ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій

Кафедра телекомунікацій, медійних та інтелектуальних технологій

ДИПЛОМНА РОБОТА

Другий (Магістерський)
Освітній рівень

Галузь знань 17 Електроніка, автоматизація та електронні комунікації
Шифр і назва галузі

Спеціальність 172 Електронні комунікації та радіотехніка
Шифр і назва спеціальності

Освітня програма 172 Електронні інформаційно-комунікаційні системи та мережі
Шифр і назва освітньої програми

на тему: Метод конвергенції технологій IoT та LoRaWAN

ДРМЕКР 052023.01.05.ПЗ

Виконав: студент 2 курсу, група $ЕКР_м$-23-1 _____ А.С. Слободянюк
підпис Ініціали, прізвище

Керівник: к.т.н., доц. _____ О.С. Пивовар
підпис Ініціали, прізвище

До захисту допускаю:

Зав. кафедри: д-р техн. наук, проф. _____ С.К. Підченко
підпис Ініціали, прізвище

12 12 2024 р.

Хмельницький, 2024

Хмельницький національний університет
Факультет *інформаційних технологій*
Кафедра *телекомунікацій, медійних та інтелектуальних технологій (ТМІТ)*
Освітній рівень *другий (магістерський)*
Галузь знань *17 – Електроніка, автоматизація та електронні комунікації*
Спеціальність *172 – Електронні комунікації та радіотехніка*
Освітня-професійна програма *172 - Електронні інформаційно-комунікаційні системи та мережі*

ЗАТВЕРДЖУЮ
Зав. кафедрою ___ТМІТ___
_____С.К. Підченко
«__01__» __вересня_ 2024_р.

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Слободянюку Андрію Сергійовичу

1 Тема роботи: *Метод конвергенції технологій IoT та LoRaWAN*

Керівник роботи Пивовар Олег Сергійович, к.т.н, доцент.
Затверджено наказом по університету від « 26 » ____08____ 2024р. № 60.
2 Строк подання студентом роботи на кафедру:01.12.2024р.
3 Вихідні дані (характеристика об'єкта, умов дослідження та ін.)
Мета роботи: оптимізація використання технології LoRaWAN в умовах щільної міської забудудов .
Об`єктом дослідження є процес передачі інформації в електронних комунікаціях.
Предметом дослідження є методики використання програмно-технічних засобів для оптимізації застосування LoRaWAN для IoT .
4. Зміст пояснювальної записки (перелік питань, що їх належить розробити)
1. Аналіз систем передачі інформації із для інтернету речей. 2. Поняття моделі систем комунікацій для IoT та їх характеристик. 3. Методики удосконалення конвергенції технологій IoT та LoRaWAN . 4. Аспекти практичної реалізації розроблених методів та методик.
5. Графічна частина : *12 демонстраційних плакатів (слайдів).*

Завдання отримав_____А.С. Слободянюк

Науковий керівник_____О.С. Пивовар

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів (розділів) дипломної роботи	Строк виконання етапів дипломної роботи	Примітка
1	*Вибір тематики*	*до 5.09.24*	*обрано*
2	*Аналіз початкових даних*	*5.09. 24-14.09. 24*	*проаналізовано*
3	*Написання вступу*		
	та 1 розділу (аналіз)	*15.09. 24-30.09. 24*	*виконано*
4	*Написання 2 розділу*		
	(аналоги та моделі)	*1.10. 24-14.10. 24*	*виконано*
5	*Оформлення та подання*		
	публікацій	*10.10. 24-21.10. 24*	*подано*
6	*Написання 3 розділу*		
	(розробка моделей)	*15.10. 24-30.10. 24*	*виконано*
7	*Імітаційне моделювання та аналіз результатів*	*1.11. 24-14.11. 24*	*виконано*
8	*Обробка експериментальн.*		
	даних, оформлення графі-		
	чної частини (4 розділ)	*10.11. 24-21.11. 24*	*виконано*
9	*Оформлення текстової*		
	частини, синтез доповіді	*21.11. 24-30.11. 24*	*виконано*
10	*Виправленя зауважень, помилок ,підгтовка*		
	до захисту	*17.11. 24-24.11. 24*	*враховано*
11	*Антиплагіат та опонування*	*21.11. 24-1.12. 24*	*пройдено*
12	*Подання готового проекту*	*1.12. 24*	*виконано*

Здобувач ступеня магістр _____ 1.09.24 _____ А.С. Слободянюк
Підпис Ініціали, прізвище

Керівник роботи _____ 1.09.24 _____ О.С. Пивовар
Підпис Ініціали, прізвище

РЕФЕРАТ

Тема дипломної роботи: Метод конвергенції технологій IoT та LoRaWAN

Автор роботи: Слободянюк Андрій Сергійович

Керівник роботи: к.т.н., доцент, Пивовар О.С.

Пояснювальна записка: 88 с., 28 рис., 5 табл., 4 дод., 50 джерел.

Об'єктом дослідження є процес оптимізації взаємодії компонентів Інтернету речей за стандартом LoRaWAN. Предметом дослідження виступають моделі, удосконалений метод і програмно-технічні засоби оптимізації взаємодії компонентів Інтернету речей за стандартом LoRaWAN. Метою дипломної роботи є оптимізація взаємодії компонентів Інтернету речей за стандартом LoRaWAN.

Наукова новизна отриманих результатів полягає в наступному:

1) Удосконалено метод оптимізації взаємодії компонентів Інтернету речей за стандартом LoRaWAN. Відмінністю запропонованого методу є врахування таких параметрів, як модуляція та поширення сигналу, втрати при поширенні, втрати проникнення в будівлі, корельоване затінювання, чутливість приймача, фізичні перешкоди, особливості функціонування шлюзу. Це дозволило забезпечити високий рівень успіху доставки пакетів.
2) Розвинено програмно-технічні засоби для оптимізації взаємодії компонентів Інтернету речей за стандартом LoRaWAN, які сприяють ефективній доставці пакетів.

Практична цінність роботи полягає в розробці програмно-технічних засобів оптимізації, що забезпечують ефективну взаємодію компонентів Інтернету речей за стандартом LoRaWAN, а також у підвищенні рівня успішної доставки пакетів до високого рівня.

ABSTRACT

Thesis topic: Method of Convergence of IoT and LoRaWAN Technologies

Author: Andrii Serhiyovich Slobodianiuk

Supervisor: Ph.D., Associate Professor, Pivovar O.S.

Explanatory note: 88 pages, 28 figures, 5 tables, 4 appendices, 50 references.

The object of the research is the process of optimizing the interaction of Internet of Things components according to the LoRaWAN standard. The subject of the research includes models, an improved method, and software-hardware tools for optimizing the interaction of Internet of Things components based on the LoRaWAN standard. The goal of the thesis is to optimize the interaction of Internet of Things components based on the LoRaWAN standard.

The scientific novelty of the obtained results is as follows:

1) The method for optimizing the interaction of IoT components based on the LoRaWAN standard has been improved. The key feature of the proposed method is the consideration of parameters such as modulation, signal propagation, propagation losses, building penetration losses, correlated shadowing, receiver sensitivity, physical obstacles, and gateway functionality. This allowed for achieving a high level of packet delivery success.
2) Software-hardware tools for optimizing the interaction of IoT components based on the LoRaWAN standard have been developed, contributing to efficient packet delivery.

The practical value of the work lies in the development of software-hardware tools for optimization, ensuring effective interaction of IoT components according to the LoRaWAN standard, and in increasing the success rate of packet delivery to a high level.

ЗМІСТ

ВСТУП

У 2024 році технології Інтернету речей (IoT) продовжують стрімко розвиватися, впливаючи на різні сфери життя та економіки. Очікується, що сукупна кількість підключених пристроїв IoT у світі досягне 1,2 трильйона до початку 2025 року, з прогнозованим зростанням до 2,4 трильйона доларів США до 2030 року, що свідчить про річний 15% темп зростання протягом п’ятирічного прогнозованого періоду (2025-2030).

У США кількість "розумних будинків" у 2024 році становитиме до 70 мільйонів, з прогнозованим зростанням до 77 мільйона у 2025 році та 90 мільйонів у 2026 році. Прогнозується, що до 2025 року кількість підключених пристроїв перевищить 75 мільярдів у всьому світі, що значно вплине на функціонування бізнесових кіл та життя людей у побуді. Крім того, Інтернет речей має потенціал генерувати від $4 трлн до $11 трлн економічної вартості щороку.

У 2024 році очікується, що три мільярди пристроїв IoT будуть встановлені з eSIM, причому зростання сприятиме смартфонам разом із попитом на IoT.

Розвиток 5G мереж, штучного інтелекту та машинного навчання сприяє створенню інтелектуальних IoT-систем, що відкриває нові можливості для бізнесу та підвищує ефективність різних галузей.

Таким чином, технології IoT продовжують розширювати свої можливості, впливаючи на економіку та повсякденне життя, з прогнозованим значним зростанням кількості пристроїв та економічного ефекту в найближчі роки.

1 ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Технології IoT: Підключення Інтернету речей

Існують різноманітні архітектури для представлення роботи IoT-пристроїв. Проте, найпростіша модель складається з трьох рівнів, кожен з яких виконує окрему функцію, як зображено на рисунку 1.1:

1) Рівень сприйняття збирає інформацію з датчиків і управляє виконуючими механізмами.
2) Мережевий рівень забезпечує зв’язок між пристроями для обміну даними між собою або з централізованим приймачем.
3) Прикладний рівень займається зберіганням, інтерпретацією та використанням зібраної інформації.

Існує декілька ключових викликів, які повинні бути вирішені для ефективного функціонування IoT на мережевому рівні:

1) Масштабованість: Очікується, що щільність пристроїв досягне 60 тисяч на квадратний кілометр, що вимагає підтримки відповідних схем модуляції та доступу до середовища, а також динамічного налаштування параметрів мережі для максимальної ефективності.
2) Вартість: Щоб пристрої IoT були конкурентоспроможними, радіочіпи повинні бути доступними за ціною, як і підписка на мережу.
3) Тривалість роботи від батареї: Більшість IoT-пристроїв працюють на батареях, тому потрібно забезпечити автономну роботу на термін від 5 до 10 років на двох батарейках AA.
4) Обмежена обчислювальна потужність: Пристрої IoT мають прості процесори, що обмежує складність мережевих протоколів, які можуть використовуватися.
5) Глибоке покриття в приміщеннях: Пристрої повинні залишатися на зв’язку навіть у умовах слабкого сигналу, особливо для критичних додатків.

Хоча згадані вимоги є важливими, такі аспекти, як пропускна здатність і постійне підключення, не є вирішальними для IoT. Зокрема, не очікується, що пристрої будуть підтримувати високу пропускну здатність, а більшість з них не потребує постійного з’єднання, що дозволяє використовувати сплячий режим для збереження енергії.

Перш ніж масово впроваджувати мережевий протокол IoT, необхідно ретельно дослідити його здатність відповідати вищезгаданим вимогам. Наукова спільнота активно досліджує архітектуру мереж LPWAN для оцінки її життєздатності у масовому IoT. В цій роботі представлено нові результати моделювання мережі LoRaWAN, які показують її високу пропускну здатність порівняно з іншими протоколами без збільшення складності MAC.

Наразі є три основні категорії конкурентів у сфері IoT-мереж, кожна з яких має власні сильні та слабкі сторони. У підсумку, одна з архітектур, ймовірно, стане домінуючою у забезпеченні підключення пристроїв IoT.

1.1.1 Низькошвидкісні бездротові персональні мережі

Технології низькошвидкісної бездротової персональної мережі (LR-WPAN) створені для формування невеликих мереж, що з'єднують пристрої, які використовуються в домашніх умовах або належать одній особі. Ці мережі орієнтовані на передачу даних на короткі відстані з низькою швидкістю, що дозволяє ефективно використовувати енергію батареї.

Стандарт IEEE 802.15.4 забезпечує основи для рівнів PHY і MAC у цих мережах, надаючи базу для доповнення іншими стандартами, такими як 6LoWPAN, Z-Wave і Thread, які підтримують сітчасту топологію. Це дозволяє пристроям встановлювати багатошарові зв’язки для підвищення надійності. Однак використання вузлів як ретрансляторів обмежує їхню можливість переходити в сплячий режим, що підвищує витрати на енергію та додає обчислювальне навантаження. При цьому один вузол зазвичай

охоплює до 10 метрів з швидкістю передачі від 20 до 250 кбіт/с залежно від частотного діапазону. Ще один популярний стандарт — Bluetooth, особливо його версія з низьким енергоспоживанням (BLE), яка підтримує до 100 метрів дальності і швидкість передачі даних до 270 кбіт/с, що робить його схожим на IEEE 802.15.4.

1.1.2 Стільниковий Інтернет речей

Стандарти стільникового Інтернету речей (CIoT) використовують ліцензовані частоти та існуючу інфраструктуру стільникового зв'язку для підключення IoT-пристроїв. Це значно скорочує час і витрати на розгортання мережі. Основні стандарти CIoT включають EC-GSM, LTE-M і NB-IoT. EC-GSM використовує покращені можливості GPRS і EDGE для підтримки більшого діапазону і покриття з мінімальними вимогами до енергоспоживання. LTE-M використовує інфраструктуру LTE і має енергозберігаючі функції для збільшення терміну служби батареї. NB-IoT орієнтований на ультранизьку потужність і також використовує LTE-інфраструктуру. Очікується, що майбутні 5G-мережі розширять можливості CIoT.

1.1.3 Глобальні мережі малої потужності

LPWAN з'явилися як альтернатива для CIoT та LR-WPAN, враховуючи обмежений діапазон останніх і ранню стадію розвитку CIoT. LPWAN забезпечують з'єднання на великі відстані у неліцензованих суб-ГГц діапазонах, часто використовуючи топологію "зірка". Вони відрізняються високою енергоефективністю, що дозволяє пристроям працювати до 10 років на двох батарейках AA.

Серед основних стандартів LPWAN – Sigfox, який використовує ультравузьку смугу (UNB) для передачі даних, дозволяючи надсилати до 140 повідомлень на день у випадковому діапазоні частот. LoRa є іншим прикладом, що використовує технологію з розширеним спектром для

досягнення високої чутливості приймача. LoRaWAN забезпечує централізоване адміністрування мережі, спрощуючи підключення нових пристроїв. LoRa пропонує передачу на відстань до 20 км за рахунок зниженої швидкості, що дозволяє використовувати мережу навіть у сільській місцевості, де потрібне розширене покриття.

1.2 Модуляція LoRa

LoRa — це технологія рівня фізичного інтерфейсу (PHY), що використовує частотну модуляцію з розширеним спектром (CSS) і є запатентованою. Через це її модуляція описана лише частково у документах Semtech і LoRa Alliance [9, 10, 11]. Проте прогалини в офіційних даних були заповнені дослідженнями ентузіастів, які дослідили й навіть змогли реконструювати модуляцію. Найдетальніший аналіз CSS представлено в роботі [12].

1.2.1 Реалізація частотної модуляції з розширеним спектром LoRa

Метод CSS передбачає використання синусоїдального сигналу зі змінною частотою та сталою тривалістю для розширення інформації на ширший діапазон частот. Це забезпечує кращий захист від шуму та перешкод, хоча й знижує спектральну ефективність. Використання CSS також може підвищити стійкість до ефекту багатопроменевості й ефекту Доплера порівняно зі звичайними методами модуляції.

У LoRa початкова частота чирпу з доступного діапазону використовується для кодування символу [13]. Кількість бітів, які модуляція LoRa може закодувати в один символ, визначається параметром SF, який дозволяє кодувати 2^SF біт на символ. Це збільшує варіативність початкових частот чирпів, що підвищує час передачі символу та стійкість сигналу до перешкод, хоча одночасно збільшує ймовірність помилок через зсув синхронізації між передавачем і приймачем.

Збільшення коефіцієнта SF також подвоює час, потрібний для передачі

кожного символу, що підвищує захист від шуму, але водночас підвищує ймовірність зіткнень під час передачі сигналів.

Через вищезазначені причини вибір коефіцієнта розповсюдження SF безпосередньо впливав на чутливість приймача, яка визначалася за наступним рівнянням:

$$S = -174 + 10 \log10(A) + N + SN \text{ дБ},$$

У цьому рівнянні перший член визначався тепловим шумом приймача на 1 Гц смуги пропускання, N — показник шуму приймача, який залишався фіксованим для конкретного апаратного забезпечення, а SN — відношення сигнал/шум, необхідне для базової схеми модуляції.

Таблиця 2.1 демонструє значення SN для різних коефіцієнтів розповсюдження, де видно, що збільшення коефіцієнта розширення сприяло підвищенню чутливості.

12	25	50
68	13	27
39	78	15
21	43	87
12	24	48
67	13	26
36	73	14

На основі рівняння (2.1) було визначено бітрейт для певної комбінації SF та смуги пропускання A за наступною формулою:$Ra=SF/Ms$.

В таблиці 1.2 представлено бітрейт [біт/с] для ряду коефіцієнтів розповсюдження та значень смуги пропускання, що дозволяє оцінити ефективність передавання даних при різних параметрах.

1.2.2 Пакети фізичного рівня LoRa

Приклад пакету LoRa було продемонстровано на рисунку 1.1, де показано спектрограму з часом на горизонтальній осі та частотою на вертикальній. У повідомленні LoRa рівня PHY складалися частотні сигнали, які розгортали смугу частот. Після кількох повторень цих частотних розгорток, що утворювали преамбулу (мінімальна довжина якої становила 4,25 сигналів), дані кодувалися у сигналі через миттєві зміни частоти або їхню відсутність.

Метод декодування було описано в [13] і складався з "де-чірпування" сигналу з подальшим швидким перетворенням Фур'є (FFT), використовуючи кількість бінів, яка дорівнювала кількості символів M, що відповідала вибраному коефіцієнту розширення. Рисунок 1.2 ілюструє

версію передачі LoRa після де-чірпування, де, аналогічно, час показано на горизонтальній осі, а частоту на вертикальній. Такий сигнал інтерпретували як промодульований багаточастотною маніпуляцією (MFSK). Виконуючи кілька перекриваючих БПФ і аналізуючи корзину з найвищим рівнем потужності, у кожному часовому кадрі можна було визначити відповідний символ.

Рисунок 1.1 Спектрограмне представлення сигналу LoRa [13]

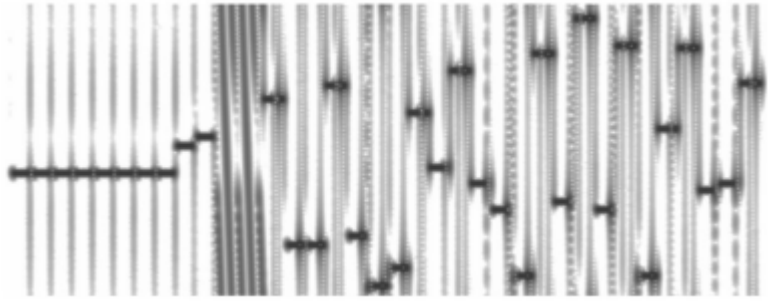


Рисунок 1.2 Версія сигналу LoRa

Крім самої модуляції, LoRa також визначала набір операцій кодування, які застосовувалися перед модуляцією та передачею:

1) Відбілювання даних використовувалося для зменшення ймовірності появи довгих однакових бітів у даних. Відбілювання також сприяло розподілу інформації по всій пропускній здатності радіоканалу. Зазначено, що в [13] виявлено, що послідовності відбілювання, зазначені в [14], відрізнялися від фактичної версії, реалізованої в чіпах, але правильну послідовність відбілювання вдалося знайти.

2) Пряме виправлення помилок (FEC) було реалізовано у вигляді коду

Хеммінга. Довжина інформаційного слова коду фіксувалася на рівні 4 бітів, а довжина кодового слова була настроюваним параметром у діапазоні [5, 8] бітів. Таким чином, швидкість коду для пакета LoRa дорівнювала

$C \in \{4/5, 4/6, 4/7, 4/8\}$.

3) Перемежування змінювало вихід FEC, щоб зробити код більш стійким до спалахів помилок. У роботі [13] зворотною інженерією було визначено, що LoRa використовує діагональний перемежувач, при цьому два найбільш значущі біти змінено.

4) Відображення сірого застосовувалося для відображення блоку бітів

SF у символи K у сукупності, що забезпечувало відмінність двох сусідніх

символів не більше ніж на 1 біт для підвищення шансів виправлення помилок каналом.

Час в ефірі пакета було розраховано за формулою [9].

$$t_{packet} = t_{preamble} + t_{payload} \tag{1.4}$$

де $t_{preamble}$ — це час, необхідний для передачі преамбули, а $t_{payload}$ — час передачі фактичних даних. Ці дві сутності виражалися наступними формулами:

$$t_{preamble} = (n_{preamble} + 4.25) \cdot ts, \tag{1.5}$$

$$t_{payload} = n_{payload} \cdot ts, \tag{1.6}$$

Таким чином, загальна кількість символів корисного навантаження $n_{payload}$, може бути визначена через наступне рівняння:

$$n_{payload} = 8 + \max\left(\left\lceil \frac{8PL - 4SF + 44 - 20H}{4(SF - 2DE)} \right\rceil (CR + 4), 0\right) \quad (1.7)$$

де:

PL – розмір корисного навантаження в байтах, що включає всі необхідні дані пакета;

H – індикатор, чи використовується заголовок PHY. Якщо заголовок увімкнений (H=1), пакет містить додаткові дані про довжину, необхідні для його декодування, що збільшує час передачі, але дозволяє адаптувати розмір пакету без необхідності попереднього узгодження. Якщо заголовок вимкнений (H=0), це економить час в ефірі, однак передавач і приймач повинні бути узгодженими щодо тривалості пакета;

DE – прапорець оптимізації низької швидкості передачі даних. Якщо DE=1, увімкнено захист від зсуву годинника, що є важливим для передачі на низьких швидкостях і тривалих символів, а також зберігає коректну синхронізацію між передавачем і приймачем. Якщо DE=0, ця оптимізація не використовується, що трохи зменшує час передачі, але робить передачу менш стійкою до дрейфу годинника;

CR – кількість доданих бітів парності, що дозволяють підвищити надійність передачі, адже більш високий коефіцієнт корекції помилок CR збільшує кількість переданих символів, що підвищує шанси успішної декодування, але при цьому збільшує загальний час передачі.

Ця формула дозволяє чітко оцінити кількість символів для передачі

корисного навантаження, залежно від параметрів пакета. Збільшення довжини символів і додаткових параметрів призводить до збільшення $n_{payload}$, а отже, і до збільшення часу передачі $t_{payload}$.

1.2.3 Ортогональність коефіцієнта поширення

Однією з ключових переваг модуляції LoRa є те, що різні коефіцієнти розповсюдження (SF) мають псевдоортогональність. Це означає, що передавачі, які використовують різні SF, можуть передавати дані на одній і тій самій центральній частоті та в одній смузі пропускання без значного впливу один на одного. Завдяки цьому одержувач може коректно декодувати пакет із SF = i навіть тоді, коли пакет із SF = j передається

одночасно (за умови, що $i \neq j$) і рівень сигналу/перешкоди та шуму (SINR)

отриманого пакету перевищує необхідний поріг. Цей поріг залежить від пар SF, що беруть участь у передачі, і називається «ізоляцією» між коефіцієнтами розповсюдження.

Завдяки псевдоортогональності мережі LoRa можуть одночасно підтримувати кілька передач з різними коефіцієнтами розповсюдження. Це підвищує загальну пропускну здатність мережі, оскільки в традиційних модуляціях подібні ситуації призвели б до збоїв або втрати пакету через колізії сигналів. Дослідження в [15] вивчали питання ізоляції, використовуючи модель LoRa, що дозволило оцінити рівень необхідного запасу ізоляції для кожної пари SF, аби забезпечити стабільність одночасної передачі.

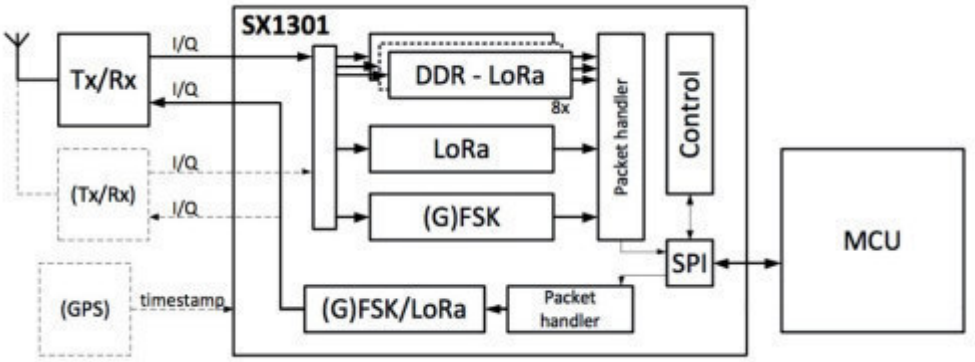


Рисунок 1.3 - Логічна схема для мікросхеми SX1301 [15]

1.2.4 Основні мікросхеми Semtech і незалежні реалізації

Через патентованість технології LoRa комерційні мікросхеми, що реалізують її модуль, доступні лише від корпорації Semtech. Вона пропонує два основні типи радіочіпів LoRa: базові моделі SX1272 і SX1273, які призначені для простих пристроїв LoRa, а також модель SX1301. Остання здатна одночасно декодувати пакети на різних частотах, що робить її оптимальним вибором для використання в агрегаційних точках (концентраторах), які можуть приймати передачі від мережі простіших LoRa-пристроїв.

Приймач SX1301, як показано на рисунку 1.3, містить 8 паралельних приймальних каналів, здатних працювати з динамічною швидкістю передачі даних (DDR). Завдяки цьому чіп може одночасно декодувати кілька пакетів, використовуючи різні коефіцієнти розповсюдження та центральні частоти, забезпечуючи правильне декодування завдяки псевдоортогональності між SF, що дозволяє розрізняти пакети, які надходять одночасно до антенипів Semtech, в останні роки з’явились проекти програмно-визначеного радіо (SDR), які дозволяють відтворювати відкриту архітектуру рівня LoRa PHY. Найбільш помітні з них – [16] і [17], які використовують GNU Radio SDK [18]. Такі відкриті реалізації, створені дослідниками та ентузіастами, дають змогу не тільки аналізувати модуляцію, але й шукати можливості її вдосконалення та виявляти потенційні вразливості безпеки.

1.3 Стандарт LoRaWAN

Хоча рівень LoRa PHY є власністю, вищий рівень протоколу, відомий як LoRaWAN, є відкритим та стандартизованим. Специфікації LoRaWAN надані в документі LoRa Alliance [11] — групою, яка об'єднує постачальників і дослідницькі установи, що прагнуть популяризувати та впроваджувати LoRa.

LoRaWAN забезпечує управління мережею, механізми аутентифікації пристроїв, а також управління енергоспоживанням, що дозволяє ефективно застосовувати пристрої LoRa в мережах Інтернету речей (IoT). Протокол описує типові для нього компоненти, серед яких кінцеві пристрої (End Devices), шлюзи (Gateways), сервери мережевого рівня (Network Servers) та сервери додатків (Application Servers). Окрім того, для ефективної роботи LoRaWAN визначено частотні діапазони для різних регіонів світу. Це дозволяє адаптувати роботу мереж відповідно до місцевих вимог, забезпечуючи надійний та інтероперабельний зв'язок в різних країнах.

1.3.1 Топологія та класи пристроїв

Мережі LoRaWAN використовують топологію "зірка-зірка", в якій кінцеві пристрої (ED) передають та приймають повідомлення бездротово через один або кілька шлюзів (GW). Шлюзи, у свою чергу, передають ці повідомлення на централізований мережевий сервер (NS) через надійне високошвидкісне з'єднання. Такий підхід дозволяє пристрою ED надсилати повідомлення одночасно кільком шлюзам, що підвищує ймовірність доставки.

