшу частину роботи без втручання людини, хоча люди можуть взаємодіяти з пристроями - наприклад, для їх налаштування, надання їм інструкцій або доступу до даних.

IoT також може використовувати штучний інтелект (AI) та машинне навчання, щоб полегшити та динамічніші процеси збору даних.

Інтернет речей допомагає людям жити і працювати розумніше, а також отримати повний контроль над своїм життям. На додаток до пропонування розумних пристроїв для автоматизації будинків, IoT є важливим для бізнесу. IoT надає компаніям можливість у реальному часі вивчити, як насправді працюють їх системи, надаючи уявлення про все - від продуктивності машин до ланцюгів поставок та логістичних операцій.

IoT дозволяє компаніям автоматизувати процеси та зменшити витрати на робочу силу. Це також скорочує витрати відходів та покращує надання послуг, роблячи дешевшим виробництво та доставку товарів, а також забезпечуючи прозорість операцій із клієнтами.

Таким чином, IoT є однією з найважливіших технологій у повсякденному житті, і вона буде продовжувати набирати силу, оскільки більше підприємств усвідомлює потенціал підключених пристроїв, щоб зберегти їх конкурентоспроможність

Інтернет речей пропонує декілька переваг для організацій. Деякі переваги є галузевими, а деякі застосовні в різних галузях. Деякі загальні переваги IoT дозволяють компаніям:

- контролювати їх загальні бізнес-процеси;
- покращити взаємодію з клієнтами;
- економити час і гроші;
- підвищення продуктивності праці працівників;
- інтегрувати та адаптувати бізнес-моделі;
- приймати кращі ділові рішення;
- приносять більше доходу.

IoT закликає компанії переосмислити способи підходу до свого бізнесу та надає їм інструменти для вдосконалення своїх бізнес-стратегій.

Як правило, IoT найбільш поширений у виробничих, транспортних та комунальних організаціях, використовуючи датчики та інші пристрої IoT; однак він також знайшов випадки використання для організацій, що займаються сільським господарством, інфраструктурою та галузями автоматизації будинків, що веде деякі організації до цифрової трансформації.

IoT може принести користь фермерам у сільському господарстві, полегшивши їм роботу. Датчики можуть збирати дані про кількість опадів, вологості, температури та вмісту ґрунту, а також про інші фактори, які допоможуть автоматизувати технології ведення сільського господарства.

Можливість моніторингу операцій навколо інфраструктури також є фактором, з яким може допомогти IoT. Наприклад, датчики можуть використовуватися для спостереження за подіями або змінами в структурних будівлях, мостах та іншій інфраструктурі. Це приносить із собою такі переваги, як економія коштів, заощаджений час, зміна робочого циклу якості та безпаперовий робочий процес.

Бізнес з домашньої автоматизації може використовувати IoT для моніторингу та управління механічними та електричними системами в будівлі. У

більш широкому масштабі розумні міста можуть допомогти громадянам зменшити відходи та споживання енергії.

IoT торкається будь-якої галузі, включаючи бізнес у галузі охорони здоров'я, фінансів, роздрібної торгівлі та виробництва.

Деякі переваги IoT включають наступне:

- можливість доступу до інформації з будь-якого місця в будь-який час на будь-якому пристрої;
- покращений зв'язок між підключеними електронними пристроями;
- передача пакетів даних через підключену мережу, економить час і гроші;
- автоматизація завдань, що сприяють підвищенню якості послуг бізнесу та зменшенню потреби в людському втручанні.

Серед недоліків IoT можна назвати такі:

- Зі збільшенням кількості під’єднаних пристроїв та передачею більше інформації між пристроями також збільшується ймовірність того, що хакер може викрасти конфіденційну інформацію;
- врешті-решт підприємствам доведеться мати справу з величезною кількістю - можливо, навіть мільйонами - пристроїв IoT, і збір та управління даними з усіх цих пристроїв буде складним завданням;
- якщо в системі є помилка, ймовірно, кожен підключений пристрій буде пошкоджений;
- оскільки для IoT не існує міжнародного стандарту сумісності, пристроям різних виробників важко взаємодіяти між собою [3].

1.2 Безпроводові сенсорні мережі для Інтернету речей

Безпроводові сенсорні мережі (WSN), як правило, можна описати як мережу вузлів, які спільно відчувають і контролюють навколишнє середовище, забезпечуючи взаємодію між людьми або комп'ютерами та навколишнім середовищем. У наш час WSN зазвичай включають вузли датчиків, вузли виконавчих механізмів, шлюзи та клієнти. Велика кількість вузлів датчиків, випадково розміщених всередині або поблизу зони моніторингу (сенсорного поля), утворює мережі за допомогою самоорганізації. Вузли датчиків відстежують зібрані дані для передачі разом з іншими вузлами датчиків за допомогою стрибків. Під час процесу передачі відстежувані дані можуть оброблятися декількома вузлами, щоб дістатися до вузла шлюзу після багатопрофільної маршрутизації і, нарешті, дістатися до вузла управління через Інтернет або супутник. Користувач налаштовує та керує WSN за допомогою вузла управління, публікує моніторингові місії та збір даних, що контролюються [5].

У міру дозрівання супутніх технологій вартість обладнання WSN різко впала, і їх застосування поступово розширюється з військових районів на промислові та комерційні галузі. Тим часом стандарти для технології WSN були добре розроблені, такі як Zigbee, WirelessHart, ISA 100.11a, бездротові мережі для промислової автоматизації - автоматизація процесів (WIA-PA) тощо. Більше того, з появою нових режимів застосування WSN у промисловій автоматизації та домашніх додатків, загальний обсяг ринку додатків WSN буде продовжувати швидко зростати.

1.2.1 Сенсорні вузли

Сенсорний вузол є однією з основних частин WSN. Апаратне забезпечення сенсорного вузла, як правило, включає чотири частини: живлення та модуль керування живленням, датчик, мікроконтролер та бездротовий приймач, див. Рисунок 1.3. Блок живлення забезпечує надійне живлення, необхідне для роботи системи. Датчик є зв'язком вузла WSN, який може отримати стан навколишнього середовища та обладнання. Датчик відповідає за збір і перетворення таких сигналів, як світло, вібрація та хімічні сигнали, в електричні сигнали, а потім передає їх на мікроконтролер. Мікроконтролер приймає дані від датчика і відповідно обробляє дані. Потім бездротовий приймач (RF-модуль) передає дані, щоб можна було досягти фізичної реалізації зв'язку. Важливо, щоб конструкція всіх частин вузла WSN враховувала особливості вузла WSN невеликого розміру та обмеженої потужності [5].

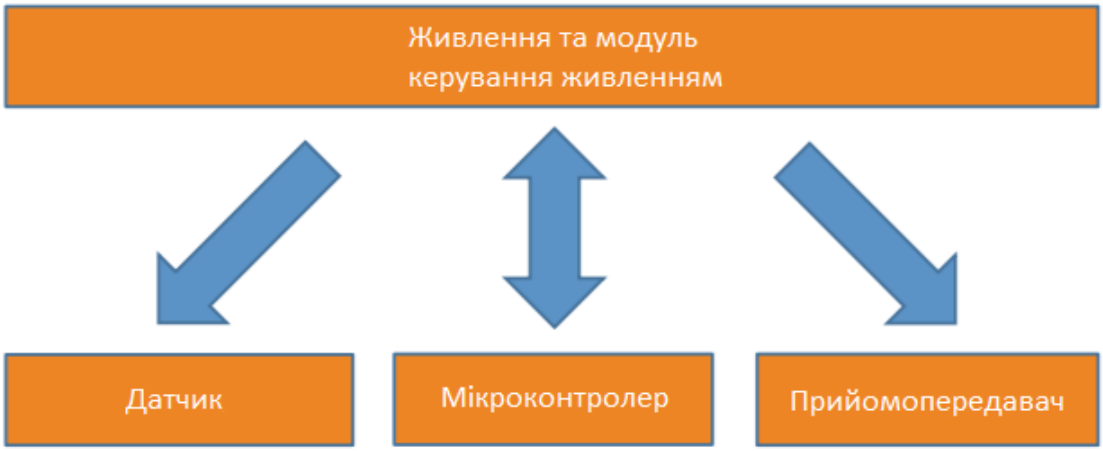

Рисунок 1.3 - Апаратна структура вузла датчика WSN

1.2.2 Технології мережі доступу

Мережа доступу, протяжність якої коливається від кількох сотень метрів до декількох миль, включає всі пристрої між магістральною мережею та

користувальницькими терміналами. Таким чином, це влучно називають "останньою милею". Оскільки магістральна мережа зазвичай використовує структуру оптичного волокна з високою швидкістю передачі, мережа доступу стала вузьким місцем усієї мережевої системи. Як показано на малюнку 3-6, через відкриту властивість бездротових каналів конфлікти траплятимуться у часі, просторі або частотному вимірі, коли канал буде спільним для кількох користувачів. Функція мережевих технологій доступу полягає в управлінні та координації використання ресурсів каналів для забезпечення взаємозв'язку та зв'язку кількох користувачів на загальному каналі.

Рисунок 1.4 - Мережа доступу

Відповідно до відстані та швидкості доступу існуючі технології доступу можна класифікувати на чотири категорії: бездротова локальна мережа (WLAN), бездротова мережа мегаполісів (WMAN), бездротова персональна мережа (WPAN) та бездротова широкосмугова мережа (WWAN). Однак загальна тенденція розвитку високих швидкостей передачі не підходить для вимог застосування WSN. Основні причини такі:

– Що стосується надійності, робоче середовище WSN, як правило, досить суворе. Погана обстановка з вузькосмуговими багаточастотними шумами, перешкодами та багатопроменевими ефектами робить надійну

комунікацію на основі рідкісних ресурсів каналу нагальною проблемою, яку потрібно вирішити;

- що стосується можливостей у реальному часі, програми для WSN та IoT мають більш суворі вимоги в режимі реального часу, ніж інші. Крихітна затримка може призвести до великого казусу. Тому у багатьох додатках має бути гарантоване жорстке спілкування в режимі реального часу;
- що стосується енергоефективності, низьке споживання енергії є ключовим фактором для підтримки тривалості незалежних пристроїв, що працюють від акумуляторів, і для зменшення витрат на обслуговування. Це також ще одна вимога до бездротових мереж та додатків IoT, особливо до пристроїв із важкими батареями, що підлягають заміні [5].

1.3 Безпроводові технологі для IoT

1.3.1 Супутникові мережі

У безпроводовому зв'язку супутникові мережі використовують електромагнітні хвилі для передавання сигналів, але ці хвилі вимагають прямої видимості. Через форму землі важко досягти зв'язку на великій відстані.

Для вирішення цієї проблеми на Землі побудовані різні антени або станції. Сигнал надсилається від Землі прямо до космосу, тому Супутники зв'язку (CS) можуть ретранслювати і підсилювати сигнали, які розширюють силу сигналу. Потім сигнал буде відправлений в інше місце на Землі. Такими сигналами можуть бути телефонні дзвінки, інтернет-дані, радіо і навіть телевізійні передачі.

У супутниковому звязку, CS дозволяють здійснювати зв'язок у більшому діапазоні, наприклад, відстань зв'язку в GSM може бути до 35 км. Крім того, на

основі швидкості підключення існують також різні комунікації, такі як GSM/GPRS/EDGE (2G), UMTS/HSPA (3G), LTE (4G) тощо.

Все має свою хорошу сторону і погану сторону, хоча стабільне з'єднання і універсальна сумісність відомі як переваги, але CS також вимагають високих щомісячних витрат, щоб зберегти їх високе енергоспоживання. Всі ці переваги і недоліки слід враховувати під час розвитку IoT, тому супутник використовується в основному в промислових цілях [4].

1.3.2 Wi-Fi

WLAN також відомий як Wi-Fi, технологія IEEE 802.11. Це бездротова локальна мережа (WLAN), яка дозволяє двом або більше мобільним пристроям використовувати Інтернет через безпроводове з'єднання. Це з'єднання базується на точці доступу, яка дозволяє користувачам переміщатися в межах певної зони покриття. На сьогоднішній день у нашому повсякденному житті широко використовується WiFi. Він простий у підключенні і доступний.

Таблиця 1.1 - Стандарти IEEE 802.11

802.11 Протокол	Рік випуску	Частота, ГГц	Швидкість передавання даних (середня)	Швидкість передавання даних (максимальна)	Радіус передавання в приміщенні, м	Радіус передавання на відкритій місцевості, м
Legacy	1997	2.4	1 Мб/с	2 Мб/с	20	100
802.11a	1999	5	25 Мб/с	54 Мб/с	35	120
802.11b	1999	2.4	6.5 Мб/с	11 Мб/с	35	140
802.11g	2003	2.4	25 Мб/с	54 Мб/с	38	140
802.11n	2009	2.4 або 5	300 Мб/с (20 МГц*4MIMO)	600 Мб/с (40 МГц* 4MIMO)	70	250

У стандартах IEEE 802.11 пристрій зазвичай «спілкується» в діапазонах частот 2.4, 3.6, 5 і 60 ГГц. Таблиця 1 показує основну інформацію, таку як швидкість передавання даних та діапазон зв'язку у стандартах 802.11. З даних таблиці не важко дізнатися, який з них є найкращим. Сьогодні IEEE 802.11n найчастіше використовується відповідно до високопродуктивних характеристик. Для того, щоб досягти високої якості, він також потребує більш високої потужності. Відповідно до проблеми великого енергоспоживання, Wi-Fi не рекомендується використовувати для малопотужних пристроїв.

Більшість мереж IEEE 802.11 використовують діапазон частот 2,4 ГГц, центральні частоти 14 каналів рознесені на 5 МГц один від одного. Це показано на рис. 1.3, кожен канал має діапазон близько 22 МГц, і вони перекриваються. Серед всіх каналів тільки канали 1, 6 і 11 не перекриваються між собою. Багато виробників модемів використовують ці три канали як канали WiFi за замовчуванням. Це налаштування може призвести до того, що канал може бути занадто навантаженим, якщо в регіоні є багато маршрутизаторів і користувачів WiFi. Надійність також вважається важливою проблемою у WiFi.

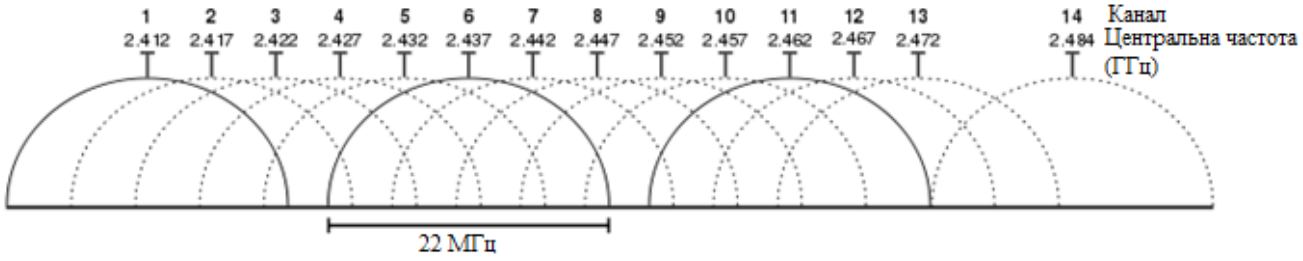

Рисунок 1.5 - Графічне представлення перекриття каналів 2,4 ГГц

Wi-Fi не настільки захищений, як проводові мережі, тому безпека безпроводового зв'язку є ще одним важливим аспектом, який ми повинні розглянути. Ваш особистий WiFi може бути відкритою мережею для всіх користувачів у регіоні, якщо його не захистити за допомогою заходів безпеки.

Такими заходами можуть бути приховування SSID, фільтрація ідентифікаторів MAC-адрес, захист від Wired Equivalent Privacy (WEP), захищений доступ Wi-Fi (WAP) тощо [4].

Основні характеристики Wi-Fi:

- базується на основі стандартів. Найбільш поширеним є 802.11n (з підтримкою також b/g);
- працює в неліцензованих діапазонах 2,4 ГГц і 5 ГГц;
- потужність передавача Wi-Fi зазвичай становить від 15 до 20 дБ;
- використовує множинний доступ з контролем несучої і униканням колізій (CSMA/CA);
- діапазон до 100 м (але зазвичай 30-50 м);
- швидкість передавання даних: 150-200 Мбіт/с характерна для 802.11n (стандарт 802.11-ac пропонує від 500 Мбіт/с до 1 Гбіт/с);
- використовує WEP, WPA і WPA2 протоколи для мережного шифрування і протокол WPA2 включає шифрування AES;
- пропонує мережу розміром до 250 вузлів. Тим не менш, продуктивність істотно знижується, коли кількість під`єднаних пристроїв у мережі перевищує 40-60;
- має визначений процес сертифікації через Wi-Fi [4].

1.3.3 Bluetooth

Bluetooth - це технологія бездротового зв'язку, яка дозволяє здійснювати обмін даними на малій відстані між фіксованим обладнанням, мобільними пристроями та персональними мережами. Він використовує короткохвильову УВЧ-радіостанцію в діапазонах ISM між 2.4 і 2.485 ГГц (Bluetooth 2010).

Продукти Bluetooth (наприклад, навушники та годинники) містять невеликий комп'ютерний чіп, радіо та програмне забезпечення, що підтримують з'єднання Bluetooth. Коли два пристрої Bluetooth хочуть обмінюватися даними, їх потрібно спочатку об'єднати у пару. Зв'язок між пристроями Bluetooth здійснюється у тимчасовій мережі короткої відстані, також відомої як пікомережа. Мережа може підключатися до двох-восьми пристроїв. Коли створюється мережне оточення, один пристрій діє як головний пристрій, а інші - як підлеглі пристрої.

Робоча група по специфікації Bluetooth (CSWG) розробляє Bluetooth. В даний час існує два основних типи Bluetooth. Вони являють собою Bluetooth з базовою швидкістю (BR)/ підвищеною швидкістю передавання даних (EDR) і Bluetooth з низьким енергоспоживанням (BLE). BR/EDR використовується в основному для динаміків і навушників, а BLE використовується для новітніх продуктів, таких як «розумний» будинок.

У Bluetooth 4.2, є кілька поліпшень:

- підтримка гнучких можливостей підключення до Інтернету (IPv6/6LoWPAN або Bluetooth Smart Gateway). Ця функція допоможе впровадити IoT;
- покращені права на конфіденційність, енергоефективність та продуктивність безпеки, що робить Bluetooth Smart розумнішим;
- підвищена швидкість і пропускна здатність пакета, що робить Bluetooth Smart швидшим [7].

1.3.4 ZigBee

Розроблений на стандарті IEEE 802.15.4, ZigBee - це самостійний, безпечний, надійний протокол, що підтримує топологію «коміркова мережа». Він

може розширюватися до тисяч вузлів у великих областях. ZigBee існує вже близько 10 років і має приблизно 1 млрд пристроїв, розгорнутих у всьому світі. Специфікація продовжує розвиватися.

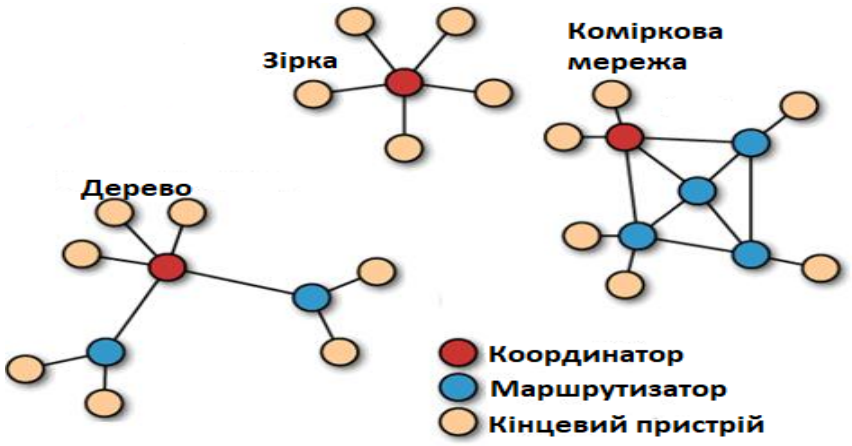

Рисунок 1.6 - Топологія «зірка», «дерево» і «коміркова мережа»

Як показано на рис. 1.5, специфікація ZigBee будується на канальному рівні 802.15.4 і підтримує інші рівні. ZigBee підтримує декілька топологій мережі, включаючи точка-точка, точка-багатоточка, та коміркову мережі.

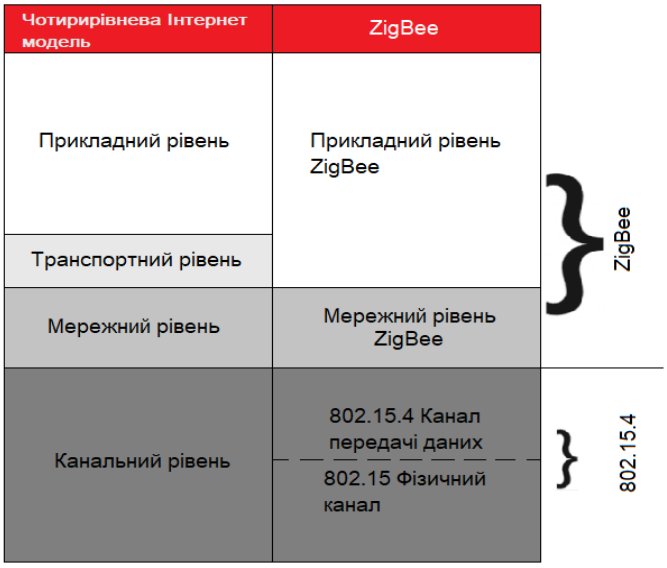

Рисунок 1.7 – Архітектура технології ZigBee

В архітектурі системи ZigBee є 3 типи пристроїв. Координатор ZigBee (ZC), маршрутизатор ZigBee (ZR) і кінцевий пристрій ZigBee (ZED). В мережі є тільки один координатор. Координатор вибирає топологію мережі, встановлює мережу та керує інформацією про конфігурацію. Він виступає як шлюз в мережу і з неї, тому він бути ввімкненим і працювати постійно. Маршрутизатори ZigBee передають інформацію та переміщують дані через мережу. Вони також можуть функціонувати як сенсорний вузол. Оскільки маршрутизатори являють собою основу мережі, вони завжди повинні бути ввімкнені. Кінцевий пристрій знаходиться на краю мережі і є джерелом або користувачем мережних даних. Зазвичай він живиться від батареї і може знаходитися в режимі низького енергоспоживання протягом тривалого часу. Кінцевий пристрій зазвичай є найменш дорогим пристроєм у мережі.

Маршрутизація - це процес вибору шляху, який використовують для передачі повідомлення від кінцевого пристрою до пристрою призначення. Координатор ZigBee і маршрутизатор ZigBee відповідають за виявлення і підтримку маршрутів по всій мережі.

Основні характеристики ZigBee:

- працює на частоті 2,4 ГГц (для глобального використання), але також стандарт визначає радіоприймачі на частоті 868 МГц і 915 МГц;
- використовує множинний доступ з контролем несучої і униканням колізій (CSMA-CA), що дозволяє багатьом пристроям спільно використовувати один і той же частотний канал;
- підтримка швидкості передавання даних до 250 Кбіт/с, хоча вона, зазвичай, набагато нижча;
- використовує зв'язок з розширеним спектром для підвищення продуктивності в середовищах радіозв'язку з багатопроменевим, шумним та низьким рівнем сигналу;

- дозволяє використовувати діапазон від 10 до 100 метрів для програм ZigBee;
- підтримує до 65000 вузлів;
- використовує асоціацію і дисоціацію, щоб дозволити пристроям приєднуватися або виходити з мережі. Цей процес дає змогу самостійно формуватися і самовідновлюватися;
- використовує прив'язку для створення логічних зв'язків між відповідними програмами;
- забезпечує захист за допомогою 128-бітного шифрування AES для безпечних з'єднань даних [5].

1.3.5 RFID

Радіочастотна ідентифікація (RFID) - це технологія бездротового зв'язку, яка дозволяє радіосигналам ідентифікувати конкретні об’єкти, читати та записувати відповідні дані без встановлення механічного або оптичного контакту між системою та конкретним об’єктом. У RFID двома основними пристроями є транспондер («мітка» або «тег») і зчитувач («рідер»).

Радіосигнали використовують радіочастотні електромагнітні поля, щоб приєднати дані до мітки і передавати їх, щоб автоматично ідентифікувати і відстежувати елемент. Мітки отримують енергію від електромагнітних полів зчитувача, тому вони не потребують батареї. Більше того, деякі мітки також мають власне джерело живлення, вони можуть самостійно відправляти радіочастоти. Мітка містить інформацію, що зберігається в електронному вигляді, ми можемо визначити її в межах кількох метрів [4].

Система радіочастотної ідентифікації в основному має ряд таких переваг:

- легко зчитується; в RFID немає потреби в прямій видимості, дані можуть бути зчитані через перешкоду. Якщо мітка має власну батарею, то ефективна відстань розпізнавання може становити до 30 метрів;
- швидкий час реакції; коли мітка знаходиться в електромагнітному полі, зчитувач може негайно прочитати інформацію. Більше того, зчитувач може працювати з декількома мітками одночасно;
- велика ємність даних; мітки RFID можуть зберігати до 10 тисяч номерів;
- тривалий час роботи; вона має герметичну упаковку і може використовуватися в поганих умовах;
- зв'язок в режимі реального часу; мітка і зчитувач можуть обмінюватися з частотою від 50 до 100 разів на секунду.

Завдяки усім цим факторам, різноманітні галузі промисловості вже використовують технологію RFID [6].

1.3.6 NFC

NFC означає «зв'язок на невеликих відстанях». Це ще одна форма RFID. Проте, на відміну від RFID, NFC - це високочастотна технологія бездротового зв'язку короткої дії, яка дозволяє безконтактну передачу даних між точками зв'язку між електронними пристроями на відстані 10 см. Він може вибрати одну з швидкостей передавання 106 Кбіт/с, 212 Кбіт/с або 424 Кбіт/с. Відмінність між NFC і Bluetooth полягає в тому, що в NFC немає парних пристроїв. Ця відмінність спрощує процедури налаштування з'єднання.