При цьому ED не прив'язані до конкретного шлюзу, а надсилають повідомлення через бездротовий канал з розрахунком, що принаймні один шлюз зможе отримати їх і передати на NS. На рівні централізованої системи сервер обробляє можливі дублікати повідомлень, обираючи найбільш оптимальний шлюз для відправки відповідей на ED.

Для забезпечення надійності мережі, LoRaWAN використовує декілька логічних каналів, де кожен пристрій, що передає пакет, обирає канал

псевдовипадковим чином, що дозволяє зменшити ймовірність виникнення конфліктів між передачами.

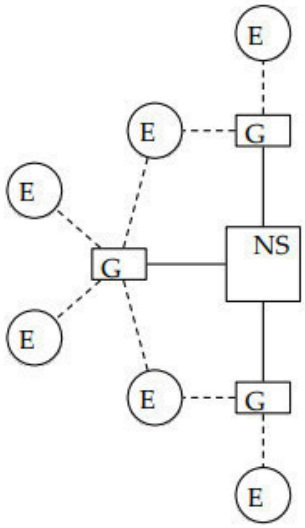


Рисунок 1.4 – Зразок топології мережі LoRa [15]

На рисунку 1.5 представлено стек протоколів для кінцевих пристроїв (ED), шлюзів (GW) та мережевого сервера (NS). Кінцеві пристрої та мережевий сервер мають повноцінний прикладний рівень, що дозволяє їм обробляти дані та виконувати конкретні завдання. Шлюзи, на відміну від них, не виконують обробки прикладного рівня, а натомість виступають прозорим проміжним вузлом, який забезпечує пересилання повідомлень між ED та NS.

Ця архітектура робить шлюзи повністю прозорими для програм кінцевих пристроїв, які взаємодіють із NS, минаючи шлюз. Таким чином, логічна взаємодія відбувається безпосередньо між ED і NS, що дозволяє зберегти структуру обміну простою та ефективною.

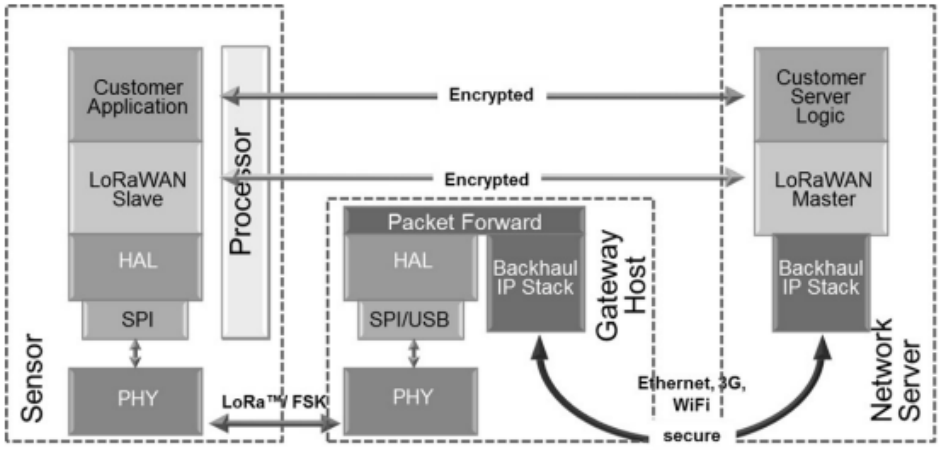


Рисунок 1.5 – Стеки протоколів різних пристроїв у LoRaWAN [15]

Згідно з [11], кінцеві пристрої LoRa можуть працювати в одному з трьох основних режимів — класах A, B або C, що відповідають різним вимогам до енерговитрат і типу зв'язку:

Клас A — це режим за замовчуванням для всіх LoRa-пристроїв. Пристрої цього класу передають дані в асинхронному режимі, використовуючи метод доступу Aloha MAC. Після кожної передачі вгору (до мережевого сервера, NS), пристрій відкриває два короткі вікна для отримання можливих відповідей. Перше вікно працює на тій же частоті, що й висхідний канал, тоді як друге відкривається на іншому каналі, узгодженому з NS. Цей клас оптимальний для пристроїв з обмеженим енергоспоживанням, оскільки більшу частину часу приймач залишається вимкненим.

Клас B — пристрої цього класу синхронізуються з мережевим сервером за допомогою періодичних маяків, що транслюються шлюзами. Завдяки цьому синхронізованому режиму вони можуть приймати пакети в строго визначені проміжки часу, незалежно від передачі даних у висхідному каналі. Це зручно для пристроїв, які потребують регулярного керування (наприклад, перемикачів або виконавчих механізмів), але також повинні зберігати енергію.

Клас C — підходить для пристроїв без обмежень на енергоспоживання, наприклад, живлених від електромережі. Приймачі в цьому режимі залишаються постійно увімкненими, готовими до негайного отримання команд по низхідній лінії зв'язку, що забезпечує мінімальні затримки в комунікації. Цей клас використовується для пристроїв, яким потрібна постійна готовність до прийому команд з низькою затримкою.

Ці класи забезпечують гнучкість LoRaWAN, дозволяючи пристроям підлаштовуватися під різні потреби в енергоспоживанні та продуктивності зв’язку.

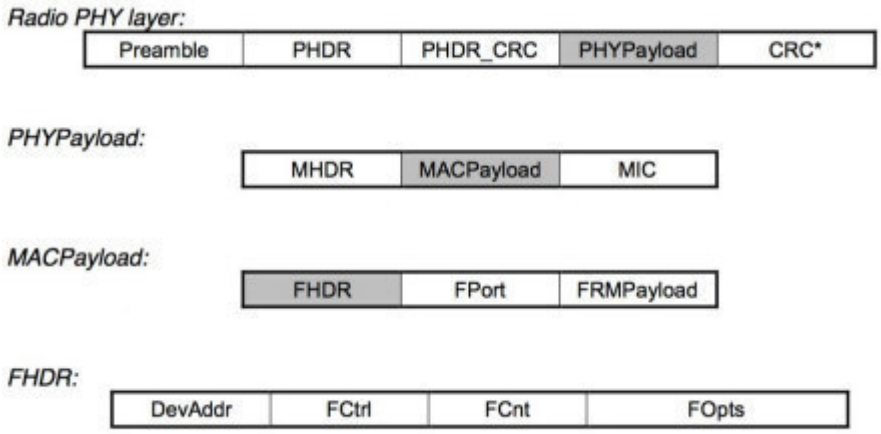


Рисунок 1.6 – Структура пакетів повідомлення LoRaWAN [11]

1.3.2 Структура пакетів і команди MAC

LoRaWAN протокол зв'язку, як зазначено в [11], включає в себе детальну структуру форматів пакетів на рівнях PHY і MAC, а також параметри, що налаштовуються для кожного кінцевого пристрою. Структура повідомлення LoRaWAN на рівні PHY складається з преамбули, заголовка, корисного навантаження і двох CRC-кодів для захисту як заголовка, так і корисного навантаження від помилок передачі. Рівень PHY передбачає важливі функції, що забезпечують стабільність передачі та сумісність з різними

пристроями мережі. Усередині рівня PHY заголовок MAC забезпечує інформацію про версію стандарту, який використовує пристрій, та тип повідомлення. Виділяють кілька типів повідомлень:

1) Пакети приєднання – це первинні пакети, які надсилає пристрій під час спроби приєднатися до мережі. Вони дозволяють пристроям зареєструватися в мережі і отримати доступ до її функцій.

2) Повідомлення даних можуть передаватися як у висхідному, так і в низхідному каналах. Це основні пакети для передачі даних між кінцевими пристроями і мережею. Повідомлення може містити опцію підтвердження, що дозволяє перевірити коректність доставки та ініціювати повторну передачу у разі втрат.

3) Власні повідомлення – передбачають нестандартні формати передачі даних. Ці повідомлення можуть передавати специфічні дані між пристроями, що підтримують особливі, додаткові розширення, які необхідні для конкретних завдань або додатків.

Корисне навантаження MAC, яке передається разом з пакетом, містить корисне навантаження Frame, порт Frame і заголовок Frame. Корисне навантаження Frame зазвичай містить дані з прикладного рівня. Поле порту Frame використовується для того, щоб визначити, для якої програми призначене повідомлення, а тому забезпечує пряме маршрутизацію в межах прикладного рівня. Деякі значення портів Frame зарезервовані для стандартизованих розширень, які будуть додані в майбутньому. Frame Header має різні поля, що забезпечують ідентифікацію пристрою в мережі LoRa. Основні поля цього заголовка включають:

1) 4-байтну коротку адресу пристрою, яка використовується для унікальної ідентифікації кожного пристрою в межах мережі. Це

дозволяє чітко відслідковувати та ідентифікувати окремі кінцеві пристрої.

2) Поле керування кадром (1 байт), яке призначене для розміщення бітів підтвердження (ACK) та бітів кадру. Це поле забезпечує управління процесом передачі даних і підтримує належну координацію між кінцевими пристроями та мережею.

3) Біти для функції ADR (2 біти), що дозволяють адаптивне регулювання швидкості передачі даних (ADR). Це поле дозволяє NS змінювати коефіцієнт розширення (SF), який використовується кінцевим пристроєм, для забезпечення стійкості з'єднання. Алгоритм ADR має можливість збільшувати SF у випадку низького сигналу або зменшувати його для зниження енергоспоживання, якщо зв'язок стабільний. Ця адаптація також знижує час в ефірі та зменшує можливість конфліктів передачі.

Варто зазначити, що ADR алгоритм у LoRaWAN не є стандартизованим, що дає можливість реалізації різних підходів з різною ефективністю та складністю, котрі можуть бути налаштовані відповідно до потреб конкретної мережі. Якщо біт ADR активовано, пристрій знає, що його швидкість передачі даних контролюється NS і що додаткові інструкції можуть міститися в полі FOpts.

Команди MAC, які передаються між кінцевим пристроєм (ED) та мережевим сервером (NS), виконують широкий спектр функцій, зокрема:

1) Перевірка зв'язку – дозволяє пристрою перевірити якість з'єднання з мережею, при цьому NS відповідає даними про рівень сигналу.

2) Запити та відповіді ADR – дозволяють керувати швидкістю передачі даних, знижуючи або підвищуючи коефіцієнт розширення,

що дозволяє підтримувати стабільний сигнал.

3) Робочий цикл – обмежує загальний час передачі пристрою, дозволяючи контролювати використання смуги пропускання та знижувати навантаження на мережу.

4) Налаштування параметрів прийомних вікон – дозволяє регулювати час відкриття вікон прийому, що забезпечує точний прийом даних в низхідному каналі.

5) Запит про стан пристрою – NS може отримати інформацію про рівень заряду батареї та параметри якості сигналу кінцевого пристрою, що дозволяє відстежувати його працездатність та надійність з'єднання.

6) Створення нових каналів – дозволяє мережевому серверу збільшити кількість радіоканалів для передачі, що забезпечує більшу гнучкість у масштабуванні мережі.

Крім зазначених команд, у протоколі передбачено ще 128 зарезервованих ідентифікаторів команд, які можуть використовуватися для реалізації власних, розширених функцій та налаштування мережі відповідно до вимог користувача або специфіки додатку. Цей гнучкий набір функцій і команд дозволяє мережам LoRaWAN забезпечувати високу масштабованість, надійність та адаптивність під різні умови та вимоги застосування.

1.3.3 Шифрування та активація пристрою

У відповідності до [11], коли кадр даних у мережі LoRaWAN містить корисне навантаження, це навантаження обов'язково підлягає шифруванню

для забезпечення конфіденційності та захисту від несанкціонованого доступу. Для цього в LoRaWAN використовується алгоритм шифрування AES (Advanced Encryption Standard), який є широко застосовуваним у багатьох бездротових технологіях, включаючи стандарт IEEE 802.15.4 [19]. Окрім шифрування, для перевірки цілісності повідомлення використовується код цілісності повідомлення (MIC, Message Integrity Code), що дозволяє виявляти будь-які спроби маніпуляцій з пакетом даних під час його передачі. Це забезпечує додатковий рівень безпеки, оскільки навіть якщо зловмисник намагатиметься змінити вміст зашифрованого повідомлення, приймач зможе виявити порушення цілісності завдяки некоректному MIC.

Для здійснення шифрування та забезпечення автентичності даних LoRaWAN використовує два різних ключі, залежно від типу повідомлення та порту кадру, на який воно орієнтоване. Це можуть бути:

1) Ключ мережі – використовується для шифрування повідомлень, що стосуються загальних мережевих операцій.
2) Ключ програми – застосовується для шифрування даних, пов'язаних із конкретними додатками, які використовують мережу LoRaWAN.

Обидва ці ключі отримуються кінцевим пристроєм (ED) під час процедури активації, яка є необхідною для підключення пристрою до мережі LoRaWAN. Під час активації пристрій також отримує 32-байтову адресу, яка є унікальним ідентифікатором пристрою в мережі, а також ідентифікатор програми, що дозволяє коректно спрямовувати дані до відповідних додатків.

LoRaWAN пропонує два основні методи активації пристроїв, що визначають, як вони отримують ключі та доступ до мережі:

1) Over-The-Air Activation (OTAA) – цей метод передбачає

активацію пристрою через серію безпечних повідомлень з мережею (NS), у ході яких пристрій отримує ключ мережі. Активування відбувається через ефір, що забезпечує високий рівень безпеки, оскільки ключі передаються безпечним чином. OTAA є найбільш рекомендованим способом активації через свою безпеку та гнучкість у розгортанні пристроїв.

2) Activation By Personalization (ABP) – при цьому методі пристрій вже має попередньо налаштовані параметри, такі як мережеву адресу та ключі, що дозволяє йому одразу підключатися до мережі без необхідності обміну повідомленнями з мережею. ABP простіший, але має менший рівень безпеки, оскільки ключі передаються на етапі налаштування і не змінюються після того, як пристрій підключений до мережі.

Обидва методи мають свої переваги та обмеження в контексті безпеки та зручності використання. OTAA зазвичай використовується для більш безпечних і масштабованих сценаріїв, оскільки ключі можуть бути знову змінені за допомогою механізмів LoRaWAN, що дозволяє пристроям адаптуватися до змін у мережі. Водночас ABP підходить для простих додатків, де не потрібна висока безпека або великий масштаб.

1.3.4 Діапазони частот

У [11] визначено три основні регіони, в яких очікується використання LoRaWAN, зокрема в Європі, Китаї та Сполучених Штатах. Кожен з цих регіонів має свої особливості, що визначають частоти та інші параметри мережі, відповідно до місцевих законодавчих вимог. Це включає налаштування параметрів, таких як:

1) Частоти каналів, що використовуються для передачі даних.

2) Преамбула, яка є частиною пакету на рівні PHY і допомагає у синхронізації передачі.
3) Дозволені коефіцієнти поширення (spreading factors), що визначають швидкість передачі даних і дальність покриття мережі.
4) Максимальний розмір корисного навантаження, що дозволяє оптимізувати використання спектра та забезпечити ефективну передачу даних.
5) Вікна прийому, які визначають періоди часу, коли кінцеві пристрої будуть відкривати приймач для отримання даних.
6) Процедури приєднання, що гарантують, що пристрої можуть безпечно підключитися до мережі в межах регіону.

Ці налаштування допомагають переконатися, що LoRaWAN відповідає місцевому законодавству та оптимально працює в кожному з регіонів.

Крім того, зазначено, що всі частотні діапазони, які використовуються для LoRaWAN, знаходяться в діапазоні 780–930 МГц, що є важливою перевагою. Вибір цього діапазону частот є більш ефективним для LPWAN (Low Power Wide Area Network) у порівнянні з іншими частотами, такими як 2,4 ГГц і 5 ГГц, що використовуються, наприклад, у стандартах IEEE 802.11. Це зумовлено тим, що частоти в діапазоні 780–930 МГц зазнають менше загасання сигналу, що дозволяє досягти кращого покриття на великих відстанях і знижує вимоги до потужності передавачів. Таким чином, використання цих частот забезпечує стабільніше і більш ефективне покриття мережі, що є критичним для досягнення широкої зони обслуговування в рамках LPWAN технологій.

1.4 Висновки

У даному розділі було проведено детальний аналіз та дослідження технологій Інтернету речей (IoT), зокрема, LPWAN і LoRa, а також

виокремлено вимоги до IoT для ефективного функціонування. Розділ охоплює основні питання, пов'язані з проектуванням та оптимізацією взаємодії компонентів IoT, їх продуктивністю та здатністю до масштабування. Виявлені як переваги, так і недоліки існуючих рішень.

Огляд технологій IoT включає різноманітні рішення для підключення до Інтернету речей, зокрема:

1) Низькошвидкісні бездротові персональні мережі (LPWAN).
2) Стільниковий Інтернет речей (Cellular IoT).
3) Глобальні мережі малої потужності (Low Power Wide Area Networks).

Розділ також аналізує основні аспекти функціонування IoT, такі як:

1) Модуляція LoRa та її реалізація.
2) Структура пакетів фізичного рівня LoRa.
3) Основні мікросхеми Semtech і незалежні реалізації.

Зокрема, розглянуто принцип роботи стандарту LoRaWAN, що включає:

1) Топологію мережі та класи пристроїв.
2) Структуру пакетів і команди MAC.
3) Механізми шифрування та активацію пристроїв.
4) Частотні діапазони, що використовуються в LoRaWAN.

Було зроблено висновок, що задача проектування та оптимізації взаємодії компонентів Інтернету речей за стандартом LoRaWAN є надзвичайно актуальною в контексті розвитку сучасних технологій IoT. Це підкреслює необхідність розроблення удосконалених методів оптимізації для досягнення максимальної ефективності та масштабованості IoT рішень на базі LoRaWAN.

2 МОДЕЛЮВАННЯ КОМПОНЕНТІВ МЕРЕЖІ LORAWAN

Для вирішення задачі оптимізації взаємодії компонентів Інтернету речей за стандартом LoRaWAN необхідно розробити відповідну модель мережі LoRa, яка буде обчислювально життєздатною. Однак для досягнення цієї мети слід зробити ряд припущень і спрощень, щоб забезпечити ефективність моделювання без надмірної складності. Щодо інших інструментів для моделювання на системному рівні, таких як симулятор Vienna Long Term Evolution (LTE) [20-23], дослідження виконано з використанням двох основних компонентів, які сприяють спрощеному відображенню фактичного ланцюга передачі.

Перша компонента — модель вимірювання лінії зв'язку — використовується для абстрагування впливу поширення сигналу на його силу. Вона також дозволяє врахувати дрібномасштабні загасання та інші ефекти, які можуть впливати на якість зв'язку. Така модель дозволяє отримати більш узагальнене уявлення про силу сигналу в різних умовах поширення, зокрема в реальних мережах LoRaWAN, де поширення сигналу може бути значно змінним.

Друга компонента — модель продуктивності лінії зв'язку — визначає ймовірність успішного отримання пакету даних. Вона здійснює розрахунки на основі зниженої складності, використовуючи лише інформацію про потужність каналу, рівень перешкод і інші ефекти, що виникають на системному рівні. Така модель дозволяє передбачити ефективність передачі даних в мережі, зокрема у контексті LoRaWAN, де взаємодія між компонентами може бути значною мірою залежною від різних зовнішніх факторів.

У наступному розділі цієї глави буде проведено дослідження того, як мережі LoRa були модульовані та змодельовані в науковій літературі. Після цього буде надано більш детальне пояснення кожної з двох згаданих

моделей, із фокусом на їх компоненти, та надано зрозуміле пояснення їхнього застосування для розробки оптимізаційних стратегій в мережах LoRaWAN.

2.1 Аналіз компонентів мережі LoRa

Одним із ключових аспектів, що визначають ефективність мережі LoRa, є система модуляції. Вона відіграє вирішальну роль у забезпеченні стабільності і надійності зв'язку, особливо у таких умовах, коли мережі IoT працюють в умовах високих перешкод або в складних середовищах. Для оптимізації взаємодії компонентів Інтернету речей за стандартом LoRaWAN важливо враховувати вплив різних факторів на функціонування мережі, зокрема:

1) Перешкоди – Мережі LoRa можуть працювати в умовах значних перешкод, тому розміщення кінцевих вузлів (ED) у певному середовищі є важливим для оцінки ефективності декодування приймачами LoRa. Це включає вплив на пропускну здатність каналу, можливість втрат пакетів через перешкоди або інші фізичні бар'єри.

2) Чутливість та дальність дії пристроїв LoRa – Один із важливих аспектів – це чутливість приймачів та їх здатність передавати сигнали на великі відстані. Дальність передачі даних у мережах LoRa залежить від кількох чинників, включаючи коефіцієнт поширення, потужність передавача, тип антен, а також умови навколишнього середовища (наприклад, вплив вітру, перепади температури або фізичні перешкоди).

3) Втрати пакетів через ефект захоплення – Один з важливих моментів у мережах LoRa – це ефект захоплення (capture effect). Коли

два пакети з однаковим коефіцієнтом розширення SF (спектральний фактор) передаються одночасно, лише один з них може бути демодульований приймачем. Якщо один пакет приходить до приймача з трохи більшою потужністю, ніж інший, то лише цей пакет буде успішно декодований, а інший буде втраченим. Це може стати серйозною проблемою в мережах з високим трафіком, оскільки навіть незначні відхилення в потужності сигналу можуть призвести до значних втрат даних.

На рисунку 2.1 можна побачити ймовірність виникнення певної події для різних зміщень при передачі "сильного" сигналу відносно "слабкого". Цей графік демонструє, як зміщення в потужності сигналу впливає на ймовірність успішного декодування одного з пакетів в умовах одночасних передач. Подібні ситуації є дуже важливими для налаштування параметрів мережі, зокрема для вибору оптимальних значень SF і визначення відповідних значень потужності передавачів для зниження втрат пакетів.

Врахування таких факторів, як перешкоди, чутливість пристроїв і ефект захоплення, дозволяє оптимізувати взаємодію компонентів у мережах LoRaWAN і забезпечити стабільну роботу таких систем навіть у складних умовах.

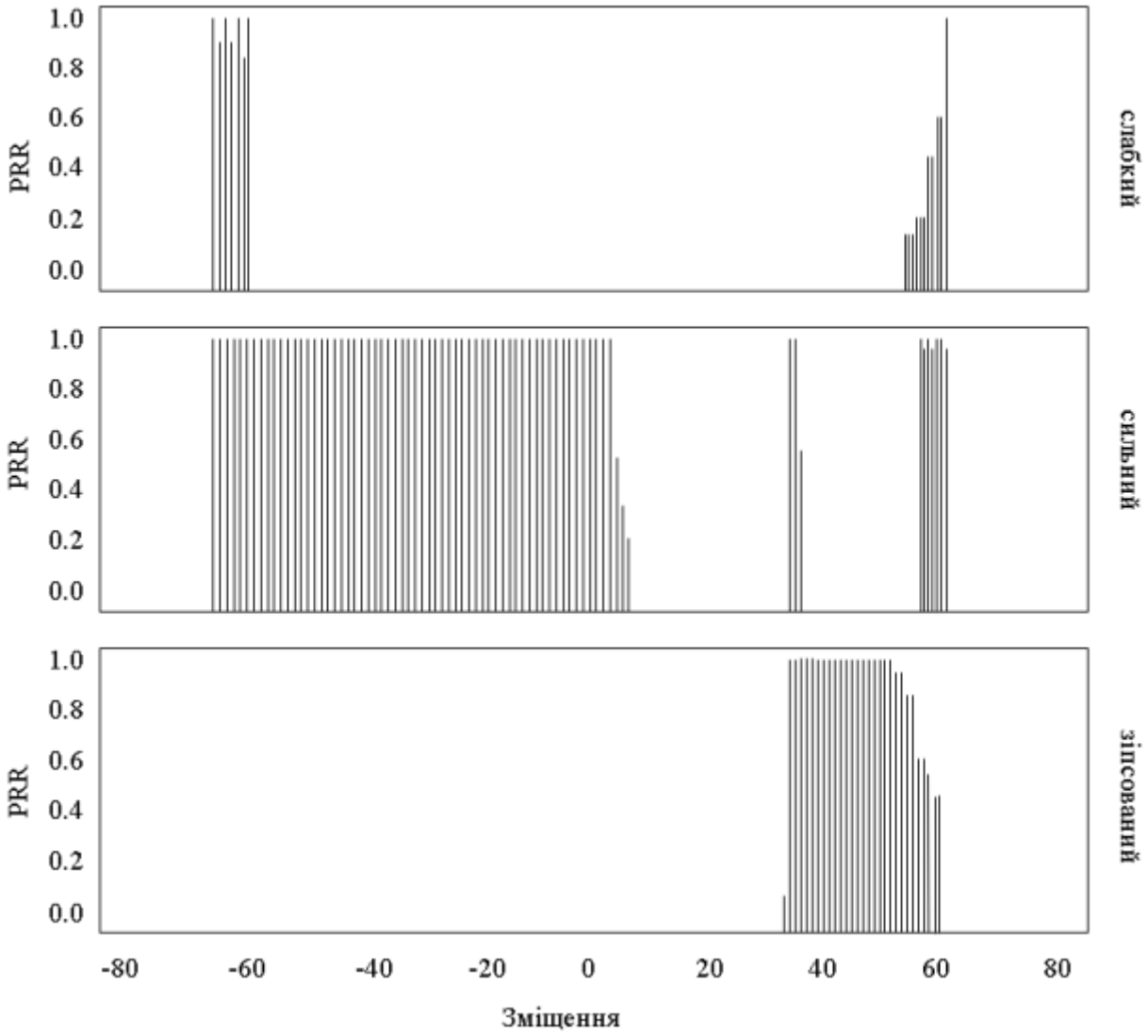


Рисунок 2.1 – Ефект захоплення на пристроях LoRa

Три графіки ілюструють ймовірність різних подій, пов’язаних з прийомом пакетів у мережах LoRa: ймовірність правильного прийому слабкого сигналу, ймовірність правильного прийому сильного сигналу та ймовірність втрати обох пакетів.

З графіків видно, що при значному негативному зміщенні, коли сильний сигнал лише частково перекриває початок слабкого пакета, ймовірність правильного прийому обох пакетів залишається високою. Однак, коли зсув наближається до нуля (повне перекриття сигналів), сильніший пакет приймається без помилок, тоді як слабший сигнал затінюється, що призводить до його постійної втрати.

Це триває, поки пакети не перекриваються повністю, після чого, навіть коли частина слабшого пакета виходить перед початком сильнішого, приймач більше не може коректно декодувати жоден з пакетів через перешкоди, що викликає їх втрату. Втрати продовжуються до того моменту, коли зміщення між пакетами стає значним, і вони знову можуть бути правильно декодовані.

Також важливо розглянути механізм виявлення активності каналу (CAD) в пристроях LoRa. CAD дозволяє визначити, чи є на каналі активність перед тим, як почнеться передача, щоб уникнути колізій. Це дає змогу уникнути перешкод, зокрема ефекту захоплення.

Виявлення активності каналу вимагає, щоб радіо працювало певний час для оцінки наявності інших сигналів. Така оцінка дозволяє пристрою вирішити, чи варто передавати дані, тим самим зменшуючи ймовірність виникнення перешкод через інші сигнали в каналі.

$$t_{on} = \frac{32}{\mathrm{A}} + \frac{2^{SF}}{\mathrm{A}} \quad . \tag{2.1}$$

Тоді для обробки отриманих даних потрібен додатковий час:

$$t_{proc} = \frac{SF \cdot 2^{SF}}{1750 \cdot 10^3} \quad . \tag{2.2}$$

2.1.2 Моделювання ефекту захоплення

Для оптимізації взаємодії компонентів Інтернету речей за стандартом LoRaWAN важливо врахувати ефект захоплення, оскільки він суттєво впливає на ефективність передачі даних. У моделі необхідно зробити припущення про повну ортогональність між різними коефіцієнтами розповсюдження сигналу, що дозволяє мінімізувати вплив перешкод і

знизити ймовірність втрати пакетів через колізії в ефірі.

Основною метрикою, яку використовують для оцінки якості роботи системи, є DER (Data Effective Rate), що визначається як відношення кількості успішно отриманих повідомлень до кількості переданих за певний період часу. Для різних налаштувань у SF (сприятливі коефіцієнти розповсюдження сигналу) існують різні стратегії налаштування мережі. У випадку SN3 всі вузли використовують однаковий коефіцієнт поширення, в той час як SN4 і SN5 змінюють SF в залежності від положення вузлів. Основна мета таких налаштувань — спочатку зменшити ефірний час, а потім (як у випадку SN5) встановити мінімальну потужність передачі, щоб зменшити кількість перешкод і забезпечити стабільне з'єднання з шлюзами.

При цьому, якщо вимога щодо швидкості успішного прийому пакету встановлюється на рівні DER > 90%, то мережа може підтримувати понад 1000 вузлів. Це свідчить про здатність LoRaWAN до масштабування при збереженні високої якості передачі даних.

Загалом, LoRaWAN має пропускну здатність, подібну до мереж ALOHA, оскільки обидва протоколи працюють за схожим принципом випадкових передач. Однак є деякі важливі відмінності у підходах, що використовуються в цих системах, зокрема у тому, як обробляються колізії та вибір параметрів передачі, що дозволяє LoRaWAN досягати більш високої ефективності при роботі в реальних умовах.

2.1.3 Протокол з кількома стрибками для пристроїв LoRa

Іншим важливим аспектом функціонування пристроїв LoRa в мережі є формування мережевого протоколу з кількома стрибками, відомого як LoRaBlink. Цей протокол призначений для мереж з низькою щільністю, обмеженим обсягом трафіку та невеликою кількістю вузлів. Він використовує синхронізацію, подібну до маяка між пристроями, що дозволяє вузлам часто переходити в режим сну, зберігаючи енергію, при

цьому забезпечуючи передачу пакетів з допустимою затримкою в режимі прорізного доступу.

Протокол LoRaBlink був протестований у реальному розгортанні, яке включало шість вузлів і один приймач. Завдяки цьому мережа змогла досягти рівня успішної доставки пакетів на рівні 80%. Це робить LoRaBlink корисним для розріджених мереж, де встановлення шлюзів є складним завданням. Використовуючи пристрої пересилання повідомлень, мережа LoRa здатна покривати набагато більші території порівняно з іншими мережами, такими як LR-WPAN, які застосовують технологію multi-hop. Завдяки великому діапазону передачі LoRa, мережі можуть охоплювати значно більшу площу, ніж це можливо з іншими стандартами.

2.2 Модель оцінювання якості зв'язку

Враховуючи пару передавач-приймач, модель вимірювання лінії зв’язку орієнтована на оцінку сили сигналу на стороні приймача. Для точного прогнозування та аналізу параметрів зв'язку важливо враховувати кілька факторів, таких як потужність передачі, вплив затінення, швидке загасання сигналу та посилення антени як на стороні приймача, так і на стороні передавача.

Позначимо коефіцієнти посилення антени передавача та приймача через

Gtx та Grc відповідно. Потужність передачі сигналу позначимо через Ptx.

Тоді отриману потужність сигналу, яку приймає приймач, можна виразити за допомогою рівняння:

$$P_{rx} = P_{tx} * G_{tx} * G_{rc} / L$$

Де P_{rx} — потужність сигналу на приймачі,

P_{tx} — потужність передачі на передавачі,

G_t — коефіцієнт посилення антени передавача,

G_{rc} — коефіцієнт посилення антени приймача,

L — загасання сигналу через затінення, швидке загасання та інші фактори, які впливають на шлях передачі.

2.2.1 Модель втрат при поширенні

Втрати при поширенні (або втрати на зовнішній трасі) можна обчислити за допомогою такої формули:

$$L = 20\log_{10}(d) + 20\log_{10}(f) + 20\log_{10}(c4\pi) - 147.55$$

У випадку, коли висота шлюзової антени становить h∈[0,50]м, цей параметр впливає на ефективність поширення сигналу. Висота антени визначає, наскільки добре сигнал може долати перешкоди та отримати покриття на великій відстані. Чим вище антена, тим кращі умови для передачі сигналу.

Якщо частота f=868 МГц, а висота h=15 м, можна підставити значення в рівняння для обчислення втрат.

2.2.2 Втрати при проникнення в будівлю

Для моделювання втрат, що виникають через зовнішні та внутрішні стіни будівель, використовується модель, яка складається з кількох компонентів, кожен з яких вносить свій внесок у загальні втрати сигналу. Загальні втрати потужності сигналу, які проходять через будівлю, можна розглядати як суму трьох основних внесків:

1) Втрати, викликані зовнішніми стінами будівель (EWL). Цей внесок описує втрати потужності сигналу, коли сигнал проходить через зовнішні стіни будівель.
2) Втрати від внутрішніх стін будівель. Втрати, пов'язані з проникненням сигналу через внутрішні перегородки і стіни.
3) Покращення потужності через розташування пристрою вище першого поверху. Враховується підвищення ефективності передачі сигналу завдяки розташуванню пристрою на вищих поверхах будівлі.

Модель для EWL передбачає, що втрати на зовнішніх стінах будівель є

випадковою величиною, що приймає значення в певному діапазоні. Ці втрати мають вигляд однорідної випадкової величини:

$$\text{EWL} \sim U(r)$$

де $U(r)$ — це рівномірний розподіл на діапазоні r, що визначає можливі значення втрат для зовнішніх стін.

У таблиці 2.1 наведено три можливі діапазони EWL і ймовірність того, що вузол (пристрій) зазнає відповідних втрат через проникнення зовнішніх стін. Це дозволяє моделювати різноманітність матеріалів і товщини зовнішніх стін у різних будівлях. Оскільки два пристрої можуть відчувати різні втрати при проникненні через зовнішні стіни, це відображає реалістичні умови, де конструкція будівлі, матеріали та товщина стін можуть значно відрізнятися, що впливає на рівень втрат сигналу.

Таблиця 2.1 – Можливі розподіли вимірюваної випадкової величини EWL

Діапазон	Рівень r
0.25	[4, 11] dB
0.65	[11, 19] dB
0.1	[19, 23] dB

Внесок внутрішніх стін у загальні втрати потужності сигналу можна

обчислити через максимальне значення між двома можливими варіантами втрат:

1) Втрати через кількість внутрішніх стін:

$$Tor1=Wi*pi$$

де Wi — це втрати через одну внутрішню стіну, рівномірно розподілені в діапазоні [4,10]дБ, а p — кількість внутрішніх стінок, що розділяють передавач і приймач. Для 15% пристроїв p=3, а решта пристроїв рівномірно розподілені між значеннями p={0,1,2}.

2) Втрати через відстань проникнення в стіну:

$$\text{Tor3}=\alpha * d$$

де α=0,6дБ/м — коефіцієнт відстані проникнення, а d — відстань між пристроями, рівномірно розподілена в діапазоні [0,15] м.

Внесок від підвищення висоти:

$$\text{GFH}=n * G_{\text{n}}$$

де G_n=1,5дБ/поверх — посилення завдяки збільшенню висоти на один

поверх, а n — кількість поверхів, рівномірно розподілена між значеннями

n={0,1,2,3,4}.

Загальні втрати потужності через будівлю для кінцевого пристрою, що знаходиться всередині, можна визначити за допомогою наступної формули:

$$L\text{d}=\text{EWL}+\max(\text{Tor1},\text{Tor3})-\text{GFH}.$$

Ця формула поєднує втрати через зовнішні стіни, внутрішні стіни та посилення, яке виникає внаслідок підвищення висоти.

2.2.3 Моделювання корельованого затінювання

Затінювання є важливим компонентом у роботі бездротових мереж LoRa, оскільки воно суттєво впливає на різні системні явища, такі як поведінка передачі, потужність перешкод та ефективність схем макророзноманіття. У процесі моделювання на системному рівні важливо враховувати кореляцію затінювання для точного прогнозування та оцінки ефективності мережі.

Існує два основних типи кореляції затінювання:

1) Кореляція за відстанню: Якщо передавач надсилає сигнал

приймачеві, то затінення, яке переживає приймач, буде корелювати з затіненням, яке впливає на інші пристрої, що знаходяться в «ближньому» просторі. Це означає, що пристрої, розташовані близько один до одного, можуть зазнавати схожі перешкоди, через що їхнє затінення буде корелювати. Така кореляція, як правило, моделюється експоненціально і залежить від відстані між пристроями. Наприклад, на рисунку 2.3 вузли b та c, будучи близькими, ймовірно, зазнають подібні перешкоди і тому їхнє затінення буде корелювати.

2) Взаємна кореляція затінювання: Якщо два пристрої, що розташовані близько один до одного, одночасно передають сигнали, то приймач може отримати сигнали, на які впливають два корельованих значення затінювання. Взаємна кореляція описує випадок, коли два вузли, як d, e та f на рисунку 2.3, спілкуються з тією ж точкою. Якщо вузол d заблокований великим об'єктом з точки зору e, то ймовірно, що f також зазнає затінення від цього ж об'єкта, що призводить до корельованих ефектів.

З урахуванням цих кореляцій можна точніше моделювати вплив затінювання на ефективність і надійність роботи мережі LoRa, зокрема в умовах, де вузли розташовані близько один до одного і зазнають схожих перешкод.

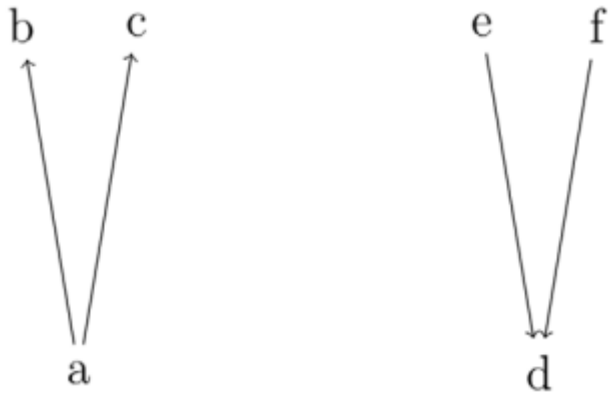


Рисунок 2.3 – Ілюстрація двох видів кореляцій затінювання

Для моделювання кореляції затінювання в бездротових мережах LoRa

зазвичай застосовується спадна експоненціальна функція відстані. Відстань між кінцевими вузлами і та j позначається через $d_{i,j}$, і кореляція затінення може бути виражена таким чином:

$$\rho_{i,j}(d_{i,j}) = e^{-d_{i,j}/d0}$$

де d_0 є параметром декореляції, який визначає відстань, при якій кореляція між двома випадковими значеннями тіні зменшується до рівня

e^{-1}, після чого вважається, що кореляція між значеннями стає незначною.

Для побудови карт затінення часто використовують методи, які створюють 2D-функції затінення для кожної точки карти, відповідно до розташування передавача. Один з популярних підходів — це факторизація Холеського, однак цей метод є обчислювально витратним, особливо коли кількість точок значно збільшується. Для зменшення обчислювальних затрат пропонується інший метод, що полягає у поетапному створенні карти, де нові зразки генеруються з використанням вже наявних точок. Ще один підхід — це фільтрація карти незалежних гауссових випадкових величин для отримання просторово корельованого процесу.

У контексті мереж LoRa, які охоплюють великі території з великою кількістю вузлів, найчастіше застосовуються евристичні методи для побудови карт затінення. Один із варіантів — це створення регулярної сітки, де кожен квадрат має сторону, що дорівнює параметру d_0, та генерування незалежних гауссових випадкових величин для кожної точки сітки. Для вузлів, які не знаходяться на точній вершині сітки, значення затінення можна інтерполювати, враховуючи кореляцію між точками.

Матриця коваріації між точками сітки визначається через функцію коваріації, яка залежить від відстані між точками. Коваріацію можна обчислити для будь-якої пари точок, навіть якщо для цієї конкретної точки немає безпосереднього спостереження.

Застосовуючи ці методи, можна побудувати картографічне представлення затінення в просторі, що дозволяє моделювати як кореляцію між затіненням для близьких пристроїв, так і взаємну кореляцію для пристроїв, що передають сигнал на одну базову станцію. Це дає змогу точно оцінювати ефекти затінювання та кореляції в реальних умовах роботи мережі LoRa, де пристрої можуть бути розташовані на значних відстанях один від одного, але зазнавати подібних перешкод через блокування сигналу.

2.3 Модель продуктивності зв’язку

Модель продуктивності каналу, враховуючи потужність прийому і передачі в системі, використовує модель вимірювання зв'язку для обчислення ефективності передач. Метою цієї моделі є абстракція реального ланцюга прийому фізичного рівня та спрощення інтерференційних обчислень. Наприклад, модель може симулювати продуктивність чіпа Semtech SX1301, який застосовується в шлюзах, або чіпа Semtech SX1272, що використовується в кінцевих пристроях. Вона емітує характеристики цих чіпів, зокрема їх здатність до паралельного декодування, чутливість до сигналу та стійкість до перешкод, що дозволяє точніше моделювати взаємодію в мережах LoRa.

2.3.1 Чутливість приймача

Позначимо через Sg(i) та Se(i) відповідно чутливість у дБ для приймача шлюзу та кінцевого пристрою при SF = i. Ці значення чутливості узагальнено у таблиці 2.2.

Таблиця 2.2 – Чутливість шлюзів і кінцевих пристроїв до різних факторів поширення.

SF	Sg(i)	Se(i)
7	-130	-127
8	-132.5	-129.5
9	-135	-132
10	-137.5	-134.5
11	-140	-137
12	-142.5	-139

Для кожного значення в таблиці 2.2 також враховується коефіцієнт посилення антени приймача Grc, який покращує прийом і, відповідно, збільшує чутливість для значень Grc > 0. Зазначено, що підвищення SF сприяє покращенню чутливості з постійним кроком у 2,5 дБ.

У випадку передачі по низхідній лінії зв'язку (DL) чутливість кінцевого пристрою вважається меншою, ніж чутливість шлюзу, тому вводиться зміщення на 3 дБ.

Значення чутливості використовуються для визначення того, чи зможе пристрій виявити пакет. Наприклад, якщо сигнал з SF = і має потужність, що на місці приймача нижча за порогове значення Sg(i), шлюз не зможе його виявити. Якщо ж отримана потужність перевищує необхідну чутливість, пакет можна буде виявити.

В подальшому припускаємо, що після того, як одержувач виявив сигнал і почав отримувати пакет, потужність сигналу, обчислена за рівнянням (2.4), залишається постійною протягом усього часу прийому. Це означає, що коли сигнал отримано з достатньо високою потужністю для початку виявлення, він буде виявлятися (тобто, перевищить чутливість) протягом усієї сесії прийому.

Нарешті, припускаємо, що якщо два або більше сигналів, потужності

яких менші за чутливість, надходять одночасно на антену приймача, вони не зможуть бути виявлені, навіть якщо їх сумарна потужність перевищує поріг чутливості. Це пояснюється тим, що навіть якщо приймач розпочав прийом одного з пакетів, сигнал буде знищений через перешкоди від інших сигналів, що одночасно надходять, і підвищують потужність, але вона все ще буде нижчою за поріг чутливості.

2.3.2 Перешкоди

Оскільки необхідно змоделювати поведінку автономної мережі LoRaWAN, припустимо, що перешкоди виникають лише від інших передач LoRa. Зробивши таке припущення, будемо використовувати властивість часткової ортогональності різних SF (спектральних факторів) для моделювання того, чи витримає пакет перешкоди від інших LoRa передач.

Введемо наступну (відносну) порогову матрицю SINR (Signal-to-Interference-plus-Noise Ratio) [30]:

$$\mathbf{T} = \begin{bmatrix} 6 & -16 & -18 & -19 & -19 & -20 \\ -24 & 6 & -20 & -22 & -22 & -22 \\ -27 & -27 & 6 & -23 & -25 & -25 \\ -30 & -30 & -30 & 6 & -26 & -28 \\ -33 & -33 & -33 & -33 & 6 & -29 \\ -36 & -36 & -36 & -36 & -36 & 6 \end{bmatrix}$$

Елемент Ti,j у наведеній вище матриці є запасом SINR (у одиницях дБ),

який повинен мати пакет, надісланий із SF = i, щоб його правильно

декодувати, якщо пакет, що перешкоджає, має SF = j. Важливо зауважити, що за наявності кількох пакетів, що заважають, необхідно задовольнити граничні умови для всіх перешкоджаючих пакетів, підсумовуючи отримані значення потужності для кожного SF.

Таким чином, для того щоб декодувати пакет, надісланий з SF = i, при наявності перешкод від пакетів з іншими SF, необхідно враховувати сумарну потужність перешкод від кожного з цих пакетів, і порівняти це з вимогами для SINR.

Для випадку Single Input Single Output (SISO) [31], загальне визначення SINR має вигляд:

$$\mathrm{SINR} = \frac{\mathrm{P}_{\mathrm{rc},0}}{\sigma_{\omega}^{2} + \sum_{l=1}^{N_{int}} \mathrm{P}_{\mathrm{rc},l}}$$

Враховуючи, що Prc,0 — це потужність розглянутого пакета, Nint — кількість пакетів, що заважають, а Prc,l — потужність l-го пакета, що перешкоджає, можна визначити запас SINR для кінцевого пристрою з використанням SF = i та набору перешкод Tj, які використовують SF = j, наступним чином.

Для кожного пакета, що заважає, сумарна потужність перешкод буде

визначатися як сума потужностей перешкоджаючих пакетів:

$$\mathrm{SINR}_{i.j}^{dB} > T_{i.j}$$

Коли два пакети не є ідеально синхронізованими, для обчислення SINR потрібно враховувати різницю в часі їхніх початків. Якщо один пакет починається в момент часу t=0 і триває деякий час, а інший починається пізніше, його енергія буде залежати від того, наскільки пізно він починається відносно першого пакета. Тобто, енергія перешкоди, яку створює другий пакет, залежить від того, скільки часу один пакет накладається на інший.

Це означає, що для правильного обчислення впливу перешкод потрібно коригувати потужність перешкод з урахуванням того, що пакети можуть частково перекриватися в часі, а не відбуваються у точній синхронізації.

$$p_{\mathrm{rc,y}}^{\mathrm{interf}} = \frac{E_{\mathrm{rc,y}}^{\mathrm{interf}}}{T_x} = \frac{P_{rc,y}(T_x - t_1)}{T_x} = P_{rc,y}\left(1 - \frac{t_1}{T_x}\right)$$

Згідно з цим припущенням, коли сигнал і перешкода не синхронізовані і перекриваються, енергію перешкоди можна «розподілити» між сигналом і перешкодами в залежності від того, на скільки часу один сигнал накладається на інший. Це дозволяє коректно обчислити вплив перешкод на прийом сигналу, враховуючи, що енергія перешкоди не повністю поглинається сигналом, а частково може впливати на кілька пакетів, якщо вони частково перекриваються.

Таким чином, для кожної пари сигналу і перешкоди потрібно оцінити, як перешкода взаємодіє з сигналом в залежності від часу, коли ці два пакети

співпадають, і після цього обчислити SINR з урахуванням цієї «розподіленої» енергії.

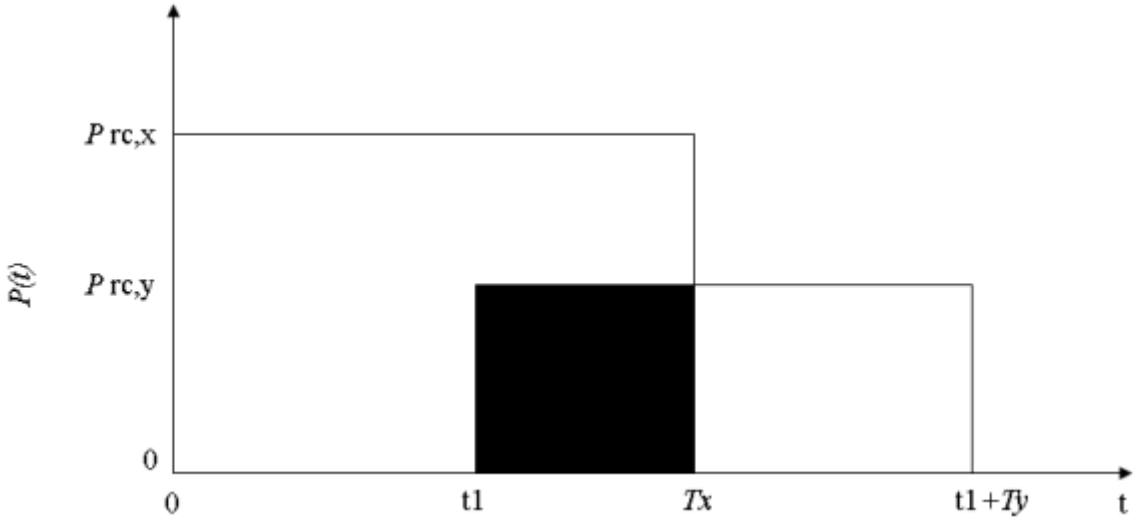


Рисунок 2.4 – Вирівнювання потужності пакетів, що стикаються.

Виділена енергія розподіляється на тривалість пакету.Враховуючи період часу, протягом якого перешкода перекривається корисним сигналом (позначений як tol), можна зробити кілька важливих зауважень. Це припущення обґрунтовується використанням канального кодування з перемежувачем, що дозволяє коректно декодувати навіть тоді, коли перешкода поширюється на кілька символів. Враховуючи це, техніка перемежування допомагає каналу виправляти помилки, викликані перешкодами, дозволяючи системі LoRa коректно отримувати сигнал, якщо він перевищує чутливість і витримує перешкоди.

Завдяки канальному кодуванню, що застосовується в LoRa, сигнал може бути правильно декодований навіть у разі сильних перешкод, оскільки криві бітової помилки різко зменшуються при зростанні SINR, як тільки воно перевищує певні порогові значення.

Це дозволяє зробити кілька цікавих спостережень щодо інтерференції між пакетами LoRa. Один із основних висновків полягає в тому, що два сигнали з однаковими коефіцієнтами розширення та рівною потужністю прийому

можуть бути коректно декодовані, якщо їх перекриття в часі буде достатньо малим, аби SINR кожного з них залишався вище порогового рівня після корекції. Такі пакети можуть витримати певний рівень перешкод, і при цьому їх SINR залишатиметься достатньо високим для декодування.

Ще одним спостереженням є те, що передачі з нижчим коефіцієнтом розширення (наприклад, SF 7) можуть пережити перешкоди від сильніших сигналів з вищими коефіцієнтами розширення (наприклад, SF 12), навіть якщо їх потужність на 20 дБ більша. Водночас, сигнали з вищими коефіцієнтами розширення є більш стійкими до перешкод, оскільки вони можуть бути декодовані навіть якщо перешкода значно сильніша.

Загальна тенденція, яку можна спостерігати, полягає в тому, що збільшення коефіцієнта розширення (SF) дає додаткову стійкість до перешкод, що зростає на 3 дБ для кожного підвищення SF. Ця асиметрія створює можливості для оптимального розподілу SF у мережі LoRaWAN, враховуючи баланс між дальністю, перешкодами та пропускною здатністю.

2.3.3 Модель шлюзу

Припущення щодо роботи шлюзу LoRa з 8 паралельними приймачами можна розглядати таким чином:

1) Центральна частота для кожного тракту прийому: Кожен тракт прийому в межах шлюзу налаштовується на свою центральну частоту, що дозволяє гнучко працювати з різними частотними діапазонами. У разі, якщо кілька трактів прийому налаштовані на одну й ту ж частоту, це не виключає можливості одночасного прослуховування кількох каналів.

2) Гнучкість у виборі SF: Будь-який коефіцієнт розширення (SF) може бути застосований без попередньої конфігурації на будь-

якому з шляхів прийому. Це дозволяє шлюзу ефективно працювати з різними типами пакетів незалежно від їх параметрів.

3) Паралельне прослуховування каналів: Якщо один і той самий канал прослуховують кілька шляхів прийому, кожен шлях може паралельно обробляти певну кількість пакетів. У разі перекриття сигналів на одному шляху прийому, інші шляхи можуть все одно виявити інші пакети. Тобто, кілька шляхів прийому на одній частоті дають можливість паралельно обробляти кілька пакетів з однаковим SF, що значно підвищує ефективність шлюзу у випадку сильного навантаження.

Втрата пакета: Якщо на певний канал LoRa приходить пакет, але немає вільних шляхів прийому для його обробки, пакет втрачається. Це відображає обмеження ресурсів шлюзу, коли кількість доступних приймачів перевищує кількість доступних шляхів для обробки сигналів.

Таким чином, шлюз LoRa, здатний працювати з кількома шляхами прийому, може значно покращити пропускну здатність і стійкість до перекриття сигналів, забезпечуючи обробку кількох пакетів одночасно та зменшуючи ймовірність втрат при високому навантаженні.

2.3.4 Модель застосування

Моделювання пристроїв для створення трафіку відповідно до моделі періодичних звітів Mobile Autonomous Reporting (MAR) у контексті мереж LoRaWAN передбачає, що пристрої періодично відправляють звіти про вимірювання різних параметрів, таких як температура, вологість, стан комунальних послуг (газ, вода, електрика) тощо. У таких сценаріях IoT, де кілька пристроїв повинні регулярно передавати дані, MAR використовується для опису цього процесу.

Основні особливості моделі MAR:

1) Розмір корисного навантаження: Корисне навантаження кожного пакету є випадковою змінною, що розподіляється за законом Парето з параметром форми $\alpha = 2,5$, мінімальним розміром 20 байт і обмеженням в 200 байт. Якщо розмір пакету перевищує 200 байт, він обрізається до цього обмеження. З метою адаптації до специфікацій LoRa, мінімальний розмір корисного навантаження зменшено до 10 байт, а обмеження встановлено на рівні 50 байт.

2) Час між надходженнями пакетів: Час між відправленнями пакетів пристроєм є випадковим, що дозволяє уникнути синхронізації всіх пристроїв в мережі. Кожен пристрій має випадкову початкову затримку звітування, після чого новий пакет генерується через певний інтервал часу (τ секунд).

3) Мережа LoRaWAN: Основна частина трафіку в мережах LoRaWAN припадає на Uplink (UL) – передачі від кінцевих пристроїв до шлюзів. Передачі Downlink (DL) від шлюзів до пристроїв не враховуються в цьому моделюванні, оскільки вони складають меншу частину трафіку в мережі.

4) Мета моделі: Ця модель допомагає оцінити потенціал мережі LoRaWAN для обробки періодичних звітів, що мають випадковий характер і певні обмеження на розмір корисного навантаження.

Таким чином, модель MAR дозволяє створювати реалістичне моделювання трафіку в мережах IoT, де пристрої періодично генерують звіти, що передаються в uplink, і допомагає оцінити, як мережа LoRaWAN буде справлятися з таким навантаженням.

Таблиця 2.4 – Розподіл часу між надходженням пакетів

Інтервал часу τ	Відсоток пристроїв
1день	40%
2 години	40%
1 година	15%
30 хвилин	5%

З описаного розповсюдження видно, що у мережах IoT з використанням LoRaWAN більшість пристроїв буде генерувати пакети з дуже низькою частотою (приблизно один пакет на добу). Однак існує невелика частка пристроїв (5%), які будуть генерувати набагато більше пакетів (48 на добу), що створює значно більший трафік порівняно з іншими пристроями. Цей дисбаланс в кількості пакетів може значно вплинути на продуктивність мережі.

Конкретно, виявляється, що загальний трафік від 5% пристроїв, які часто передають дані, виявляється в шість разів більшим за трафік від 40% пристроїв, які передають рідше. Така ситуація підкреслює важливість налаштування періодичності передачі навіть для невеликої кількості пристроїв. Це може мати суттєвий вплив на загальну ефективність і продуктивність мережі LoRaWAN, зокрема на управління каналами зв’язку та уникнення перевантажень у мережі.

Таким чином, правильне налаштування частоти передачі і розподілу трафіку є важливим для забезпечення стабільності і ефективності роботи всієї мережі.

2.4 Висновки

У цьому розділі були представлені моделі різних компонентів системи LoRaWAN, що є основою для подальших досліджень та оптимізації мереж.