В даний час NFC зазвичай реалізується в мобільних телефонах. Існує п'ять основних програм з технологією NFC:

- торкніться та йдіть: мобільний телефон стає ключем;

- торкніться і платіть: користувач розмістив частину NFC на POS-машині, щоб виконати платіж, наприклад, «ApplePay»;
- торкніться та підключіть: користувач може підключити два телефони за допомогою передавання даних рівноправною передачею. Наприклад, за допомогою цієї програми користувач може завантажувати музику, обмінюватися фотографіями або контактами тощо;
- торкніться і досліджуйте: користувач може отримати доступ до інформації про дорожній рух шляхом сканування смарт-публічного телефону з підтримкою NFC або плакатів на вулиці;
- завантаження та дотик: користувач може завантажити інформацію та отримати доступ до платежу [8].

Висновки до розділу

1. Інтернет речей розширює підключення до Інтернету за межами традиційних пристроїв, таких як настільні та портативні комп'ютери, смартфони та планшети, до різноманітних пристроїв та щоденних речей, які використовують вбудовані технології для спілкування та взаємодії із зовнішнім середовищем, все через Інтернет.

2. Всі прилади в Інтернеті речей з’єднуються між собою за допомогою мережних технологій. Bluetooth - це комунікаційна технологія короткого діапазону, інтегрована в більшість смартфонів і мобільних пристроїв, що є головною перевагою для особистих продуктів, зокрема одягу. Wi-Fi - це технологія безпроводового радіозв'язку пристроїв. Він пропонує швидку передачу даних і здатний обробляти великі обсяги даних. Супутникові мережі здатні передавати великі обсяги даних, але споживання енергії та витрати також високі. ZigBee - це безпроводова мережа з низькою потужністю і низькою швидкістю передачі даних, яка використовується в основному в промислових умовах. NFC дозволяє клієнтам підключатися до електронних пристроїв, використовувати цифровий вміст і здійснювати безконтактні платежі. Він працює на відстані до 4 см (між пристроями), дозволяючи пристроям обмінюватися інформацією. RFID використовує електромагнітні поля так, щоб ідентифікувати об'єкти. Короткочасна радіочастотна ідентифікація становить близько 10 см. Але далекобійна радіочастота може досягати 20 см.

2 ТЕХНОЛОГІЯ LORA ТА LORAWAN

Абревіатурою LoRa (Long Range) позначають вид модуляції, тобто рівень L1 по моделі OSI. Протокол канального рівня носить ім'я LoRaWAN. Але найчастіше «Лорою» називають сукупну систему, яка використовує LoRa на фізичному і LoRaWAN на канальному рівні.

Архітектура була спочатку розроблена Cycleo у Франції, але потім придбана Semtech Corporation (французьким виробником електроніки змішаних сигналів) в 2012 р. за 5 мільйонів доларів готівкою. Альянс LoRa був сформований в березні 2015 р. Альянс є органом стандартизації для специфікації і технології LoRaWAN. Туди також входить процес дотримання і сертифікації для забезпечення сумісності і відповідності стандарту. Альянс підтримується IBM, Cisco і більш ніж 160 іншими учасниками.

LoRaWAN запрацювала в Європі з розгортанням мереж KPN, Proximus, Orange, Bouygues, Senet, Tata і Swisscom.

Оскільки LoRa є нижньою частиною стека, вона був прийнята в конкуруючих архітектурах в LoRaWAN. Наприклад, SymphonyLink - це рішення LPWAN від Link Labs на основі LoRaPHY, що використовує восьмиканальну базову станцію з субгігагерцами для промислових і муніципальних розгортань IoT. Ще одним конкурентом, що використовує LoRa, є Haystack, який виробляє систему DASH7. DASH7 - повний мережевий стек на LoRaPHY (а не тільки рівень MAC) [9].

2.1 Фізичний рівень LoRa

LoRa являє собою фізичний рівень мережі LoRaWAN. Вона керує модуляцією, потужністю, приймачем і передавальними радіостанціями, а також формує сигнали.

Архітектура заснована на наступних діапазонах в просторі SM без ліцензування:

- 915 МГц - в США з обмеженнями потужності, але без обмеження робочого циклу;
- 868 МГц - в Європі з 1% -им і 10% -им робочим циклом;
- 433 МГц - в Азії.

Похідним від Chirp Spread Spectrum (CSS) є метод модуляції, що використовується в LoRa. CSS балансує швидкість передачі даних з чутливістю в смузі фіксованого каналу. CSS був вперше використаний в 1940-х рр. для військового довгохвильового зв'язку з використанням модульованих імпульсів чірпа для кодування даних і був визнаний особливо стійким до перешкод, ефектів Доплера і багатопроменевого розповсюдження. Чірпи - це синусоїдальні хвилі, які з часом збільшуються або зменшуються. Оскільки вони використовують весь канал для зв'язку, вони відносно надійні в плані перешкод. Ми можемо уявити сигнали чірпів зі збільшенням або зменшенням частот (звук, як поклик кита). Частота передачі бітів - бітрейт, де LoRa є функцією швидкості чірпа і швидкості передачі символів. Бітрейт представлений R, коефіцієнт розширення S, смуга пропускання B. Тому бітрейт (біт/с) може варіюватися від 0,3 до 5 Кбіт/с і виводиться як:

$$R_b = S \times \frac{1}{\left[\frac{2^S}{B}\right]}.$$

Така форма модуляції допускає малу потужність для великих відстаней, як показали військові. Дані кодуються з використанням збільшення або зменшення частоти, і кілька передач можуть бути відправлені з різною швидкістю передачі даних на тій же частоті. CSS дозволяє отримувати сигнали на рівні 19,4 дБ нижче рівня шуму, використовуючи FEC. Група також поділяється на кілька піддіапазонів. LoRa використовує канали 125 кГц і виділяє шість каналів 125 кГц

і стрибкоподібне пересилання псевдовипадкових каналів. Кадр буде передаватися з певним коефіцієнтом розширення. Чим вище коефіцієнт розширення, тим повільніше передача, але тим довший діапазон передачі. Кадри в LoRa є ортогональними, що означає, що кілька кадрів можуть відправлятися одночасно, поки кожен відправляється з іншим коефіцієнтом розширення. Всього є шість різних коефіцієнтів розширення (від $SF = 7$ до $SF = 12$).

Типовий пакет LoRa містить преамбулу, заголовок і корисне навантаження від 51 до 222 байт.

Мережі LoRa мають потужну функцію, звану Adaptive Data Rate (ADR). По суті, це дозволяє динамічно масштабувати ємність, ґрунтуючись на щільності вузлів і інфраструктурі. ADR контролюється управлінням мережею в хмарі. Вузли, близькі до базової станції, можуть мати більш високу швидкість передачі даних через достовірность сигналу. Вузли, що знаходяться в безпосередній близькості, можуть передати дані і звільнити свою смугу пропускання і швидко увійти в стан сну в порівнянні з віддаленими вузлами, які передають з меншою швидкістю.

У таблиці 2.1 описані властивості висхідної і низхідної лінії зв'язку.

Таблиця 2.1 – Стандарти IEEE 802.11

Властивість	Висхідне з'єднання	Низхідне з'єднання
Модуляція	CSS	CSS
Втрати радіоканалу	156 дБ	164 дБ
Швидкість передачі (адаптивна)	Від 0.3 до 5 кб/с	Від 0.3 до 5 кб/с
Розмір повідомлення на корисне навантаження	0-250 байт	0-250 байт
Тривалість повідомлення	Від 40 мс до 1.2 с	Від 20 до 160 мс
Енергія, витрачена на повідомлення	$E_{tx} = 1.2s * 32mA = 11uAh$ При повній чутливості прийому $E_{tx} = 40ms * 32mA = 0.36uAh$ При мінімальній чутливості прийому	$E_{tx} = 160ms * 11mA = 0.5uAh$

2.2 Рівень MAC LoRaWaN

LoRaWAN представляє MAC, який знаходиться поверх LoRaPHY. MAC-адреса LoRaWAN є відкритим протоколом, в той час як PHY закритий. Існує три протоколи MAC, які є частиною рівня каналу передачі даних. Всі три балансують затримки і використання енергії. Клас А є найкращим для зменшення енергоспоживання при максимальній затримці. Клас В знаходиться між класом А і класом С. Клас С має мінімальну затримку, але найвищий рівень використання енергії.

Двонаправлені кінцеві пристрої «класу А» (Bi-directional end-devices, Class A). Кінцеві пристрої «класу А» дозволяють організувати двонаправлений обмін. Причому зв'язок може ініціювати тільки кінцевий пристрій, після чого виділяються два тимчасових вікна, протягом яких очікується відповідь від мережі. Інтервал передачі планується кінцевим пристроєм на основі власних потреб в зв'язку з невеликими випадковими тимчасовими флуктуаціями (протокол типу ALOHA). Кінцеві пристрої «класу А» застосовуються в додатках, де передача даних від мережі можлива тільки як відповідна реакція на отримання даних від кінцевого пристрою і потрібно максимальний час роботи від автономного джерела живлення [9].

Двонаправлені кінцеві пристрої «класу Б» (Bi-directional end-devices, Class B) на додаток до функцій пристроїв «класу А», відкривають додаткові вікна прийому за розкладом. Для того, щоб відкрити вікно прийому, кінцеве пристрій синхронізується за спеціальними сигналами від шлюзу (по маяках - Beacon). Це дозволяє мережі знати час, коли кінцевий пристрій готовий приймати дані [9].

Двонаправлені кінцеві пристрої «класу С» з максимальним прийомним вікном (Bi-directional end-devices, Class C). Кінцеві пристрої «класу С» мають майже безперервно відкрите вікно прийому. Приймальне вікно закривається тільки на час передачі даних. Цей тип кінцевих пристроїв підходить для задач, коли необхідно отримувати великі обсяги даних і не потрібна тривала робота від автономного джерела живлення [9].

Стек протоколу LoRa / LoRaWAN можна візуалізувати так, як показано в таблиці 2.2.

Таблиця 2.2 – Стек протоколів LoRa і LoRaWAN. Порівняння зі стандартною моделлю OSI

<table>
<tr><td colspan="3">Стек протоколів LoRa /LoRaWAN</td><td>Спрощена модель OSI</td></tr>
<tr><td colspan="3">Прикладний рівень</td><td>7. Прикладний рівень</td></tr>
<tr><td colspan="3">Рівень LoRaWAN</td><td rowspan="2">2. Канальний рівень</td></tr>
<tr><td>Клас А</td><td>Клас В</td><td>Клас С</td></tr>
<tr><td colspan="3">Модуляція LoRaPHY</td><td rowspan="3">1. Фізичний рівень</td></tr>
<tr><td colspan="3">LoRaPHY регіональний діапазон ISM</td></tr>
<tr><td>LoRaPHY Європейський діапазон 868 МГц</td><td>LoRaPHY Європейський діапазон 433 МГц</td><td>LoRaPHY Європейський діапазон 915 МГц</td></tr>
</table>

Для безпеки LoRaWAN шифрує дані з використанням моделі AES128. Одна з відмінностей в безпеці від інших мереж - LoRaWAN відокремлює аутентифікацію і шифрування. Аутентифікація використовує один ключ (NwkSKey), а призначені для користувача дані - окремий ключ (AppSKey).

Щоб під'єднатися до мережі LoRa, пристрої відправлять запит JOIN. Шлюз відповість адресою пристрою і маркером аутентифікації. Ключ додатку і мережевого сеансу буде отримано під час процедури JOIN. Цей процес називається Over the Air Activation (OTAA). В якості альтернативи пристрій на основі LoRa може використовувати активацію за допомогою персоналізації. У цьому випадку постачальник/оператор LoRaWAN попередньо розподіляє 32-розрядні мережеві і сеансові ключі, і клієнт повинен замовити план підключення і відповідний набір ключів. Ключі будуть замовлятися у виробника кінцевої точки з ключами, вбудованими в пристрій.

LoRaWAN - це асинхронний протокол на основі ALOHA. Чистий протокол ALOHA був спочатку розроблений в Гавайському університеті в 1968 р. як форма зв'язку з множинним доступом до тих пір, поки не існували такі технології, як CSMA. У ALOHA клієнти можуть передавати повідомлення, не знаючи, чи знаходяться інші клієнти в процесі передачі одночасно. Немає ніяких застережень або методів мультиплексування. Основним принципом є хаб (або шлюз в разі LoRaWAN), який негайно ретранслює отримані пакети. Якщо кінцева точка зауважує, що один з її пакетів не був підтверджений, він буде чекати, а потім повторно передасть пакет. У LoRaWAN колізії виникають тільки в тому випадку, якщо при передачах використовуються одні й ті ж канали та частота поширення [9].

2.2.1 Фізичний рівень (PHY Layer)

На фізичному рівні забезпечується негарантована передача блоків даних між кінцевим пристроєм (End Node) і шлюзом LoRa (Gateway).

На стороні передавального пристрою виконується:

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

На стороні приймального пристрою виконується:

– виявлення преамбули і визначення початку фізичного блоку даних;
– демодуляція сигналу;
– декодування фізичного заголовка пакета (PHDR + PHDR_CRC) і перевірка його контрольної суми;
– декодування блоку корисних даних (PHYPayload + CRC) і перевірка його контрольної суми;
– підтвердження прийнятих даних (для відповідних типів повідомлень);
– передача даних на MAC рівень [10].

На рисунку 2.1 наведені формати фізичних блоків даних низхідного (DL) і висхідного (UL) каналів:

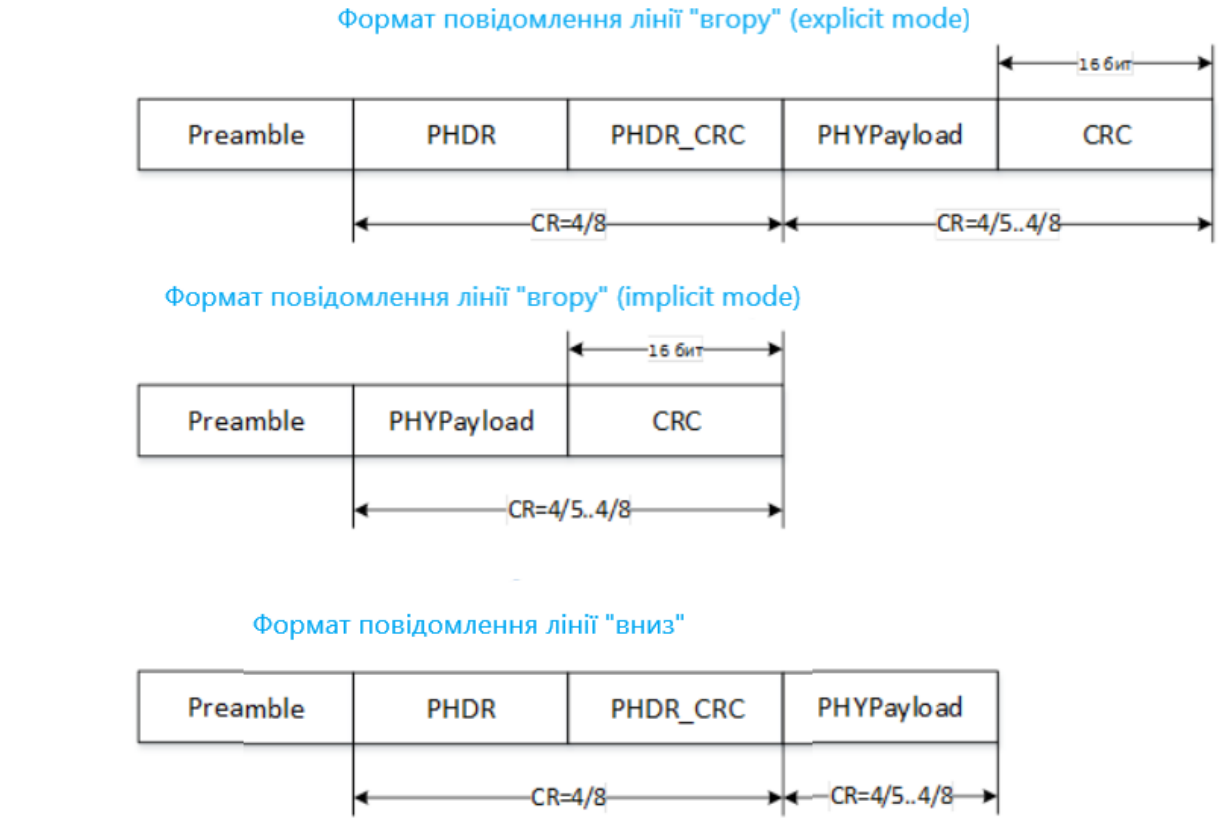

Рисунок 2.1 – Формати фізичних блоків даних низхідного і висхідного каналів

Де:

1. Preamble - преамбула, яка використовується для синхронізації приймача з вхідним потоком і визначення початку фізичного блоку даних. Довжина преамбули для чіпа Semtech SX1272 є програмованою.
2. PHDR - фізичний заголовок пакета. Присутній тільки при використанні явного режиму (explicit mode) і містить:

– довжину корисного навантаження в байтах;
– швидкість кодування;
– наявність у фізичному блоці даних опціонального поля CRC.

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

3. PHDR_CRC - контрольна сума поля PHDR.

4. PHYPayload - корисне навантаження (блок даних, отриманий від рівня MAC / переданий на рівень MAC).

5. CRC - контрольна сума поля PHYPayload (опціональне поле).

При цьому заголовок PHDR кодується надлишковим кодом з фіксованою швидкістю 4/8; корисне навантаження - з програмованої швидкістю [10].

2.2.2 MAC рівень

На MAC рівні забезпечується:

– передача блоків даних між кінцевим пристроєм та сервером (можлива передача повідомлень з підтвердженням і без підтвердження отримання);

– шифрування (на рівні мережі) корисного навантаження, що передається між кінцевим пристроєм і додатком;
– управління виділенням вікон передачі даних в лінії «вниз»;
– адаптація швидкості передачі даних[10].

На рисунку нижче наведений формат повідомлень MAC рівня:

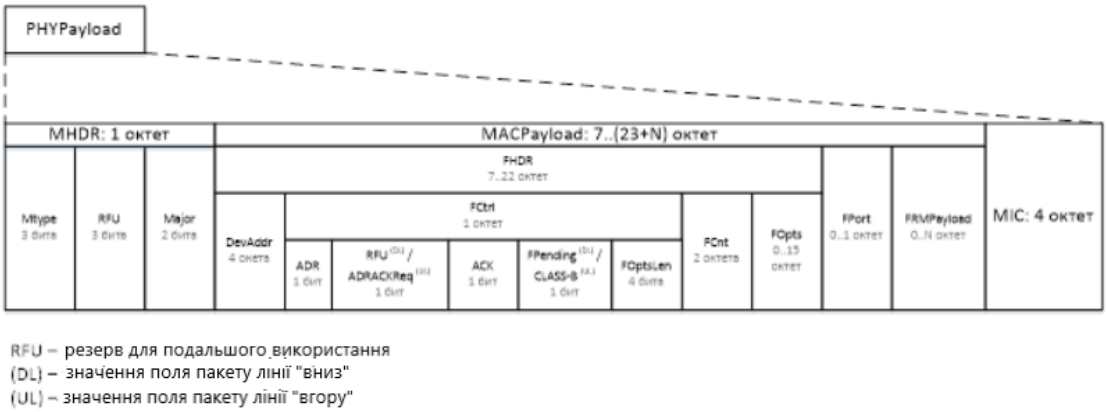

Рисунок 2.2 – Формат повідомлень MAC рівня

1. MHDR - заголовок пакета MAC рівня містить:

– Поле Major (2 біта) - визначає major частину версії формату повідомлень процедури активації по повітрю (OTA - over-the-air). Визначено лише одну версія (00 - "LoRaWAN R1").
– Поле MType - тип повідомлення (3 біта). Визначено шість типів повідомлень:

Таблиця 2.3 – Типи повідомлень пакета MAC рівня

MType	Опис
000	Запит процедури активації по повітрю (OTA - over-the-air) - join request

001	Підтвердження процедури активації по повітрю (OTA - over-the-air) - join accept
010	Передача даних без підтвердження "вгору" (unconfirmed data up)
011	Передача даних без підтвердження "вниз" (unconfirmed data down)
100	Передача даних з підтвердженням "вгору" (confirmed data up)
101	Передача даних з підтвердженням "вниз" (confirmed data down)
110	RFU
111	Для приватних рішень

2. MACPayload - фрейм даних.

Максимальна довжина фрейму даних (M) визначається обмеженнями фізичного рівня. Залежність M від швидкості передачі наведена в таблиці нижче:

Таблиця 2.4 – залежність довжини фрейму даних від швидкості передавання даних

Швидкість передавання	M, октет
0	59
1	59
2	59
3	123
4	230
5	230
6	230
7	230
8…15	Не визначено

Фрейм даних (MACPayload) складається з наступних підполів:

2.1. FHDR - заголовок фрейму. Включає в себе:

2.1.1. DevAddr - адреса кінцевого пристрою.

2.1.2. FCtrl - октет керуючої інформації фрейма в складі:

- ADR - прапор активації режиму адаптації швидкості.
- ADRACKReq - прапор запиту кінцевим пристроєм підтвердження факту отримання мережею повідомлень від даного пристрою. Може встановлюватися в режимі адаптації швидкості.
- ACK - прапор, що індикує отримання однією стороною (мережею або кінцевим пристроєм) повідомлення від іншої сторони. Використовується при передачі даних, що вимагають підтвердження (MType = 100/101). Не встановлюється для підтвердження отримання повідомлень в рамках процедури адаптації швидкості.
- FPending (тільки в DL каналі) - прапор, індикує наявність запиту з боку мережі на необхідність передачі кінцевому пристрою додаткових даних понад обсяг, який може бути переданий в рамках вікна передачі.
- CLASS-B (тільки в UL каналі) - прапор, індикує, що кінцеве пристрій переключено в режим "клас B".
- FOptLen - актуальний розмір поля опцій FOpt заголовка MAC рівня.

2.1.3. FCnt - номер фрейма.

Кінцевий пристрій і мережевий сервер після процедури активації по повітрю (OTA - over-the-air) (join accept) ініціалізують два лічильника - лічильник кількості переданих фреймів і лічильник кількості прийнятих фреймів (FCntUp / FCntDown). Специфікацією допускається використання 16-ти і 32-х бітних лічильників. Надсилаючи звіт про проблеми зустрічній стороні кінцеве пристрій / мережевий сервер вказують номер переданого фрейму (в поле FCnt заголовка MAC рівня). При цьому, з огляду на те, що поле FCnt має розрядність 16 біт, при

використанні 32-х бітних лічильників старші 16 біт не передаються. При отриманні кожного нового повідомлення приймаюча сторона (кінцеве пристрій / мережевий сервер) порівнює поле FCnt зі значенням внутрішнього лічильника прийнятих фреймів (FCntUp / FCntDown). Якщо різниця перевищує величину MAX_FCNT_GAP, приймається рішення про значну кількість втрачених пакетів.

2.1.4. FOpt - опціональні дані фрейма (до 15-ти октетів). Використовуються для передачі MAC команд. При цьому MAC команди можуть відправлятися як в поле FOpt (в цьому випадку FOptLen> 0, FPort> 0), так і в поле корисного навантаження фрейма FRMPayload (в цьому випадку FOptLen = 0, FPort = 0).

2.2. FPort - номер порта фрейма.

- значення 0 означає, що поле корисного навантаження фрейма (FRMPayload) містить MAC команду (див. п 2.1.4);
- значення 1..223 визначаються рівнем додатків (application specific);
- значення 224-225 зарезервовані для подальшого використання.

2.3. FRMPayload - корисне навантаження фрейма. Переносить дані між кінцевим пристроєм (End Node) і цільовим додатком (Application). Вміст поля FRMPayload шифрується стандарту AES або на рівні додатку (з використанням ключа AppSKey), або на рівні мережного сервера (з використанням ключа NwkSKey). Обидва ключі мають довжину 128біт.

3. MIC - код контролю цілісності. Обчислюється по всім полям повідомлення на основі алгоритму AES128 і секретного ключа NwkSKey [10].

2.2.3 Підтвердження отримання повідомлень

Технологія LoRa визначає два типи повідомлень - повідомлення, що вимагає підтвердження отримання та повідомлення без підтвердження. Тип

повідомлення - Confirmed (UL / DL) / Unconfirmed (UL / DL), визначається значенням поля MType (MessageType) заголовка MAC рівня.

Якщо відправником повідомлення, що вимагає підтвердження, є кінцевий пристрій (End Node), то мережа підтверджує отримання такого повідомлення всередині вікон прийому, відкритих кінцевим пристроєм відразу після сеансу передачі [10].

Якщо відправником повідомлення, що вимагає підтвердження, є мережа (LoRa gateway - шлюз), то момент передачі підтвердження визначається кінцевим пристроєм (End Node). Підтвердження може бути послано негайно (в т.ч. в складі порожнього повідомлення), що спрощує логіку функціонування End Node, або в складі чергового повідомлення, що несе корисне навантаження, що скорочує завантаження радіоканалу.

У будь-якому випадку, підтверджується завжди тільки останнє отримане повідомлення. Повідомлення, що є підтвердженням, характеризується встановленим бітом ACK заголовка MAC рівня. Повторна передача підтверджень не передбачена.

Необхідність повторної передачі непідтверджених повідомлень (або його видалення), а також моменти передачі і кількість повторів визначається логікою функціонування мережевого сервера і кінцевого пристрою відповідно. При кожній повторній передачі можливе зниження швидкості потоку даних (data rate), що підвищує перешкодозахищеність. Також передбачена можливість забезпечення параметрів повторної передачі в кінцеві пристрої з боку мережі.

У разі неотримання мережевим сервером встановленого числа підтверджень від кінцевого пристрою, дане кінцеве пристрій може бути промарковано як недоступне (unreachable) аж до отримання від нього будь-якого першого вхідного повідомлення [10].