Зокрема, розглянуті основні моделі перешкод, моделі трафіку та поширення сигналів, що дозволяють краще розуміти, як сигнали передаються через мережу та як перешкоди можуть впливати на її продуктивність.

Моделювання різних аспектів функціонування мережі LoRa, таких як аналіз модуляції, поширення сигналу, модель вимірювання зв'язку, втрати при поширенні, проникнення сигналу через стіни, корельоване затінювання, чутливість приймачів, перешкоди та модель роботи шлюзу, допомагає створити більш точну картину про роботу мережі.

Загалом, ці моделі є основою для подальшої розробки удосконаленого методу оптимізації взаємодії компонентів системи IoT за стандартом LoRaWAN, що дозволить підвищити ефективність та надійність таких мереж у реальних умовах.

3 УДОСКОНАЛЕНИЙ МЕТОД ОПТИМІЗАЦІЯ ВЗАЄМОДІЇ КОМПОНЕНТІВ ІНТЕРНЕТУ РЕЧЕЙ ЗА LORAWAN СТАНДАРТОМ

3.1 Основи покращеного методу оптимізації компонентів IoT у LoRaWAN

Для вирішення задачі оптимізації взаємодії компонентів IoT у мережі LoRaWAN розроблено удосконалений метод на основі моделей, запропонованих у попередньому розділі. Цей метод складається з наступних етапів:

1) Створення топології: формування мережі вузлів, які відображають фізичне розташування пристроїв та їх мобільність.
2) Побудова моделі: налаштування стека протоколів для кожного вузла, що забезпечує створення, надсилання, отримання та інтерпретацію пакетів.
3) Конфігурація: встановлення параметрів протоколів та створення зв'язків між вузлами через PHY шари.
4) Запуск моделювання: імітація функціонування мережі із записом даних для подальшого аналізу.

5) Оцінка продуктивності: аналіз зібраних даних для оптимізації роботи мережі.

Кожен із цих кроків розглядається детально для ефективної реалізації методу.

3.1.2 Опис компонентів мережі для оптимізації

Для успішного проектування та оптимізації взаємодії компонентів IoT необхідно врахувати кілька важливих змінних:

1) Масштаб мережі: збільшення кількості пристроїв (ED) підвищує ймовірність перешкод, а додаткові шлюзи покращують покриття, особливо у приміщеннях.
2) Модель трафіку: зменшення інтервалу між пакетами чи синхронізація їх надсилання збільшують кількість зіткнень.
3) Модель втрат на шляху: впливає на дальність покриття сигналу. Менші втрати у будівлях сприяють кращому поширенню сигналу.

Крім того, для оцінки продуктивності розглядаються такі показники:

1) Розподіл коефіцієнтів поширення.
2) Частка втрачених повідомлень на різних рівнях.
3) Пропускна здатність мережі, яка демонструє ефективність вилучення даних.

3.1.3 Обчислення коефіцієнта поширення (SF)

Для проєктування системи кожному пристрою призначається коефіцієнт поширення (SF) за алгоритмом, що включає такі етапи:

1) Обчислення потужності сигналу: визначення рівня потужності, який кожен шлюз отримує від кінцевого пристрою (ED).
2) Вибір шлюзу: визначається шлюз із найвищою отриманою потужністю.
3) Призначення SF: пристрою призначається найнижчий

можливий SF, що перевищує чутливість вибраного шлюзу, щоб мінімізувати час передачі (ToA) і зменшити ризик зіткнень сигналів.

Особливості алгоритму:

1) Через затінення або наявність будівель найближчий шлюз не завжди є найкращим.
2) Процес налаштування SF виконується один раз і не потребує адаптації (ADR).

Приклад:

Якщо найкращий шлюз отримує потужність -137 дБм, враховуючи чутливість шлюзу, SF = 10 є оптимальним, оскільки він забезпечує прийом сигналів з мінімальним ToA.

Візуалізація:

На рисунку 3.1 представлені результати імітації з різними моделями поширення:

1) Модель Log-Distance: пристрої, що знаходяться на відстані до 3,5 км від шлюзу, використовують SF 7, тоді як для більшої відстані необхідний вищий SF. Максимальний радіус передачі – 7,5 км.
2) Модель із затіненням: межі між зонами різних SF стають нечіткими, деякі пристрої стикаються з гіршими умовами через затінення.
3) Модель із будівлями: пристрої в будівлях, навіть поблизу шлюзу, змушені використовувати вищі SF через втрати на проникнення, тоді як зовнішні пристрої підпорядковуються аналогічним правилам, як у моделі із затіненням.

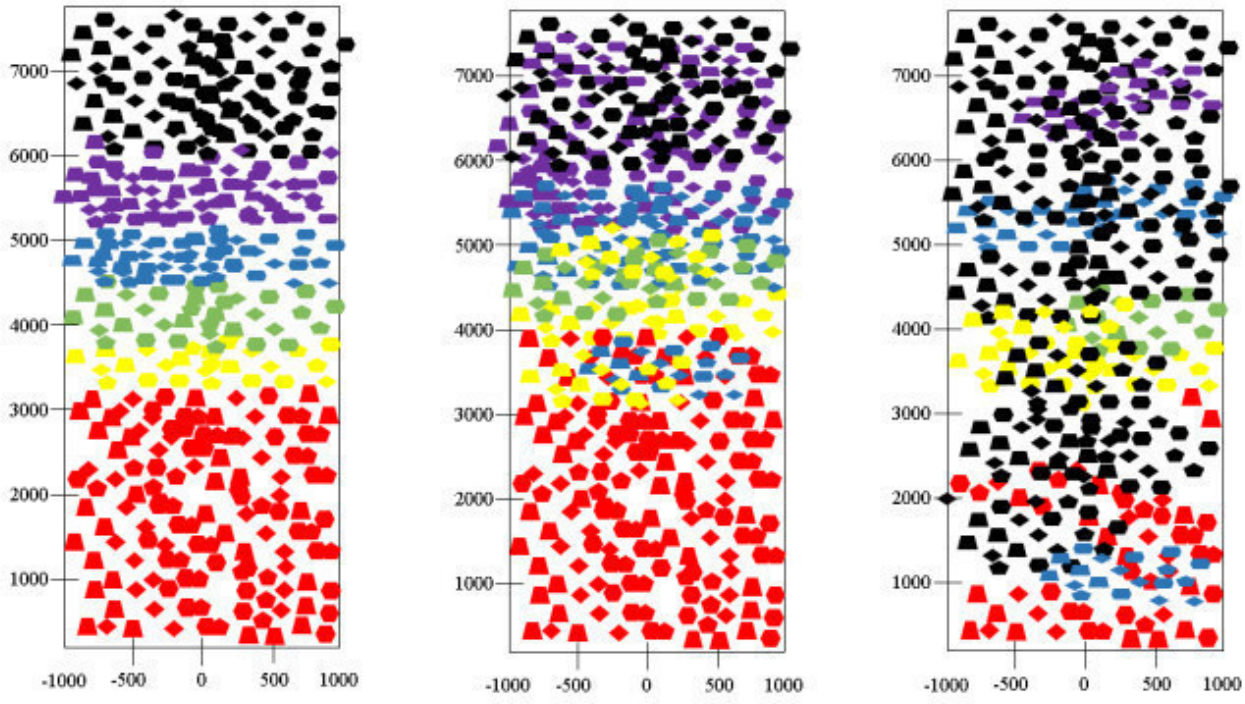


Рисунок 3.1 – Розподіл факторів розповсюдження для різних моделей поширення:

а) Звичайне поширення сигналу: показує, як відстань між пристроєм і шлюзом впливає на коефіцієнт поширення (SF).

б) Поширення сигналу із затінюванням: враховуються перешкоди від різних об'єктів, які можуть викликати зміни в сигналу та викривлення меж між зонами з однаковим SF.

в) Поширення сигналу із затінюванням та перешкодами, спричиненими будівлями: сигнал проходить через будівлі, що призводить до ще більших втрат на проникнення і, як результат, до підвищення SF.

Алгоритм 3.1 – Обчислення показника поширення (SF):

Вхідні дані: Si = чутливість шлюзу GW до SF i.

Кроки алгоритму:

1) Для кожного кінцевого пристрою (ED) e в мережі:

2) Для кожного шлюзу (GW) g в мережі:

3) Обчислити отриману потужність сигналу для передачі від e до g.

4) Вибрати шлюз g, який отримав найсильніший сигнал з потужністю P.

5) Призначити кінцевому пристрою e найнижчий SF, такий, що P > Si.

6) Повернути результат.

3.2.1 Продуктивність пропускної здатності

Перша імітаційна кампанія була спрямована на оцінку пропускної здатності мережі S як функції пропонованого мережею трафіку G.

Сценарій моделювання:

1) Один центральний шлюз (GW) та N кінцевих пристроїв (ED), рівномірно розподілених по колу з радіусом r = 7500 м навколо шлюзу.

2) Вибір радіусу r обумовлений тим, що це максимальна відстань, на якій шлюз може обмінюватися інформацією з кінцевим пристроєм, використовуючи SF = 12 з вище чутливістю лише з урахуванням втрат поширення.

Моделювання:

1) Використовувався один логічний канал LoRa.

2) Шлюз був налаштований для включення тільки одного шляху прийому для всіх симуляцій, що вимірюють пропускну здатність.

Процес обчислення пропускної здатності:

1) Кожен кінцевий пристрій ED генерує пакет кожні Ti секунд, і для його передачі потрібно tp,i секунд, що займає канал.

2) Обмеження робочого циклу не застосовувалися для цього моделювання.

Ціль: Тестувати схему доступу LoRaWAN незалежно від місцевих правил, які можуть змінити її продуктивність.

Пропонований трафік і пропускна здатність $G = \sum_{i=1}^{N} \frac{t_{p,i}}{T_i}$

Пропонований трафік (G) виражає частку часу, протягом якого канал використовується для передачі пакетів кінцевими пристроями. Якщо G < 1, це означає, що канал не використовується повністю, оскільки існують моменти, коли передача через канал не відбувається. Якщо G > 1, це вказує на те, що, навіть за ідеальної синхронізації пристроїв, деякі пакети намагатимуться одночасно використовувати канал, викликаючи зіткнення.

Пропускна здатність (S) для заданого значення G:

Пропускна здатність S обчислюється через ймовірність успіху передачі пакета Psucc, яка апроксимується як відношення кількості успішно прийнятих пакетів до загальної кількості надісланих пакетів під час моделювання.

1) Мережа, яка пропонує трафік G = 1 і має ідеальну синхронізацію між пристроями для уникнення зіткнень, буде мати пропускну здатність S=1
2) У реальних умовах, де ідеальна синхронізація неможлива, пропускна здатність S буде меншою за 1.

Для мереж, де пристрої здійснюють доступ до каналу незалежно один від одного, як-от LoRaWAN, пропускна здатність буде наближатися до форми протоколу доступу до середовища ALOHA.

Перевірка симулятора:

1) Припускається, що всі пристрої налаштовані на передачу з SF = 7, а всі пакети мають однаковий час перебування на каналі (ToA).
2) Перекриваються пакети вважаються втраченими, що означає, що при найменшому перекритті двох пакетів виникають руйнівні перешкоди.
3) Інтерференційна матриця рівнянь дозволяє врахувати, що пакети з однаковим SF мають ізоляцію 6 дБ, тому деякі пакети, що

перекриваються, можуть пережити зіткнення.

Результати моделювання показують типову криву пропускної здатності для ALOHA.

$$S = G * e^{-2G}$$

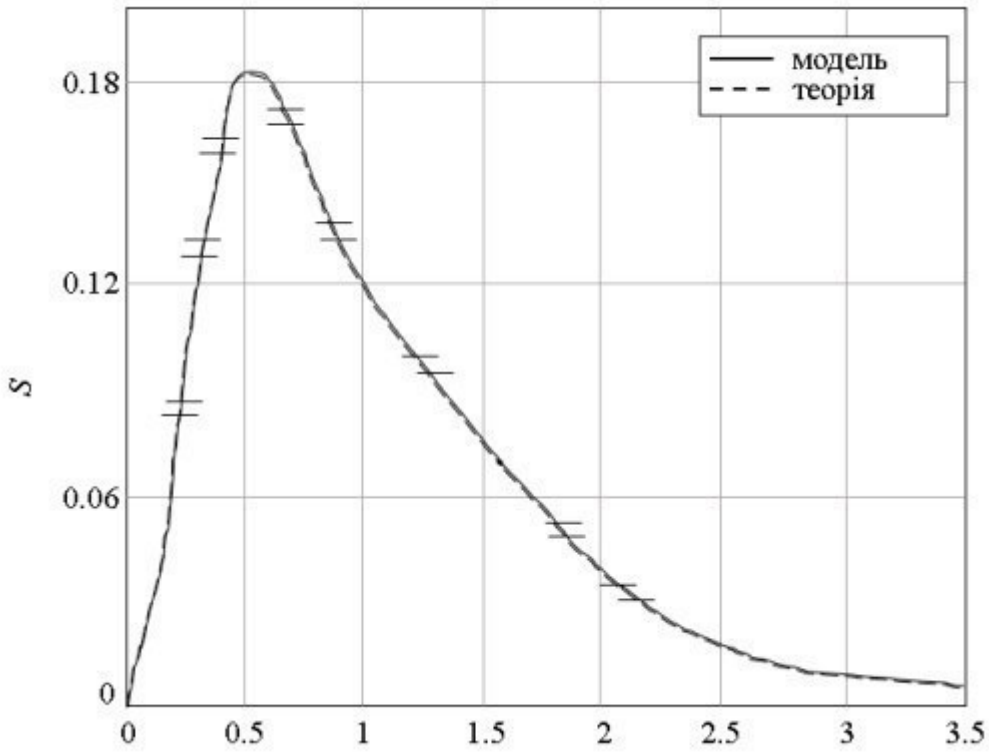


Рисунок 3.2 – Пропускна здатність для SF = 7 і ідеальних зіткнень пакетів

Оцінка впливу реального бездротового каналу та використання різних SF:

Після початкової перевірки симулятора, наступним кроком стало оцінювання впливу реального бездротового каналу та використання різних Spread Factor (SF) на пропускну здатність мережі.

Важливі аспекти оцінювання:

1) Реальний канал:

1.2) Використання логарифмічної моделі вимірювання каналу дозволяє моделювати реальні умови передачі.

1.3) Реальний канал стимулює застосування всіх доступних SF, що забезпечує кращу можливість зв’язку різних пристроїв із шлюзом (GW).

2) Використання множинних SF:

2.1) Застосування декількох SF забезпечує квазіортогональність передач,

що дозволяє одночасну передачу даних від різних пристроїв.

2.2) Матриця зіткнень T враховує цю ортогональність, дозволяючи знизити рівень колізій між пакетами, навіть якщо вони передаються одночасно.

3) Результати моделювання:

3.1) Пропускна здатність значно зросла у порівнянні з попереднім сценарієм, де використовувався лише один SF (SF = 7).

3.2) Це підтверджує, що використання множинних SF та реального каналу покращує ефективність передачі, зменшує кількість зіткнень і підвищує загальну пропускну здатність мережі.

Висновок: Використання різних SF та врахування реальних умов каналу дозволяє суттєво підвищити продуктивність мереж LoRaWAN, зокрема у великих і насичених трафіком мережах.

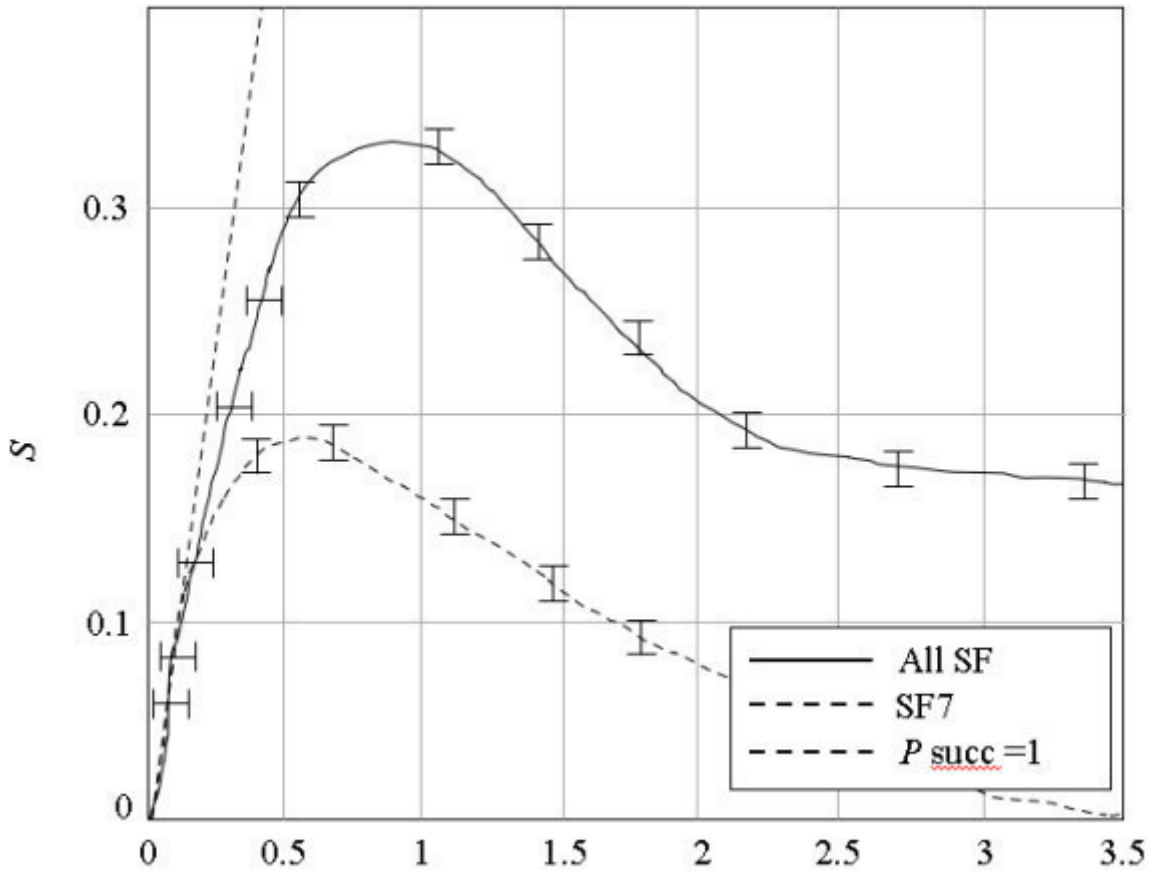


Рисунок 3.3 – Пропускна здатність мережі LoRa з реальним бездротовим каналом (суцільна лінія) і без нього (пунктир)

Дослідження впливу передач із SF = 12 на продуктивність мережі LoRa

У рамках дослідження було проаналізовано вплив передач кінцевих пристроїв (ED), налаштованих на SF = 12, на продуктивність мережі, зокрема їхній внесок у загальний рівень перешкод.

Сценарій симуляції:

1) Обмеження передач SF = 12:

1.1) У моделюванні передбачалося, що пристрої, налаштовані на SF = 12, не мають права передавати пакети.

1.2) Однак, обсяг трафіку, який вони генерують, враховувався у загальному навантаженні мережі.

1.3) Пакети, які мали бути передані пристроями з SF = 12, вважалися втраченими, і це впливало на загальний показник успіху передач (P_{succ}).

2) Зменшення перешкод:

При виключенні передач з SF = 12 пристрої не створюють перешкод для інших кінцевих пристроїв у мережі.

Результати моделювання:

1) Підвищення ймовірності успіху:

Завдяки зменшенню рівня колізій у мережі, ймовірність успішної передачі зросла.

Гарантовано приріст продуктивності мережі на $S_{gain} = 0.12$ у порівнянні зі сценарієм, де пристроям з SF = 12 дозволено передавати.

2) Оптимізація при великому навантаженні:

Виключення пристроїв з найвищим SF є особливо вигідним за умов високого навантаження на мережу, оскільки воно мінімізує ризик перешкод

від пристроїв з тривалим Time on Air (ToA).

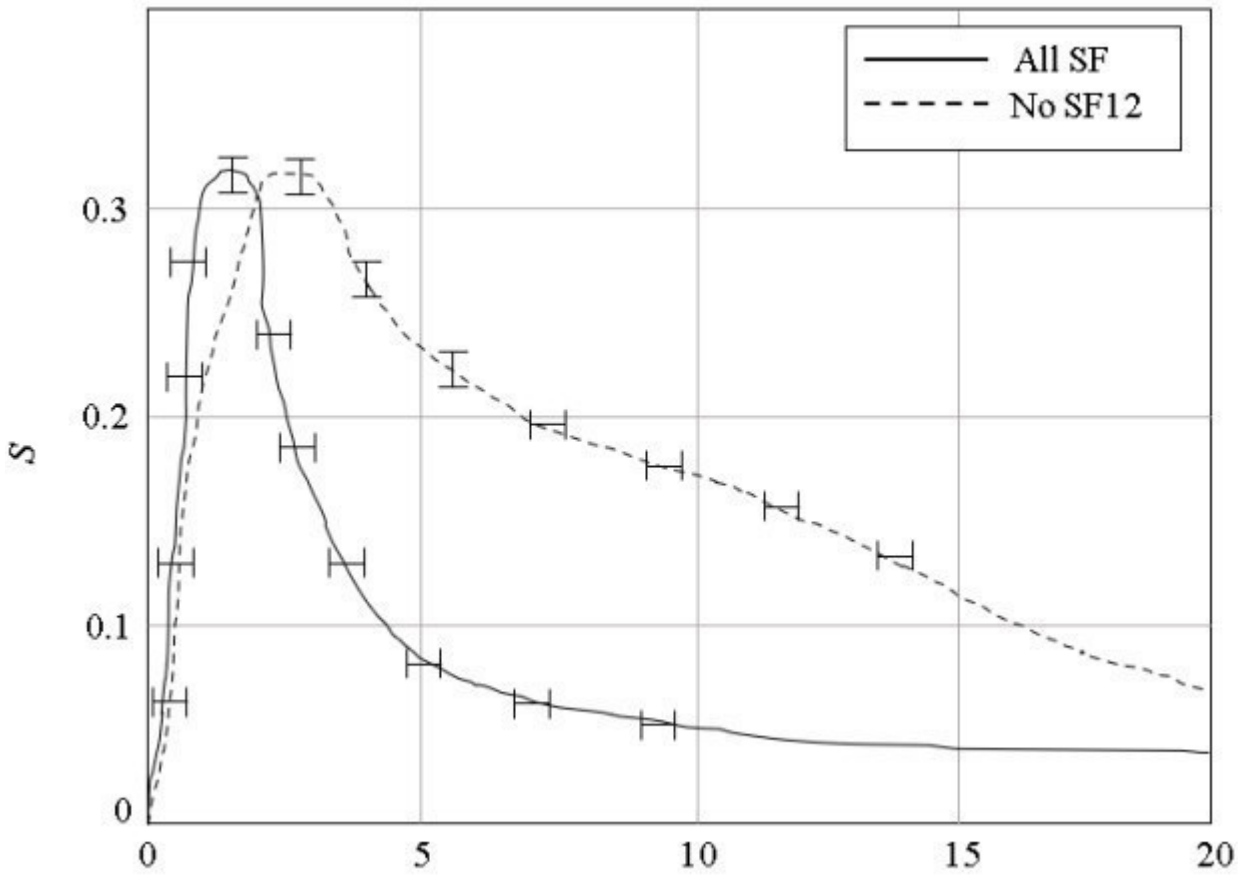


Рисунок 3.4 – Порівняння пропускної здатності з SF = 12 і без нього

Вплив обмеження передач та використання SF = 12 на пропускну здатність LoRa-мереж. Ключові результати.

1) Вплив низького трафіку:

1.1) Втрати пропускної здатності при низькому трафіку:

У разі низьких значень пропонованого трафіку, коли перешкоди не обмежують пропускну здатність, виключення передач з SF = 12 призводить

до втрат у продуктивності до $S_{\text{loss}} = 0.1$.

Це пояснюється тим, що деякі пакети не передаються, що знижує

загальну ефективність мережі.

1.2) Мандат LoRa Alliance:

LoRa Alliance рекомендує виключати кінцеві пристрої, які використовують лише SF = 12 і не адаптують його.

Хоча такі пристрої можуть мати вищу ймовірність успішної доставки пакетів через підвищену чутливість шлюзу, вони негативно впливають на продуктивність мережі в цілому.

2) Обмеження робочого циклу (1%):

2.1) Ефект на продуктивність:

Обмеження передачі пакетів кінцевими пристроями до фіксованої максимальної швидкості, яка відповідає робочому циклу 1%, виявилося ефективним.

Вищі значення SF використовують канал довше, тому такі пристрої частіше досягають межі робочого циклу.

2.2) Результати моделювання:

Застосування обмеження стабілізує пропускну здатність на рівні $S_{1\%}$= 0.14.

Це протидіє безперервному падінню продуктивності, яке виникає зі зростанням трафіку без обмежень.

3) Переваги застосування обмежень:

Зменшення руху та, відповідно, кількості колізій у мережі.

Стабілізація пропускної здатності навіть за високих рівнів навантаження.

Забезпечення виграшу в продуктивності при незначній додатковій складності програмного забезпечення кінцевих пристроїв.

4) Довірчі інтервали:

Для всіх експериментів обчислено довірчі інтервали, які підтверджують надійність результатів та досягнутий виграш у продуктивності.

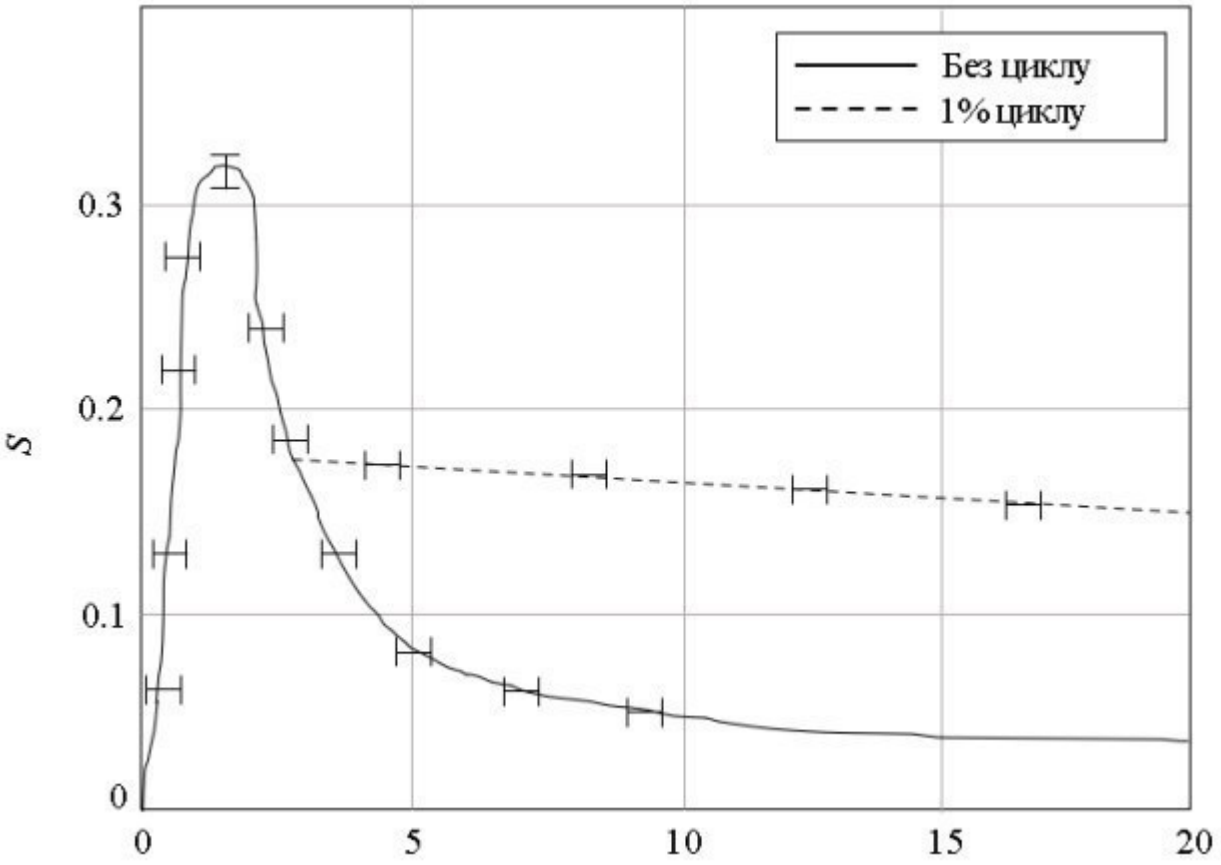


Рисунок 3.5 – Вплив обмежень робочого циклу на пропускну здатність

3.2.2 Ефективність ймовірності успіху

Друга імітаційна кампанія: Оцінка ймовірності успішного отримання пакета в мережі LoRa

Ключові аспекти моделювання:

1) Мережевий сценарій:

Топологія: 36 шлюзів, розташованих у гексагональній сітці навколо центрального шлюзу. Кожен шлюз покриває радіус 1,5 км, загальна область охоплення — коло радіусом 7,5 км.

Фокус зони інтересу: Зібрані дані стосуються лише пристроїв у зоні

центрального шлюзу, але враховуються міжстільникові перешкоди.

2) Реалістичність сценарію:

Будівлі та затінення: Область містить будівлі, пристрої "всередині" будівель зазнають втрат через проникнення сигналу.

Генерація трафіку: Використовується модель Mobile Autonomous Reporting. Розмір корисного навантаження випадковий, згідно з розподілом Парето, у діапазоні [10, 30 байтів].

3) Оптимізація моделювання:

Відсікання нерелевантних пристроїв: Відсікаються пристрої, які знаходяться за межами певного радіусу r, де їх внесок у перешкоди є незначним.

Критерій: Ir: пристрої всередині кола радіусу r. Or: пристрої за межами цього кола. Відсікаються пристрої з множини Or, якщо $EIr \ll EOr$, де EIr і EOr — енергії сигналу пристроїв Ir та Or відповідно.

4) Процедура відсікання:

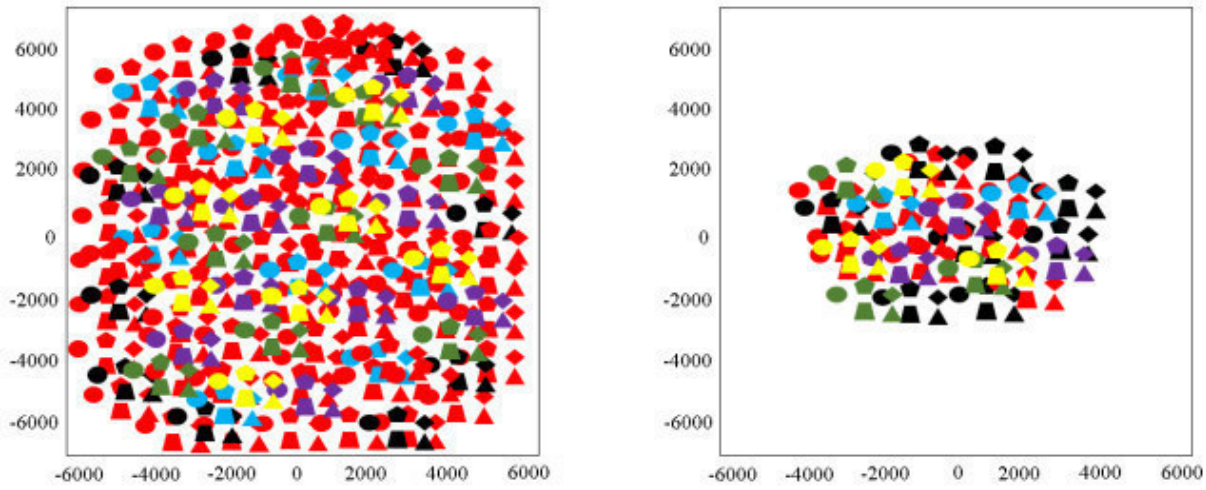
Описана в Алгоритмі 3.2. Від’єднується фізичний рівень (PHY) пристроїв

із Or, після чого вони видаляються з моделювання.

Результати моделювання:

Ефекти відсікання: Відсікання дозволяє моделювати перешкоди ефективніше, включаючи як внутрішньостільникові, так і міжстільникові перешкоди. Зменшення обчислювальної складності забезпечує швидшу симуляцію.

Графіки та висновки: Рисунок 3.6 ілюструє, як ця оптимізація зберігає точність у моделюванні перешкод і ефективно відображає поведінку реальних систем.



а) б)

Рисунок 3.6 – Ефекти алгоритму обрізання: а) усі пристрої; б) пристрої, що залишилися після обрізки

Алгоритм 3.2 – Оцінювання ефекту міжстільникових перешкод

Опис алгоритму: Цей алгоритм використовується для визначення, на якій відстані від центрального шлюзу енергетичний вплив пристроїв поза зоною покриття стає незначним у порівнянні з пристроями всередині зони

покриття.

Ініціалізація: r=0: Початковий радіус для оцінювання.

вихід=помилка: Індикатор завершення оцінювання.

Перебір по SF (спред-фактор):Для кожного SF від 7 до 12:

Внутрішній цикл оцінювання: Поки r<радіус і вихід=false:

Ініціалізація енергій:

Внутрішня енергія=0

Зовнішня енергія=0

Оцінка енергії для кожного кінцевого пристрою e: Якщо e має SF = sf:

енергія=енергія e для передачі

Якщо e знаходиться на відстані <r:

Додати енергія до внутрішньої енергії.

Інакше: Додати енергія до зовнішньої енергії.

Порівняння енергій:

Якщо зовнішня енергія<внутрішня енергія/10

вихід=правда

Інакше: Збільшити $r=r+\epsilon$, де ϵ — невелике додаткове значення.

Завершення:

Повернути результат.

Результат моделювання:

На Рисунку 3.7 показана залежність ймовірності успішного отримання пакета (P_{succ}) від кількості кінцевих пристроїв у зоні покриття центрального шлюзу.

Ключові висновки: Збільшення кількості пристроїв у зоні покриття збільшує ймовірність виникнення міжстільникових перешкод.Застосування алгоритму дозволяє ефективно визначати зону впливу перешкод і оптимізувати мережеві ресурси.

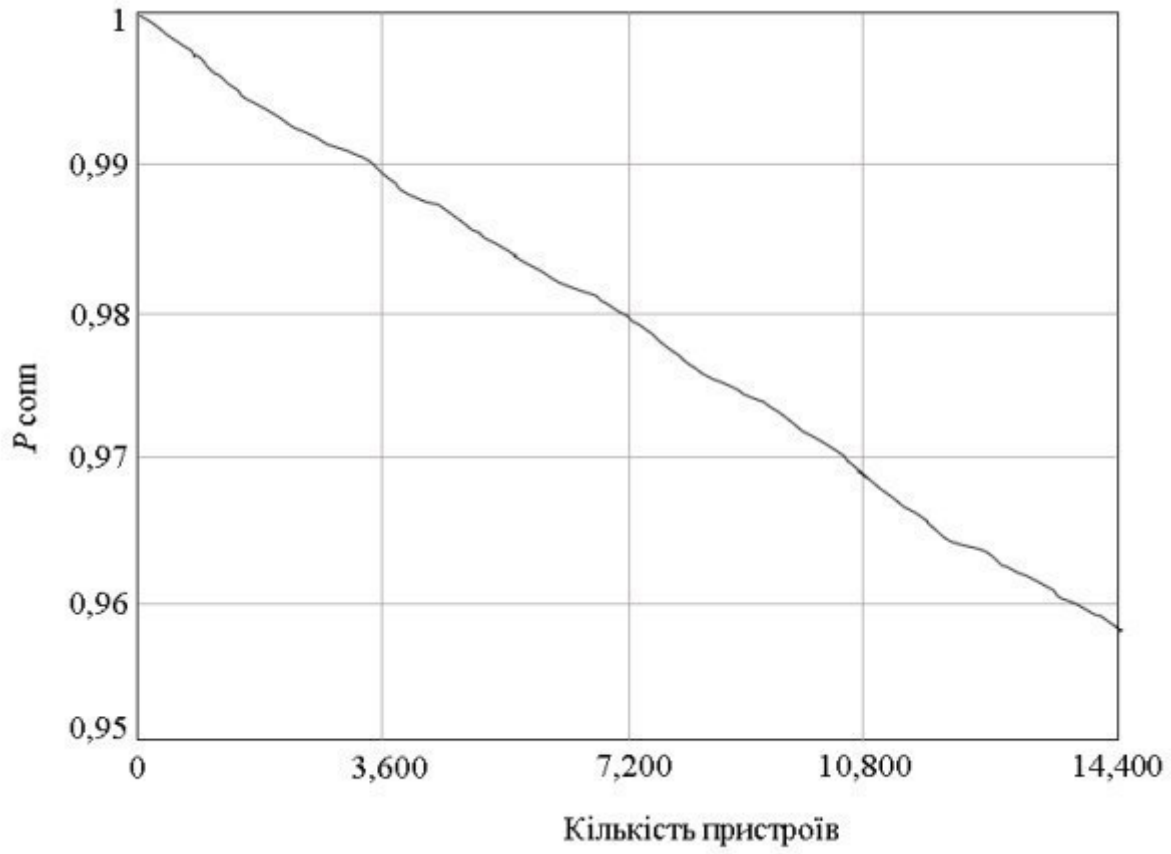


Рисунок 3.7 – Імовірність того, що пакет успішно отримано, як функція кількості кінцевих пристроїв

Оцінка ймовірності успішного отримання пакета в цьому сценарії базується на реалістичному моделюванні LoRa-мережі з урахуванням впливу затінення, втрат через будівлі та міжстільникових перешкод.

Ключові моменти моделювання:

1) Фільтрація даних: Ігнорувалися пакети, що надходили до центрального шлюзу з рівнем сигналу, нижчим за чутливість через затінення чи втрати на проникнення в будівлі.

Таким чином, зниження ймовірності успіху (P_{succ}) враховувало лише

вплив перешкод і недоступність адекватних шляхів прийому.

2) Відсоток недосягнутих вузлів: У даному сценарії 20% вузлів не змогли досягти шлюзу з достатньою потужністю сигналу.
3) Тривалість симуляції: Симуляція тривала 1 день і повторювалася 10 разів для покриття різних сценаріїв затінення та розташування кінцевих пристроїв (ED).
4) Довірчі інтервали: Використання довірчих інтервалів гарантує статистичну достовірність отриманих результатів.

Результати:

1) Лінійне зниження продуктивності: Ймовірність успішної передачі зменшувалася лінійно із збільшенням кількості пристроїв у мережі.
2) Продуктивність шлюзу при високому навантаженні: Для центрального шлюзу, обслуговуючого 14000 ED, ймовірність успіху передачі становила 96%.

3) Порівняння з Semtech: Узгодженість з рекомендаціями Semtech: шлюз здатен підтримувати мережу з ~10,000 вузлів при цільовій ймовірності успіху P_{succ}=95%.

3.2.3 Статистика факторів розповсюдження

Результати моделювання показали, що в умовах мережі LoRaWAN із 8000 пристроями, розміщеними у колі радіусом 7500 м, ймовірність успіху передачі пакетів залишається високою, особливо для факторів розширення (SF) до 11. Для цих параметрів ймовірність успіху перевищує 90%, а втрати

через перешкоди та недоступність шляхів прийому майже не впливають на загальну продуктивність.

Натомість SF 12 демонструє дещо гірші результати, хоча ймовірність успіху все одно залишається вище 80%. Основною причиною цього є тривалий час передачі для цього SF, який створює додаткове навантаження на шлюз. Хоча всі пристрої в цій моделі могли досягти шлюзу завдяки відсутності втрат сигналу через затінення або будівлі, обмеження на кількість доступних прийомних шляхів шлюзу сприяло збільшенню втрат саме для SF 12.

Ці результати підтверджують, що LoRaWAN працює особливо ефективно в умовах низького навантаження, коли перешкоди не є визначальним фактором втрат. Водночас стає зрозуміло, що для густонаселених мереж використання SF 12 потребує обережного підходу, оскільки тривалий час передачі суттєво впливає на ефективність системи.

Таким чином, LoRaWAN підтверджує свою здатність забезпечувати надійність передачі для великих мереж за умови оптимального розподілу факторів розширення серед пристроїв. Це вказує на важливість правильного планування ресурсів, зокрема мінімізації використання високих SF у густонаселених середовищах.

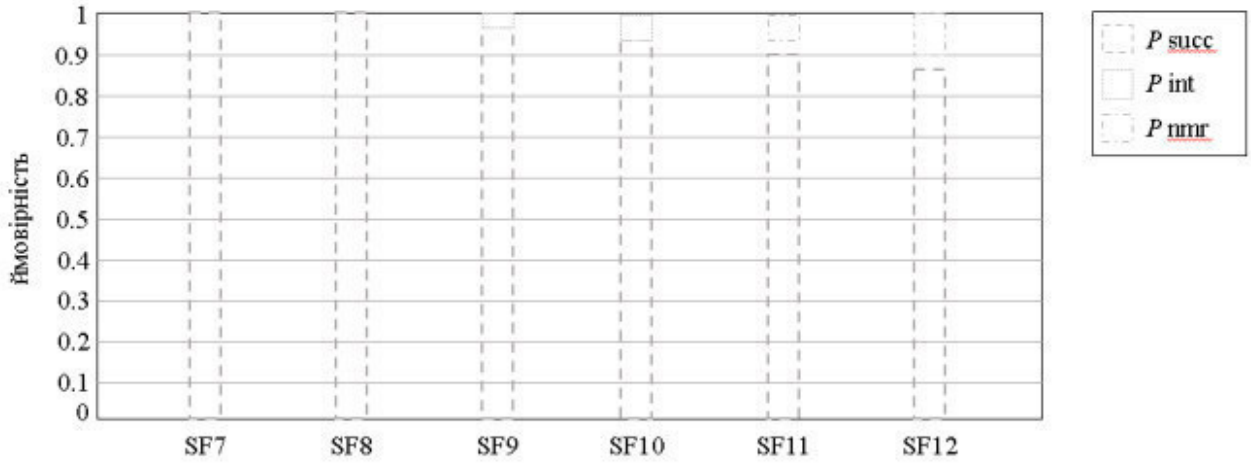


Рисунок 3.8 – Статистика SF для мережі з низьким трафіком

У ході моделювання було виявлено загальну закономірність: із

підвищенням значення SF пристрою зростає ймовірність втрати його пакетів через перешкоди. Це пов’язано з тим, що триваліший час передачі для вищих SF призводить до збільшення ймовірності зіткнень пакетів у мережі. Вищі SF створюють більшу кількість потенційних перешкод для інших пристроїв, а також самі стають більш вразливими до впливу цих перешкод.

Ця тенденція підкреслює важливість оптимізації використання SF у мережах LoRaWAN, особливо в умовах великої кількості пристроїв. Розподіл навантаження між пристроями, що використовують різні SF, дозволяє зменшити кількість втрат пакетів і підвищити загальну продуктивність системи.

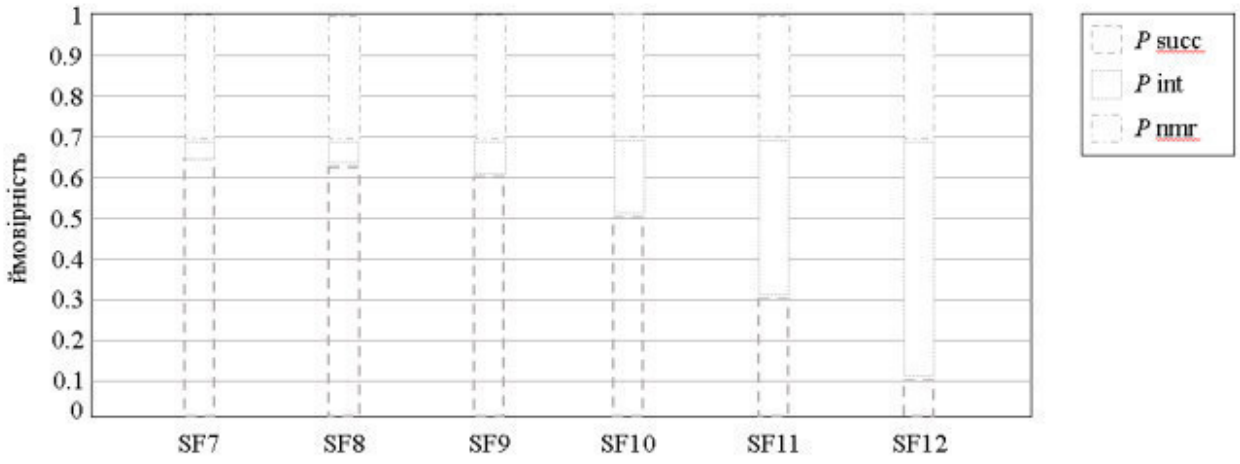


Рисунок 3.9 – Статистика SF для мережі з великим трафіком

У сценарії з низьким трафіком спостерігалося, що пакети практично не втрачалися через недоступність шляхів прийому, оскільки система мала достатній ресурс для обробки всіх передач. Однак при переході до сценарію з інтенсивним трафіком, як показано на рисунку 3.10, ситуація значно змінилася.

Інтенсивніший трафік призвів до того, що зросла кількість втрат пакетів через перешкоди, особливо для пристроїв із вищими SF. Це закономірно, оскільки вищі SF передбачають довший час передачі, що збільшує ризик накладень передач і, відповідно, втрат.

Крім того, у випадку високого навантаження системи значною причиною втрат стала перевантаженість шлюзу, яка однаково впливала на всі пристрої, незалежно від їхнього SF. Ця проблема виникала через нестачу доступних шляхів прийому на шлюзі, що унеможливлювало обробку великої кількості одночасних передач. Це підкреслює важливість розробки стратегій для зменшення перевантаженості шлюзів, особливо в умовах інтенсивного використання мережі.

3.2.4 Оцінка покриття шлюзу

У фінальній серії моделювання було досліджено, як збільшення кількості шлюзів впливає на ймовірність підключення кінцевих пристроїв (ED) до мережі. Цей аспект є критично важливим для додатків, де необхідно забезпечити прийом пакета хоча б одним шлюзом.

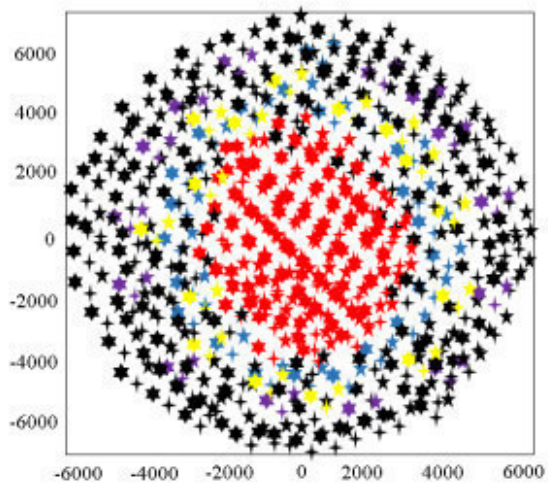
Для моделювання використовувалася кругова міська область радіусом 7,5 км із фіксованою кількістю ED, обслуговуваних все більшою кількістю шлюзів, розташованих у гексагональній сітці. Використання моделі поширення з урахуванням затінення від будівель створювало реалістичний сценарій, в якому багато пристроїв зазнавали значних втрат сигналу.

На рисунку 3.11 зображено залежність ймовірності підключення ED до хоча б одного шлюзу від кількості розгорнутих шлюзів. Результати показують, що для забезпечення понад 90% ймовірності підключення кожен шлюз повинен покривати площу приблизно 6 км² (радіус покриття близько 1200 м). Щоб досягти 95% покриття, відстань між сусідніми шлюзами має бути не більше 2000 м.

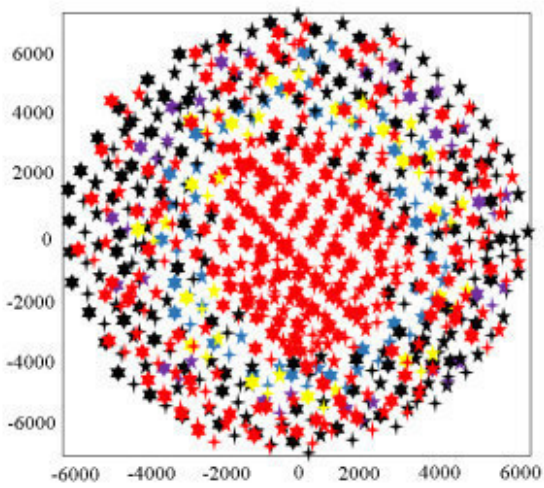
Порівняння із CIoT-сценаріями, де типовий радіус покриття базових станцій становить 577 м, свідчить про те, що LoRaWAN потребує меншої щільності шлюзів для досягнення якісного покриття.

На додаток, збільшення кількості шлюзів призводить до зниження частки пристроїв із високими SF (> 7), як показано на рисунку 3.10. Це сприяє

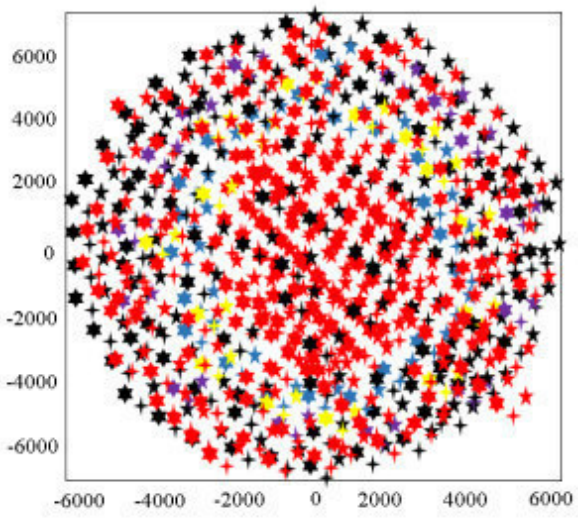
формуванню мережі, де більшість пристроїв використовують SF 7, що зменшує час передачі, знижує ймовірність перешкод і підвищує ефективність системи.



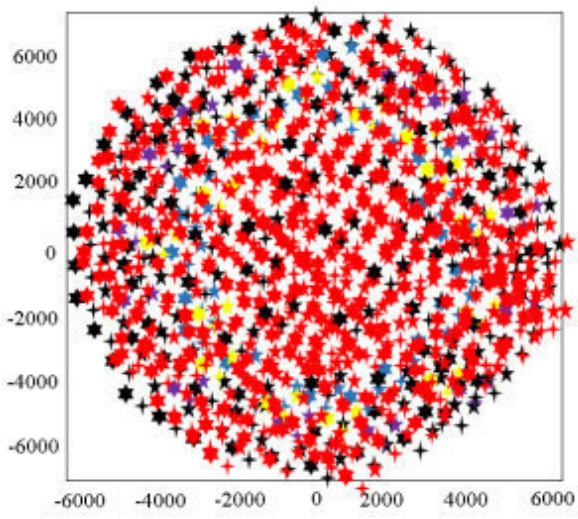
а) 1 шлюз.



(b) 7 шлюзів.



(c) 19 шлюзів.



(d) 37 шлюзів.

Рисунок 3.10 – Покриття для різної щільності шлюзу

На рисунку 3.11 проілюстровано вплив використання одного SF великою кількістю пристроїв у мережі. Таке явище призводить до збільшення кількості зіткнень між пакетами, адже відсутність різноманітності в модуляції не дозволяє використовувати ортогональність SF. У реальних

мережах LoRa механізм ADR повинен підтримувати стан, у якому SF зберігають свою ортогональність, що допомагає збільшувати пропускну здатність.

Моделювання демонструє ефективність квазіортогональності SF у мережах LoRa. Завдяки цій властивості пристрої досягають пропускної здатності, що перевищує показники стандартних систем ALOHA, без додаткових навантажень на MAC-рівень, таких як координація, синхронізація або зондування несучого сигналу. Ця особливість робить LoRaWAN оптимальним вибором для IoT-мереж, дозволяючи масштабування за умови низької складності.

Крім того, висока чутливість модуляції LoRa забезпечує розгортання в міських умовах із меншою щільністю шлюзів порівняно з мережами CIoT. Налаштування SF дозволяє мережевому серверу оптимізувати продуктивність, знаходячи баланс між опором до перешкод і максимальним покриттям.

Важливою перевагою LoRaWAN є те, що ED не прив'язані до конкретного шлюзу, оскільки стандарт не передбачає фіксованих клітин. Це дозволяє розгортати шлюзи вільно, без жорсткої схеми, що є ключовим для краудсорсингових рішень, як-от The Things Network. Такий підхід сприяє швидкому розширенню мережі, заохочуючи користувачів встановлювати власні шлюзи для підвищення покриття та продуктивності.

Однак ця властивість також створює виклики. Зокрема, ED, які знаходяться ближче до одного шлюзу, можуть взаємодіяти з іншим через кращі умови поширення сигналу. З одного боку, це дозволяє кільком шлюзам приймати пакети від одного ED і уникати тягаря хендовера. З іншого боку, шлюзи з вигідним розташуванням можуть перевантажуватися зворотним зв’язком (DL) для пристроїв, які географічно ближчі до інших GW.

Ця проблема стає особливо важливою, коли GW обмежені робочим циклом. Потенційні рішення, спрямовані на балансування навантаження

між шлюзами, можуть бути досліджені в майбутніх симуляціях за допомогою інструментів, розроблених у рамках цієї роботи.

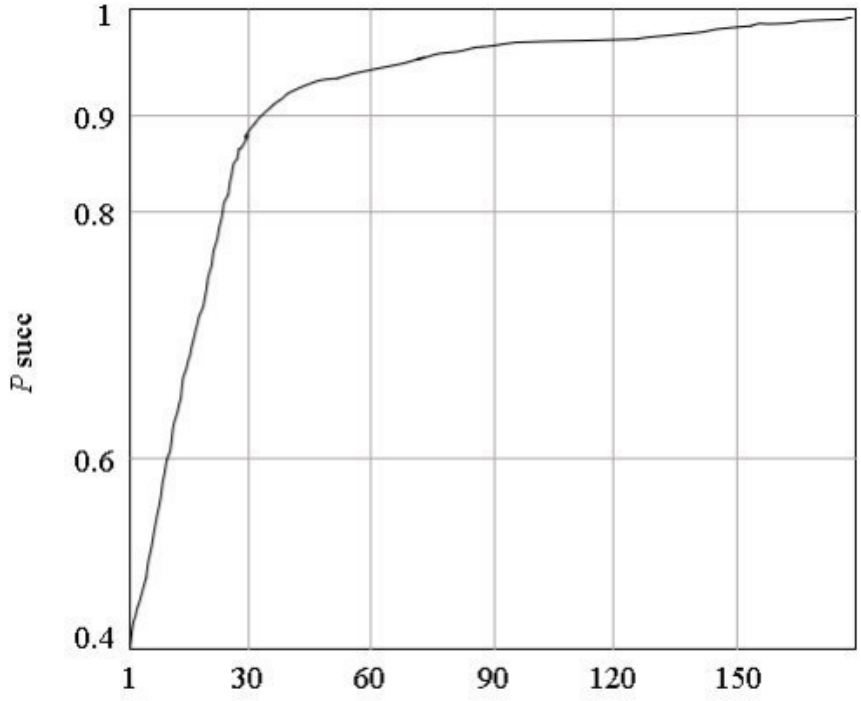


Рисунок 3.11 – Імовірність правильного отримання пакету на мережевому сервері як функція кількості шлюзів, що охоплюють кругову область радіусом 7,5 км

3.5 Висновок

У цьому розділі представлено вдосконалений метод оптимізації взаємодії компонентів інтернету речей (IoT) за стандартом LoRaWAN. Метод включає кілька етапів:

1) Створення топології: на першому етапі формуються вузли мережі (тобто пристрої, які будуть взаємодіяти в мережі).
2) Побудова моделі: на основі створеної топології застосовується певний стек протоколів для кожного вузла, що визначає їх взаємодію.
3) Побудова конфігурації: після того, як протоколи налаштовуються, встановлюються параметри для кожного пристрою, а також створюються з’єднання між вузлами мережі, що визначають їх

маршрутизацію та зв'язки.