2.2.4 Адаптивна швидкість передачі (Adaptive Data Rate - ADR)

В технології LoRa передбачені механізми адаптації швидкості передачі даних кінцевих пристроїв з тим, щоб оптимізувати завантаження мережі і забезпечити кожному кінцевому пристрою можливість роботи на максимальних швидкостях, що забезпечують належну стійкість в тих радіо умовах, в яких даний пристрій знаходиться.

Адаптацію швидкості передачі даних кінцевих пристроїв (End Node) виконує мережевий сервер за допомогою відповідних MAC команд. Рішення про вибір тієї чи іншої швидкості приймається на підставі оцінки якості прийнятого від End Node сигналу [10].

Механізми адаптації швидкості доречно використовувати тільки на пристроях, місце розташування яких постійне і не змінюється з часом (статичні пристрої), тому що для таких пристроїв і радіо умови в цілому будуть досить стабільні від одного сеансу зв'язку до іншого. На мобільних пристроях, наприклад, встановлених на автомобілях, тварин та ін. Радіо умови між сеансами зв'язку змінюються непередбачувано. Отже, на таких пристроях доречно використовувати постійні (встановлені за замовчуванням) швидкості передачі. Статичні пристрої повинні ініціювати використання мережею режиму адаптації за допомогою установки ADR біта заголовка MAC рівня [10].

Якщо кінцевий пристрій використовує швидкість передачі даних вище встановленої за замовчуванням швидкості (відповідно до команди MAC рівня, отриманої від мережевого сервера), він повинен періодично контролювати факт отримання мережею повідомлень (навіть при використанні режиму передачі без підтвердження) відповідно до такої процедури:

- кінцеве пристрій (End Node) інкрементує лічильник ADR_ACK_CNT при кожному переданому в висхідному каналі повідомленні (UL-Msg) і

скидає його при отриманні вхідного повідомлення по низхідному каналу (DL-Msg) у вікні прийому (receive window);

- при досягненні лічильником ADR_ACK_CNT порога ADR_ACK_LIMIT кінцевий пристрій (за допомогою установки біта ADRACKReq) запитує мережу направити йому будь-який DL-Msg, підтвердивши тим самим, що повідомлення від даного кінцевого пристрою досягають мети; підтвердження повинно бути направлено у вікні прийому одного з наступних UL-Msg (але не більше, ніж задано порогом ADR_ACK_DELAY);
- при відсутності підтвердження кінцевий пристрій знижує швидкість передачі на один крок;
- подальше зниження швидкості передачі на один крок буде відбуватися після передачі кожних ADR_ACK_LIMIT UL-Msg до отримання підтвердження, або до досягнення наперед визначеної швидкості за замовчуванням [10].

2.2.5 Основні константи стека протоколів LoRaWAN

RECEIVE_DELAY1 (тривалість тимчасового вікна прийому RX1) - 1 сек.

RECEIVE_DELAY2 (тривалість тимчасового вікна прийому RX2) - 2 сек.

JOIN_ACCEPT_DELAY1 - 5 сек.

JOIN_ACCEPT_DELAY2 - 6 сек.

MAX_FCNT_GAP (максимальна різниця значень внутрішнього лічильника прийнятих пакетів і номера отриманого фрейму - FCNT) - 16384.

ADR_ACK_LIMIT (в режимі адаптації швидкості передачі - гранична кількість фреймів, направивши які, кінцевий пристрій запитує підтвердження з боку мережі) - 64.

ADR_ACK_DELAY (в режимі адаптації швидкості - час очікування підтвердження з боку мережі після запиту кінцевим пристроєм) - 32.

ACK_TIMEOUT - випадкове значення в діапазоні від 1 до 3 сек [10].

2.2.6 Команди MAC рівня

MAC команди можуть відправлятися як в поле FOpt (в цьому випадку FOptLen> 0, FPort> 0), так і в поле корисного навантаження фрейма FRMPayload (в цьому випадку FOptLen = 0, FPort = 0). Команди MAC рівня наведені в таблиці 2.5 [10].

Таблиця 2.5 – Команди MAC рівня

CID	Команда	Передається		Опис
		EN	GW	
0x02	LinkCheckReq	X		Використовується кінцевим пристроєм для перевірки підключення до мережі.
0x02	LinkCheckAns		X	Відповідає на команду LinkCheckReq. Містить оцінку якості прийому і кількість шлюзів (LoRa Gateway), які взяли команду LinkCheckReq від кінцевого пристрою.
0x03	LinkADRReq		X	Здійснює запит до кінцевого пристрою на зміну швидкості передачі даних, потужності передачі, кількості повторення

				кожного повідомлення і списку доступних для передачі "вгору" каналів.
0x03	LinkADRAns	X		Підтверджує прийом LinkRateReq команди.
0x04	DutyCycleReq		X	Встановлює максимальний сукупний робочий цикл передачі кінцевого пристрою. Змінюється в межах від 1 (доступ без обмежень) до 2-15.
0x04	DutyCycleAns	X		Підтверджує прийом DutyCycleReq команди.
0x05	RXParamSetupReq		X	Встановлює параметри вікон прийому. Для RX1 - зміна швидкості передачі в лінії «вниз» в порівнянні зі швидкістю передачі в лінії «вгору». Для RX2 - частотний канал і зміна швидкості передачі.
0x05	RXParamSetupAns	X		Підтверджує прийом RXParamSetupReq команди.
0x06	DevStatusReq		X	Запитує стан кінцевого пристрою.
0x06	DevStatusAns	X		Повертає стан кінцевого пристрою, а саме рівень заряду батареї і якість сигналу.

0x07	NewChannelReq		X	Дозволяє використання кінцевим пристроєм певних радіоканалів, встановлює їх частоту (за винятком 3-х радіоканалів, встановлених за замовчуванням відповідним регіональним стандартом), а також допустимі межі швидкості.
0x07	NewChannelAns	X		Підтверджує прийом NewChannelReq команди
0x08	RXTimingSetupReq		X	Встановлює тимчасову затримку між закінченням передачі по лінії «вгору» (UL) і відкриттям першого вікна прийому. Друге вікно прийому відкривається через одну секунду після першого.
0x08	RXTimingSetupAns	X		Підтверджує прийом RXTimingSetupReq команди.
0x800xFF	Proprietary	X	X	Зарезервовано для приватних рішень.

2.3 Топологія LoRaWAN

LoRaWAN заснований на топології зірки. В цьому відношенні можна сказати, що він підтримує зірку топології зірок. Модель LoRaWAN може

використовуватися не як одна модель з хабом, а як кілька хабів. Вузол може бути пов'язаний з декількома шлюзами.

Мережева служба має правила і логіку для обслуговування необхідних верхніх рівнів мережевого стека. Побічним ефектом цієї архітектури є те, що передача обслуговування від одного шлюзу до іншого не потрібна. Якщо вузол мобільний і переміщається від антени до антени, мережеві служби будуть захоплювати кілька ідентичних пакетів з різних шляхів. Ці хмарні мережеві служби дозволяють системам LoRaWAN вибирати кращий маршрут і джерело інформації, коли кінцевий вузол пов'язаний з декількома шлюзами. Обов'язки мережевих служб включають:

- ідентифікацію і видалення повторного пакету;
- послуги безпеки;
- маршрутизацію;
- повідомлення про підтвердження.

Крім того, LPWAN-системи, такі як LoRaWAN, матимуть на 5-10 менше базових станцій для аналогічного покриття мережі 4G. Всі базові станції прослуховують один і той же набір частот, тому вони логічно є однією дуже великою базовою станцією. Це, звичайно ж, підтверджує твердження про те, що системи LPWAN можуть мати більш низьку вартість, ніж традиційна мережа (рис. 2.2).

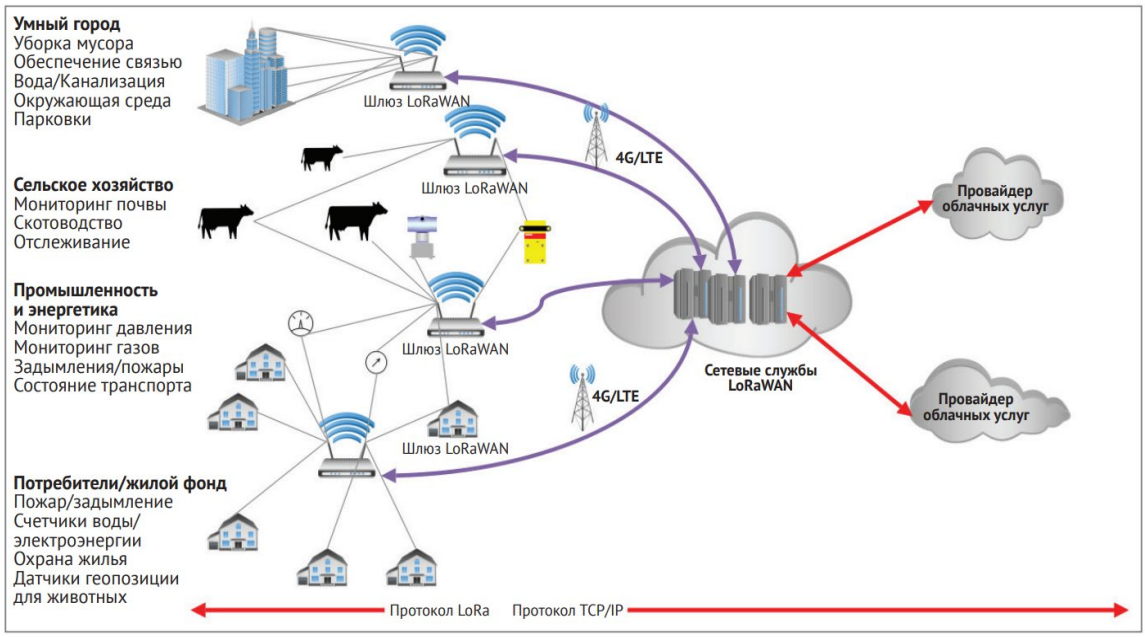

Рисунок 2.3 - Мережева топологія LoRaWAN.

LoRaWAN побудований на топології зірки зі шлюзами, діючими в якості концентраторів, а також агентами зв'язку в порівнянні з традиційними IP-мережами для адміністрування LoRaWAN в хмарі. Кілька вузлів можуть зв'язуватися з декількома шлюзами LoRaWAN [9].

2.4 Переваги та недоліки технології LoRa

Нижче наведені переваги LoRaWAN:

– Однією з головних переваг використання модуляції, коли частота змінюється з часом, є зменшення і майже усунення перешкод, спричинених відлунням та доплерівським зсувом;
– не вимагає синхронізації, яка існує в інших методах модуляції. Таким чином, низька затримка з'єднання з меншим "часом ефіру", отже, триваліший час автономної роботи.;

- варіативна пропускна здатність, можна вибрати меншу відстань, вищу пропускну здатність або більшу відстань, меншу пропускну здатність;
- крім того, LoRa має методи адаптивної швидкості передачі даних, які можуть змінювати швидкість передачі даних у межах вибраної смуги пропускання, наприклад, використовуючи смугу пропускання 125 кГц, ви можете вибрати від 300 біт/с до 27 кбіт/с.;
- можна налаштувати коефіцієнт розширення спектру, що надає подальший контроль над вихідною потужністю передавача;
- Оскільки LoRa заснована на модуляції FSK, використовувані підсилювачі потужності набагато дешевші та ефективніші, ніж інші методи модуляції;
- LoRa має набагато кращий "бюджет зв'язку", ніж інші дешеві радіочастотні комунікації. Link Budget - це складний розрахунок ефективності від передавача до приймача;
- низька вартість розгортання;

Серед недоліків технології можна виділити такі:

- швидкість передачі даних - не очікуйте, що LoRa зможе передавати відеопотоки високої якості на відстані 10 км. Максимальна швидкість передачі даних, яку ви побачите, становить 50 кбіт/с;
- затримка - незважаючи на те, що це модуляція з низькою затримкою, вона недостатньо низька для програм, які вимагають дуже чуйного спілкування в режимі реального часу [11];

Висновки до розділу

1. В основі технології LoRa лежить однойменний метод модуляції, який був запатентований компанією Semtech. Цей метод ґрунтується на принципі розширення спектра і лінійної частотної модуляції. В процесі передачі дані кодуються широкосмуговими імпульсами з частотою, що зменшується або збільшується в певному часовому діапазоні. Дане рішення дозволяє зробити приймач стійким до відхилень частоти від номінального значення, що знижує вимоги до якості генератора і дозволяє використовувати прості кварцові резонатори.

2. На MAC рівні забезпечується передача блоків даних між кінцевим пристроєм та сервером (можлива передача повідомлень з підтвердженням і без підтвердження отримання); шифрування (на рівні мережі) корисного навантаження, що передається між кінцевим пристроєм і додатком; управління виділенням вікон передачі даних в лінії «вниз»; адаптація швидкості передачі даних.

3. LoRaWAN - відкритий протокол зв'язку, який визначає архітектуру системи. Цей протокол передбачає топологію типу «зірка». LoRaWAN розроблявся з метою організації зв'язку між недорогими пристроями, які можуть працювати від батарей (акумуляторів). Для забезпечення прийнятного відносини швидкості передачі до енергоспоживання, протокол передбачає різні класи вузлів. Протокол LoRaWAN визначає конкретний набір швидкостей передачі даних, але реалізація фізичного рівня моделі OSI буде залежати від обраної мікросхеми.

4. При максимальній швидкості передачі даних близько 50 Кбіт/с LoRa має найнижчу швидкість передачі даних в порівнянні з більшістю інших технологій, що робить його не ідеальним для певних програм, де потрібна висока швидкість передачі даних. Без всякого сумніву можна сказати, що в концепції "Інтернету

Речей" закладений величезний потенціал, проте будь-яка створена людиною система не є досконалою і має свої переваги і недоліки.

3 ДОСЛІДЖЕННЯ ПАРАМЕТРІВ МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІЇ LORA

Протягом останніх років з'являється все більше радіотехнологій, що забезпечують бездротовий зв'язок на великі відстані і з низьким енергоспоживанням. Ультравузькосмугові технології, такі як Sigfox (Лабже, Франція) та Weightless-N [12] (Кембридж, Великобританія), а також технології розширеного спектру, такі як LoRa [13] (Сан-Рамон, Каліфорнія, США), дозволяють спілкуватися на відстані декількох кілометрів і будувати широкополосні мережі з низьким енергоспоживанням (LPWAN), які не потребують побудови та обслуговування складних багатохопних топологій.

Ключовою характеристикою технологій LPWAN насправді є можливість обмінювати пропускну здатність для діапазону і навпаки, тобто є можливість точно налаштувати параметри фізичного рівня (PHY), щоб вибрати більш чутливу (але повільну) конфігурацію, яка дозволяє спілкуватися через більшу відстань. Ця гнучкість робить технології LPWAN особливо привабливими для розробників програм Інтернету речей (IoT), що вимагають зв'язку на великі відстані з відносно низькою швидкістю передачі даних. У той же час, однак, можливість точної настройки параметрів PHY вимагає глибокого розуміння їх впливу на продуктивність мережі, особливо на надійність та енергоефективність зв'язку.

Нещодавно дослідницька спільнота приділяла значну увагу ролі параметрів PHY в контексті LPWAN, особливо технології LoRa. З існуючих технологій LPWAN LoRa залучила великий обсяг робіт завдяки наявності комерційних готових радіоприймачів та платформ, а також здатності працювати без інфраструктури та створювати рекламу). Мережі, засновані на LoRa, були розгорнуті в декількох умовах, починаючи від внутрішнього та міського середовища, закінчуючи морським та гірським сценаріями. Ці розгортання продемонстрували вплив параметрів PHY на діапазон підключення та чутливість,

а також створили перше враження про коефіцієнт прийому пакетів, який можна досягти на різних відстанях за допомогою різних апаратних платформ та конфігурацій фізичного рівня. Вчені також показали за допомогою моделювання, що вибір параметрів PHY впливає на кількість вузлів LoRa, які можуть одночасно отримувати доступ до каналу, що впливає на масштабованість мереж LoRa [14]. Крім того, Бор та Редиг представили результати систематичних експериментів у приміщенні, які показують, що набір налаштувань LoRa, що призводить до найбільш енергоефективної роботи, динамічно змінюється з часом [15]. На основі цих результатів автори запропонували протокол, який періодично перевіряє різні параметри і який динамічно вибирає ті, що мінімізують споживання енергії під час роботи.

Взаємодія між налаштуваннями PHY та якістю посилань. Незважаючи на те, що вищезазначені роботи почали проливати світло на те, як здійснити оптимальний вибір налаштувань PHY LoRa, усі вони мають спільне припущення: найкраща продуктивність досягається за наявності високонадійних посилань. Більшість робіт, насправді, конкретно націлені на налаштування PHY, що максимізують якість зв'язку, тобто зосереджені на виборі конфігурацій фізичного рівня, які дозволяють підтримувати коефіцієнт прийому пакетів 90% або вище. На цю практику, ймовірно, впливає поведінка не опортуністичних малопотужних бездротових протоколів збору даних для радіостанцій IEEE 802.15.4, які надають перевагу високоякісним посиланням на проміжні та з втратами. Однак коригування PHY-налаштувань радіостанції з метою максимізації якості зв'язку має важливі наслідки, посилаючись на енергоефективність при використанні бездротових технологій великої дальності, таких як LoRa. Максимізація якості зв'язку, справді, зазвичай передбачає збільшення потужності передачі та накладних витрат на дані, а також вибір більш чутливої (і, отже, повільної) конфігурації фізичного рівня. Як результат, збільшується не тільки ймовірність прийому пакетів, але й енергоспоживання радіостанції завдяки більшій

потужності передачі та часу включення радіосигналу через більші накладні витрати PHY. Це спостереження піднімає питання на яке, поки що немає відповіді: чи варто вибирати налаштування PHY, щоб зменшити швидкість передачі даних, для підвищення якості посилання? Це питання особливо актуальне, коли два вузли знаходяться на межі діапазону зв'язку: якщо вибрати один параметр, який зменшує швидкість передачі даних, щоб підвищити надійність зв'язку (і прагнути до зв'язку, що досягає високого коефіцієнта прийому пакетів), або, скоріше, прийняти наявність посилання проміжної якості (тобто, наявна якась втрата пакетів), але з високою швидкістю передачі даних, і зверху реалізувати схему повторної передачі? Як цей вибір впливає на енергоефективність мережі, ще потрібно дослідити.

Вплив умов навколишнього середовища на ефективність спілкування. Характеристики LPWAN роблять їх придатними для розгортання на відкритому повітрі у великих масштабах, і тому важливо детально вивчити вплив навколишнього середовища, такого як зміни метеорологічних умов, а також коливання температури та вологості на продуктивність мережі. На жаль, на сьогоднішній день все ще мало розуміння щодо впливу навколишнього середовища на надійність зв'язку LoRa, особливо для посилань, які знаходяться на межі їх діапазону зв'язку. Вчені повідомили про вразливість комунікацій LoRa до факторів навколишнього середовища, таких як наявність рослинності та коливання температур, але без кількісної оцінки їх впливу [16]. Інші роботи в галузі малопотужного бездротового співтовариства показали, що деякі радіостанції IEEE 802.15.4 особливо вразливі до змін температури, і що навіть щоденні коливання, зафіксовані на відкритому повітрі, можуть зробити хороший канал марним. Однак ці результати залежать від платформи і не можуть бути узагальнені для приймачів LoRa. Тому, як і наскільки температура впливає на ефективність зв’язку LoRa, ще не відповіли.

3.1 Основні параметри технології LoRa та зв'язок між ними

Широкообласні мережі з низьким енергоспоживанням доповнюють бездротові технології короткого діапазону, такі як Wi-Fi, Bluetooth Low Energy та IEEE 802.15.4, і представляють цікаву альтернативу стільниковим технологіям для міських програм IoT. Успіх LPWAN обумовлений їх здатністю забезпечувати зв’язок на великі відстані з тисячами пристроїв з мінімальними витратами та обмеженими витратами енергії. Більший діапазон зв'язку дозволяє значно спростити робочий цикл та мережевий протокол, оскільки LPWAN можуть утворювати зіркові топології, де малопотужні кінцеві пристрої можуть безпосередньо спілкуватися з більш потужним оркестратором. Це також дозволяє розробляти асиметричні схеми зв'язку та переносити навантаження на більш потужний центральний пристрій.

Для збільшення діапазону зв'язку технології LPWAN повинні покращити відношення сигнал/шум (SNR) на приймачі, або звужуючи смугу пропускання приймача (зменшуючи рівень шуму приймача), або розподіляючи енергію сигналу по ширший діапазон частот (ефективно зменшує спектральну щільність потужності сигналу). Наприклад, NB-IoT та Weightless-P кодують сигнал у низькій смузі пропускання (<25 кГц), щоб зменшити рівень шуму та зберегти конструкцію трансивера якомога простішою та дешевшою. Sigfox та Weightless-N додатково звужують сигнал на надвузькі смуги, до 100 Гц, ще більше зменшуючи сприйманий шум.

Технологія LoRa. Порівняно з цими технологіями, LoRa поширює сигнал у більш широкому діапазоні частот і є більш стійкою до заглушок та перешкод. LoRa - це запатентована технологія LPWAN від Semtech (Камарілло, штат Каліфорнія, США), яка нещодавно привернула значну увагу завдяки своїй здатності ефективно торгувати діапазоном комунікацій проти високої швидкості передачі даних, тим самим дозволяючи додатки IoT у міських масштабах.

Основою технології LoRa є її модуляція Chirp Spread Spectrum (CSS): несучий сигнал LoRa складається з чірпів, сигналів, частота яких збільшується або зменшується з часом. Чірпи LoRa дозволяють сигналу проходити великі відстані і бути демодульованим, навіть коли його потужність на 20 дБ нижча від рівня шуму. Через цей аспект зондування несучої в LoRa є досить складним: радіостанції LoRa дозволяють виявляти несучі через режим САПР, спеціальний стан прийому, який споживає половину енергії порівняно зі звичайним режимом прийому. Однак сигнали, що видаються різними мережами LoRa, що працюють за різними налаштуваннями, можуть створювати перешкоди, що призводять до помилкових виявлень [17].

Ефективність зв'язку LoRa можна точно налаштувати, змінюючи вибір декількох параметрів PHY, включаючи пропускну здатність, коефіцієнт розповсюдження, швидкість кодування, потужність передачі та несучу частоту, як підсумовано в таблиці 1. Далі детально пояснюється вплив кожного параметра PHY щодо швидкості передачі даних, чутливості приймача (включаючи стійкість до перешкод), діапазону передачі та енергоефективності.

Таблиця 3.1. Короткий зміст налаштовуваних параметрів LoRa та їх вплив на продуктивність зв'язку

Налаштування	Значення	Ефекти
Пропускна здатність	125. . . 500 кГц	Більша пропускна здатність дозволяє передавати пакети з більш високою швидкістю передачі даних (1 кГц = 1 кілоцикл/с), але зменшує чутливість приймача та діапазон зв'язку.
Фактор розповсюдження	$2^6 \dots 2^{12} \frac{\text{чірпи}}{\text{символ}}$	Більші коефіцієнти розповсюдження збільшують відношення сигнал/шум, а

		отже, і радіочутливість, збільшуючи діапазон зв'язку за рахунок довших пакетів і, отже, більших витрат енергії
Швидкість кодування	4/5…4/8	Більші швидкості кодування збільшують стійкість до сплесків перешкод і помилок декодування за рахунок довших пакетів і більших витрат енергії
Потужність передачі	-4…20 дБм	Більш високі потужності передачі зменшують відношення сигнал/шум за рахунок збільшення споживання енергії передавача.

Пропускна здатність (BW). Змінюючи діапазон частот (пропускну здатність), по якому розповсюджується чірп LoRa, можна обмінювати радіоефірний час з радіочутливістю, таким чином, ефективність використання енергії залежить від діапазону зв'язку та надійності. Чим більша пропускна здатність, тим коротший ефірний час і нижча чутливість. Менша пропускна здатність також вимагає більшої чистоти, щоб мінімізувати проблеми, пов'язані з «дрейфом годинника». Задано смугу пропускання BW, як правило, в діапазоні 125…500 кГц, швидкість обчислення LoRa RC (chip-rate) обчислюється як:

$$R_c = BW \frac{\text{чіп}}{\text{с}},$$

Фактор розповсюдження (SF). Для передачі інформації LoRa «розподіляє» кожен символ на декілька мікросхем (коефіцієнт розповсюдження), щоб ще більше підвищити чутливість приймача. Коефіцієнт розповсюдження LoRa SF може бути обраний між 6 і 12, в результаті чого швидкість розповсюдження коливається від 2^6 до 2^{12} чіпи/символ а швидкість передачі символів RS обчислюється як:

$$R_s = \frac{R_c}{2^{SF}} = \frac{BW}{2^{SF}} \frac{\text{символ}}{\text{с}},$$

що призводить до модуляції швидкості бітової передачі, яка може бути виражена як:

$$R_M = SF \cdot R_s = SF \cdot \frac{BW}{2^{SF}} \frac{\text{біт}}{\text{с}},$$

Зверніть увагу, що в LoRa пакети, передані з різними факторами розповсюдження, є ортогональними між собою і не викликають зіткнень, якщо передаються одночасно.

Швидкість кодування (CR). Щоб підвищити стійкість до пошкоджених бітів, LoRa підтримує методи виправлення помилок вперед із змінним числом CR надлишкових бітів, що варіюється від 1 до 4. Отримана швидкість передачі даних BR LoRa стає:

$$BR = R_M \cdot \frac{4}{4 + CR} = SF \cdot \frac{BW}{2^{SF}} \cdot \frac{4}{4 + CR} \frac{\text{біт}}{\text{с}},$$

Чим більше сплесків перешкод очікується, тим вища швидкість кодування, яку слід використовувати для максимізації ймовірності успішного прийому пакетів. Зауважте, що радіостанції LoRa з різними швидкостями кодування все ще можуть обмінюватися даними, оскільки заголовок пакета (переданий з використанням максимальної швидкості кодування 4/8) може включати швидкість кодування, що використовується для корисного навантаження.