4) Запуск системи: на наступному етапі запускається моделювання, і клас Simulator проходить через події, виконуючи відповідні виклики функцій для симуляції взаємодії між пристроями та шлюзами.
5) Аналіз продуктивності: після завершення моделювання зібрані дані можуть бути проаналізовані та візуалізовані, щоб оцінити ефективність запропонованої схеми.

Результати роботи методу продемонстрували, що схема доступу LoRaWAN забезпечує вищу пропускну здатність порівняно з типовою схемою на основі ALOHA завдяки частковій ортогональності між її поширенням та факторів, що впливають на мережу. Крім того, було доведено, що архітектура LoRaWAN добре масштабується: збільшення кількості шлюзів значно покращує покриття та надійність висхідного зв'язку.

Застосування цього удосконаленого методу в умовах реалістичної моделі трафіку, де задіяні кілька шлюзів, показало, що успіх доставки пакетів для шлюзу може досягати понад 95%. Це підтверджує ефективність і надійність LoRaWAN як технології для масштабованих IoT-систем.

4 ПРАКТИЧНА РЕАЛІЗАЦІЯ КОМПОНЕНТІВ ІНТЕРНЕТУ РЕЧЕЙ ЗА LORAWAN СТАНДАРТОМ

4.1 Реалізація стенду для симуляції мережі LoRa

З метою апробації ефективності розробленого удосконаленого методу оптимізації взаємодії компонентів інтернету речей за стандартом LoRaWAN було проведено серію експериментальних досліджень. Для цього використано програмне забезпечення Network Simulator 3 (NS3), яке є пакетом дискретного моделювання подій (Discrete Event Simulation, DES) з відкритим вихідним кодом.

Для реалізації моделювання було створено спеціальний модуль lora, який включає моделі, специфічні для LoRaWAN. Структура NS3 дозволяє деталізувати аспекти мережі, використовуючи об’єкти мови C++ або Python для визначення топології, моделей протоколів і параметрів взаємодії пристроїв.

Короткий опис NS3:

NS3 є потужним інструментом для дослідження та навчання, ліцензованим відповідно до GNU GPL. Система базується на об’єктно-орієнтованому підході, де кожен клас відповідає за певний аспект мережі. Наприклад, модуль wifi містить класи для моделювання точок доступу, пристроїв, рівня WiFi MAC і бездротових каналів. Ці класи можуть бути поєднані з іншими модулями, які моделюють мобільність пристроїв, поширення сигналу та ядро системи, для створення комплексних симуляцій.

Принцип роботи NS3:

Симулятор працює за принципом дискретного моделювання подій, що полягає у виконанні серії подій, кожна з яких має конкретний час виконання. Події можуть викликати зміну стану системи або запланувати

інші події. Наприклад, передача пакета по бездротовому каналу викликає функцію PHY рівня пристрою, яка планує подію отримання пакета іншим пристроєм після відповідної затримки.

Цей підхід дозволяє оптимізувати виконання симуляцій, виконуючи лише необхідні події. При цьому між подіями, які віддалені в часі, симулятор не виконує непотрібних операцій, що підвищує ефективність моделювання.

Генератор випадкових чисел NS3:

Для забезпечення випадковості у моделюванні NS3 має вбудований генератор псевдовипадкових чисел (PRNG). Він забезпечує величезний

період, що досягає $3{,}1*10^{57}$, і підтримує $1{,}8*10^{19}$ незалежних потоків

випадкових чисел із мільйонами підпотоків, що гарантує точність і репрезентативність результатів моделювання.

Розробка модуля lora та його інтеграція у NS3 дозволила деталізовано оцінити вплив різних факторів на продуктивність мережі LoRaWAN, зокрема на пропускну здатність, надійність передачі пакетів і покриття.

Для забезпечення точності та відтворюваності моделювання в NS3 використовується генератор псевдовипадкових чисел (PRNG), який підтримує різні потоки. Кожній випадковій величині присвоюється окремий потік PRNG, що забезпечує відсутність небажаної кореляції між випадковими величинами. Це дозволяє налаштовувати повторювані "прогони" симуляцій із незалежними потоками, що сприяє достовірності отриманих результатів.

Система відстеження NS3

NS3 оснащений системою відстеження, яка дозволяє моніторити змінні в процесі моделювання. Ця функція корисна для збору даних у випадках, коли стандартний вивід програми недоступний через вимкнення журналювання

для підвищення продуктивності.

Процес створення мережі LoRaWAN

1) Створення каналу LoRa реалізується через клас LoraChannel, що включає відповідні моделі втрат поширення. Вузли кінцевих пристроїв (ED) розташовуються рівномірно випадковим чином у межах кола радіуса r, використовуючи клас UniformDiscPositionAllocator.

2) У налаштуванні стеку LoRaWAN використовується клас LoraHelper, який призначає кінцевим пристроям стек LoRaWAN і підключає їх до створеного каналу. У моделюванні відсутня необхідність у процедурі приєднання, оскільки всі ED попередньо налаштовані на роботу в мережі.

3) Розміщення шлюзів. Шлюзи (GW) розподіляються у вигляді гексагональної сітки, налаштовуються на використання стеку LoRaWAN, а також підключаються до каналу. Для збору інформації про стан моделювання до джерел трасування додаються функції зворотного виклику.

4) Реалізація будівель. Для моделювання впливу будівель створюється сітка прямокутників, яка охоплює всю зону моделювання. Будівлі мають розміри 130*64м, з відстанями між ними 32 м (з півночі на південь) і 17 м (зі сходу на захід).

Приклад макета будівель подано на рисунку 4.1, де будівлі зображені у

вигляді сірих квадратів.

Спрощення моделювання

Для зменшення складності в моделюванні були відключені підтвердження повідомлень, що пришвидшило симуляції. ED та GW залишаються нерухомими протягом усього моделювання, що дозволяє зосередитися на аналізі інших параметрів мережі.

Після завершення етапу створення будівель і налаштування топології мережі відбувається остаточна підготовка до моделювання. На цьому етапі модель втрат поширення стає готовою до використання. Вона враховує затінення, спричинене будівлями, і дозволяє налаштувати коефіцієнт розповсюдження сигналу для кожного кінцевого пристрою (ED). Ця інформація є критично важливою для точного моделювання реальних умов роботи мережі, оскільки відображає вплив фізичних перешкод і відстані на якість зв'язку.

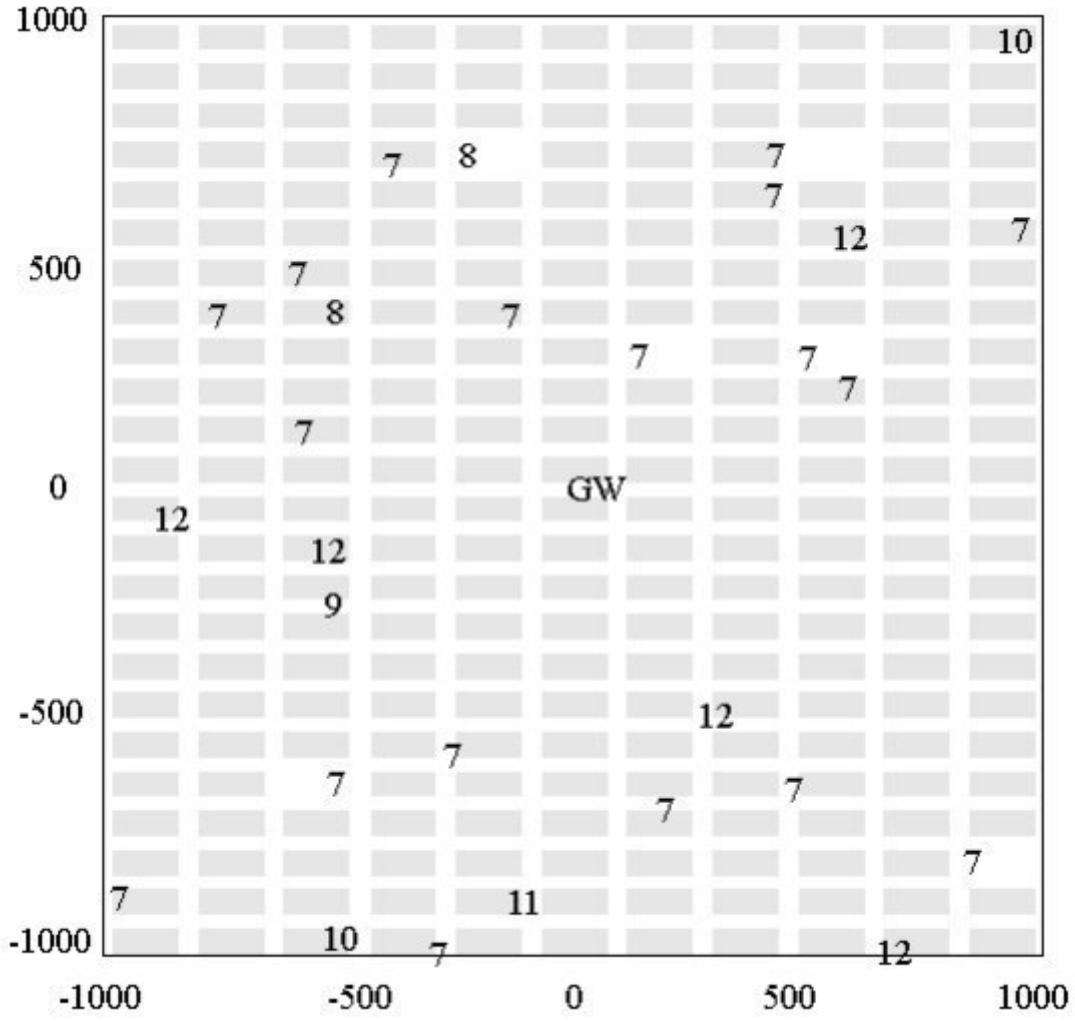


Рисунок 4.1 – Приклад випадкового розподілу вузлів навколо шлюзу

Після цього, залежно від потреби, можна виконати додатковий необов’язковий етап, який передбачає видалення з моделі тих пристроїв, які фізично не здатні підключитися до шлюзу. Причиною цього може бути надмірно сильне затінення або велика відстань між пристроєм та шлюзом. Такий підхід дозволяє уникнути зайвих обчислень і зосередитися на аналізі пристроїв, які перебувають у зоні досяжності мережі.

Наступним кроком є налаштування програм PeriodicSender для кожного ED. Ці програми забезпечують періодичне надсилання даних із пристроїв у мережу. Їх конфігурація включає встановлення часу запуску й завершення роботи, що дозволяє точно змоделювати роботу IoT-пристроїв у різних сценаріях. Це особливо корисно для дослідження продуктивності мережі в умовах різної інтенсивності трафіку.

Після завершення всіх налаштувань моделювання запускається. У процесі симуляції система генерує й обробляє події, які моделюють передачу даних, зміни стану пристроїв і взаємодію з мережею. Після завершення моделювання зібрані дані обробляються. Результати можуть бути збережені у файлах для подальшого аналізу або виведені безпосередньо під час виконання програми для оперативного перегляду. Цей підхід дозволяє не лише оптимізувати роботу мережі, а й досліджувати її поведінку в реалістичних умовах, що є ключовим для проектування високоефективних IoT-рішень.

4.2 Модуль lora

Для моделювання поведінки мереж LoRaWAN було створено спеціальний модуль lora, який забезпечує точну симуляцію роботи пристроїв та шлюзів на різних рівнях протоколу, починаючи з фізичного (PHY) і закінчуючи рівнем програми. Цей модуль є набором взаємодіючих класів, які дозволяють детально описати роботу LoRa ED (End Devices) та GW (Gateways). Структура модулю забезпечує реалізацію ключових характеристик LoRaWAN, що дозволяє моделювати реальні сценарії використання.

Основні класи, які використовуються для моделювання стеку протоколів, наведені на рисунку А.1 у додатку А. Вони включають класи, що відповідають окремим рівням стеку, такі як LoraPhy (фізичний рівень) і LoraMac (рівень керування доступом до середовища). Ці класи дозволяють моделювати передачу і прийом даних, враховуючи ключові аспекти модуляції LoRa.

Окрім основних компонентів стеку, у модулі lora передбачено класи для опису специфічних особливостей мережі. Вони включають моделі втрат сигналу, спричинених будівлями, корельовану тінь, що враховує перешкоди, та обмеження, пов’язані з робочим циклом. Ці додаткові класи забезпечують точне моделювання реальних умов роботи мереж LoRaWAN,

що є важливим для оцінки продуктивності системи.

Розробка модуля зосередилася на моделюванні функціональності кінцевих пристроїв та шлюзів, оскільки саме на цьому рівні використовується специфічна модуляція LoRa. Завдяки цій модуляції мережі LoRaWAN демонструють унікальні властивості, такі як підвищена пропускна здатність, хороша масштабованість і можливість роботи в умовах низької щільності мережі. Модуль lora став ключовим інструментом для проведення симуляцій і дослідження поведінки системи, забезпечуючи необхідний рівень деталізації для отримання достовірних результатів.

4.2.1 PeriodicSender

Клас прикладного рівня PeriodicSender реалізує генерацію пакетів для моделювання роботи кінцевих пристроїв у мережі LoRaWAN. Його основною функцією є створення пакетів із корисним навантаженням, заповненим нулями, та їх регулярна передача. Розмір корисного навантаження вибирається випадковим чином, проте цей параметр не впливає на результати моделювання, оскільки моделі зв’язку в симуляції абстрагуються від змісту пакетів.

Періодичність передач визначається атрибутом m_interval, який встановлює інтервал між подіями надсилання пакетів. Після кожної передачі нова подія автоматично планується через заданий інтервал, що забезпечує регулярність роботи програми. При цьому, сам процес передачі на рівні програми означає лише пересилання пакета до рівня LoRa MAC, де відбувається подальша його обробка.

Робота програми продовжується доти, доки вона не буде зупинена спеціальним викликом функції. Для моделювання початкового стану роботи вузла вводиться випадкова затримка перед першою передачею пакета. Ця

затримка вибирається рівномірно з діапазону [0,$m\_interval$], що гарантує

уникнення одночасних передач від усіх вузлів одразу після початку симуляції.

4.2.2 LoraMac

Клас LoraMac моделює рівень MAC для пристроїв LoRaWAN, забезпечуючи ключову функціональність, пов'язану з доступом до каналів та дотриманням обмежень робочого циклу, визначених нормативами. Цей клас використовує об’єкт LogicalLoraChannelHelper для відстеження доступних мережевих каналів та забезпечує контроль за надсиланням повідомлень. Якщо надсилання пакета порушує правила робочого циклу, пакет не відправляється одразу, а ставиться в чергу для передачі у більш відповідний час.

Для відокремлення логіки управління робочим циклом був створений допоміжний клас DutyCycleHelper, який дозволяє відстежувати різні робочі цикли для різних піддіапазонів частот. Завдяки цьому клас LoraMac зосереджується на основних функціях MAC-рівня, делегуючи управління робочим циклом на допоміжний модуль.

EndDeviceLoraMac і GatewayLoraMac є підкласами, які реалізують поведінку для кінцевих пристроїв (ED) і шлюзів (GW) відповідно.

EndDeviceLoraMac відповідає за визначення класу пристрою (наприклад, класу A) та контроль поведінки ED. Цей клас також забезпечує управління станом радіомодуля PHY, зокрема переходом пристрою зі сплячого режиму для відкриття вікон прийому або постійного прослуховування для пристроїв класу C. Хоча поточна реалізація підтримує лише пристрої класу A,

використання спадковості дозволяє легко додати підтримку інших класів у майбутньому.

Крім цього, EndDeviceLoraMac обробляє передачу пакетів, отриманих від прикладного рівня, до рівня PHY. Для цього ED вибирає випадковий канал для ініціації передачі. Система підтримує зберігання лише одного пакета в черзі, але за необхідності можна реалізувати чергу із затримкою для обробки кількох пакетів одночасно.

GatewayLoraMac реалізує спрощений MAC-рівень, орієнтований на пряме пересилання даних. Ця спрощена структура відповідає особливостям GW, який не генерує власний трафік, а лише передає його між ED та мережею.

Обидва класи також здатні інтерпретувати команди MAC, що містяться в полі FOpts або в полі FRMPayload пакета LoRa. Незважаючи на те, що ці функції наразі не реалізовані повністю, вони можуть бути легко додані в майбутніх ітераціях.

Пакети LoRa зі своєю специфічною структурою були створені як розширення базового класу пакетів, що дозволяє ефективно моделювати їхні унікальні властивості.

4.2.3 LoraPhy

Клас LoraPhy моделює фізичний рівень пристроїв LoRaWAN, відображаючи поведінку мікросхем Semtech LoRa SX1272 та SX1301 в кінцевих пристроях (ED) і шлюзах (GW) відповідно. Цей клас відповідає за передачу та прийом сигналів, обчислення перешкод і визначення успішності прийому пакетів на основі їх потужності та рівня перешкод.

Основна роль LoraPhy включає:

1) Передача сигналів: Під час передачі клас отримує пакет із рівня MAC і передає його до каналу для подальшої обробки.
2) Обробка вхідних сигналів: Під час прийому клас аналізує,

чи потужність сигналу достатня для прийому, і враховує вплив перешкод, які можуть спричинити втрату пакета.

3) Керування станами пристрою: Клас використовує атрибут m_state, що представляє стан пристрою:

TX: передача пакета;

RC: прийом пакета;

IDLE: прослуховування сигналів;

SLEEP: режим низького споживання енергії.

Стан пристрою впливає на споживання енергії, що може бути враховано в майбутніх ітераціях роботи через інтеграцію моделі енергоспоживання.

Підкласи LoraPhy

EndDeviceLoraPhy: представляє фізичний рівень кінцевих пристроїв.

GatewayLoraPhy: моделює шлюзи, які мають складнішу структуру через наявність кількох шляхів прийому.

Обробка сигналів і перешкод

Обидва підкласи використовують клас LoraInterferenceHelper для відстеження сигналів, які надходять на пристрій, і обчислення впливу перешкод. Коли сигнал надходить до антени, виконується наступне:

1) Сигнал реєструється в LoraInterferenceHelper через виклик Add. Це створює об’єкт події (Event), що містить інформацію про:

- тривалість дії сигналу;
- потужність сигналу;
- коефіцієнт розповсюдження;
- логічний канал.

2) Потужність сигналу порівнюється з чутливістю пристрою. Якщо потужність достатня, планується подія завершення прийому.

3) Навіть якщо сигнал нижче чутливості чи пристрій перебуває в режимі SLEEP, він все одно враховується для оцінки перешкод.

Після завершення прийому перевіряється, чи був пакет знищений через

перешкоди. Якщо пакет успішно отримано, він передається до рівня MAC. Незалежно від результату, пристрій повертається у режим SLEEP.

Розширення для шлюзів

Клас GatewayLoraPhy має додаткову складність через підтримку кількох шляхів прийому. Для цього використовується список об’єктів ReceptionPath, які відповідають за прийом сигналів. Кожен шлях:

- пов’язується з сигналом, якщо він вільний і канал збігається;
- позначається зайнятим до завершення обробки сигналу.

Теги пакетів.

Клас LoraPhy також впроваджує систему тегів пакетів через клас LoraTag. Ці теги додаються до пакетів для зберігання інформації про:

- фактор розповсюдження пакета;
- причини втрати (наприклад, через перешкоди).

Теги дозволяють відстежувати долю кожного пакета в симуляції, забезпечуючи детальний аналіз втрат на фізичному рівні.

4.2.4 LoraChannel

Клас LoraChannel в моделюванні мереж LoRaWAN є критично важливим елементом, який забезпечує взаємодію між всіма фізичними рівнями (PHY) різних пристроїв у мережі. Його основне завдання — це моделювання бездротового каналу зв'язку, по якому передаються пакети між передавачем та приймачем. Він також відповідає за правильне обчислення потужності сигналу, врахування впливу різних перешкод, таких як зниження потужності через відстань, та затримки сигналу, що виникають при передачі.

Реєстрація PHY пристроїв

Під час конфігурації мережі клас LoraChannel реєструє всі PHY пристрої, які будуть брати участь у передачі та прийомі даних. Це дозволяє класу ефективно обробляти запити на передачу та отримання сигналів. Коли PHY

пристрій хоче передати повідомлення, він викликає метод Send, де передає основні параметри передачі, такі як:

1) Коефіцієнт поширення (Spreading Factor), який визначає швидкість передачі та чутливість сигналу.
2) Пакет, що містить дані, які необхідно передати.
3) Тривалість передачі, що визначає, як довго сигнал буде активним.
4) Потужність сигналу, яка може бути варіативною залежно від типу передавача та параметрів конфігурації.
5) Номер каналу, на якому здійснюється передача.

Канал отримує ці параметри і аналізує їх. Зокрема, для кожного PHY пристрою, який прослуховує цей канал, планується подія Receive, яка відбудеться після певної затримки, обчисленої на основі моделі поширення сигналу.

Моделювання затримок

Затримка сигналу є важливим аспектом для точного моделювання бездротового зв'язку, оскільки вона визначає час, необхідний для того, щоб сигнал досягнув приймача. Для цього в LoraChannel використовується модель ConstantSpeedPropagationDelayModel, яка базується на відстані між передавачем та приймачем. У простій версії ця модель обчислює час, необхідний сигналу для проходження відстані між двома точками. Однак для більш складних сценаріїв можна використовувати інші моделі затримок, залежно від умов середовища.

Розрахунок потужності та перешкод

Важливою частиною роботи LoraChannel є обчислення отриманої потужності сигналу на приймачі, що враховує різні фактори поширення сигналу в просторі. Для цього використовується клас PropagationLossModel, який базується на кількох підмоделях втрат потужності. У конкретному випадку використовуються три основні моделі:

1) LogDistancePropagationLossModel — це модель, яка

обчислює втрати потужності на основі відстані між передавачем та приймачем. Ця модель є стандартною і широко використовуваною у більшості бездротових симуляцій.

2) CorrelatedShadowingPropagationLossModel — модель, що враховує корельовані тіньові ефекти. Вона базується на ідеї, що в реальному світі частина сигналу може бути затемнена через об'єкти, розташовані між передавачем та приймачем, як наприклад будівлі чи дерева. Модель обчислює тіньовий ефект для кожної з позицій, зберігаючи значення у вигляді сітки для кращої точності.

3) BuildingPenetrationLoss — користувацька модель, яка враховує втрати сигналу при проходженні через стіни або інші конструкції будівель. Цей клас використовує дані про будівлі, що отримуються з BuildingsHelper, для точного обчислення втрат при проникненні через різні матеріали стін, а також для врахування висоти поверхів будівель.

Ці моделі втрат працюють разом, щоб надати точну інформацію про потужність сигналу, яку отримує пристрій на іншому кінці каналу. Залежно від розташування пристроїв, їх стану та умов навколишнього середовища, канал може зазнати значних змін у потужності сигналу.

Подія прийому

Коли передача сигналу завершується, канал викликає подію Receive, яка ініціюється в усіх пристроях PHY, що слухають цей канал. Метод StartReceive у LoraPhy відповідає за обробку цієї події. Якщо сигнал був отриманий успішно і потужність сигналу достатня для прийому, то він передається до відповідного PHY пристрою для подальшої обробки. Якщо ж сигнал виявився слабким або зазнав значних перешкод, пристрій може не отримати пакет.

Взаємодія з іншими пристроями

Особливо важливою функцією є те, що LoraChannel надає можливість одночасного прийому і передачі для різних пристроїв у мережі, зокрема

пристроїв типу EndDevice та Gateway. Усі PHY пристрої можуть бути підключені до одного каналу, що дозволяє їм взаємодіяти між собою та обмінюватися пакетами. Завдяки реєстрації пристроїв і плануванню подій прийому, канал забезпечує ефективний зв'язок між усіма пристроями в мережі.

Пороги потужності та оптимізація

Щоб прискорити процес симуляції, особливо при моделюванні мереж з великими розмірами, можна використовувати поріг потужності. Це дозволяє зменшити кількість обчислень, оскільки пакети з потужністю нижчою за цей поріг просто ігноруються і не передаються до PHY рівня. Це дозволяє значно зекономити ресурси при моделюванні великих мереж.

4.2.5 LoraNetDevice

Клас LoraNetDevice моделює «мережеву карту LoRa», яку можна підключити до вузла, дозволяючи програмам на ньому використовувати її для надсилання даних іншим пристроям LoRa. Він виконує функцію об'єднання всіх необхідних об'єктів LoRa, таких як LoraPhy та LoraMac, в один пристрій. Важливою особливістю є те, що клас LoraNetDevice базується на абстрактному класі NetDevice, який орієнтований на IP-зв'язок. Зокрема, у документації API LrWpanNetDevice зазначається, що методи, такі як GetMulticast, Send і SendTo, в ньому не повністю підходять для реалізації специфічних функцій для 802.15.4 MAC. Тому в дизайні лора модуля NetDevice служить інкапсулятором, який використовує стандартну версію Send, адаптовану для обробки базового рівня MAC, без підтримки таких концепцій, як багатоадресні або IPv6-адреси.

4.2.6 Інші класи системи

Для полегшення управління моделюванням був створений набір додаткових класів. Одним із таких класів є HexGridPositionAllocator, який використовується для обчислення позицій шлюзів у вигляді гексагональної

сітки. Клас працює наступним чином: перший шлюз розміщується в центрі простору моделювання, а потім створюються «кільця» навколо нього, відповідно до шаблону гексагональної сітки. Отже, шлюзи розміщуються у центральних точках кожного шестикутника. Це розташування демонструється на рисунку 4.2, де на кожному з шестикутників розташовується шлюз. Знаючи кількість кілець на гексагональній сітці, можна обчислити загальну кількість шлюзів за спеціальною формулою.

$$N = 3n^2 - 3n_r + 1.$$

Для переміщення логіки керування каналом за межі реалізації LoraMac був створений допоміжний клас, який отримав назву LogicalLoraChannelHelper. Цей клас містить список об'єктів LogicalLoraChannel, кожен з яких має свої характеристики, зокрема частоту, пропускну здатність і номер каналу. Очікується, що цей клас буде використовуватися для управління доступними каналами для зв’язку, а також для додавання та видалення каналів у відповідь на команди MAC у майбутніх версіях.

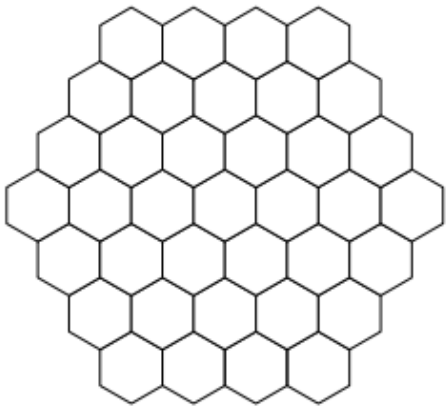


Рисунок 4.2 – Шестикутна сітка, створена за допомогою HexGridPositionAllocator [47]

LoraMacHeader і LoraFrameHeader є підкласами класу Header, який використовується для представлення заголовка пакета. Ці класи підтримують серіалізацію та десеріалізацію ряду полів, що залежать від протоколу. Хоча в поточній версії дипломної роботи ці заголовки

заповнюються нулями з метою зменшення складності системи, в майбутніх версіях вони будуть використовуватись для передачі команд MAC, стандартного основного номера версії, адрес і іншої інформації.

4.3 Помічники та тести

Окрім основних компонентів, описаних раніше, для полегшення налаштування мережі LoRa був розроблений набір допоміжних класів. Помічники (хелпери) в NS3 призначені для спрощення налаштування топологій та вузлів, що повністю налаштовані для використання необхідного модуля. Кожного разу, коли створюється екземпляр програми PeriodicSender, необхідно встановити її період. Щоб полегшити правильну конфігурацію цих класів, програми можуть бути розгорнуті на кількох вузлах за допомогою класу PeriodicSenderHelper, який визначає звітний період вузла відповідно до специфікації для коректного розподілу періодів між вузлами.

Також були розроблені інші допоміжні класи для налаштування та конфігурації стеку LoRa на наборі вузлів. Класи LoraHelper, LoraPhyHelper та LoraMacHelper забезпечують синергію для створення та розгортання об'єктів LoraNetDevice, LoraMac та LoraPhy, що дозволяє налаштувати рівні зв'язку та коректно під'єднати рівень PHY до екземпляра LoraChannel.

Окрім того, разом із модулем було розроблено набір тестів для перевірки коректності програмного забезпечення після оновлень та відповідності рекомендаціям NS3. Тести перевіряють базову доставку повідомлень, щоб переконатися, що рівень PHY на кінцевому пристрої може отримати повідомлення від пристрою в межах досяжності. Тести перевірки поділу каналів гарантують, що пристрій, який прослуховує канал i, не отримає повідомлення, надіслані на канал j, коли $i \neq j$. Перевірка перешкод виявляє, чи може пакет бути знищений перешкодою з достатньо високою потужністю. Крім того, тестується, що комунікації по різних каналах не заважають одна одній. Нарешті, тести потужності паралельного

декодування шлюзу перевіряють, чи може шлюз одночасно приймати до 8 повідомлень.

4.4 Результати роботи

Аналізуючи різні показники, отримані за допомогою модуля LoRa, доданого до NS3, спочатку оцінюється продуктивність змодельованої мережі. Для цього налаштовується мережа з реалістичним середовищем і моделлю трафіку, щоб вивчити ймовірність втрати пакета в LoRaWAN. Після цього проводяться експерименти, щоб оцінити вплив різних коефіцієнтів розповсюдження на перешкоди, а також визначити, як швидкість успішної доставки пакетів змінюється в залежності від коефіцієнта поширення. В кінці були проведені тести покриття в реалістичних умовах для оцінки необхідної щільності шлюзів для покриття міста, яке має глибоку тінь від будівель (Додаток Б, рисунок Б.1).

4.5 Висновки

У розділі представлено програмно-апаратну реалізацію удосконаленого методу оптимізації взаємодії компонентів інтернету речей за стандартом LoRaWAN, а також результати експериментальних досліджень. Для цього було використано програмне забезпечення Network Simulator 3 (NS3) з пакетом для симуляції дискретних подій (DES) з відкритим кодом. Симулятор був розширений шляхом створення модуля lora, який реалізує різні моделі. Спочатку надається загальна інформація про програмне забезпечення NS3, а потім описується структура та впровадження нового модуля lora. Експериментальні дослідження спроектованої мережі LoRa, що базуються на програмно-апаратній реалізації удосконаленого методу оптимізації взаємодії компонентів інтернету речей за стандартом LoRaWAN, показали загальну оптимізацію взаємодії компонентів мережі. Зокрема, успіх доставки пакетів для шлюзу становив понад 95%.

ВИСНОВКИ

У першому розділі проведено аналіз та дослідження технологій Інтернету речей, зокрема LPWAN і LoRa, а також визначено вимоги до IoT. Визначено основні рішення для проектування та оптимізації взаємодії компонентів Інтернету речей, проаналізовано їх продуктивність і здатність до масштабування, а також виявлено переваги та недоліки. Окрім того, розглянуто огляд технологій IoT, зокрема рішень для підключення пристроїв до Інтернету, таких як низькошвидкісні бездротові персональні мережі, стільниковий Інтернет речей та глобальні мережі малої потужності. Також розглянуто основні аспекти функціонування IoT, зокрема модуляцію LoRa, її реалізацію, пакети фізичного рівня, основні мікросхеми Semtech та незалежні реалізації. Досліджено принцип роботи стандарту LoRaWAN, зокрема топологію та класи пристроїв, структуру пакетів і команди MAC, шифрування, активацію пристроїв та діапазони частот. Визначено, що проектування та оптимізація взаємодії компонентів Інтернету речей за стандартом LoRaWAN є надзвичайно актуальним, що підкреслює необхідність розробки удосконаленого методу оптимізації цих компонентів.

У другому розділі представлені моделі різних компонентів системи LoRaWAN, зокрема моделі перешкод, трафіку та поширення сигналів. Розглянуто моделювання аспектів функціонування мережі LoRa, таких як аналіз модуляції, модель вимірювання зв'язку, модель втрат при поширенні сигналу, втрат через проникнення в будівлю, корельоване затінювання, модель продуктивності зв'язку, чутливість приймача, перешкоди та модель шлюзу.

Третій розділ містить опис удосконаленого методу оптимізації взаємодії компонентів IoT за стандартом LoRaWAN. Цей метод включає наступні

кроки: створення топології (набір вузлів), побудова моделі (встановлення протоколів на вузли), налаштування конфігурації (налаштування параметрів моделі протоколу та зв'язки між вузлами), запуск системи (моделювання через клас Simulator), та аналіз продуктивності (збір і аналіз даних після зупинки моделювання). Результати показали, що схема доступу LoRaWAN має вищу пропускну здатність у порівнянні з типовою схемою на основі ALOHA, завдяки частковій ортогональності її поширення. Архітектура LoRaWAN добре масштабується, оскільки збільшення кількості шлюзів покращує покриття та надійність зв'язку.

У четвертому розділі представлено програмно-апаратну реалізацію удосконаленого методу оптимізації взаємодії компонентів IoT за стандартом LoRaWAN через проведення експериментальних досліджень. Для цього використовувалося програмне забезпечення Network Simulator 3 (NS3) з пакетом для симуляції дискретних подій (DES). Симулятор був розширений завдяки створенню модуля lora, що реалізує різні моделі. Спочатку надається введення в програмне забезпечення NS3, а потім описується структура та впровадження модуля lora. Експериментальні дослідження показали, що спроектована мережа LoRa, реалізована за допомогою удосконаленого методу оптимізації, забезпечує успіх доставки пакетів більше 95% для шлюзу, що свідчить про ефективність оптимізації взаємодії компонентів мережі за стандартом LoRaWAN.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. URL:lorawan-range-part-1-the-most-important-factors-for-a-goodlorawan-signal-

2. P. Chaudhari, A. K. Tiwari, S. Pattewar and S. N. Shelke. Smart Infrastructure Monitoring using LoRaWAN Technology. International Conference on System, Computation, Automation and Networking (ICSCAN), 2021, pp. 1-6, doi: 10.1109/ICSCAN53069.2021.9526490.

3. S. E. Efimov, N. V. Stepanov and A. M. Turlikov. Research LoRaWAN Collide Signals with Used SDR, Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), 2021, pp. 1-5, doi: 10.1109/WECONF51603.2021.9470748.

4. A. Xanthopoulos, A. Valkanis, G. Beletsioti, G. I. Papadimitriou and P. Nicopolitidis. On the Use of Backoff Algorithms in Slotted ALOHA LoRaWAN Networks," 2020 International Conference on Computer, Information and Telecommunication Systems (CITS), 2020, pp. 1-4, doi: 10.1109/CITS49457.2020.9232577.

5. H. E. Elbsir, M. Kassab, S. Bhiri and M. H. Bedoui, "Evaluation of LoRaWAN Class B efficiency for downlink traffic. 16th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2020, pp. 105-110, doi: 10.1109/WiMob50308.2020.9253405.

6. A. I. Petrariu, A. Lavric and E. Coca, LoRaWAN Gateway: Design, Implementation and Testing in Real Environment. IEEE 25th International Symposium for Design and Technology in Electronic Packaging (SIITME), 2019, pp. 49-53, doi: 10.1109/SIITME47687.2019.8990791.

7. Y. Jeon and Y. Kang. Implementation of a LoRaWAN protocol processing module on an embedded device using Secure Element. 34th International Technical 95 Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), 2019, pp. 1-3, doi: 10.1109/ITC-CSCC.2019.8793333.

8. F. L. de Almeida, M. Barros de Almeida and A. Petronio. Análise experimental e melhorias de desempenho de junção à rede via OTAA através de estratégias de ciclo útil em redes LoRAWAN, 14th IEEE International Conference on Industry Applications (INDUSCON), 2021, pp. 324-331, doi: 10.1109/INDUSCON51756.2021.9529921.

9. X. Xiong, K. Zheng, R. Xu, W. Xiang, P. Chatzimisios. Low power wide area machine- to-machine networks: key techniques and prototype. IEEE Communications Magazine. 2015. vol. 53. no. 9. pp. 64–71.

10. LoRa-Alliance, LoRa AllianceOR FAQs is there really a need for lpwan. URL: https:// lora-alliance.org/about-lora-alliance.

11. R. Sanchez-Iborra, J. Sanchez-Gomez, J. Ballesta-Vin˜as, M.-D. Cano, A. F. Skarmeta. Performance evaluation of lora considering scenario conditions. Sensors. 2018. vol. 18. no. 3. p. 772.

12. R. Sanchez-Iborra and M.-D. Cano. State of the art in lp-wan solutions for industrial iot services. Sensors. 2016. vol. 16. no. 5. p. 708.

13. F. C. Commission. Fcc regulations: 2013. Cfr 47. part 15.247 operation within the bands 902–928 mhz, 10–1–13 Edition). URL: https://www.govinfo.gov/content/pkg/CFR-2013-title47-vol1/pdf/CFR-2013title47-vol1-sec15-247.pdf.

14. K. Mekki, E. Bajic, F. Chaxel, and F. Meyer. A comparative study of lpwan technologies for large-scale iot deployment. ICT express. 2019. vol. 5. no. 1. pp. 1–7.

15. IoT Analytics iot connectivity. URL: https://iot-analytics.com/iotsegments/ iot-connectivity.

16. LoRa-Alliance, LoRa Alliance about the lorawan specification. URL:https:// LoRa-alliance.org/LoRawan-for-developers.

17. LoRa-Alliance, LoRa Alliance about lora alliance. URL: https://loraalliance.org/ about-lora-alliance.

18. LoRa-Alliance. A technical overview of lora and lorawan. White paper. 2015. URL: https: //lora-alliance.org/resource-hub/what-lorawanr.

19. R. S. Sinha, Y. Wei, and S.-H. Hwang. A survey on lpwa technology: Lora and nb-iot. Ict Express. 2017. vol. 3. no. 1. pp. 14–21.

20. S. Corporation, Sx1272/3/6/7/8: Lora modem. Designer's Guide AN1200.13. 2013. URL: https://www.rs-online.com/designspark/rel-assets/dsassets/uploads/ knowledge-items/application-notes-for-the-internet-of-things/LoRa% 20Design%20Guide.pdf.

21. LoRa / LoRaWAN Tutorial 16 snr limit receiver sensitivity. URL: https://www.mobilefish. com/download/lora/lora_part16.pdf.

22. Semtech-Corporation. Lora modulation basics, AN1200.22. 2015.

23. Leverege - LPWAN White Pape link budget. Dec 2016. URL:https://www.leverege.com/ research-papers/lpwan-white-paper.

24. SmartMakers GmbH lorawan-range. part 1: The most important fac- tors for a good lorawan radio range. URL: https://smartmakers.io/en/.

25. L. Maziero et al. Monitoring of Electric Parameters in the Federal University of Santa Maria Using LoRaWAN Technology. PES Innovative Smart Grid Technologies Conference - Latin America (ISGT Latin America), 2019, pp. 1-6, doi: 10.1109/ISGT-LA.2019.8895425.

26. LoRa-Alliance. Lorawan security full end-to-end encryption for iot application providers. White Paper. 2017. URL: https://lora-alliance.org/resource-hub/ lorawan-security-whitepaper,

27. Semtech - LoRa and LoRaWAN: A Technical Overview lorawan network elements: Security. URL: https://lora-developers.semtech.com/library/tech-papersand-guides/ lora-and-lorawan/.

28. A. J. Wixted, P. Kinnaird, H. Larijani, A. Tait, A. Ahmadinia, N. Strachan.Evaluation of lora and lorawan for wireless sensor networks. IEEE SENSORS. 2016.pp. 1–3.

29. J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler. 97 Integration of lorawan and 4g/5g for the industrial internet of things. IEEE Communications Magazine. 2018. vol. 56. no. 2. pp. 60–67.

30. A. Lavric and V. Popa. Internet of things and loraTM low-power widearea

networks: a survey. IEEE International Symposium on Signals, Circuits and Systems (ISSCS). 2017. pp. 1–5.

31. R. Parada, D. Ca´rdenes-Tacoronte, C. Monzo, and J. Melia`-Segu´ı. Internet of things area coverage analyzer (ithaca) for complex topographical scenarios.Symmetry. 2017. vol. 9. no. 10. p. 237.

32. G. Callebaut and L. Van der Perre. Characterization of lora point-to-point path-loss: Mea- surement campaigns and modeling considering censored data. IEEE Internet of Things Jour- nal. 2019.

33. R. El Chall, S. Lahoud, and M. El Helou. Lorawan network: radio propagation models and performance evaluation in various environments in lebanon.IEEE Internet of Things Journal. 2019. vol. 6. no. 2. pp. 2366–2378.

34. Dragino Products lora iot development kit. URL: https://www.dragino.com/products/LoRa/item/120-LoRa-iot-kit.html.

35. Adeunis Wireless Products and Solutions iot sensors fdt network tester. URL: https://www.adeunis.com/en/produit/ftd-network-tester/.

36. Dragino compare list for dragino lora gateway. URL: https://www.dragino.com/downloads/ index.php?dir=LoRa_Gateway/.

37. Semtech-Corporation. Lora and lorawan: A technical overview. Technical Paper. 2019.

38. CloudRF radio planning tool. URL: https://cloudrf.com/.

39. Semtech what is lora?. URL: https://lora-developers.semtech.com/get started/ what-is-lora/.

40. Semtech SX1276 products wireless rf. URL:98 https://www.semtech.com/products/ wireless-rf/lora-transceivers/sx1276.

41. Semtech SX1301 products wireless rf. URL:https://www.semtech.com/ products/wireless-rf/lora-gateways/sx1301.

42. LoRa-Alliance. Lorawan 1.1 specification, technical specification. 2017.URL: https: //lora-alliance.org/resource-hub/lorawanr-specification-v11.

43. LoRa Overview cayenne docs. URL: https://developers.mydevices.com/cayenne/docs/ lora/#lora.

44. R. Wenner. LoRa CHIRP Spread Spectrum lora chirp. URL: https://www.youtube.com/ watch?v=dxYY097QNs0.

45. M. Knight. Decoding LoRa exploring next-generation wireless networks. URL: https://github.com/matt-knight/research/tree/master/2016.

46. Qoitech. How Spreading Factor affects LoRaWAN device battery life the things conference partner. URL: https://www.thethingsnetwork.org/article/ howspreading-factor-affects-lorawan-device-battery-life.

47. ETSI. Etsi tr 103 526: Technical characteristics for low power wide area networks chirp spread spectrum (lpwan-css). ETSI Technical Report. 2018.

48. Federal Communications Commission what we do. URL: https://www.fcc.gov/about-fcc/ what-we-do, Jul 2017.

49. LoRa-Alliance, Rp002-1.0.0 lorawan regional parameters, Regional Parameters, 2010. URL: https://https://lora-alliance.org/sites/default/files/2019-11/rp_ 2-1.0.0_final_release.pdf.

Додаток А

(обов’язковий)

Набір класів, необхідних для моделювання стеку протоколів на пристрої

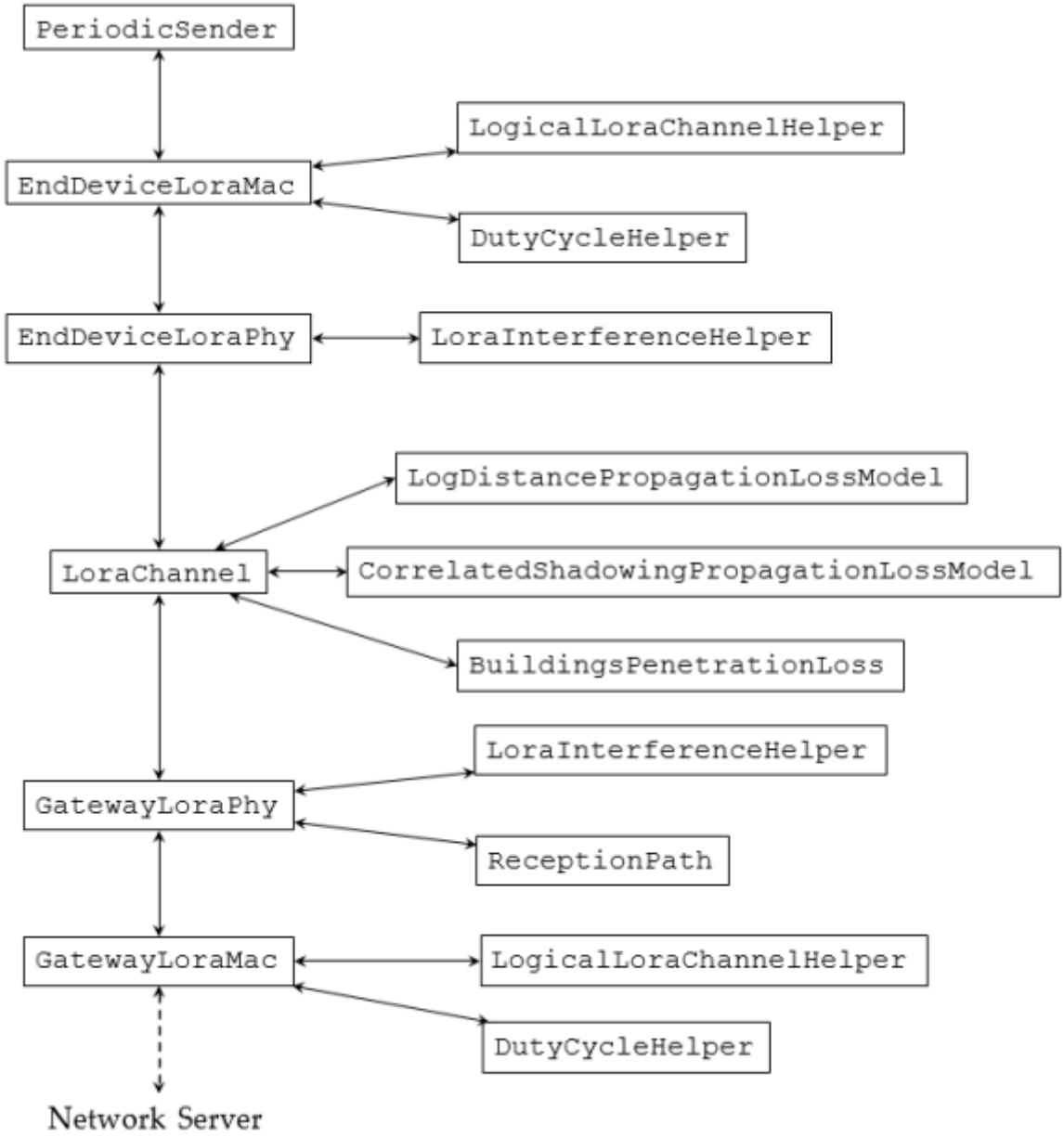


Рисунок А.1 – Стек LoRaWAN, як він був представлений у модулі lora

Додаток Б

(обов’язковий)

Розподіл факторів розповсюдження для різних моделей поширення

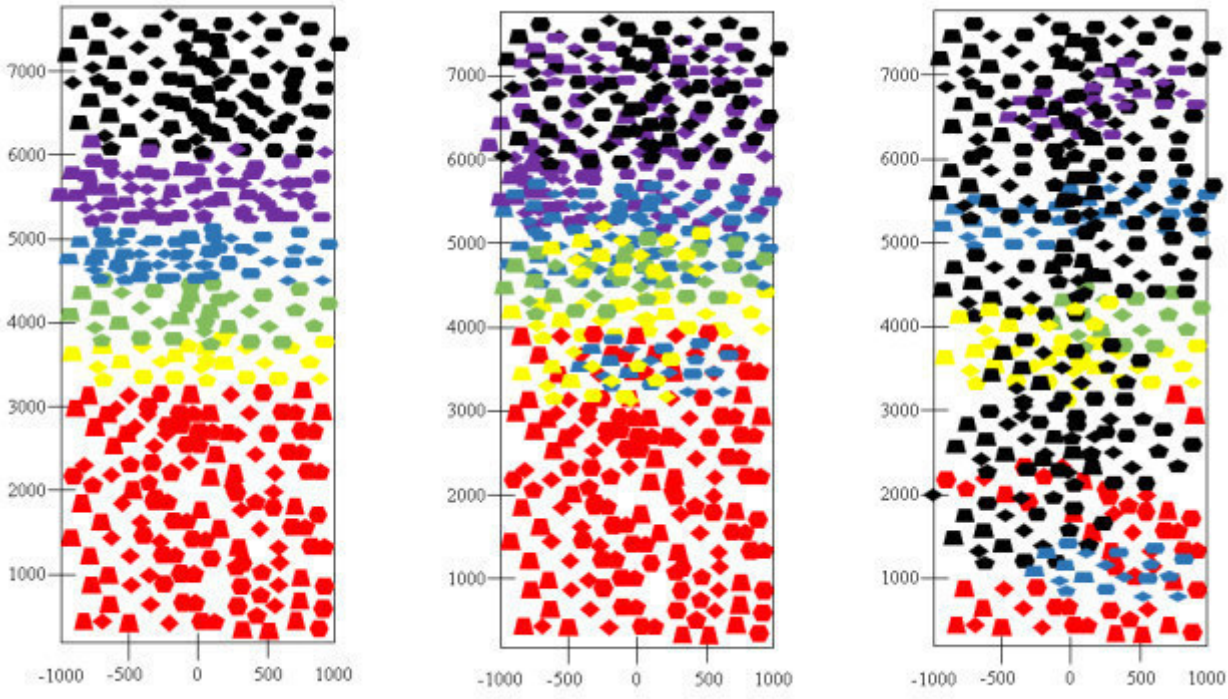


Рисунок Б.1 – Розподіл факторів розповсюдження для різних моделей поширення:

а) звичайне поширення сигналу;

б) поширення сигналу із затінюванням;

в) поширення сигналу із затінюванням та перешкодами, спричиненими будівлями

Додаток В

(обов’язковий)

Копія тез доповіді на Всеукраїнській науково-практичній конференції

ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ

XX Міжнародної науково-практичної конференції

**«Військова освіта і наука:
сьогодення та майбутнє»**

29 листопада 2024 року

Київ – 2024

Військова освіта і наука: сьогодення та майбутнє : зб. тез доповідей XX Міжнародної науково-практичної конференції, м. Київ, 29 листопада 2024 р. Київ : Військовий інститут Київського національного університету імені Тараса Шевченка, 2024. 532 с.

Рекомендовано до друку Вченою радою Військового інституту Київського національного університету імені Тараса Шевченка
(протокол від 21.11.2024 № 3).

У збірнику тез доповідей друкуються матеріали виступів наукових і науково-педагогічних працівників, курсантів (студентів) Військового інституту Київського національного університету імені Тараса Шевченка та інших вищих військових та закладів вищої освіти України.

У публікаціях розглядаються: технічні проблеми озброєння і військової техніки та технології подвійного призначення; актуальні проблеми лінгвістичного забезпечення Збройних Сил України; актуальні питання військової психології та соціальної роботи; інформаційна та психологічна боротьба у воєнній сфері; інформаційно-медійне забезпечення МОУ та ЗСУ в умовах правового режиму воєнного стану; фінанси; актуальні проблеми військового права в умовах воєнного стану; актуальні проблеми геопросторової підтримки військ в умовах ведення російсько-української війни; наукові проблеми воєнної політології та морально-психологічного впливу; аналіз бойового застосування частин (підрозділів) Сухопутних військ Збройних Сил України у сучасному загальновійськовому бою (тактичних діях)

Зміст

Таким чином, ефективність управління логістичними процесами у сфері речового забезпечення військових частин України відіграє вирішальну роль у забезпеченні боєздатності армії. Впровадження сучасних методів управління, зокрема ERP-систем та автоматизованих складів, значно покращує процеси забезпечення, скорочує час на доставку матеріальних ресурсів та підвищує ефективність використання наявних ресурсів. Однак для досягнення максимальних результатів необхідно розв'язувати питання фінансування та підготовки кадрів, а також адаптувати логістичні системи до умов війни.

Слободянюк А.С. (ХмНУ)
к.т.н., доц. Пивовар О.С. (ХмНУ)
д.т.н., проф. Лєнков С.В. (ВІКНУ)

ОПТИМІЗАЦІЯ ВЗАЄМОДІЇ ТЕХНОЛОГІЙ IoT та LoRaWAN

На даний час різноманітні Інтернет технології широко застосовуються як для цивільних, так і для військових потреб. Необхідність економії електричної енергії стала повсякденною необхідністю і парадигма застосування глобальних мереж низького енергоспоживання LPWAN в діючих стандартах передачі різноманітних даних потребує глибокого дослідження в рамках організації конкуренції із іншими існуючими стандартами передачі даних.

Саме в цьому контексті концепція технології LoRaWAN дозволяє отримати позитивні результати, через забезпечення дещо вищої пропускної спроможності та часу подвійного оберту(ping) без суттєвого збільшення складності системного забезпечення керування доступом.

Докладне моделювання поширення сигналів LoRa на системному рівні, що враховує реалістичний сценарій розташування мережевих вузлів для інтеграції в IoT дозволяє провести оцінку доцільності розробки модулів, що поєднують в собі найкращі риси IoT та LoRa.

Розроблена та досліджена модель програмно-апаратної реалізації удосконаленого методу оптимізації конвергенції компонентів IoT та LoRaWAN на базі програмного забезпечення Network Simulator (DES) із згенерованим модулем Lora та проведено ряд експериментальних досліджень.

Сценарій для побудови моделі - міська забудова радіусом близько 7 км, що охоплюється шлюзом таким чином, щоб кінцеві пристрої також обслуговувались суміжними шлюзами діючими в рамках глобальної гексагональної сітки. шлюзами так що вся територія все ще покривалася одним шлюзом, де кінцеві пристрої охоплюють глобальною гексагональною сіткою. В рамках такої моделі великий відсоток вузлів та кінцевих споживачів IoT попадають в зону радіотіні. В рамках позаміської плаской місцевості це відповідає радіусу горизонту огляду людини.

Дослідження під час моделювання показало, що для досягнення надійності обслуговування абонентів понад 95% шлюзи LoRaWAN мають бути розгорнуті таким чином, щоб кожен шлюз забезпечував радіус покриття близько 1,3км. Розроблений модуль симуляції дозволяє проводити оцінку

параметрів мережі Lora в рамках обслуговування пристроїв IoT на заданій території із заданою якістю на рівнях MAC та PHY та по відношенню до типової схеми ALOHA забезпечує просту доступність масштабування та покращений рівень надійності висхідного зв'язку із коефіцієнтом втрати пакетів в найгіршому випадку не більше 3%.

доктор філософії Стецюк М.В. (ХмНУ)
Панько Р. (ХмНУ)

КІБЕРЕТИКА ТА ПРАВО: ЕТИЧНІ ПИТАННЯ У КІБЕРПРОСТОРІ, ПРОБЛЕМИ ЗЛАМІВ, КІБЕРШПИГУНСТВА, ВПЛИВ НА ПРАВА І СВОБОДИ ЛЮДИНИ

Проблема зламів та прав людини: Кіберінструменти на зразок шпигунських програм, як-от Pegasus, можуть перетворити смартфон на засіб для 24-годинного спостереження, що порушує приватність користувачів і часто використовується не за призначенням, наприклад, для утисків активістів і журналістів. Це вимагає встановлення жорстких міжнародних обмежень на продаж та використання таких технологій.