Потужність передачі (TP). Як і більшість бездротових радіостанцій, приймачі LoRa також дозволяють регулювати потужність передачі, різко змінюючи енергію, необхідну для передачі пакета. Наприклад, перемикаючи потужність передачі з -4 на +20 дБм, споживання енергії збільшується з 66 мВт до 396 мВт при використанні трансивера RFM95 (HopeRF, Шеньчжень, Китай) [18]. Зауважте також, що для потужностей передачі, що перевищують +17 дБм, апаратні обмеження та законодавчі норми обмежують робочий цикл радіо максимум до 1%.

Носійна частота (CF). Приймачі LoRa використовують для зв'язку частоти під ГГц: серед інших, промислові, наукові та медичні (ISM) діапазони 433 МГц, 868 МГц (Європа) та 915 МГц (Північна Америка). Загальні модулі LoRa, такі як Semtech SX1272 [19] та HopeRF RFM95 [20], підтримують зв'язок у діапазоні частот 860–1020 МГц і програмуються з кроком 61 Гц. Десять каналів з різною пропускною здатністю можуть бути використані для зв'язку за допомогою LoRa в європейському діапазоні ISM 868 МГц.

На Рис. 3.1 наведено вигляд ЛЧМ сигналу у часовій області, а на Рис. 3.2 і Рис. 3.3 показаний його спектр при BW = 125кГц і базою рівній 128 (SF = 7) і 4096 (SF = 12) відповідно

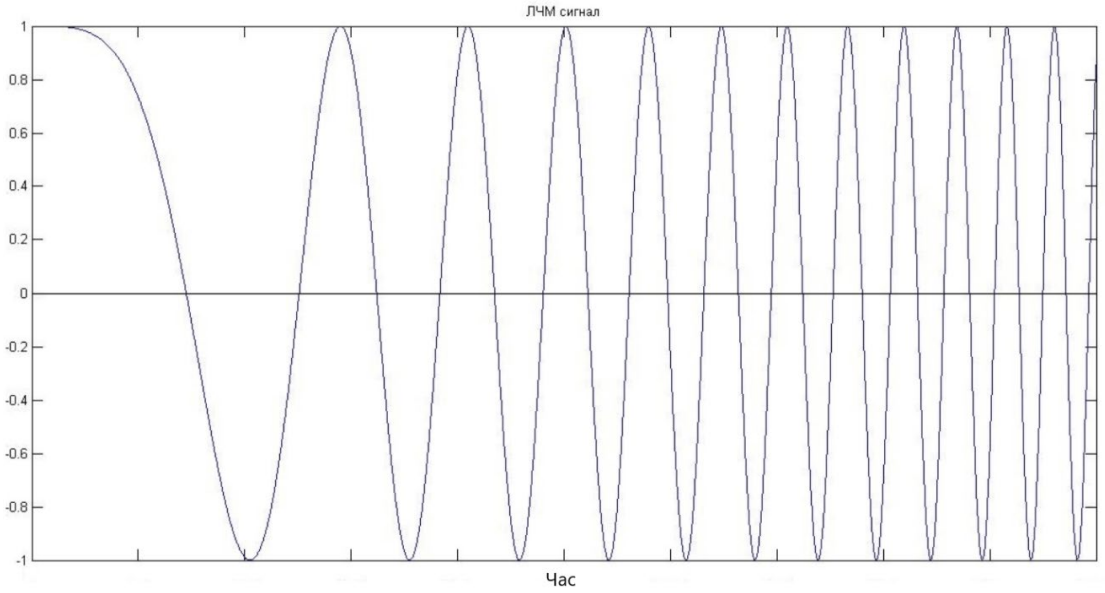

Рисунок 3.1 – ЛЧМ сигналу у часовій області

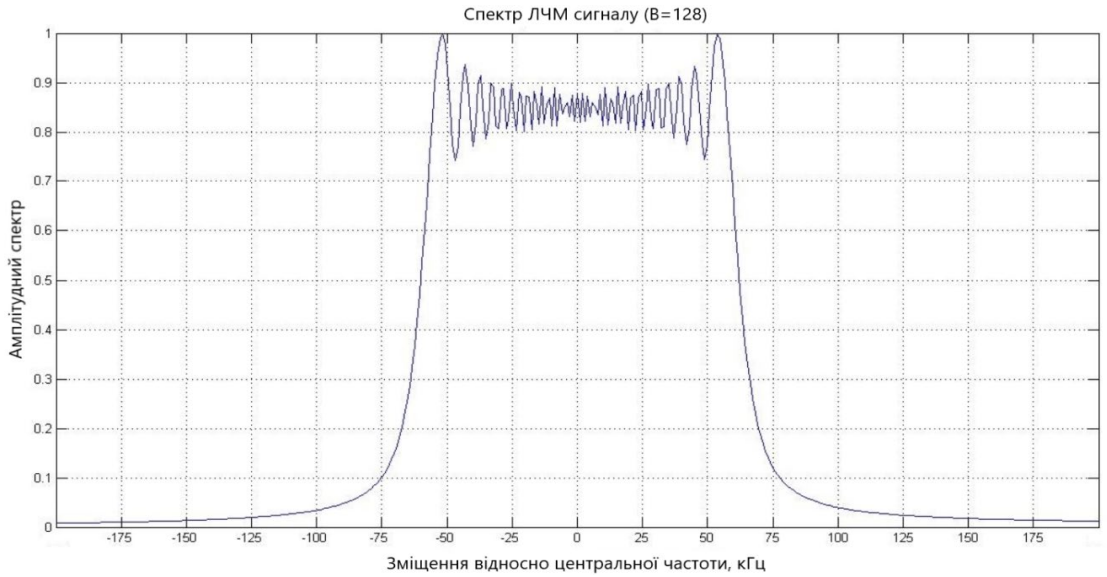

Рисунок 3.2 – Спектр ЛЧМ сигналу при BW=128кГц і базою 128 (SF=7)

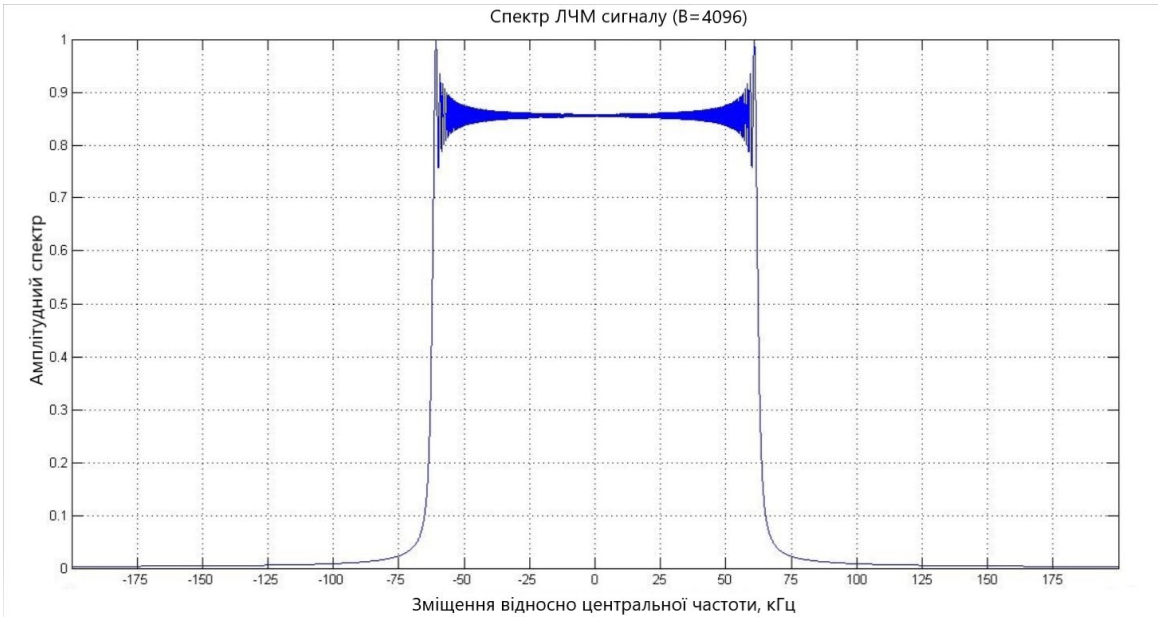

Рисунок 3.3 – Спектр ЛЧМ сигналу при BW=128кГц і базою 4096 (SF=12)

Передавачі LoRa формують CSS радіосигнали з шириною спектра (BW) 125, 250 або 500 кГц. При фіксованій ширині спектра радіосигналу BW зміна його бази здійснюється за рахунок зміни тривалості T_{sym} і швидкості зміни частоти μ (Рис. 3.4) [10].

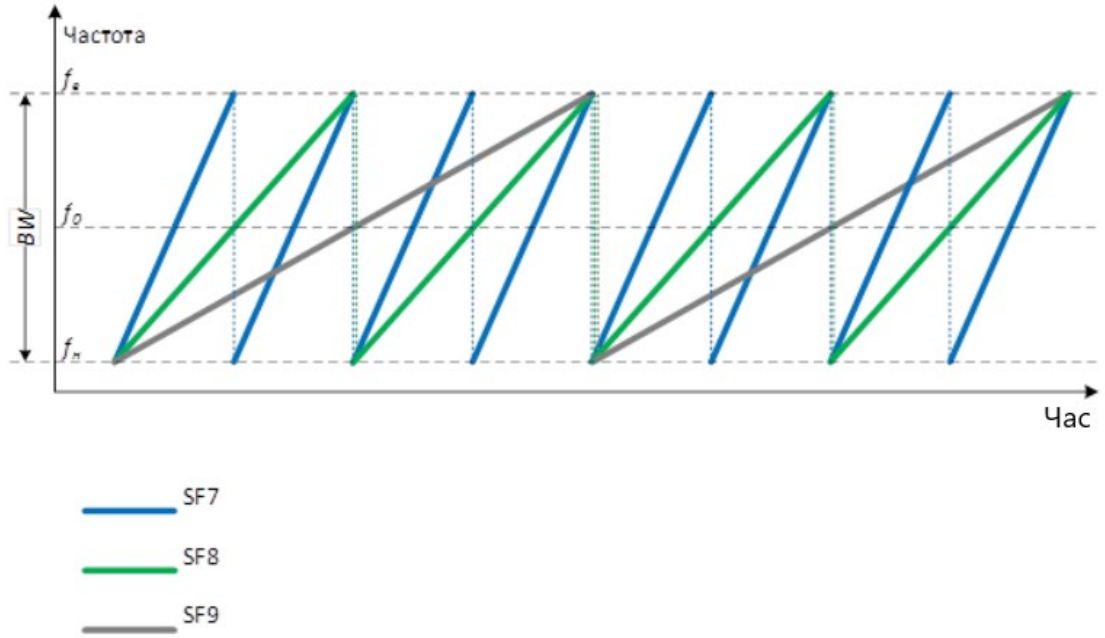

Рисунок 3.4 – Зміна бази при фіксованій ширині спектра

Для успішного функціонування будь-якої системи обміну інформацією необхідна взаємна синхронізація приймача і передавача, що дозволяє визначити часові межі прийому-передачі як цілого блоку даних (або кадру), так і одиничних символів.

Технологія LoRa використовує асинхронний режим прийому-передачі при якому передавач може почати генерацію радіосигналу в будь-який момент часу. В цьому випадку потрібен механізм, що забезпечує синхронізацію приймача по сигналу від передавача (аналог "старт-біта" протоколу RS232). В якості такого механізму використовується преамбула, що передує кожному сеансу зв'язку. Преамбула включає в себе послідовність символів, що дозволяють приймачу виявити активність передавача, визначити використовуваний передавачем коефіцієнт розширення спектра (SF) і виконати символьну синхронізацію. Тривалість преамбули є конфігурується величиною і повинна бути не менше, ніж $T1 + 2 \bullet T2$, де $T1$ визначає максимальний час знаходження приймача в стані "сну" (Sleep), $T2$ - визначає час пошуку приймачем преамбули (Рис. 3.5) [10].

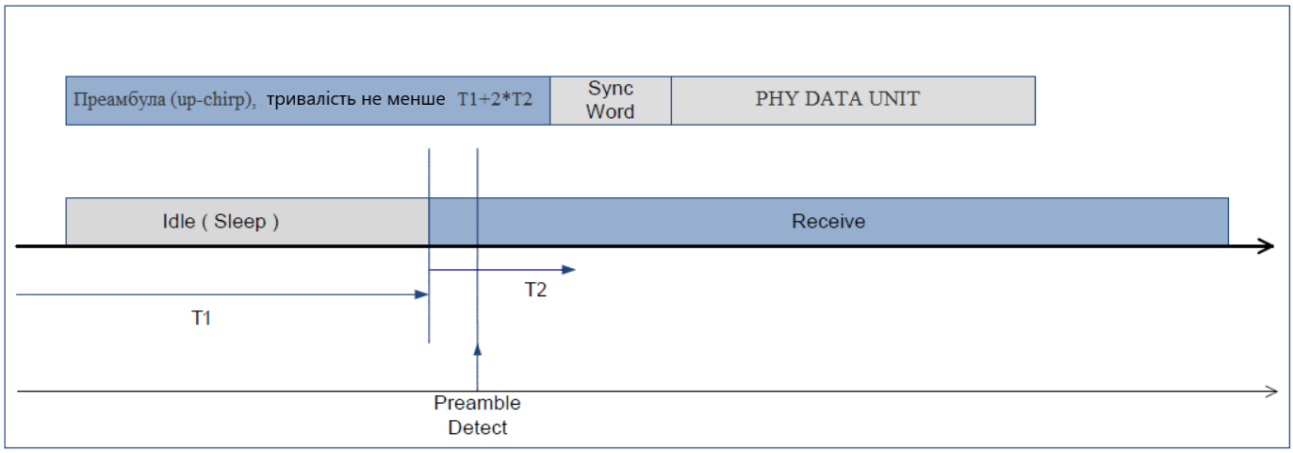

Рисунок 3.5 – Тривалість преамбули

По завершенні преамбули слід слово синхронізації (Sync Word) і блок даних фізичного рівня. Довжина слова синхронізації налаштовується в діапазоні від 1 до 8 байт. Специфікацією LoRa визначено ряд специфічних значень Sync Word - 0x34 для публічних мереж (public networks), 0x12 - для приватних мереж (private networks) і 0xC194C1 - для каналів з FSK модуляцією.

На Рис. 3.6 показана загальна структура кадру, що забезпечує передачу одного блоку даних [10].

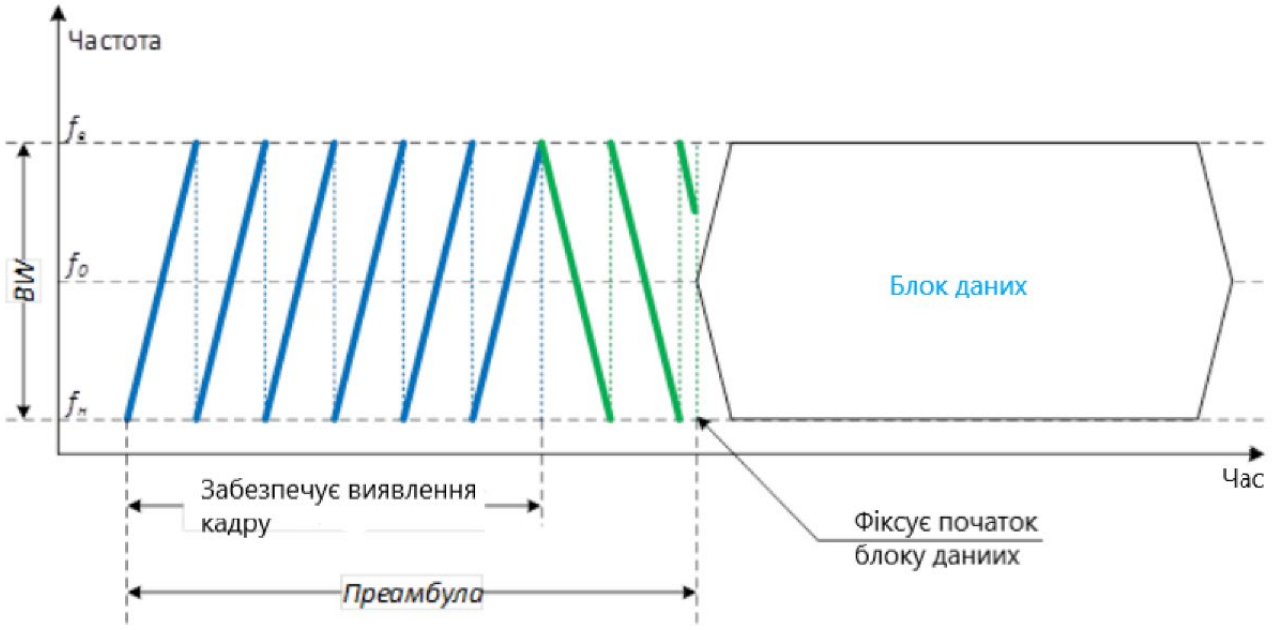

Рисунок 3.6 – Загальна структура кадру

Механізм функціонування детектора преамбули заснований на використанні узгодженого фільтра (УФ), чия імпульсна характеристика комплексно пов'язана з CSS радіосигналом в частотної області і має дзеркальне відображення його в часі:

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

Принцип передачі символів інформації блоку даних фізичного рівня (PHY DATA UNIT) за допомогою широкосмугового радіосигналу LoRa полягає в частотному зсуві $e^{j \cdot \Delta\omega \cdot k \cdot t}$ відносного опорного ЛЧМ сигналу $e^{j \cdot (\omega_н \cdot t + \mu \cdot t^2)}$, де $k = 0,1,2, \ldots, 2^{SF}$ – інформаціний символ, розміром SF біт (Рис. 3.7):

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

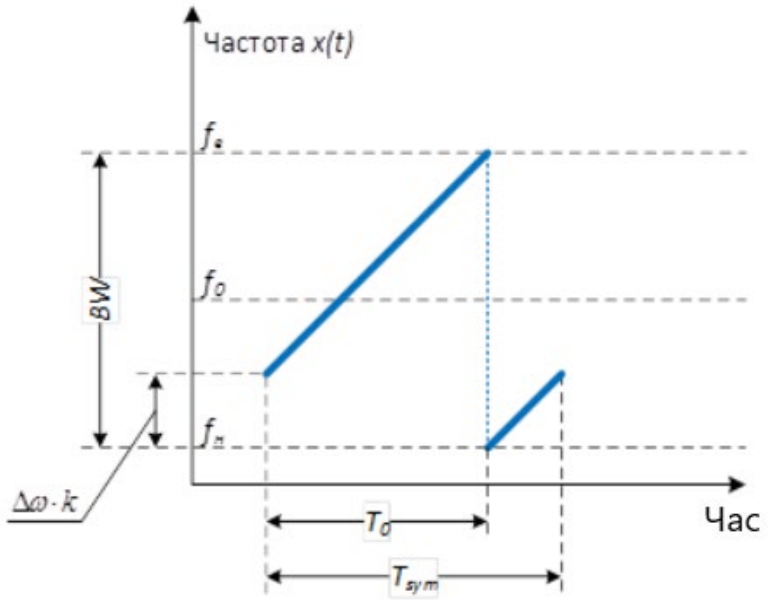

Рисунок 3.7 – Принцип передачі символів

Приклад залежності частоти радіосигналу від часу для LoRa кадру показаний на Рис. 3.8.

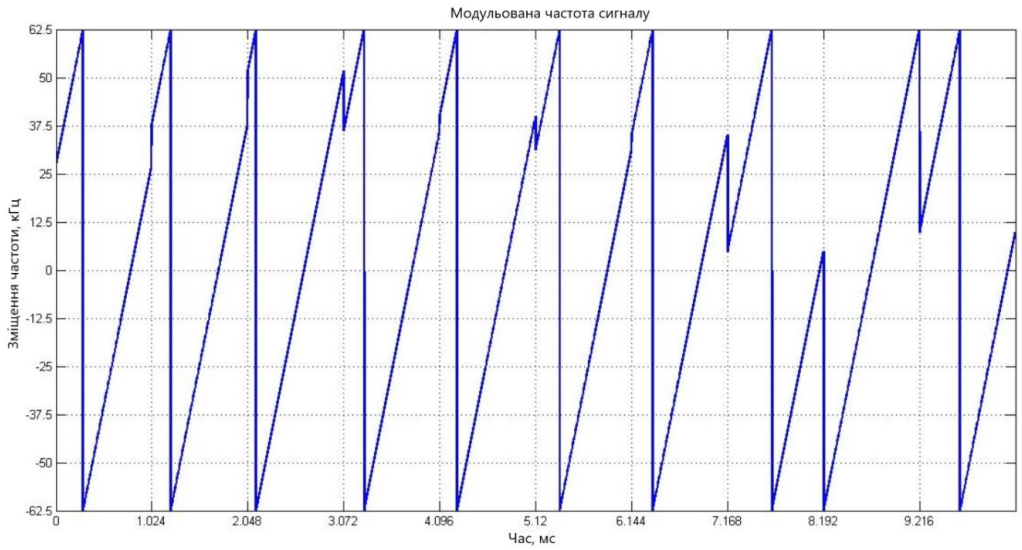

Рисунок 3.8 – Залежність частоти радіосигналу від часу

Можлива схема приймача сигналу LoRa, що переносить блок даних фізичного рівня, показана на Рис. 3.9 [10].

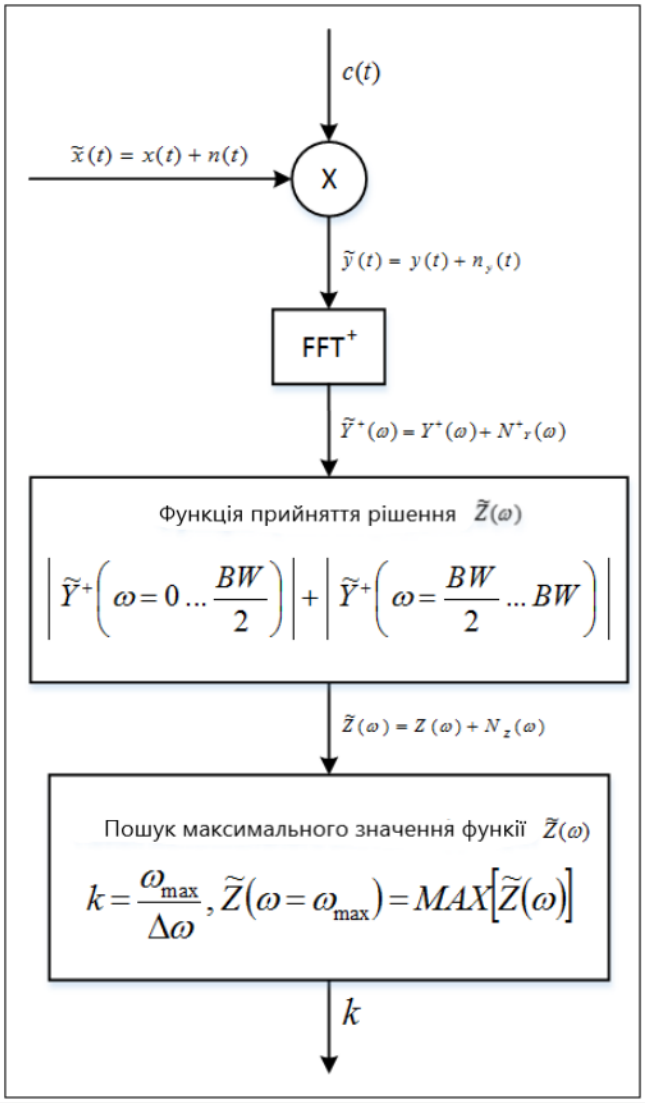

Рисунок 3.9 – Схема приймача сигналу LoRa

Тут:

$\mathrm{c}(t) = A_1 \cdot \cos\left(\omega_{\text{н}} \cdot t + \frac{\mu}{2} \cdot t^2\right), 0 \le t < T_{sym}$ – еталонний ЛЧМ сигнал,

$n(t) = 0 \le t < T_{sym}$ – адитивний білий Гаусівський шум,

Де-chirped сигнал: $y(t) = x(t) \cdot c(t) = \frac{A_0 \cdot A_1}{2} \cdot$

$$\begin{cases} \cos(\Delta\omega \cdot k \cdot t) + \cos(2 \cdot \omega_{\text{н}} \cdot t + \Delta\omega \cdot k \cdot t + \mu \cdot t^2), \ 0 \le t < T_0), \\ \cos(BW - \Delta\omega \cdot k \cdot t) + cos(2 \cdot \omega_{\text{н}} \cdot t + \Delta\omega \cdot k \cdot t - BW \cdot t + \mu \cdot t^2), \ T_0 \le t < T_{sym} \end{cases}$$

$$n_y(t) = n(t) \cdot c(t).$$

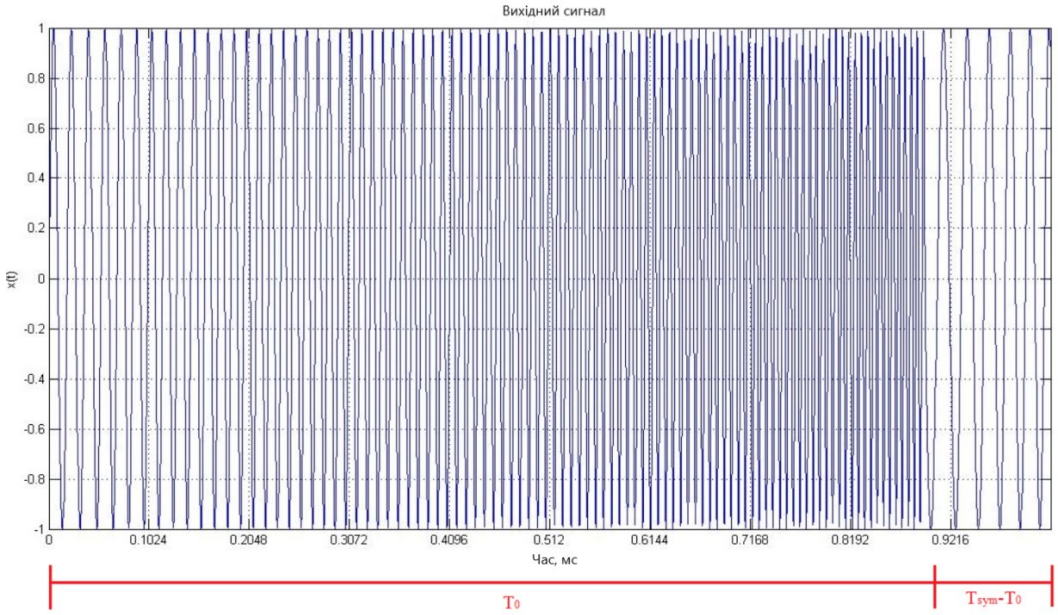

Рисунок 3.10 – Вихідний сигнал

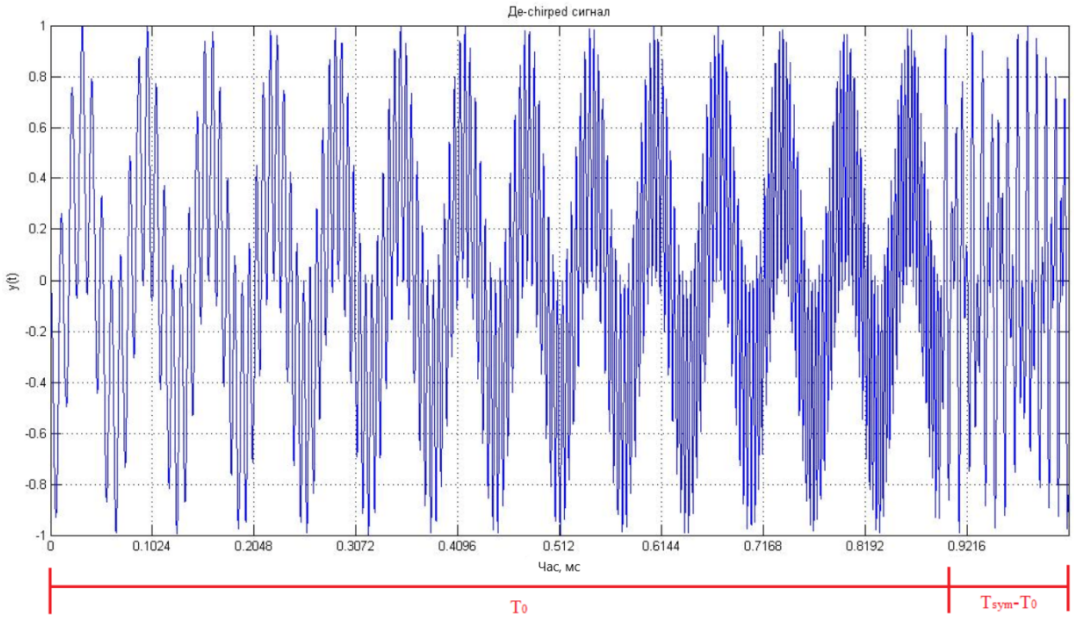

Рисунок 3.11 – Де-chirped сигнал

Відкинувши в вираженні для $y(t)$ другі доданки в фігурних дужках (як високочастотні складові):

$$y(t) = \frac{A_0 \cdot A_1}{2} \cdot \begin{cases} cos(\Delta\omega \cdot k \cdot t), & 0 \le t < T_0 \\ cos([BW - \Delta\omega \cdot k] \cdot t), & T_0 \le t < T_{sym} \end{cases}$$

на виході блоку перетворення Фур'є (FFT^+) отримуємо наступний комплексний сигнал:

$$Y(\omega) = \int_{-\infty}^{\infty} y(t) \cdot e^{-i\omega t} dt =$$

$$= \frac{A_0 \cdot A_1}{4} \times e^{-j(\omega - \Delta\omega k)\frac{T_0}{2}} \cdot T_0 \cdot \frac{sin[(\omega - \Delta\omega k) \cdot T_0/2]}{(\omega - \Delta\omega k) \cdot T_0/2} +$$

$$+ \frac{A_0 \cdot A_1}{4} \times e^{-j(\omega - (BW - \Delta\omega k))\frac{T_0 + T_{sym}}{2}} \cdot (T_{sym} - T_0) \cdot \frac{sin[(\omega - (BW - \Delta\omega k)) \cdot (T_{sym} - T_0)/2]}{(\omega - (BW - \Delta\omega k)) \cdot (T_{sym} - T_0)/2} +$$

$$+ \frac{A_0 \cdot A_1}{4} \times e^{-j(\omega + \Delta\omega k)\frac{T_0}{2}} \cdot T_0 \cdot \frac{sin[(\omega + \Delta\omega k) \cdot T_0/2]}{(\omega + \Delta\omega k) \cdot T_0/2} +$$

$$+ \frac{A_0 \cdot A_1}{4} \times e^{-j(\omega + (BW - \Delta\omega k))\frac{T_0 + T_{sym}}{2}} \cdot (T_{sym} - T_0) \cdot \frac{sin[(\omega + (BW - \Delta\omega k)) \cdot (T_{sym} - T_0)/2]}{(\omega + (BW - \Delta\omega k)) \cdot (T_{sym} - T_0)/2}$$

Далі позбавляємося від двох останніх доданків, що мають істотний вплив в області негативних частот і низький в області позитивних:

$Y^+(\omega) = Y_1(\omega) + Y_2(\omega)$, де

$$Y_1(\omega) = \frac{A_0 \cdot A_1}{4} \times e^{-j(\omega - \Delta\omega k)\frac{T_0}{2}} \cdot T_0 \cdot \frac{sin[(\omega - \Delta\omega k) \cdot T_0/2]}{(\omega - \Delta\omega k) \cdot T_0/2} +$$

$$Y_2(\omega) = \frac{A_0 \cdot A_1}{4} \times e^{-j(\omega - (BW - \Delta\omega k))\frac{T_0 + T_{sym}}{2}} \cdot (T_{sym} - T_0) \cdot \frac{sin[(\omega - (BW - \Delta\omega k)) \cdot (T_{sym} - T_0)/2]}{(\omega - (BW - \Delta\omega k)) \cdot (T_{sym} - T_0)/2}$$

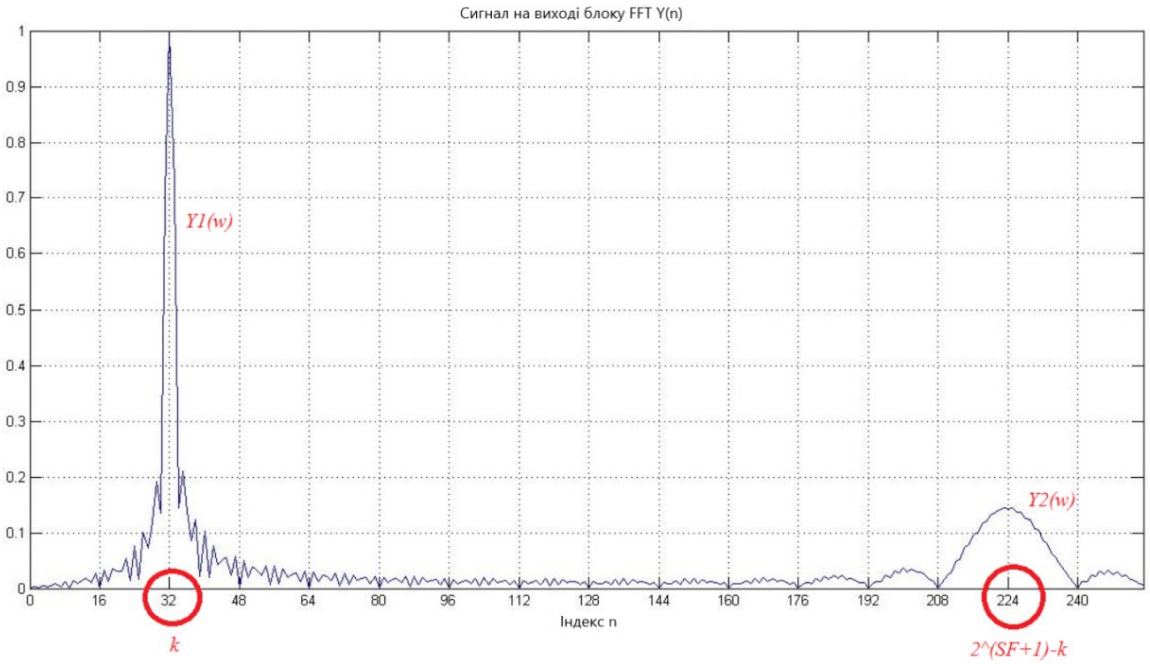

Рисунок 3.12 – Сигнал на виході блоку FFT

Для того щоб уникнути перекриття двох доданків $Y^+(\omega)$ при різних значеннях k має виконуватися нерівність:

$$\Delta\omega < \frac{BW}{2 \cdot k}.$$

Звідси,

$$\Delta\omega = \frac{BW}{2^{SF+1}},$$

$$T_0 = \frac{(2^{SF+1} - k)}{2^{SF+1}} \cdot T_{sym}.$$

На наступному етапі обчислюється функція прийняття рішення $Z(\omega)$, що являє собою суму модулів функції $Y_1(\omega)$ і функції $Y_2(\omega)$, дзеркально відбитої щодо точки $\omega = BW$:

$$Z(\omega) = Y_1(\omega) + Y_2(BW - \omega) \approx Y^+(\omega) + Y^+(BW - \omega),$$

Де $\omega = 0 \ldots \frac{BW}{2}$.

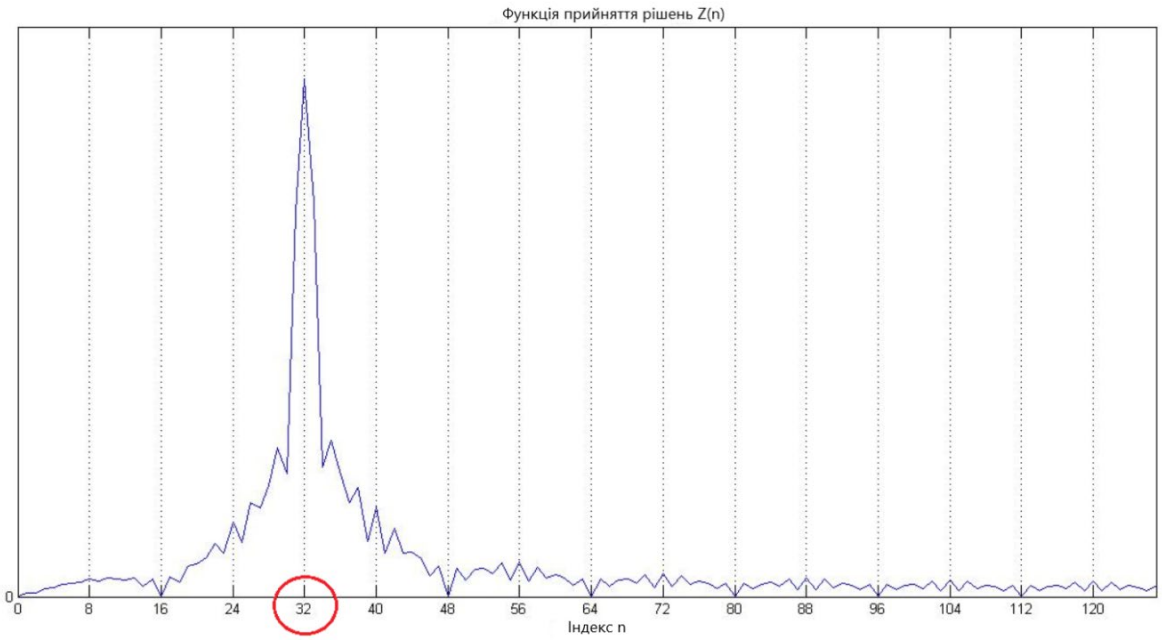

Рисунок 3.13 – Функція прийняття рішень

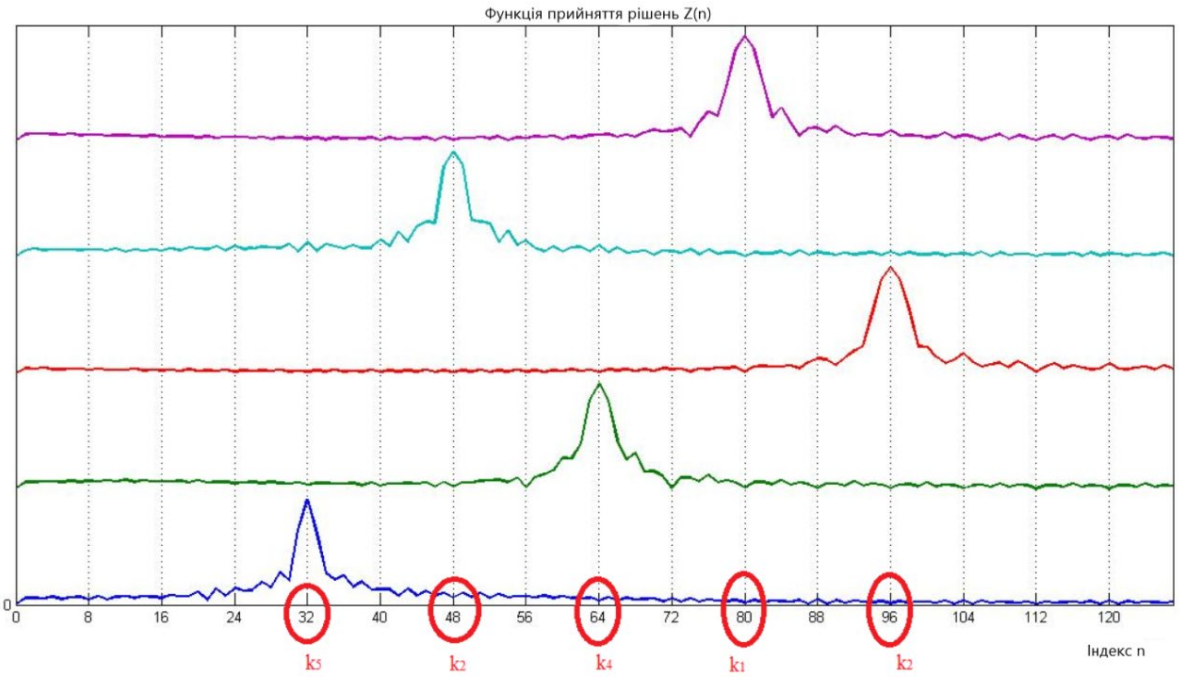

Рисунок 3.14 – Функція прийняття рішень при різних значеннях інформаційного символу k

Нарешті визначаємо значення декодованого приймачем інформаційного символу k.

Для цього знаходимо частоту ω, при якій функція прийняття рішення $Z(\omega)$ набуває максимальне значення (ω_{max}):

$$Z(\omega = \omega_{max}) = MAX[Z(\omega)]$$

$$k = \frac{\omega_{max}}{\Delta\omega}$$

Ключовою особливістю радіоінтерфейсу LoRa (як уже згадувалося вище) є його висока стійкість. Рисунки 3.15, 3.16 демонструють функціонування описаного детектора сигналу LoRa в умовах адитивного білого гаусівського шуму (відношення сигнал / шум SNR = 0dB). А в Табл. 3.2 наведені результати моделювання в середовищі Matlab роботи детектора при різних відносинах сигнал / шум і коефіцієнтах розширення спектра [10].

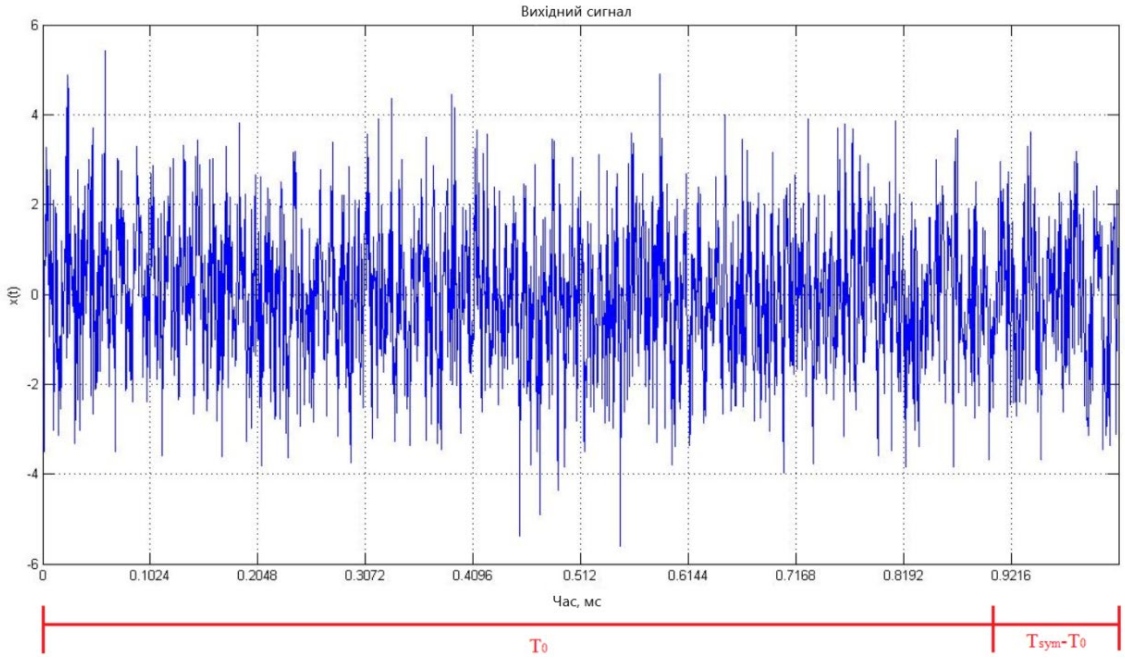

Рисунок 3.15 – Вихідний сигнал LoRa в умовах адитивного білого гаусівського шуму

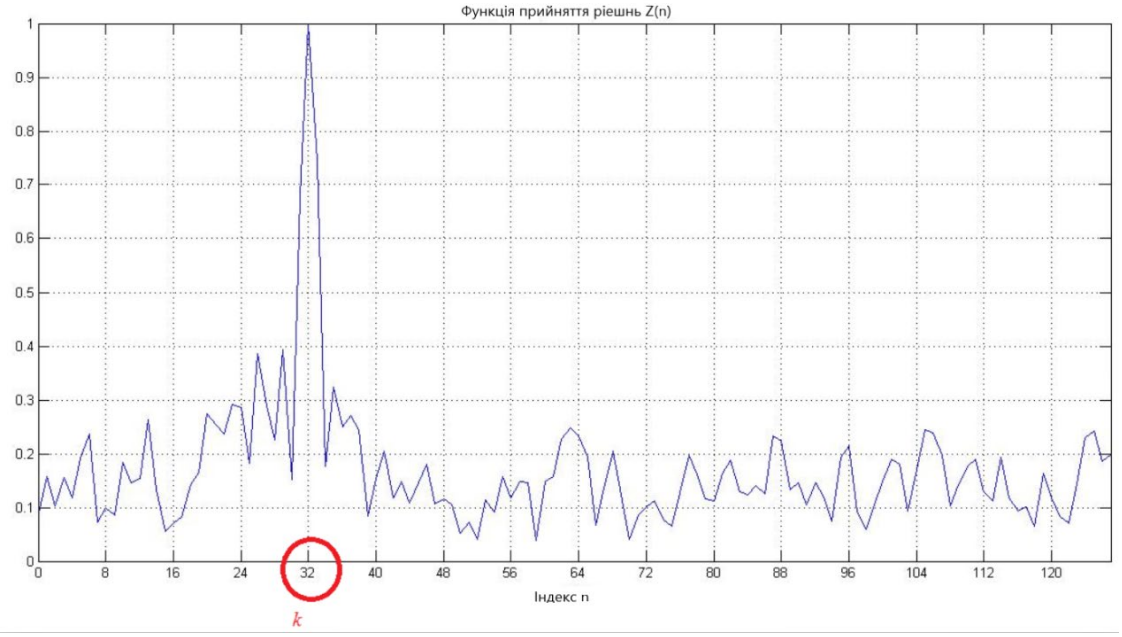

Рисунок 3.16 – Функція прийняття рішень в умовах адитивного білого гаусівського шуму

Таблиця 3.2 – Помилка детектування [10].

SNR/SF	SF7	SF8	SF9	SF10	SF11	SF12
0 дБ	0,9%	0,5%	0,2%	0,1%	0,1%	0,0%
-3 дБ	0,9%	0,6%	0,2%	0,1%	0,1%	0,0%
-6 дБ	2,0%	0,6%	0,2%	0,1%	0,0%	0,0%
-9 дБ	6,9%	1,5%	0,2%	0,1%	0,1%	0,0%
-12 дБ	18,0%	5,8%	1,3%	0,1%	0,0%	0,0%
-15 дБ	42,2%	17,6%	5,4%	0,6%	0,1%	0,0%
-18 дБ	68,9%	44,2%	18,0%	5,1%	1,1%	0,1%
-21 дБ	87,5%	73,7%	49,3%	18,9%	5,2%	0,8%

3.2 Методика оцінювання впливу параметрів фізичного інтерфейсу LoRa на надійність мережі

Характеристика продуктивності LoRa. Оскільки технологія LoRa є закритим джерелом, насправді доступні лише деякі подробиці щодо її роботи - переважно отримані з патенту Semtech, що описує технологію модуляції, або з приміток до заявки, написаних, щоб допомогти розробникам додатків точно налаштувати характеристики трансивера відповідно до своїх потреб. Багато дослідників вважали цю інформацію занадто обмеженою і розпочали порівняльний аналіз та інженерію технології, щоб краще зрозуміти її механізм та характеристики.

Вплив навколишнього середовища на радіостанції малої потужності. Велика кількість робіт досліджувала вплив умов навколишнього середовища на продуктивність мережі бездротових бездротових радіостанцій, особливо на радіоприймачах, сумісних з IEEE 802.15.4. Кілька авторів повідомляють про вплив метеорологічних умов на прийом пакетів, включаючи вплив погодних умов та вологості, а також наявність рослинності. Одне з найбільш всебічних досліджень бездротових вузлів, розміщених на відкритому повітрі, було проведено вченими, які підкреслили, що коефіцієнт прийому пакетів та потужність отриманого сигналу найбільше корелюють з температурою, тоді як кореляція з іншими факторами, такими як абсолютна вологість та кількість опадів, є менш вираженою.

Сильний вплив температури на продуктивність зв'язку підтверджено кількома іншими роботами, також майже повністю зосередженими на трансиверах IEEE 802.15.4. Банністер та ін. [21] показали кореляцію між температурою та потужністю сигналу в дислокації в пустелі Сонoран, і виявили в контрольованій температурою камері, що рівень отриманого сигналу радіостанції TI CC2420 послаблюється при високих температурах через вплив

температури на низький рівень шуму та підсилювачі потужності. На основі цієї роботи Боано та ін. [22] підтвердили ці висновки також на інших платформах, таких як TI CC1020 та CC2520, а також підкреслили, як це може спричинити повне порушення бездротового зв'язку. Автори також продемонстрували, як не можна нехтувати впливом температури при розробці протоколів управління доступом до робочого циклу для бездротових радіостанцій із низьким енергоспоживанням. Для полегшення вивчення того, як температура впливає на роботу малопотужних бездротових протоколів у більшому масштабі, ніж у камері з контролем температури, було запропоновано кілька недорогих інфраструктур тестових стендів, найпопулярнішими з яких є TempLab та HotBox [23].

Вплив умов навколишнього середовища на радіостанції LPWAN, натомість, ще не досліджено детально. Іова та ін. [16] розгорнули низку мереж LoRa у міському та гірському середовищі та повідомили, що такі фактори навколишнього середовища, як наявність рослинності та коливання температур, можуть негативно вплинути на ефективність зв'язку. Однак автори не визначили кількісно вплив цих факторів навколишнього середовища, і їх робота ще не з'ясовує, чи погіршують високі температури якість зв'язків LoRa подібним чином, як це спостерігається на декількох трансиверних платформах IEEE 802.15.4.

3.2.1 Безпека в мережах LoRa

У мережі LoRaWAN забезпечується повна конфіденційність даних при проходженні всіх задіяних в ланцюжку пристроїв, при цьому вміст пакета доступно тільки відправнику (кінцевому пристрою) і одержувачу (з додатком), для якого воно призначене. Мережевий сервер оперує даними в зашифрованому вигляді, виробляє аутентифікацію і перевіряє цілісність кожного пакету, але при цьому не має доступу до корисного навантаження, тобто до інформації від

підключених сенсорів (за винятком використання не рекомендованих сценаріїв, в яких шифрування корисного навантаження виконує мережевий сервер з використанням ключа NwkSKey, а не сервер додатків; надалі даний сценарій не розглядається) [10].

Рисунок 3.17 – Шифрування

У мережі використовуються три види ключів. Ключ аутентифікації додатку AppKey відомий тільки кінцевому пристрою і серверу додатків. У разі якщо кінцевий пристрій підключається до мережі в режимі Over-The-Air-Activation (OTAA), ключ аутентифікації додатки AppKey використовується для обчислення мережевого ключа NwkSKey і ключа додатки AppSKey. У разі якщо кінцевий пристрій підключається до мережі в режимі Activation By Personalization (ABP), ключі NwkSKey і AppSKey встановлені на кінцевому пристрої. Ключ NwkSKey відомий мережному серверу і кінцевому пристрою і використовується для перевірки цілісності кожного повідомлення, використовуючи Message Integrity Code (MIC). MIC обчислюється за алгоритмом AES-CMAC, який аналогічний контрольній сумі, за винятком того, що він запобігає навмисній підробці повідомлень. Ключ додатку AppSKey використовується для шифрування корисного навантаження, використовуючи алгоритм AES-128, між кінцевим пристроєм і сервером додатків [10].