Етичні принципи у кібервійнах: Міждержавні кібератаки часто мають серйозні наслідки, однак їх регулювання досі залишається недосконалим. Професор Маріаросарія Таддео підкреслює необхідність пропорційного та відповідального підходу до кібернападів, зокрема відокремлення цільових військових об'єктів від цивільних у кіберпросторі. Крім того, існує потреба в нових етичних та правових рамкових документах, щоб врахувати унікальні ризики, пов'язані з кібероперaціями.

Приватність та цифровий моніторинг: За даними ООН, зростаюча кількість цифрових технологій для моніторингу, включаючи розпізнавання облич та аналіз соціальних мереж, підривають право на приватність і часто порушують права людини. Це вимагає запровадження контролю над застосуванням біометричних технологій та масового збору даних, а також прозорості державних програм спостереження.

Наслідки цифрового стеження для демократії: Використання шпигунського ПЗ та інших засобів масового спостереження підриває основи демократії, адже вони здатні обмежувати свободу слова та зменшувати плюралізм думок. Згідно з ООН, цифрове стеження часто виходить за межі своєї заявленої мети – боротьби з тероризмом – і стає інструментом контролю за журналістами, правозахисниками та опозиційними політиками, що робить його загрозою для прав людини.

Етичні стандарти для військових кібероперацій: Професор Маріаросарія Таддео підкреслює необхідність узгодження міжнародних етичних принципів для кібероперацій, зокрема на основі Міжнародного гуманітарного права. Ці принципи включають пропорційність дій, чітке розмежування військових і цивільних цілей, а також необхідність обмеження масштабів атаки, щоб мінімізувати побічний збиток і уникнути непоправних наслідків для цивільних.

Наукове видання

ТЕЗИ ДОПОВІДЕЙ

XX Міжнародної науково-практичної конференції

«Військова освіта і наука: сьогодення та майбутнє»

Тексти тез представлено у авторській редакції. Автори несуть повну відповідальність за зміст, добір, точність наведених фактів, цитат, власних імен, дат та інших відомостей.

Збір, технічне редагування та комп'ютерна верстка – Бадрук О.О.
Оригінал-макет та обкладинка – Халіманенко С.М.

Підписано до друку 21.11.2024. Формат 60x84/16.
Гарнітура Times. Папір офсетний. Друк ризограф. Тираж 10.
Умов. друк. аркушів 18. Заказ № 41-16.

Надруковано в навчальному картографічному комплексі ВІКНУ
03189, Київ, вул. Юлії Здановської, 81
521-32-89

НКК ВІКНУ

531

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ

Направляється студент Слободянюк Андрій Сергійович на захист дипломного проєкту (роботи)
(прізвище, ім'я, по батькові)

за спеціальністю 172 - Електронні комунікації та радіотехніка

На тему: Метод конвергенції технологій IoT та LoRaWan

Дипломний проєкт (робота), рецензія і довідка про перевірку на плагіат додаються.

Декан факультету _____ Тетяна Товстюк
(підпис) (ім'я, прізвище)

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ДОВІДКА УСПІШНОСТІ

Слободянюк А. С. за період навчання на факультеті інформаційних технологій з 2023 по 2024 роки повністю виконав навчальний план спеціальності з таким розподілом оцінок за:
національною шкалою: відмінно 37,50 %, добре 50,00 %, задовільно 12,50 %.
шкалою ЄКТС: A 30,77 %, B 23,08 %, C 23,08 %, D 7,69 %, E 15,38 %.

Методист факультету _____ Тетяна Бондар
(підпис) (ім'я, прізвище)

ВИСНОВОК КЕРІВНИКА ДИПЛОМНОГО ПРОЄКТУ (РОБОТИ) ТА ОБГРУНТУВАННЯ ОЦІНКИ

Студент Андрій Слободянюк, під час виконання кваліфікаційної роботи виявив творчий підхід до виконання роботи із програмно-апаратними засобами сучасних прогресивних технологій зв'язку, досягнув бажаного та гарного керівника, дотримувався вимог оформлення, результати можуть бути корисними в сучасних умовах

Оцінка дипломного проєкту (роботи) відмінно

Керівник дипломного проєкту 12.12.24 Олег ПИВОВАР
(підпис) (ім'я, прізвище)

"12" грудня 2024 р.

ВИСНОВОК КАФЕДРИ ПРО ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ)

Дипломний проєкт (роботу) розглянуто. Студент Слободянюк А. С. допускається до захисту цього проєкту (роботи) в екзаменаційній комісії.

Завідувач кафедри Телекомунікацій, медійних та інтелектуальних технологій
(назва)

Сергій ПІДЧЕНКО "12" грудня 2024 р.
(підпис, ім'я, прізвище)

Завідувачу кафедри
телекомунікацій, медійних та
інтелектуальних технологій (ТМІТ)
Сергію ПІДЧЕНКО
здобувача вищої освіти студента
2 курсу, гр. ТРм-22-1
Андрія СЛОБОДЯНЮКА

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщена та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Strikeplagiarism та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

11.12.24 _____ Слободянюк А.С.

дата підпис

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Андрій СЛОБОДЯНЮК

Співавтор:

Назва: Метод конвергенції технологій IoT та LoRaWAN

Експерт: Олег ПИВОВАР, к.т.н., доц

Підрозділ: Кафедра телекомунікацій, медійних та інтелектуальних технологій

Коефіцієнт подібності 1:17.4%

Коефіцієнт подібності 2:4.7%

Мікропробіли: 0

Заміна букв: 2

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2024-12-11 08:02:09.0

Після аналізу **Звіту подібності констатую наступне:**

☑ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

Дата 11.12.24 експерт Доц. каф. ТМІТ Пивовар О.С.

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 2.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 7%**

ID: 157768 Назва: Метод конвергенції технологій IoT та LoRaWan Додано в БД: 2024-12-11 Автора: Слободянюк Андрій Сергійович Керівники: Пивовар Олег Сергійович Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	101616	1642	2136 (2%)	35 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ КАФЕДРИ

ТЕЛЕКОМУНІКАЦІЙ, МЕДІЙНИХ ТА ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Синтез хаотичної системи звязку із нелінійним каналом передачі

Автор: **Слободянюк Андрій Сергійович**

Спеціальність: **172 Електронні комунікації та радіотехніка**

Освітня програма: Електронні інформаційно-комунікаційні системи та мережі

Науковий керівник: **к.т.н., доц. Пивовар Олег Сергійович**

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	**Відповідає**
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження: Запозичення у розмірі 17,4% є випадковими збігами переважно із бібліографічним записом джерел посилань та типовими бланками, та не є плагіатом.

Відповідальний за контроль плагіату за системою:

StrikePlagiarism 11.12.24р. _____ Олег ПИВОВАР

Antiplagiarism 11.12.24р. _____ Віктор СТЕЦЮК

Зав. каф. ТМІТ 11.12.24р. _____ Сергій ПІДЧЕНКО

РЕЦЕНЗІЯ

на дипломну роботу студента групи ЕКРм-23-1

Слободянюка Андрія Сергійовича

«Метод конвергенції технологій IoT та LoRaWAN»

Кваліфікаційна робота магістра присвячена питанням оптимізації взаємодії компонентів Інтернету речей за стандартом LoRaWAN із застосуванням удосконалених методів і програмно-апаратних засобів.

Робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел, що налічує 50 позицій, та додатків. Загальний обсяг основного змісту роботи становить 92 сторінки, які включають 48 рисунків, розміщених на 40 сторінках тексту, та 35 формул. Повний обсяг роботи – 107 сторінок.

У вступі обґрунтовано актуальність тематики роботи, враховуючи значний ріст IoT-технологій у світі. Визначено мету, завдання, наукову новизну та практичну цінність дослідження.

Перший розділ присвячено аналізу технологій IoT, зокрема стандарту LoRaWAN, а також дослідженню основних вимог до систем Інтернету речей. Окремо розглянуто особливості модуляції LoRa, структуру протоколу LoRaWAN, діапазони частот, шифрування та класи пристроїв.

Другий розділ зосереджено на моделюванні компонентів системи LoRaWAN. Розроблено моделі поширення сигналу, втрат у будівлях, чутливості приймачів та впливу перешкод. Проведено аналіз модуляції LoRa та розроблено модель шлюзу, що враховує фізичні та мережеві параметри.

Третій розділ містить опис удосконаленого методу оптимізації взаємодії компонентів IoT за стандартом LoRaWAN. Цей метод передбачає створення топології вузлів, налаштування протоколів та аналіз продуктивності мережі. Отримані результати показують підвищення ефективності доставки пакетів до 95%, що перевищує показники стандартних підходів.

Четвертий розділ присвячено програмно-апаратній реалізації розробленого методу. Для моделювання мережі використовувалося програмне забезпечення Network Simulator 3 (NS3) із розширенням у вигляді спеціального модуля lora. Проведено експериментальні дослідження, які підтвердили масштабованість системи та її придатність для впровадження у великих мережах.

Процес висвітлення завдань є логічно пов'язаним, припущення роботи достатньо обґрунтовані, а оформлення пояснювальної записки відповідає вимогам університету.

Серед позитивних сторін роботи варто відзначити:

- актуальність тематики у контексті розвитку IoT-технологій;
- комплексний підхід до моделювання та оптимізації систем LoRaWAN;
- високий рівень деталізації експериментальних досліджень;
- значний практичний потенціал розробленого програмно-апаратного рішення.
-

До недоліків роботи можна віднести:

- недостатнє дослідження впливу зовнішніх чинників на роботу мережі;
- обмежене представлення варіацій вхідних параметрів у моделюванні;
- місцями недостатньо детальний опис реалізації модуля lora для NS3.

Загалом дипломна робота магістра є актуальною, має значні наукові та практичні результати, і заслуговує на оцінку "відмінно".

Рецензент: Денис МАКАРИШКІН

12.12.2024

доцента к.т.н.,
кафедри АКІТтаР

Метод конвергенції технологій IoT LoRaWAN

Студент: Слободянюк Андрій Сергійович

Керівник: Пивовар Олег Сергійович

Мета роботи: Оптимізація взаємодії компонентів Інтернету речей за стандартом LoRaWAN для підвищення ефективності передачі даних у мережах IoT.

Об’єкт дослідження: Процес оптимізації взаємодії компонентів Інтернету речей за стандартом LoRaWAN.

Предмет дослідження: Моделі, удосконалений метод та програмно-технічні засоби оптимізації взаємодії компонентів Інтернету речей за стандартом LoRaWAN.

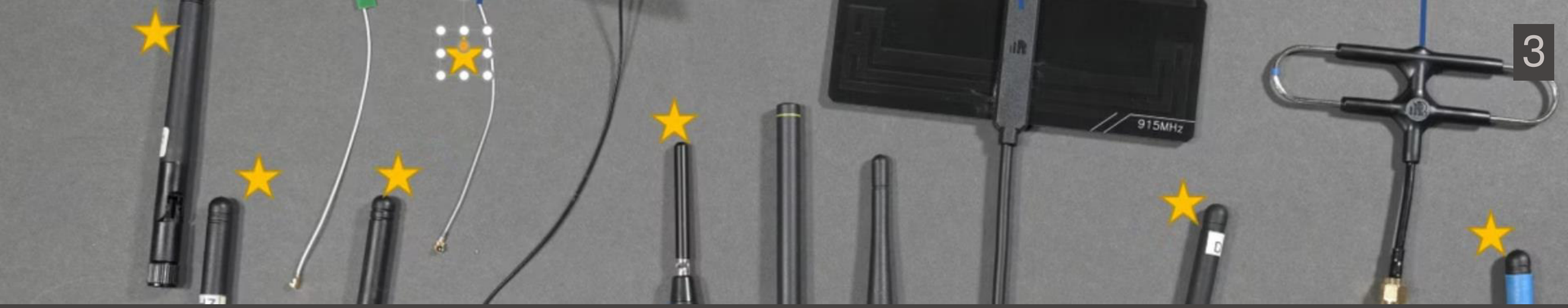
ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

Різноманітність галузей

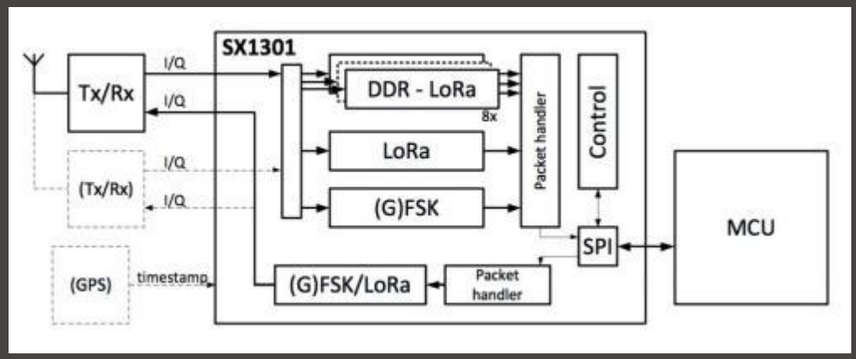
IoT технології застосовують в різноманітних сферах: виробництво, сільське господарство, охорона здоров'я, транспорт та ін.

З'єднання пристроїв

Ключовим завданням IoT є забезпечення зв'язку та обміну даними між різними пристроями, датчиками та системою.



Особливості технології LoRaWAN



Довготривала автономність

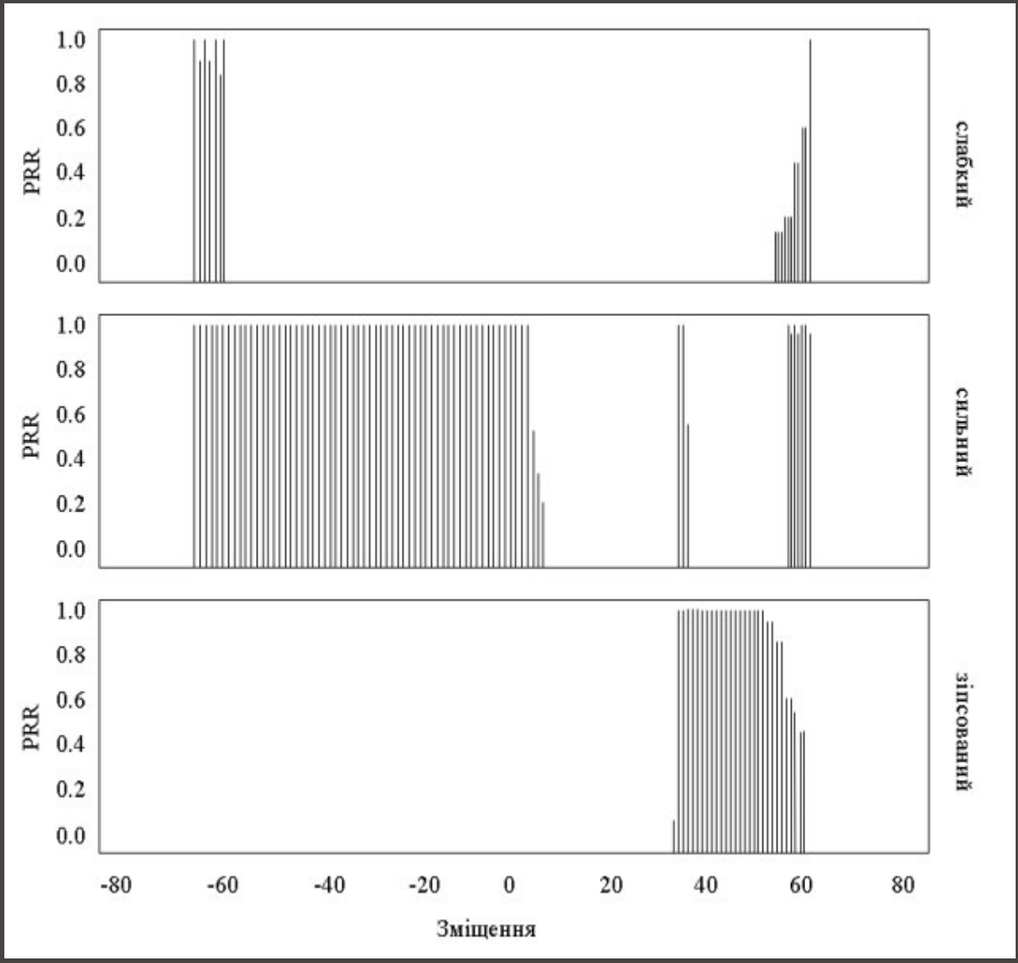
LoRaWAN дозволяє пристроям працювати на батареях до 10 років, забезпечуючи тривалу роботу без обслуговування.

Низьке енергоспоживання

Використовує мало енергії, ідеально для датчиків, які розташовані в важкодоступних місцях.

Дальність покриття

Сигнал LoRaWAN може поширюватися на великі відстані, ідеально для сільськогосподарських або промислових об'єктів.



Переваги та обмеження LoRaWAN

Переваги

Доступність, надійність, масштабованість, низька вартість, тривале життя батареї, гнучка архітектура.

Обмеження

Відносно низька швидкість передачі даних, обмежена пропускна здатність, можливі проблеми із затримкою.

Концепція конвергенції технологій

Інтеграція

Об'єднання різних технологій IoT, таких як LoRaWAN, Wi-Fi, Bluetooth, для досягнення синергічного ефекту.

Посилення

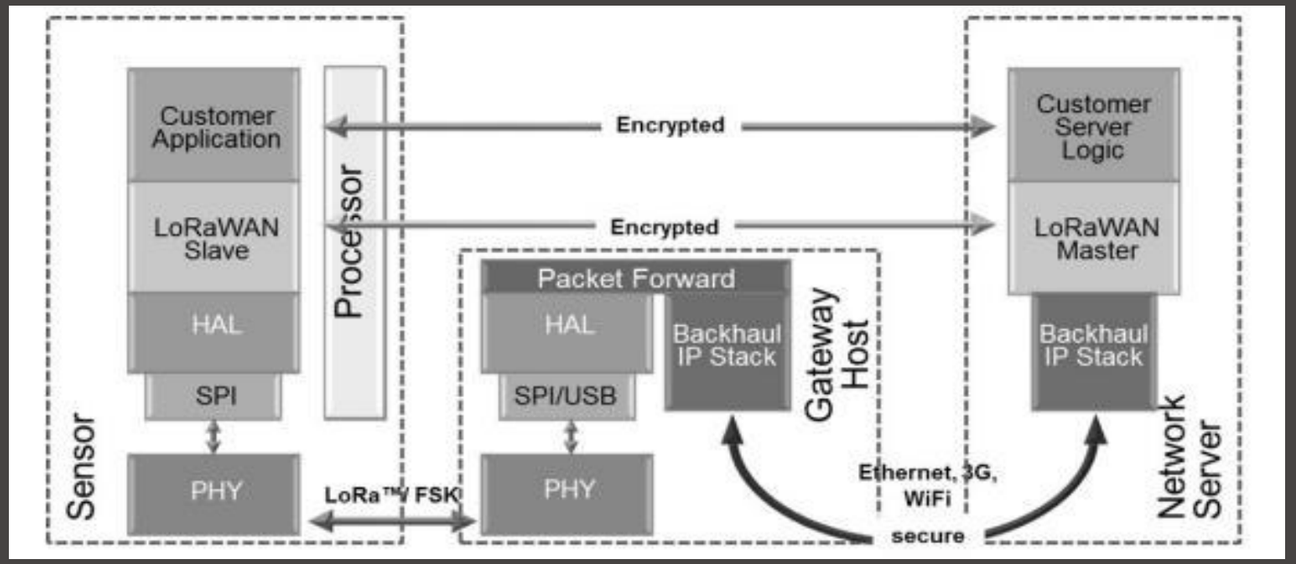
Конвергенція дозволяє доповнити сильні сторони однієї технології іншою, покращуючи загальну ефективність.

Ефективність

Конвергентні системи IoT забезпечують більш ефективне використання ресурсів та підвищення продуктивності.

Етапи реалізації методу конвергенції

1. Визначення потреб та вимог для системи IoT, включаючи функціональні та не функціональні аспекти.
2. Вибір оптимальних технологій та стандартів для кожного шару системи, враховуючи їх сильні сторони.
3. Розробка та реалізація архітектури системи IoT, яка інтегрує різні технології та протоколи.
4. Тестування та налаштування системи IoT для забезпечення її правильної роботи та відповідності вимогам.
5. Впровадження системи IoT в реальному середовищі, включаючи інтеграцію з існуючими системами та обслуговування.



Архітектура конвергентної IoT системи

1

Шари IoT системи:

2

Пристрої: датчики, актуатори, контролери.

3

Мережеві технології: LoRaWAN, Wi-Fi, Bluetooth, Ethernet.

4

Програмне забезпечення: платформи IoT, хмарні сервіси, аналітика даних.

Приклади практичного застосування

1

Сільське господарство

Моніторинг стану ґрунту, управління зрошенням та автоматизація процесів.

2

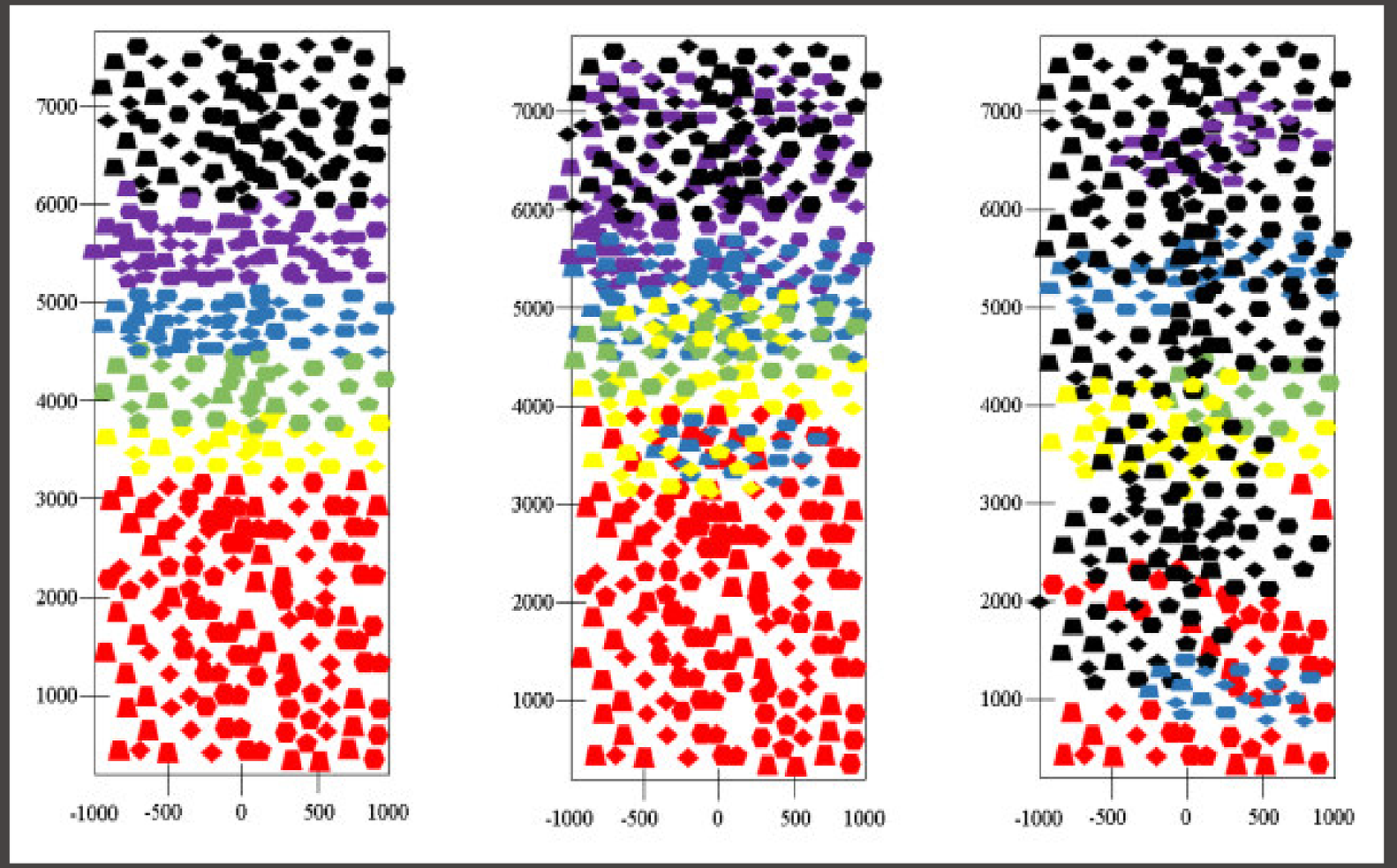
Промисловість

Відстеження руху товарів, контроль якості продукції та оптимізація виробничих процесів.

3

Охорона здоров'я

Моніторинг стану пацієнтів, віддалене управління медичним обладнанням та дистанційна діагностика.

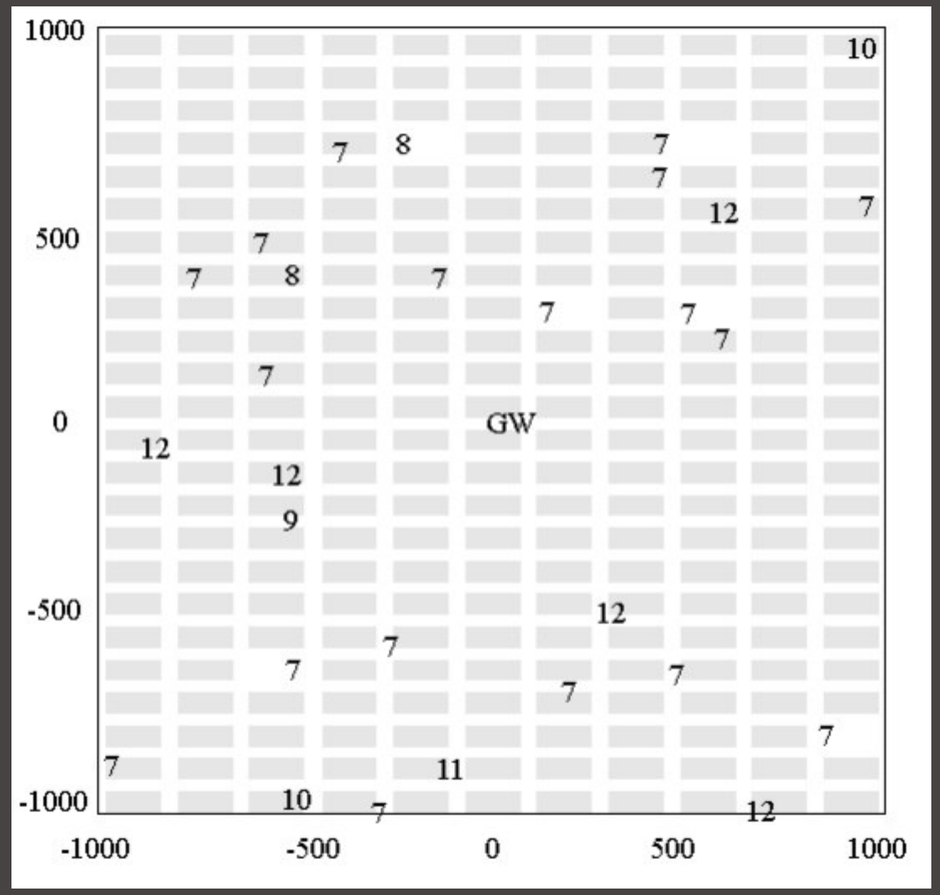


Розподіл факторів розповсюдження для різних моделей поширення

а) Звичайне поширення сигналу

б) Поширення сигналу із затінюванням

в) Поширення сигналу із затінюванням та перешкодами, спричиненими будівлями



Розподіл вузлів навколо шлюзу мережі

Висновки та перспективи розвитку

Конвергенція технологій IoT LoRaWAN відкриває безліч можливостей для створення інноваційних рішень. Перспективи розвитку включають в себе розширення масштабів застосування, підвищення ефективності та безпеки, а також інтеграцію з іншими технологіями.