3.2.2 Активація кінцевих пристроїв

Для підключення до мережі LoRaWAN кожен кінцевий пристрій повинен бути ідентифікований та активований в мережі.

Передбачено два режими активації кінцевих пристроїв, активація по повітрю - Over-The-Air Activation (OTAA) і активація персоналізацією - Activation by Personalization (ABP) [10].

3.2.2.1 Активація по повітрю - Over-The-Air Activation (OTAA)

При активації по повітрю кінцеві пристрої LoRa не прив'язані жорстко до якоїсь конкретної мережі. На кінцевих пристроях LoRa прописуються ідентифікатор пристрою (DevEUI), ідентифікатор додатку (AppEUI) і ключ додатку (AppKey). Кінцевий пристрій при активації ініціює JOIN процедуру. Ключі шифрування (AppSKey і NwkSKey), необхідні для передачі інформації, обчислюються самим кінцевим пристроєм. Даний метод активації забезпечує високий рівень безпеки і рекомендується для використання.

Рисунок 3.18 – Активація по повітрю (OTAA)

Формат повідомлень JOIN_REQUEST і JOIN_ACCEPT показаний на рисунках нижче:

Size (bytes)	8	8	2
Join Request	AppEUI	DevEUI	DevNonce

Рисунок 3.19 – Формат повідомлення Join Request

Size (bytes)	3	3	4	1	1	(16) Optional
Join Accept	AppNonce	NetID	DevAddr	DLSettings	RxDelay	CFList

Рисунок 3.20 – Формат повідомлення Join Accept

Де:

- AppEUI - ідентифікатор додатки в адресному просторі IEEE EUI64;
- DevEUI - глобальний ідентифікатор пристрою в адресному просторі IEEE EUI64;
- DevNonce - випадкове число, що генерується кінцевим пристроєм (використовується при розрахунку NwkSKey і AppSKey);
- AppNonce - випадкове число, що генерується сервером додатків (використовується при розрахунку NwkSKey і AppSKey);
- - NetID - ідентифікатор мережі, старші 7 біт якого (31..25) відповідають ідентифікатору NwkID, молодші 17 біт можуть довільно призначатися оператором;
- DevAddr - адреса кінцевого пристрою, старші 7 біт якого відповідають ідентифікатору NwkID, молодші 25 біт є адресою кінцевого пристрою в мережі NwkAddr;
- DLSettings - вказує на зсув швидкості передачі даних в DL каналі вікна прийому RX1 (щодо швидкості передачі даних в UL каналі) і швидкість передачі даних в DL каналі вікна прийому RX2;

- RXDelay - затримка між завершенням передачі даних в UL каналі і відкриттям вікна прийому RX1;
- CFList - список радіочастотних каналів з Freq Ch4 по Freq Ch8 (перші три канали є обов'язковими і незмінними).

Формули обчислення мережевого ключа NwkSKey і ключа додатку AppSKey наведені нижче:

NwkSkey=aes128_encrypt(AppKey,0x01|AppNonce|NetID|DevNonce|pad_{16})

AppSkey=aes128_encrypt(AppKey,0x02|AppNonce|NetID|DevNonce|pad_{16}) [10].

3.2.2.2 Активація персоналізацією - Activation by Personalization (ABP)

При активації персоналізацією кінцеві пристрої жорстко прописуються для роботи в конкретній мережі оператора. Кінцеві пристрої прошиваються з певними мережевим ключем (NwkSKey) і ключем додатки (AppSKey). Даний метод активації (в зв'язку з низьким рівнем безпеки і складністю реалізації) не рекомендується використовувати для комерційних мереж [10].

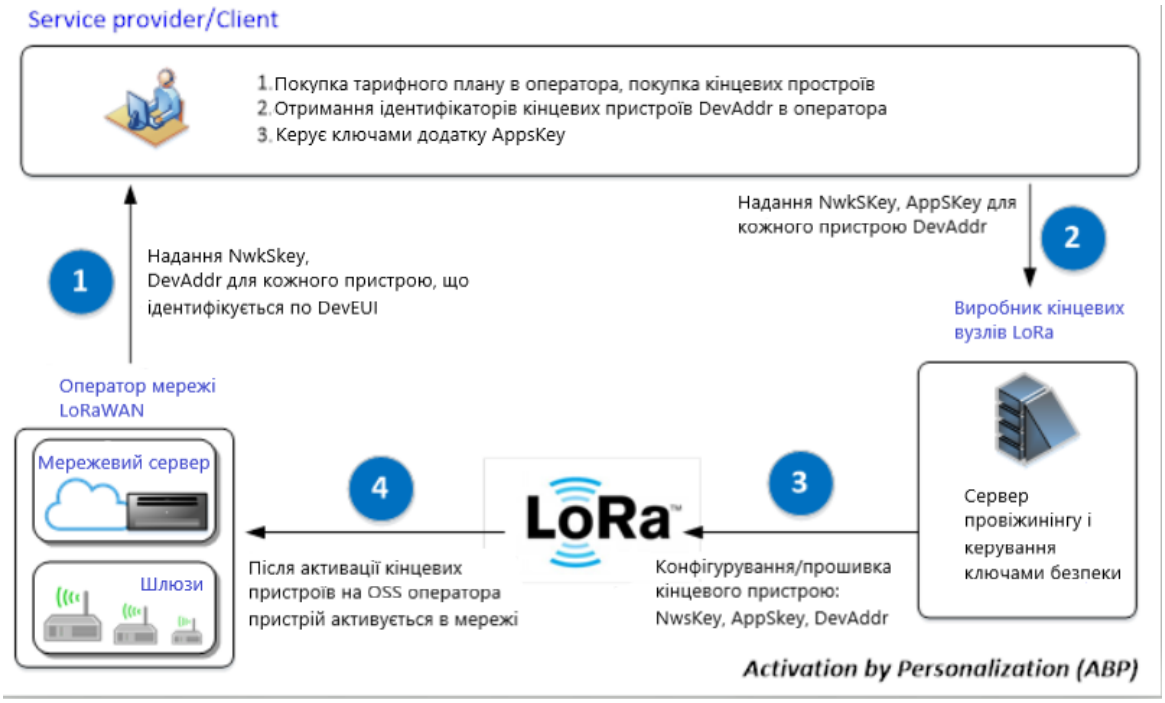

Рисунок 3.21 – Активація персоналізацією

3.3 Особливості роботи пристроїв Class-B

3.3.1 Передача даних в каналі "вниз"

Функціональність класу "B" оптимізована для мобільних і стаціонарних кінцевих пристроїв, що працюють від автономних джерел живлення.

Кінцеві пристрої здійснюють роботу в класі "B" при наявності запитів на відкриття приймальних вікон в фіксовані інтервали часу для можливості забезпечення відсилання повідомлень в DL каналі на вимогу сервера.

Для мережі з підтримкою кінцевих пристроїв класу "B" всі шлюзи повинні синхронно передавати сигнал маяка (beacon), забезпечуючи відліки синхронізації для кінцевих пристроїв. Ґрунтуючись на цих відліках синхронізації, кінцеві пристрої можуть періодично відкривати приймальні вікна (ping slots), які можуть використовуватися мережевою інфраструктурою для ініціації передачі по каналу DL. Ініційована мережею передача в DL каналі в одному з прийомних вікон (ping

slot), називається «ping». Шлюз, призначений для передачі даних в DL каналі, вибирається мережевим сервером, ґрунтуючись на індикаторах якості сигналу кінцевого пристрою в UL каналі (в рамках останнього сеансу зв'язку). У зв'язку з цим, при переміщенні кінцевого пристрою і виявленні змін ідентифікатора в прийнятому маяку, кінцевий пристрій повинен відправити повідомлення по UL каналу мережному серверу, щоб сервер оновив базу даних шляхів маршрутизації каналу DL.

Всі кінцеві пристрої починають роботу як кінцеві пристрої класу "A". Сервер додатків може прийняти рішення про переключення кінцевого пристрою в клас "B". Це відбувається виконанням такої процедури:

1) В рамках вікна прийому класу "A" сервер додатків запитує кінцевий пристрій на перемикання в режим класу "B". Кінцевий пристрій шукає маяк мережі і повертає значення BEACON_LOCKED якщо маяк мережі був виявлений і прийнятий, яке значення BEACON_NOT_FOUND в іншому випадку. Для прискорення виявлення маяка може використовуватися команда «BeaconTimingReq», яка буде описана пізніше.

2) Ґрунтуючись на потужності сигналу маяка і обмеження щодо терміну служби батареї, сервер додатків вибирає швидкість передачі даних і періодичність вікон прийому (ping slot), після чого запитує установку даних параметрів на кінцевому пристрої.

3) При роботі в режимі класу "B" кінцевий пристрій встановлює в одиницю прапор CLASS-B (4-ий біт поля FCtrl рівня MAC) в кожному переданому кадрі UL, вказуючи тим самим мережному серверу, що пристрій переключено в режим класу "B" . Коли прийом маяка проведено успішно, кінцевий пристрій пересилає вміст маяка додатку разом з виміряним рівнем потужності. Кінцевий пристрій при прийомі повідомлення в DL каналі враховує максимально можливий зсув

синхронізації (втрати частоти) при плануванні часу відкриття приймального слота маяка і ping slot. Коли передане в DL повідомлення успішно демодулюване кінцевим пристроєм протягом ping slot, воно обробляється також, як повідомлення DL, описане в специфікації на пристрої класу "A".

4) Мобільний кінцевий пристрій повинен періодично інформувати мережевий сервер про власне місцезнаходження для поновлення маршруту передачі повідомлень в каналі DL. Це досягається шляхом передачі звичайного (можливо порожнього) «непідтверджуваного» або «підтверджуваного» повідомлення в каналі UL. Цей функціонал може бути реалізований більш ефективно, якщо додаток буде визначати переміщення пристрою на основі аналізу змісту маяка. В даному випадку, для запобігання колізій при передачі в каналі UL, кінцевий пристрій повинен застосовувати випадкову затримку між прийомом маяка і передачею повідомлення.

5) Якщо маяк не приймався протягом певного періоду, синхронізація з мережею вважається втраченою. У цьому випадку кінцевий пристрій перемикається назад в режим класу "A" і, як наслідок, скидає в 0 прапор CLASS-B у всіх повідомленнях UL каналу. Сервер додатків періодично може робити спроби перемикання пристрою назад в клас "B". Це призведе до перезапуску процесу, починаючи з пошуку сигналу маяка.

Наступна діаграма показує концепцію приймального слота маяка і ping slots.

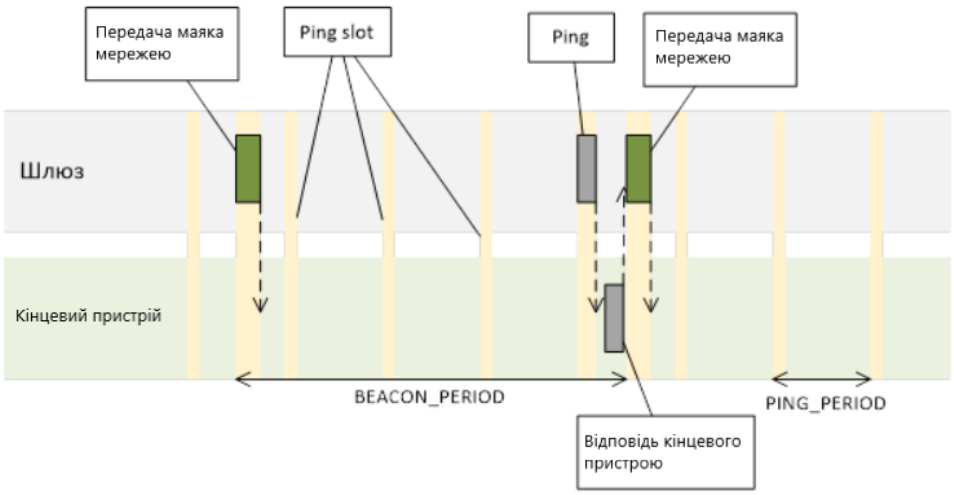

Рисунок 3.22 – Концепція приймального слота маяка і ping slots

В даному прикладі (вісь часу не відображено на рисунку) період посилання сигналу маяка становить 128 секунд, кінцевий пристрій відкриває приймальний ping slot кожні 32 секунди для можливості прийому повідомлення ping. Велику частину часу ping slot не використовуються сервером і, отже, приймальне вікно кінцевого пристрою закривається, як тільки радіоприймач розуміє, що преамбула в радіоканалі відсутня. Якщо преамбула виявляється, радіоприймач залишається включеним до тих пір, поки кадр DL не буде демодулювати. Далі MAC-рівень кінцевого пристрою буде обробляти кадр, перевіряючи, що поле адреси відповідає адресі кінцевого пристрою і що повідомлення Message Integrity Check коректне, перед передачею відповіді на сервер додатків [10].

3.3.2 Формат кадру Ping в DL каналі (при роботі в режимі класу "B")

3.3.2.1 Формат кадру фізичного рівня

У каналі DL повідомлення Ping використовує той же формат, що при роботі в режимі класу "A", але може слідувати іншим планом частотного каналу [10].

3.3.2.2 Індивідуальні та групові MAC повідомлення

Повідомлення поділяються на «індивідуальні» і «багатоадресні». Індивідуальні повідомлення надсилаються одиничному кінцевому пристрою, багатоадресні повідомлення розсилаються на кілька кінцевих пристроїв. Всі пристрої в багатоадресній групі спільно використовують одну і ту ж групову адресу і пов'язаний з нею ключ шифрування.

Специфікація LoRaWAN для пристроїв класу "B" не визначає засоби для віддаленого налаштування таких багатоадресних груп або безпечного розподілу матеріалів необхідних для групового ключа. Це виконується або через індивідуальну настройку кожного кінцевого пристрою, або через рівень програми [10].

3.3.2.3 Формат індивідуального повідомлення канального рівня

MAC Payload в індивідуальному повідомленні Ping в DL каналі використовує формат, визначений в специфікації до класу "A" [10].

3.3.2.4 Формат багатоадресного повідомлення канального рівня

Багатоадресні кадри мають в основному той же формат, що і індивідуальні з деякими винятками:

- вони не можуть переносити MAC-команди ні в поле FOpt, ні в корисне навантаження (з FPort = 0), оскільки багатоадресна розсилка в DL не має такої ж надійності аутентифікації, як індивідуальні кадри;
- прапори ASK і ADRASKReq заголовка MAC рівня повинні бути скинуті (= 0);
- поле MType має нести значення Unconfirmed Data Down.

Наявність біта FPending вказує, що є додаткові дані для багатоадресної розислки. Якщо даний біт встановлений, в наступному багатоадресну приймальному слоті будуть передаватися дані. Якщо даний біт не встановлений, в наступному слоті дані можуть передавати або не бути передані. Даний біт може використовуватися кінцевими пристроями для визначення пріоритетів для конфліктуючих слотів прийому [10].

3.3.3 Синхронізація тимчасового інтервалу в DL каналі для пристроїв класу "B"

Для коректної роботи в режимі B, кінцевий пристрій повинен відкривати приймальні слоти в точно визначені моменти часу по відношенню до інфраструктури маяка.

Інтервал між двома послідовними маяками називається beacon period. Передача кадру маяка поєднана з початком інтервалу BEACON_RESERVED. Кожному маяку передує захисний часовий інтервал, в якому не може розташовуватися ping slot. Довжина захисного інтервалу визначається часом в ефірі найдовшого доступного кадру. Це зроблено, щоб гарантувати, що передача повідомлення в каналі DL, ініційована під час інтервалу ping slot, матиме достатньо часу для завершення передачі без перетину з передачею маяка. У зв'язку з цим, прийнятний часовий інтервал для ping slot розташовується між закінченням зарезервованого тимчасового інтервалу маяка (BEACON_RESERVED) і початком наступного захисного інтервалу маяка (BEACON_GUARD).

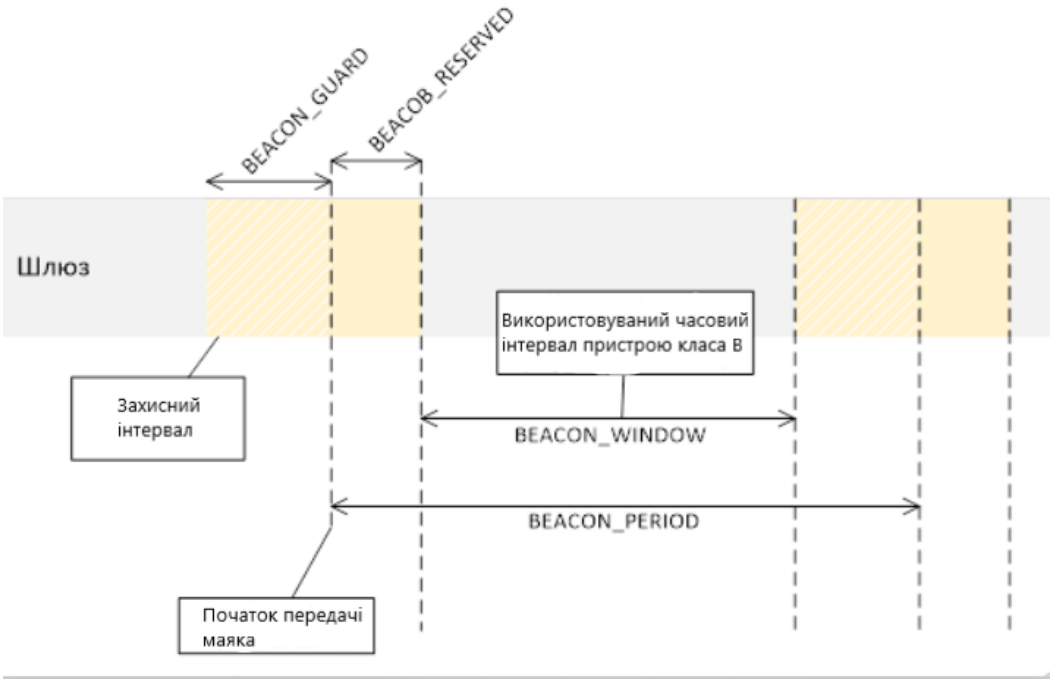

Рисунок 3.23 – Концепція передачі маяка

Таблиця 3.3 – Тривалість інтервалів при передачі маяка

Beacon_period	128 секунд
Beacon_reserved	2,12 секунди
Beacon_guard	3 секунди
Beacon_window	122,88 секунди

Кадр маяка в радіоефірі насправді більш короткий, ніж зарезервований часовий інтервал маяка (BEACON_RESERVED), щоб в подальшому мати можливість додавання широкомовного кадру мережевого управління.

Інтервал вікна маяка (beacon window) розділений на 212 = 4096 ping slot по 30 мс кожен, пронумерованих від 0 до 4095 (N - slot index).

Кінцевий пристрій, що використовує ping slot номер N, має включити приймач точно через T_{on} секунд після початку маяка, де:

$$T_{on} = beacon_{reserved} + N \cdot 30\text{мс}$$

Останній ping slot починається через $beacon\_reserved + 4095 \bullet 30\text{мс} = 124\,970\text{мс}$ після початку маяка або за 3030 мс перед початком передачі наступного маяка [10].

3.3.4 Випадковий вибір слота

Щоб уникнути систематичних колізій або ймовірності прослуховування (over-hearing), індекс слота для конкретного кінцевого пристрою випадковий і змінюється в кожному новому періоді маяка. Для цього використовуються такі параметри:

DevAddr	32 бітна мережева адреса пристрою (індивідуальний чи багатоадресний)
pingNb	Кількість «ping slot» кінцевого пристрою в періоді маяка. Воно повинно бути цілим числом ступеня двійки: $pingNb = 2^k$, де $1 <= k <= 7$
pingPeriod	Період, протягом якого приймач пристрою включений, виражається в кількості слотів: $pingPeriod = 212 / pingNb$
pingOffset	Випадковий зсув обчислюється при кожному запуску маяка. Значення знаходиться в діапазоні від 0 до ($pingPeriod - 1$)
beaconTime	Час визначається в полі BCNPayload. Це час, що безпосередньо передує кадру маяка.
slotLen	Довжина одного ping slot = 30 мс

У кожен період маяка кінцевий пристрій і сервер обчислюють нове псевдовипадкове зміщення для вирівнювання приймального слота. Для визначення псевдовипадкового значення використовується AES шифрування з фіксованим ключем з усіх нулів:

Key =16 x 0x00

Rand = aes128_encrypt(Key, beaconTime | DevAddr | pad16)

pingOffset=(Rand[0] + Rand[1]x256)modulo8

Слот, який використовується для даного періоду маяка (beacon period): pingOffset + N • pingPeriod, де N=[0:pingNb - 1]

Отже, кінцевий пристрій буде відкривати приймальні слоти починаючи з наступного часу:

Slot 1	Beacon_reserved + pingOffset x slotLen
Slot 2	Beacon_reserved + (pingOffset + pingPeriod) x slotLen
Slot 3	Beacon_reserved + (pingOffset + 2 x pingPeriod) x slotLen
…	…

Якщо кінцевий пристрій обслуговує одночасно індивідуальний і один або більше багатоадресних слотів, даний розрахунок виконується кілька разів на початку кожного нового періоду маяка. Один раз для індивідуальної адреси (адреса кінцевого пристрою мережі) і один раз для кожної багатоадресної адреси (multicast group address).

У разі, коли багатоадресний ping slot і індивідуальний ping slot перетинаються, і не можуть обслуговуватися приймачем кінцевого пристрою, кінцевий пристрій повинен переважно слухати багатоадресний слот. Якщо колізія виникла між багатоадресними прийомними слотами, значення біта FPending попереднього багатоадресного кадру може використовуватися для установки пріоритетів.

Випадкова схема розподілу запобігає систематичним колізіям між індивідуальними і багатоадресними слотами. Якщо колізія виникає протягом періоду одного маяка, то навряд чи вона повториться протягом наступного періоду [10].

3.3.5 Частотні канали DL для індивідуальної і групової передачі

3.3.5.1 EU 863-870MHz ISM Band

Всі індивідуальні та багатоадресні повідомлення, що направляються кінцевим пристроям класу "B", використовують один частотний канал, певний MAC-командою «PingSlotChannelReq». Частота, встановлена за замовчуванням - 869,525MHz [10].

3.3.5.2 US 902-928MHz ISM Band

За замовчуванням використовується функція визначення каналу DL пристроїв класу "B" на підставі значення поля часу останнього маяка і значення поля DevAddr.

$$\textbf{Class B downlink channel} = [\textbf{DevAddr} + \text{ціла частина}((\textbf{Beacon\_Time})/(\textbf{Beacon\_Period}))] \ \textbf{modulo 8},$$

Де:

- Beacon_time - 32-х бітове поле Time поточного періоду маяка;
- Beacon_period - довжина періоду маяка (128 секунд);
- Ціла частина (x) позначає округлення числа x вниз до цілого значення;
- DevAddr - 32 бітна мережева адреса кінцевого пристрою.

Канал DL пристроїв класу "B" послідовно здійснює стрибки через 8 каналів в ISM діапазоні і все кінцеві пристрої класу B рівномірно розподіляються між 8 каналами DL.

Якщо команда «PingSlotChannelReq» з коректним не нульовим аргументом використовується для установки частоти DL класу B, тоді всі наступні ping slot повинні бути відкриті на цій єдиній частоті незалежно від останньої частоти передачі маяка.

Якщо команда «PingSlotChannelReq» посилається з нульовим аргументом, кінцевим пристроям слід відновити частотний план за замовчуванням, при цьому ідентифікатор ping slot пристроїв класу "B" буде перескакувати через 8 каналів.

Основна ідея - дозволити мережевим операторам, які мають виділений частотний ресурс, конфігурувати кінцеві пристрої для використання однієї ліцензованої частоти для передачі DL повідомлень пристроїв класу "B", і зберегти можливість великого частотного розносу при використанні ISM діапазону [10].

3.4 Особливості роботи пристроїв Class-C

Кінцеві пристрої класу "C" - це пристрої з постійно відкритим прийомним вікном в DL каналі. Такі пристрої використовуються у випадках, коли є достатня ємність з харчування і в зв'язку з цим не потрібно обмежувати час роботи приймача. Кінцеві пристрої класу "C" не можуть працювати в режимі класу "B".

Кінцеві пристрої класу "C" постійно слухають радіоефір з параметрами вікна RX2, за винятком випадків, коли пристрій передає дані або відкриває приймальне вікно RX1 відповідно до опису класу "A". Таким чином, приймальне вікно з параметрами RX2 відкривається кінцевим пристроєм:

- між закінченням передачі в UL каналі і початком приймального вікна RX1;
- після закриття приймального вікна RX1 і аж до початку передачі в UL каналі [10].

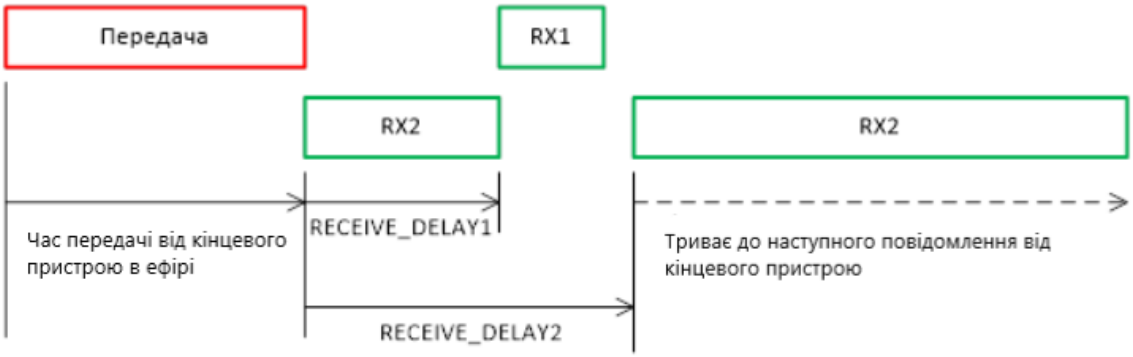

Рисунок 3.24 – Схема передачі повідомлення через пристрій класу «С»

3.4.1 Групова передача повідомлень для пристроїв класу С

Так само, як і в класі "B", пристрої класу "C" можуть приймати багатоадресні кадри від LoRa-шлюзу. Багатоадресна адреса, ключ сесії мережі і ключ сесії додатки повинні бути отримані від сервера додатків. При цьому аналогічні обмеження, як і для класу "B", застосовуються до пристроїв класу "C":

- забороняється застосовувати MAC-команди ні в поле FOpt, ні в корисне навантаження на порту 0, оскільки групове повідомлення не має тієї ж надійністю аутентифікації, що і індивідуальний кадр;
- біти ASK і ADRACKReq повинні бути рівні «0»;
- поле MType має нести значення Uniformed Data Down;
- біт FPending показує, що є додаткові групові дані для відправки (враховуючи, що пристрій класу "C" зберігає свій систему включеною протягом тривалого часу, біт FPending не викликає будь-якої реакції кінцевого пристрою) [10].

Висновки до розділу

1. Пропускна здатність (BW). Чим більша пропускна здатність, тим коротший ефірний час і нижча чутливість. Менша пропускна здатність також вимагає більшої частоти, щоб мінімізувати проблеми, пов'язані з «дрейфом годинника». Фактор розповсюдження (SF). Для передачі інформації LoRa «розподіляє» кожен символ на декілька мікросхем (коефіцієнт розповсюдження), щоб ще більше підвищити чутливість приймача. Швидкість кодування (CR). Чим більше сплесків перешкод очікується, тим вища швидкість кодування, яку слід використовувати для максимізації ймовірності успішного прийому пакетів. Потужність передачі (TP). Як і більшість бездротових радіостанцій, приймачі LoRa також дозволяють регулювати потужність передачі, різко змінюючи енергію, необхідну для передачі пакета. Носійна частота (CF). Приймачі LoRa використовують для зв'язку частоти під ГГц: серед інших, промислові, наукові та медичні (ISM) діапазони 433 МГц, 868 МГц (Європа) та 915 МГц (Північна Америка). Загальні модулі LoRa, такі як Semtech SX1272 та HopeRF RFM95, підтримують зв'язок у діапазоні частот 860–1020 МГц і програмуються з кроком 61 Гц.

2. Оскільки технологія LoRa є закритим джерелом, насправді доступні лише деякі подробиці щодо її роботи - переважно отримані з патенту Semtech, що описує технологію модуляції, або з приміток до заявки, написаних, щоб допомогти розробникам додатків точно налаштувати характеристики трансивера відповідно до своїх потреб. Сильний вплив температури на продуктивність зв'язку підтверджено кількома іншими роботами, також майже повністю зосередженими на трансиверах IEEE 802.15.4. Банністер та ін. показали кореляцію між температурою та потужністю сигналу в дислокації в пустелі Сонoран, і виявили в контрольованій температурою камері, що рівень отриманого сигналу радіостанції TI CC2420 послаблюється при високих

температурах через вплив температури на низький рівень шуму та підсилювачі потужності. Вплив умов навколишнього середовища на радіостанції LPWAN, натомість, ще не досліджено детально. Іова та ін. розгорнули низку мереж LoRa у міському та гірському середовищі та повідомили, що такі фактори навколишнього середовища, як наявність рослинності та коливання температур, можуть негативно вплинути на ефективність зв'язку.

4 ОСОБЛИВОСТІ ФОРМУВАННЯ РАДІОПОКРИТТЯ ТА ЄМНОСТІ МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІ LORA

4.1 Особливості радіопокриття LoRa

4.1.1 Розрахунок параметрів

Беремо базові дані, які необхідні для моделювання, тобто частоту розгортання мережі, смугу частот одного радіоканалу й проводимо такі розрахунки.

Загальна кількість каналів :

$$n_{\text{к}} = \text{int}(\frac{F}{\Delta f_{\text{к}}}),$$

де F – смуга частот, виділена оператору за умовами ліцензії для розгортання системи, МГц;

$\Delta f_{\text{к}}$ – смуга частот одного радіоканалу, МГц

Визначимо кількість частотних каналів для обслуговування абонентів в одному секторі одного стільника:

$$n_{\text{чкс}} = \text{int}(\frac{n_{\text{к}}}{M \cdot C}),$$

де M – кількість секторів в стільнику; C – розмір кластера.

Визначаємо пропускну здатність БС в секторі (з врахуванням канального кодування і наявність циклічної приставки) R, Мбіт/с:

$$R = \frac{n_{\text{чк\_с}} \cdot N_{\text{рб}} \cdot n_{\text{пн}} \cdot N_{\text{сим}}^{\text{рб}} \cdot V_{cc} \cdot m}{T_{\text{рб}}},$$

де $N_{\text{рб}}$ – кількість ресурсних блоків у виділеній смузі частот радіоканалу (табл. 2.2);

$n_{\text{пн}}$ – кількість носійних частот в ресурсному блоці, $n_{\text{пн}} = 12$;

$N_{\text{сим}}^{\text{рб}}$ – кількість символів OFDM в часовому слоті, що утворює ресурсний блок , $N_{\text{сим}}^{\text{рб}} = 7$;

Vcc – швидкість канального коду, $Vcc = 1/3$;

m – кількість рівнів модуляції, біт/символ;

$T_{\text{рб}}$ – тривалість часового слоту, що утворює ресурсний блок, $T_{\text{рб}}$ = 0,5 мс [2].

Кількість рівнів модуляції m визначимо з виразу:

$$m = k \cdot \log_2 M',$$

де M' – кількість можливих станів модуляції (максимальна пропускна здатність буде при 64 – QAM, отже M' = 64);

k – коефіцієнт, що враховує застосування технології MIMO (для схеми MIMO 2x2 k = 2, за відсутності технології MIMO k=1).

$$m = 2 \cdot \log_2 64.$$

Визначаємо кількість абонентів в стільнику $N_{\text{аб\_с}}$:

$$N_{\text{аб\_с}} = \frac{M \cdot R}{R_{\text{аб}}} \cdot k_{os},$$

де $R_{\text{аб}}$ – гарантована швидкість для одного абонента, Мбіт/с;

k_{os} – коефіцієнт, який враховує, що для заданого виду трафіку кількість користувачів може бути збільшено через конкурентний доступ до середовища.

Далі розрахуємо чутливість приймачів БС і МС:

$$P_{\text{пр}} = N + 10 \cdot \lg(\Delta f_{\text{к}}) + NF + SNR,$$

де N – спектральна густина потужності теплового шуму приймача, N = -174 дБм/Гц;

$\Delta f_{\text{к}}$ – смуга частот радіоканалу; на лінії вниз відповідає значенню з початкових даних табл. 2.1, на лінії вгору відповідає смузі для передавання 2 ресурсних блоків у рамках SC-FDMA;

NF – внутрішній шум приймача, *NF* = 2,5 дБ для МС, *NF* = 7 дБ для БС;

SNR – допустиме відношення сигнал-шум, *SNR* = 2 дБ для МС, *SNR* = 1 дБ для БС.

Знайдемо втрати в радіолінії в напрямках від БС L_{DL} і до БС L_{UL} :

$$L_{\text{DL}} = P_{\text{пер\_БС}} + G_{\text{БС}} + G_{\text{МС}} - P_{\text{пр\_МС}} - L_{\text{фід}}.$$

$$L_{\text{UL}} = P_{\text{пер\_МС}} + G_{\text{АС}} + G_{\text{БС}} - P_{\text{пр\_БС}} - L_{\text{фід}}.$$

Враховуючи запас на затінення радіотраси, запас на внутрішньосистемні завади і втрати на проникнення в будівлі, максимально допустимі втрати складають $L_{\text{доп}}$:

$$L_{\text{доп}} = L_{UL} - M_{\text{зат}} - M_{\text{вн}} - L_{\text{буд}} + M_h,$$

де $M_{\text{зат}}$ – запас на затінення радіотраси, (6…10) дБ;

$M_{\text{вн}}$ – запас на внутрішньосистемні завади, 2дБ;

$L_{\text{буд}}$ – втрати на проникнення в будівлі,*13 дБ;*

M_h – запас на хендовер, 2,5 дБ.

Використовуємо удосконалену модель Окамура-Хата, яка визначає медіанне значення допустимих втрат в умовах міста, та передбачає задіяння частотних меж від 2000 до 3000 МГц, що відповідає умовам поставленої задачі.

$$L_{50|_{\text{місто}}} = 46{,}3 + 33{,}9\lg f + 10\lg(\frac{f}{2000}) - 13{,}82\lg h_{BS} + \alpha\left(h_{MS}\right) + \left(44{,}9 - 6{,}55\lg h_{BS}\right)\lg R - K.$$

З даної моделі знайдено радіус стільника для подальшого визначення кількості базових станцій.

Визначаємо кількість базових станцій:

$$N_{\text{БС}} = \frac{2S}{R_{\text{ст}}{}^2 3\sqrt{3}}$$

та кількість сенсорів та приладів, що можна обслуговувати:

$$N_{\text{А}} = N_{\text{БС}} N_{\text{аб\_с}}.$$

4.1.2 Моделювання мережі

Результати моделювання в програмному середовищі Atoll представлено на рис 4.1-4.2. Моделювання радіопокриття вважають завершеним, якщо відсоток території покриття з рівнем сигналу менше -100 дБм (нижче порогу чутливості МС) не перевищує 10%.

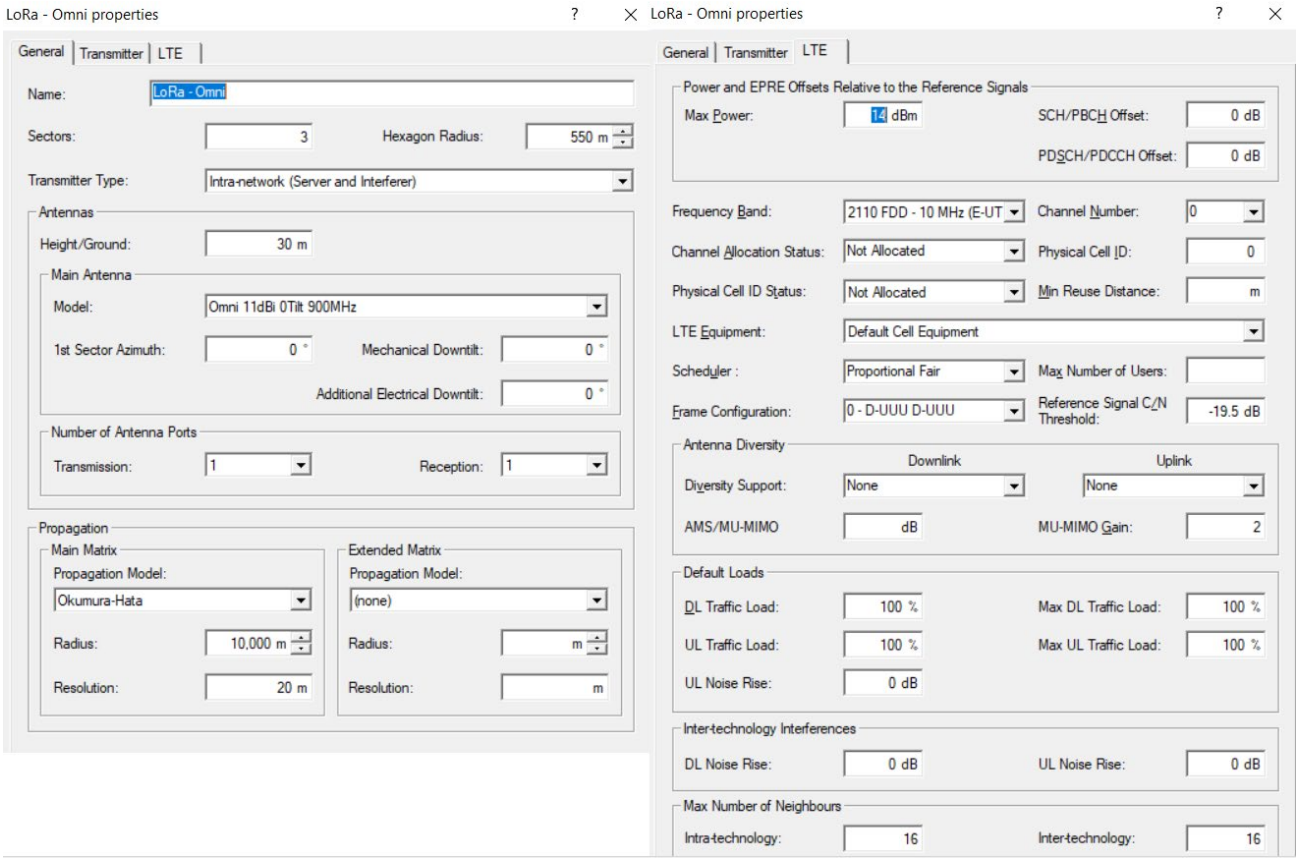

Рисунок 4.1 – Встановлення параметрів БС LoRa

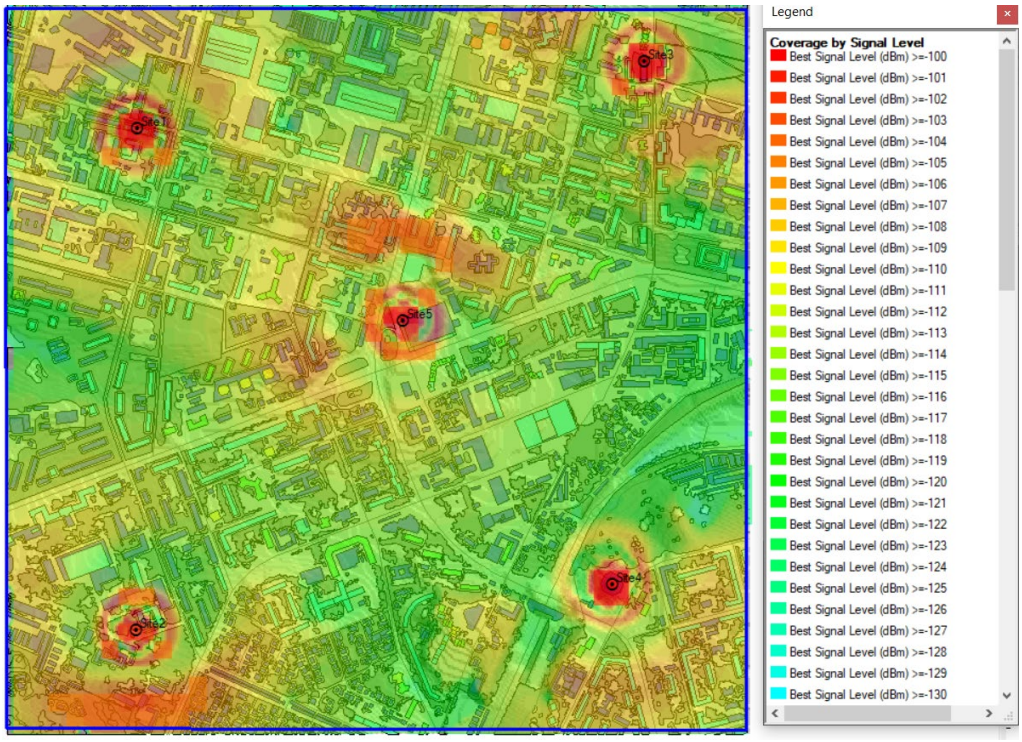

Рисунок 4.2 – Результати моделювання мережі LoRa на території міста Києва.

Візуалізація отриманого рівня сигналу на гістограмі представлена на рис. 4.3.

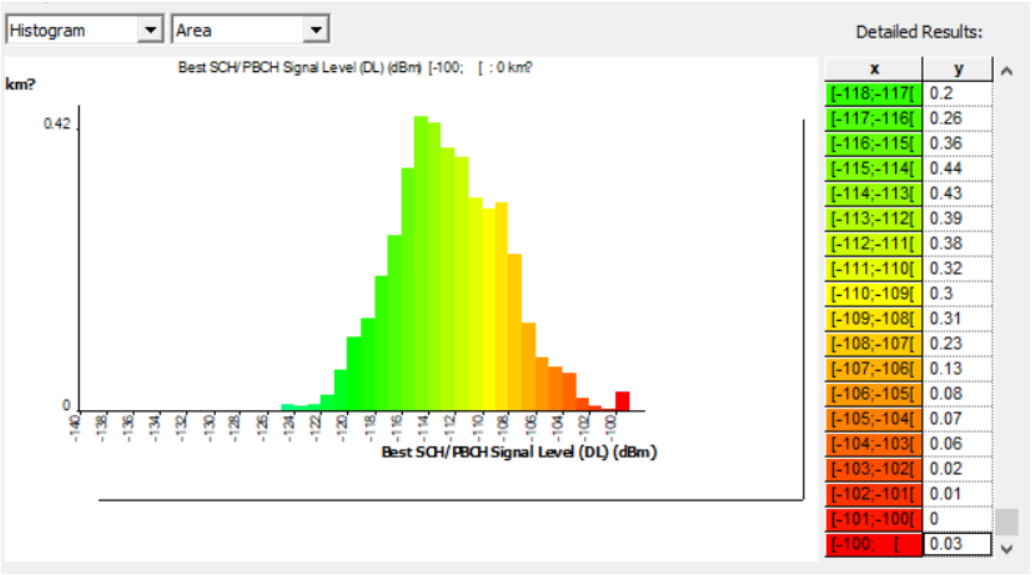

Рисунок 4.3 – Гістограмна візуалізація отриманого рівня сигналу в мережі LoRa на території міста Києва

Аналізуючи результати, можна зробити такі висновки: покриття мережі з задовільним рівнем сигнала (більше -120 дБм) є досить значним (більше 97%) та охоплює всю фактичну зону розгортання, з чого можна зробити висновок, що більшість користувачів, представлених у вигляді датчиків й пристроїв в даній місцевості, матимуть доступ до мережі з швидкістю, яка відповідає даному типу категорії (близько 10 кбіт/с) [2].

4.2 Особливості формування ємності мережі LoRa

Усі пристрої LoRaWAN класу "A", включаючи кінцеві пристрої, а також LoRa-шлюз, використовують довільний (не синхронізований) доступ до загального середовища передачі. При цьому тимчасові інтервали відправки пакетів плануються кінцевими пристроями на основі власних потреб. Даний механізм доступу вдає із себе протокол типу "чиста ALOHA" (pure ALOHA) на ім'я першої комп'ютерної мережі передачі даних з пакетною комутацією (ALOHAnet), розробленої в 1968-1970-х роках групою вчених Гавайського університету під керівництвом Нормана Абрамсона і використала в якості середовища доступу до неї бездротову технологію.

Оцінка пропускної здатності системи "чиста ALOHA" визначається при наступних припущеннях:

- користувацькі дані, призначені для передачі, надходять на термінали випадково, утворюючи пуассонівский потік;
- відкинуті через помилки передачі пакети передаються повторно, утворюючи також пуассонівский потік;
- всі пакети даних мають однакову довжину і передаються однаковий час;

– в мережі знаходиться нескінченне число віддалених терміналів (при цьому якщо якийсь термінал вже передає дані, це ніяк не впливає на ймовірність передачі даних іншими терміналами).

В цьому випадку:

– імовірність того, що за час передачі одного пакета T надійде ще k пакетів від всіх терміналів мережі визначається формулою Пуассона:

$$Pr(k) = \frac{G^k \cdot e^{-G}}{k!},$$

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

– колізія не виникне, якщо на інтервалі передачі повідомлення, а також на одному попередньому інтервалі не з'являться ще пакети для передачі від інших кінцевих пристроїв мережі (k = 0). Отже, ймовірність успішної передачі становить $P = e^{-2G}$;

– середнє число успішно переданих за час T пакетів, тобто пропускна здатність мережі, становить $S = G \cdot P = G \cdot e^{-2G}$. Графік пропускної здатності наведено на рисунку нижче:

Максимальне значення пропускної здатності досягається при інтенсивності надходження пакетів (G) 0,5 і становить 0,184 (при цьому ймовірність втрати пакетів через колізію - PLOSS складе 63%).

При інтенсивності надходження пакетів (G) 0,0256 ймовірність втрати пакетів через колізії (p_LOSS) становить 5%.

Рисунок 4.4 – Графік пропускної здатності

Максимальне значення пропускної здатності досягається при інтенсивності надходження пакетів (G) 0,5 і становить 0,184 (при цьому ймовірність втрати пакетів через колізію - PLOSS складе 63%).

При інтенсивності надходження пакетів (G) 0,0256 ймовірність втрати пакетів через колізії (PLOSS) становить 5%.

Модель-1

Розглянемо мережу LoRa з наступними характеристиками:

- кількість радіочастотних каналів (N_f) - 8;
- кількість символів в преамбулі ($n_{preamble}$) - 6;
- середній розмір корисних даних, що передаються в поле FRMPayload - 10 байт;
- середня частота передачі пакетів одним кінцевим пристроєм - 1 пакет на годину;

– передача заголовка включена (explicit mode - H = 0), передача CRC включена (CRC = 1), оптимізація швидкостей вимкнена (DE = 0);
– швидкість кодування (CR) - 4/5;
– пакети передаються тільки від кінцевих пристроїв (без підтвердження доставки);
– допустима ймовірність втрати пакетів через колізії (p_{loss}) - 5%;
– суміщення за часом в одному радіоканалі двох пакетів від різних джерел вважається колізією незалежно від використовуваних коефіцієнтів розширення спектра (SF).

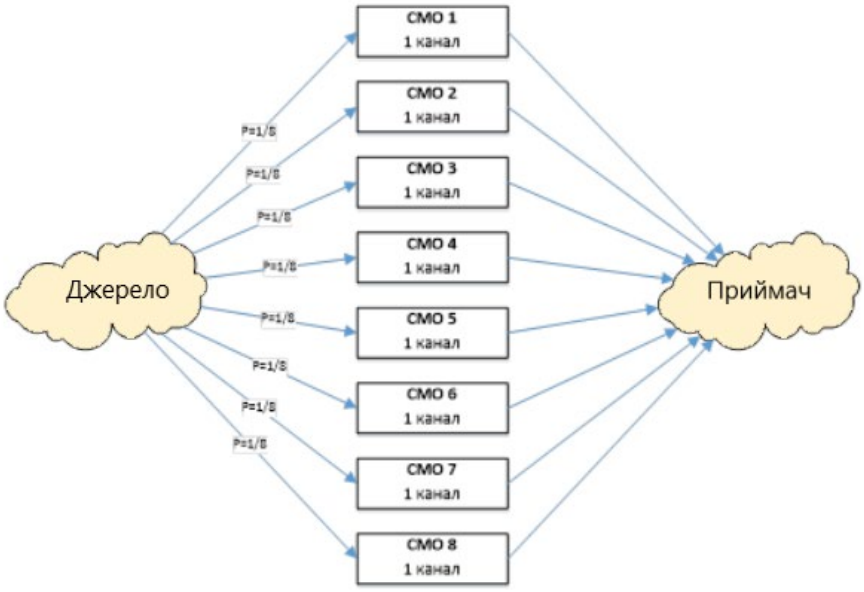

Рисунок 4.5 – Трафікова модель шлюза LoRa з параметрами Моделі-1

Допустима кількість пакетів на LoRa GW на добу становить:

$$Throughput = N_f \cdot \frac{24 \cdot 3600 \cdot G_{5\%}}{T},$$

де $G_{5\%} = 0{,}0256$ – інтенсивність надходження пакетів при $P_{LOSS} = 5\%$.

Таблиця 4.1 - Результати розрахунків для різних коефіцієнтів розширення спектра (SF)

Коефіцієнт розширення спектра	**SF**	**7**	**8**	**9**	**10**	**11**	**12**
Імовірність колізії	p	5%	5%	5%	5%	5%	5%
Кількість частотних каналів	N_f	8	8	8	8	8	8
Кількість пакетів на пристрій за добу	$N_{ENpackets}$	24	24	24	24	24	24
Тривалість передачі одного UL пакета, мс	$T_{ULpacket}$	59,65	109,06	197,63	354,3	708,61	1253,38
Навантаження на 1 канал, Ерл (= частка задіяння 1-го каналу для передачі трафіку)	A	0,0256	0,0256	0,0256	0,0256	0,0256	0,0256
Кількість пакетів на	$N_{LGpackets}$	297,19	162,55	89,7	50,03	25,02	14,14

LoRa GW на добу, тис. шт.							
Кількість пристроїв на LoRa GW, тис. шт.	N_{EN}	12,38	6,77	3,74	2,08	1,04	0,59

Якщо використовується режим з підтвердженням отримання мережевим сервером кожного пакета від кінцевого пристрою (з передачею етикетки підтвердження в першому часовому вікні прийому), то в якості часу передачі одного повідомлення візьмемо сумарний час передачі пакета даних кінцевим пристроєм і передачі етикетки підтвердження.

Таблиця 4.2 - Результати розрахунків для різних коефіцієнтів розширення спектра (SF)

Коефіцієнт розширення спектра	**SF**	**7**	**8**	**9**	**10**	**11**	**12**
Імовірність колізії	p	5%	5%	5%	5%	5%	5%
Кількість частотних каналів	N_f	8	8	8	8	8	8
Кількість пакетів на пристрій за добу	$N_{ENpackets}$	24	24	24	24	24	24

Тривалість передачі одного UL пакета, мс	$T_{ULpacket}$	59,65	109,06	197,63	354,3	708,61	1253,38
Тривалість передачі одного DL пакета, мс	$T_{DLpacket}$	39,17	68,1	136,19	231,42	462,85	925,7
Навантаження на 1 канал, Ерл (= частка задіяння 1-го каналу для передачі трафіку)	A	0,0256	0,0256	0,0256	0,0256	0,0256	0,0256
Кількість пакетів на LoRa GW на добу, тис. шт.	$N_{LGpackets}$	179,35	100,07	53,1	30,26	15,13	8,14
Кількість пристроїв на LoRa GW, тис. шт.	N_{EN}	7,47	4,17	2,21	1,26	0,63	0,34

Модель-2

Розглянемо мережу LoRa з наступними характеристиками:

– кількість радіочастотних каналів (N_f) - 8;

– кількість символів в преамбулі ($n_{preamble}$) - 6;

- середній розмір корисних даних, що передаються в поле FRMPayload - 10 байт;
- середня частота передачі пакетів одним кінцевим пристроєм - 1 пакет на годину;
- передача заголовка включена (explicit mode - H = 0), передача CRC включена (CRC = 1), оптимізація швидкостей вимкнена (DE = 0);
- швидкість кодування (CR) - 4/5;
- пакети передаються від кінцевих пристроїв з наступним підтвердженням доставки від мережевого сервера в першому часовому вікні;
- допустима ймовірність втрати пакетів через колізії (p_{loss}) - 5%;
- суміщення за часом в одному радіоканалі двох пакетів від різних джерел вважається колізією незалежно від використовуваних коефіцієнтів розширення спектра (SF).

Трафікова модель такого шлюзу LoRa еквівалентна 48-ми одноканальним системам масового обслуговування з відмовами, згрупованих у 8 груп (за кількістю радіочастотних каналів) по 6 СМО в кожній групі (за кількістю доступних коефіцієнтів розширення спектра)

Рисунок 4.6 - Трафікова модель шлюза LoRa з параметрами Моделі-2

В цьому випадку:

– ймовірність використання відповідного SF для передачі пакета (PSF) визначається моделлю розподілу кінцевих пристроїв по території радіопокриття;
– дозволена кількість пакетів на LoRa GW на добу становить:

$$Throughput = N_f \cdot \sum_{SF} P_{SF} \cdot \frac{24 \cdot 3600 \cdot G_{5\%}}{T_{SF}}$$

Розрахуємо ємність системи для двох моделей розподілу ймовірності використання кінцевими пристроями відповідних SF (P_{SF}):

– рівномірний розподіл;
– розподіл по площі зон радіопокриття:

$$P_{SF} = \{4{,}8\%; 3{,}9\%; 11{,}8\%; 16{,}7\%; 25{,}6\%; 37{,}2\%\}$$

В останньому випадку дані взяті з дослідження: «Analysis of the Capacity and Scalability of the LoRa Wide Area Network Technology», підготовленого співробітниками центру бездротового зв'язку університету Oulu, Фінляндія (Konstantin Mikhaylov, Juha Petajajarvi, Tuomo Hanninen) - див. Табл. 4.3, Рис. 4.7.

Таблиця 4.3 - Розподіл по площі зон радіопокриття

SF	DR	Rb (біт/с) при CR = 4/5	Бюджет лінії	SNR	Радіус зони, км	Площа зони, км^2	Частка кінцевих пристроїв (P_{SF})
SF7	DR5	5 468,75	138дБ	-7,5дБ	2,46	19,01	4,8%
SF8	DR4	3 125,00	141дБ	-10дБ	3,31	15,41	3,9%
SF9	DR3	1 757,81	144дБ	-12,5дБ	4,45	46,80	11,8%
SF10	DR2	976,56	147дБ	-15дБ	6,00	66,29	16,7%
SF11	DR1	537,11	149дБ	-17,5дБ	7,32	102,04	25,6%
SF12	DR0	292,97	151дБ	-20дБ	8,92	147,92	37,2%

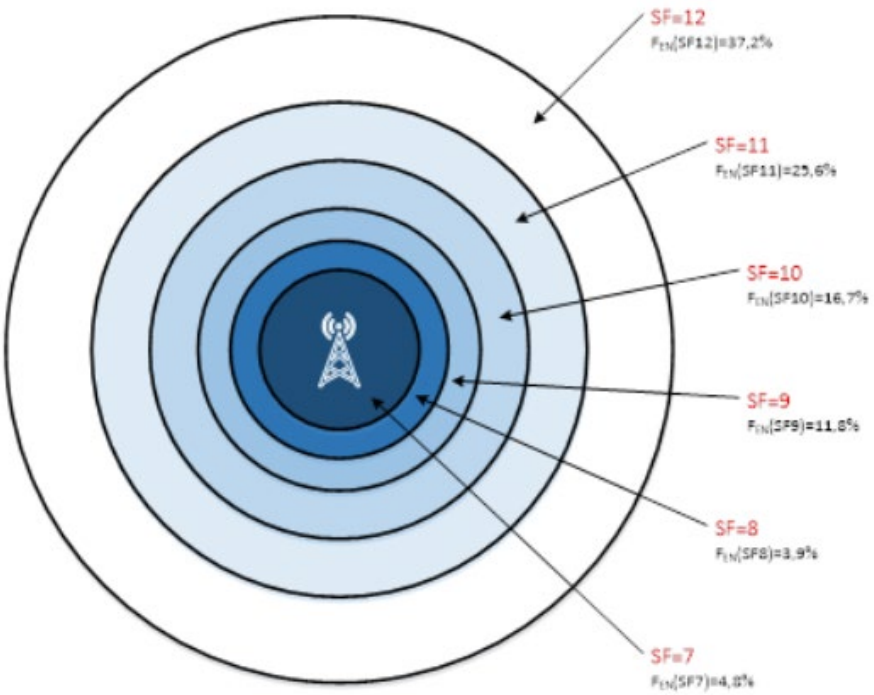

Рисунок 4.7 - Розподіл по площі зон радіопокриття

Для рівномірного розподілу отримуємо:

– кількість повідомлень на добу на 8-ми канальну систему = 64 349;
– кількість пристроїв на LoRa GW (при $N_{ENpackets}$ = 24) = 2 681.

Для розподілу по площі зон радіопокриття отримуємо:

– кількість повідомлень на добу на 8-ми канальну систему = 30 672;
– кількість пристроїв на LoRa GW (при $N_{ENpackets}$ = 24) = 1 278 [24].

Висновки до розділу

1. Проведено розрахунки сенсорної мережі з використанням технології LoRa. В результаті розрахунку встановлено, що для розгортання мережі на території 3.85 км^2 необхідно обрати 5 БС з радіусом стільника 550 м. Обладнання задовольняє необхідні технічні вимоги, що були висунуті внаслідок розрахунків мережі. Проведено моделювання в програмному середовищі Atoll, за його результатами можна стверджувати наступне: зона покриття мережі LoRa на частоті 900 МГц та 5 БС виявилася (більше 97% території з рівнем сигналу в діапазоні вище -120 дБм).

2. Час передачі пакетів по мережі LoRa, а також ємність мережі визначаються використовуваним для передачі коефіцієнтом розширення спектра, а в кінцевому підсумку - якістю сигналу мережі. Так, тривалість передачі одного up-link пакета з корисним навантаженням 10 байт при мінімальному коефіцієнті розширення спектра (SF = 7) складає 59,65мс, а при максимальному (SF = 12) - 1253,38мс. Додатково на ємність мережі LoRa впливатимуть такі фактори як: переповтори повідомлень, втрачених через помилки на радіоінтерфейсу і колізій; ефект множинного прийому при знаходженні клієнтських пристроїв в зоні дії декількох LoRa-шлюзів; використання другого вікна прийому (RX2).

5 СТАРТАП-ПРОЕКТ

5.1 Основні відомості про проект

Сутність стартап-проекту. Досліджуючи ринок мережевих дових технологій було виявлено можливість впровадження IoT рішень з використанням технології LoRa.

Зміст ідеї стартапу та визначення її характер бізнес-моделі стартапу наведено в табл. 5.1 та табл. 5.2.

Таблиця 5.1 – Зміст ідеї стартап-проекту

Зміст ідеї	**Напрямки застосування**	**Вигоди для користувача**
Оптимізаця вивозу сміття за допомогою встановлення сенсорів на сміттєві баки	1. «Розумне місто»	Покращення умов вивозу сміття

Таблиця 5.2 – Визначення бізнес-моделі стартапу

№ п/п	Варіанти бізнес-моделі стартапу	(потенційні) товари/концепції конкурентів		W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Запропонований метод	Загальновживаний метод			
1.	Продаж ліцензій на виготовлення продукту	Дає змогу	Дає змогу	-	Підтримка користувачів, оновлення ПЗ	Дозволяє отримувати прибуток на основі інтелектуальної власності без необхідності виробляти продукт
2.	Співпраця з операторами мобільного зв’язку (B2B)	Дає змогу	Не дає змогу	-	Потребує детального опрацювання усіх аспектів співпраці	Зменшення ризиків споживачів, пов'язаних з купівлею продукту/послуги
3.	Продаж ідеї стартапу	Дає змогу	Дає змогу	Відсутність подальшого розвитку	-	Відсутність будь-яких ризиків
4.	Створення повноцінного бізнесу	Не дає змогу	Не дає змогу	Потребує великих капіталовкладень	-	Можливість комерційної та дотаційної реалізації

Обрана бізнес-модель стартапу: B2B співпраця з іншими компаніями (операторами мобільного зв’язку та ЖКХ) з використанням існуючих мереж та обладнання [1].

5.2 Технологічний аудит ідеї стартап-проекту

У таблиці 5.3 оцінено можливість технологічної реалізації ідеї стартапу та показано технології, які можна застосувати для реалізації проекту.

Таблиця 5.3 – Технологічна здійсненність ідеї проекту

№ п/п	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Оптимізаця вивозу сміття за допомогою встановлення сенсорів на сміттєві баки	Спеціалізоване обладнання для організації сенсорної мережі	Наявне	Доступне
2		Використання існуючих стільникових мереж операторів мобільного зв’язку	Наявні	Доступні
3		Використання технології LoRa	Наявні	Відсутні на ринку в Україні

5.3 Аналіз можливостей ринку для запуску проекту

У таблиці 5.4 показано попередню характеристику потенційного ринку стартап-проекту.

Таблиця 5.4 – Попередня характеристика потенційного ринку стартапу

№ п/п	Показники ринку (найменування)	Характеристика
1	Якісна оцінка тенденцій ринку	Зростаюча
2	Кількість основних гравців, од	3
3	Обсяг продажів, грн/ум.од	295000
4	Середня норма рентабельності в цій галузі, %	295000/210000 = 140% висока
5	Специфічні вимоги до стандартизаціїї та сертифікації	Ліцензія
6	Обмежень для входу (характер обмежень)	Немає

У таблиці 5.5 показано характеристику потенційних клієнтів стартап-проекту.

Таблиця 5.5 – Характеристика потенційних клієнтів стартап-проекту

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у потребах потенційних цільових груп клієнтів	Вимоги споживачів до товару
2	Можливість своєчасного оповіщення, для запобігання накопиченню сміття	Житлово-комунальні послуги	Різні стандарти передачі даних	Забезпечення неперервної передачі даних

У табл. 5.6 наведено основні загрози реалізації стартап-проекту.

Таблиця 5.6 – Фактори загроз

№ п/п	Фактор	Опис загрози	Планове реагування компанії
1	Висока вартість реалізації	«Сміттєві» сенсори досить дорого коштують	Налагодження власного виробництва датчиків

У табл.5.7 наведено основні можливості під час реалізації стартап-проекту [1].

Таблиця 5.7 – Основні можливості

№ п/п	Фактор	Опис можливості	Планове реагування компанії
1	Лідерські позиції на ринку	Зростання попиту на товари та послуги	Збільшення обсягів виробництва продукту, якісна підтримка користувачів, регулярне оновлення ПЗ
2	Впровадження запропонованих технологій на існуючих стільникових мережах	Збільшення об’ємів закупівель	Якісне та кількісне збільшення обсягів виробництва продукту

У табл. 5.8 представлено сильні та слабкі сторони проекту.

Таблиця 5.8 – Порівняльний аналіз сильних та слабких сторін проекту

№ п/п	Фактор конкурентоспроможності	Бали 1-20	Порівняння рейтингу товарів-конкурентів						
			–3	–2	–1	0	+1	+2	+3
1	Якість	16				+			
2	Ціна	13				+			
3	Затребуваність	15						+	

ВИСНОВКИ

1. Всі прилади в Інтернеті речей з’єднуються між собою за допомогою мережних технологій. Bluetooth - це комунікаційна технологія короткого діапазону, інтегрована в більшість смартфонів і мобільних пристроїв, що є головною перевагою для особистих продуктів, зокрема одягу. Wi-Fi - це технологія безпроводового радіозв'язку пристроїв. Він пропонує швидку передачу даних і здатний обробляти великі обсяги даних. Супутникові мережі здатні передавати великі обсяги даних, але споживання енергії та витрати також високі. ZigBee - це безпроводова мережа з низькою потужністю і низькою швидкістю передачі даних, яка використовується в основному в промислових умовах. NFC дозволяє клієнтам підключатися до електронних пристроїв, використовувати цифровий вміст і здійснювати безконтактні платежі. Він працює на відстані до 4 см (між пристроями), дозволяючи пристроям обмінюватися інформацією. RFID використовує електромагнітні поля так, щоб ідентифікувати об'єкти. Короткочасна радіочастотна ідентифікація становить близько 10 см. Але далекобійна радіочастота може досягати 20 см.

2. В основі технології LoRa лежить однойменний метод модуляції, який був запатентований компанією Semtech. Цей метод ґрунтується на принципі розширення спектра і лінійної частотної модуляції. В процесі передачі дані кодуються широкосмуговими імпульсами з частотою, що зменшується або збільшується в певному часовому діапазоні. Дане рішення дозволяє зробити приймач стійким до відхилень частоти від номінального значення, що знижує вимоги до якості генератора і дозволяє використовувати прості кварцові резонатори.

3. LoRaWAN - відкритий протокол зв'язку, який визначає архітектуру системи. Цей протокол передбачає топологію типу «зірка». LoRaWAN розроблявся з метою організації зв'язку між недорогими пристроями, які можуть

працювати від батарей (акумуляторів). Для забезпечення прийнятного відносини швидкості передачі до енергоспоживання, протокол передбачає різні класи вузлів. Протокол LoRaWAN визначає конкретний набір швидкостей передачі даних, але реалізація фізичного рівня моделі OSI буде залежати від обраної мікросхеми.

4. Пропускна здатність (BW). Чим більша пропускна здатність, тим коротший ефірний час і нижча чутливість. Менша пропускна здатність також вимагає більшої чистоти, щоб мінімізувати проблеми, пов'язані з «дрейфом годинника». Фактор розповсюдження (SF). Для передачі інформації LoRa «розподіляє» кожен символ на декілька мікросхем (коефіцієнт розповсюдження), щоб ще більше підвищити чутливість приймача. Швидкість кодування (CR). Чим більше сплесків перешкод очікується, тим вища швидкість кодування, яку слід використовувати для максимізації ймовірності успішного прийому пакетів. Потужність передачі (TP). Як і більшість бездротових радіостанцій, приймачі LoRa також дозволяють регулювати потужність передачі, різко змінюючи енергію, необхідну для передачі пакета. Носійна частота (CF). Приймачі LoRa використовують для зв'язку частоти під ГГц: серед інших, промислові, наукові та медичні (ISM) діапазони 433 МГц, 868 МГц (Європа) та 915 МГц (Північна Америка). Загальні модулі LoRa, такі як Semtech SX1272 та HopeRF RFM95, підтримують зв'язок у діапазоні частот 860–1020 МГц і програмуються з кроком 61 Гц.

5. Проведено розрахунки сенсорної мережі з використанням технології LoRa. В результаті розрахунку встановлено, що для розгортання мережі на території 3.85 км^2 необхідно обрати 5 БС з радіусом стільника 550 м. Обладнання задовольняє необхідні технічні вимоги, що були висунуті внаслідок розрахунків мережі. Проведено моделювання в програмному середовищі Atoll, за його результатами можна стверджувати наступне: зона покриття мережі LoRa на

частоті 900 МГц та 5 БС виявилася (більше 97% території з рівнем сигнала в діапазоні вище -120 дБм).

6. Час передачі пакетів по мережі LoRa, а також ємність мережі визначаються використовуваним для передачі коефіцієнтом розширення спектра, а в кінцевому підсумку - якістю сигналу мережі. Так, тривалість передачі одного up-link пакета з корисним навантаженням 10 байт при мінімальному коефіцієнті розширення спектра (SF = 7) складає 59,65мс, а при максимальному (SF = 12) - 1253,38мс. Додатково на ємність мережі LoRa впливатимуть такі фактори як: переповтори повідомлень, втрачених через помилки на радіоінтерфейсу і колізій; ефект множинного прийому при знаходженні клієнтських пристроїв в зоні дії декількох LoRa-шлюзів; використання другого вікна прийому (RX2).

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Особливості впровадження технології NB-IoT операторами мобільного зв'язку. Дипломна робота / С. В. Єфіменко. – Київ, 2019.

2. Перспективи застосування технології LTE в межах концепції «розумного міста. Магістерська дисертація / П. О. Боковий. – Київ, 2019.

3. Internet of Things (IoT) URL: https://www.techopedia.com/definition/28247/internet-of-things-iot

4. Wu Mengdi. Wireless communiaction technologies in Internet of Things (IOT) - University of Vaasa, 2016

5. Internet of Things: Wireless Sensor Networks URL: https://www.ipwea.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=e0619c58-f639-080a-86c2-055ae9c8af4d

6. IoT Systems and Medium Range Radio Solutions URL: https://dzone.com/articles/iot-systems-and-medium-range-radio-solutions

7. Bluetooth. (2010). How it works URL: https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics/br-edr

8. GSMArena. (2016). Near Field Communication URL: http://www.gsmarena.com/glossary.php3?term=nfc

9. Перри Ли - Архитектура интернета вещей / пер. с анг. М. А. Райтмана- М.: ДМК Пресс, 2019.– 247-253с.

10. Обзор технологии LoRa | Технологии связи URL: https://itechinfo.ru/content/обзор-технологии-lora

11. What is LoRa? // Technology - MickMake - Live. Learn. Make. URL: https://www.mickmake.com/post/what-is-lora-technology/

12. Real Wireless Ltd. A Comparison of UNB and Spread Spectrum Wireless Technologies as Used in LPWA M2M

13. LoRa Alliance. LoRa: Wide Area Networks for IoT, 2017 URL: http://www.lora-alliance.org/ What-Is-LoRa/Technology

14. Bor, M.; Roedig, U.; Voigt, T.; Alonso, J.M. Do LoRa Low-Power Wide-Area Networks Scale? In Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), Valletta, Malta, 13–17 November 2016; pp. 59–67.

15. Bor, M.; Roedig, U. LoRa Transmission Parameter Selection. In Proceedings of the 13th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), Ottawa, ON, Canada, 5–7 June 2017.

16. Iova, O.; Murphy, A.L.; Ghiro, L.; Molteni, D.; Ossi, F.; Cagnacci, F. LoRa from the City to the Mountains: Exploration of Hardware and Environmental Factors. In Proceedings of the 2nd International Workshop on New Wireless Communication Paradigms for the Internet of Things (MadCom), Uppsala, Sweden, 20–22 February 2017.

17. Bor, M.; Vidler, J.; Roedig, U. LoRa for the Internet of Things. In Proceedings of the 1st International Workshop on New Wireless Communication Paradigms for the Internet of Things (MadCom), Graz, Austria, 15–17 February 2016; pp. 361–366.

18. Hope RF Microelectronics. RFM95/96/97/98(W)—Low Power Long Range Transceiver Module, v1.0; Hope RF Microelectronics: Shenzhen, China, 2016.

19. Semtech Corporation. SX1272/73—860 MHz to 1020 MHz Low-Power Long-Range Transceiver, Revision 3.1; Semtech Corporation: Camarillo, CA, USA, 2017.

20. Hope RF Microelectronics. RFM95/96/97/98(W)—Low Power Long Range Transceiver Module, v1.0; Hope RF Microelectronics: Shenzhen, China, 2016

21. Bannister, K.; Giorgetti, G.; Gupta, S.K. Wireless Sensor Networking for Hot Applications: Effects of Temperature on Signal Strength, Data Collection and

Localization. In Proceedings of the 5th International Workshop on Embedded Networked Sensors (HotEmNets), Charlottesville, VA, USA, 2–3 June 2008.

22. Boano, C.A.; Brown, J.; Tsiftes, N.; Roedig, U.; Voigt, T. The Impact of Temperature on Outdoor Industrial Sensornet Applications. IEEE Trans. Ind. Inform. 2010, 6, 451–459.

23. Boano, C.A.; Zúñiga, M.A.; Brown, J.; Roedig, U.; Keppitiyagama, C.; Römer, K. TempLab: A Testbed Infrastructure to Study the Impact of Temperature on Wireless Sensor Networks. In Proceedings of the 13th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), Berlin, Germany, 15–17 April 2014; pp. 95–106.

24. Емкость сети LoRa | Технологии связи URL: https://itechinfo.ru/content/емкость-сети-lora

Додаток А

РЕФЕРАТ
АНГЛІЙСЬКОЮ МОВОЮ ЗА ТЕМОЮ ДИПЛОМНОЇ РОБОТИ

ABSTRACT

LoRa Alliance developers believe that LoRa technology has significant advantages over WiFi and cellular networks, due to the ability to deploy machine-to-Machine (M2M) connections over a distance of up to 20 km at speeds up to 50 Kbps, and also has minimal power consumption providing several years of autonomous operation on one AA battery. The range of applications for this technology is great: from home automation and the Internet of Things to industry and smart cities.

LoRa is the next step in the development of the LPWAN solution, which was developed and patented by the Semetch Corporation. The essence of the technology boils down to a variation of chirp spread spectrum (CSS). The technology uses data coding with broadband pulses with frequencies that decrease or increase over a certain time interval. This solution allows the receiver to be robust against frequency deviations from the nominal value and simplifies the requirements for the clock generator, thereby allowing the use of inexpensive crystal resonators.

The system uses Forward Error Correction (FEC) and operates in the sub-gigahertz frequency range: 169, 433 and 915 MHz in the US, and in Europe in the 868 MHz range. The most commonly used operating frequencies are 868 and 915 MHz. Also, due to the high level of external influence, the operating range of 2.4 MHz is limited. According to the specification, LoRa (as well as SIGFOX) uses cyclically a single transmission option that limits the rate at which messages are generated. However, by supporting multiple channels, LoRa allows end nodes to participate in communications by changing the carrier frequency while respecting the duty-free cycle limit on each channel. The choice of data rate is a trade-off between coverage area and data volume, messages with different data rates do not interfere with each other. LoRa data rates range from 0.3 to 50 kbps. To maximize endpoint battery life and overall network bandwidth, LoRa's network infrastructure can control the baud rate for each device individually through adaptive baud rate.

While the LoRa implementation is proprietary, the rest of the protocol stack, known as LoRaWAN, remains open and is being developed by the LoRa Alliance, led by IBM.

A distinctive feature of the LoRa network is that it provides three classes of devices for solving various problems and applications in the network.

"Class A" defines the default functional mode in LoRa networks. In "class A" the communication session is carried out by the end device. The node transmits data in short bursts according to a specified schedule to the gateway. After each data transmission, the terminal opens one receiving window for a certain period of time, waiting for the next command sent by the server. If there is no response, the node goes into sleep mode, thereby reducing power consumption. The second window opens in a different sub-band (previously agreed with the server) in order to increase the stability against channel fluctuations. The server accumulates data and sends it as soon as the node connects. "Class A" networks are primarily intended for monitoring applications, they are the most energy efficient and the most common in practice.

In "class B" an additional reception window is allocated, which is opened by the device on schedule. On a special signal "beacon" from the gateway, the end device synchronizes the internal time with the network time, thereby making a schedule. Thus, thanks to this additional window, the server has the opportunity to start transferring data at a predetermined time.

Finally, "Class C" devices have a maximum, almost continuous receive window that closes only during data transmission. This allows them to be used to solve problems that require a large amount of data. This class of devices draws the most power, so it usually does not use battery power, but receives data from the network server with the least latency.

The end node (End-Node) is designed to implement control, monitoring and measurement functions. It contains a set of necessary sensors and control elements. They are usually battery powered. Nodes include data transmission only for a certain

period of time (usually 1–5 seconds), after which two time windows are opened for receiving data. The rest of the time, the end-node transceiver is either inactive or receiving, depending on the device class (A, B, or C).

A device that receives data from end devices using a radio channel and transmits it to the transit network - LoRa Gateway (Gateway / Concentrator). Transit networks can be Ethernet, WiFi, cellular networks and any other telecommunication channels. The gateway and end devices form a star network topology. Often this device contains multi-channel transceivers for processing signals in several channels at the same time or even several signals in one channel. Accordingly, multiple such devices provide network coverage and transparent bi-directional data transfer between end nodes and the server.

The Network Server is designed to manage the network: setting the schedule, adapting the speed, storing and processing the received data.

The Application Server can remotely monitor the operation of end nodes and collect the necessary data from them.

A LoRa network usually has a star topology in which devices are connected via LoRa gateways, which in turn are connected to a common network server (NetServer) via standard IP protocols.

In LoRaWAN, network nodes are not associated with a specific gateway. Each gateway forwards the received packets from end nodes to the cloud server of the network through some kind of transport (cellular, local area network, satellite or Wi-Fi Internet).

Gateways act as a kind of repeaters / bridges and simply forward to their associated NetServer all successfully decoded messages sent by any end device, after adding some information regarding the reception quality. NetServer is therefore responsible for filtering out duplicate and unwanted packets. Gateways are thus completely transparent to end devices that are directly logically attached to the NetServer. It is important that the current full-fledged LoRa gateway provides parallel

processing of up to 9 LoRa channels, where the channel is identified by a specific subband and spreading factor.

This mode greatly simplifies end-node network access control. In addition, end nodes can freely move through the network cells served by different gateways without creating any additional signaling traffic in the access network. Finally, there has been an increase in the number of gateways that serve certain endpoints, which can improve the reliability of the Netserver connection.

The content of each message can be up to 242 octets, compared to 12 for SIGFOX. Laura is better suited for applications that require high data rates (spread spectrum based protocol).

LPWAN is essentially different from the classic implementation of the device networking model. Experimental studies that have been carried out using LoRa technology have shown that LPWAN models should complement the existing IoT standards.

In LoRaWAN networks, the standard provides for mandatory two-level data encryption with two different AES-64 and 128 keys to protect against unauthorized access and distortion, or interception of data transmitted by terminal devices.