UNICHECK

Ім'я користувача:
приховано налаштуваннями конфіденційності

ID перевірки:
1015438560

Дата перевірки:
05.06.2023 16:51:31 EEST

Тип перевірки:
Doc vs Library

Дата звіту:
05.06.2023 16:54:54 EEST

ID користувача:
100011372

Назва документа: **Кирилів Д. Н. гр ТК-41**

Кількість сторінок: **50** Кількість слів: **10707** Кількість символів: **79606** Розмір файлу: **1.81 MB** ID файлу: **1015099476**

3.68%
Схожість

Найбільша схожість: **1.36%** з джерелом з Бібліотеки (ID файлу: **1011186488**)

Пошук збігів з Інтернетом не проводився

3.68% Джерела з Бібліотеки | 28 ..... Сторінка 52

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | 1

1 ОГЛЯД ТЕХНОЛОГІЇ LORA

1.1 Характиристика технології LoRaWAN та її архітектура

LoRa – одна з перших технологій сучасних мереж LPWA, яка призначена для обслуговування IoT-пристроїв. Ця технологія є частотним розширенням спектра, яке було запатентовано в 2008 році компанією Cycleo (Франція). Cycleo розробляла рішення для бездротового зв'язку і напівпровідників, розумні лічильники і різні продукти як для споживчого, так і корпоративного ринків.

Технологія LoRa належить компанії чіпів - Semtech, яка придбала її у - Cycleo. Компанія Semtech створила Альянс LoRa, який розробляє глобальні стандарти та робить це доступним за ліцензійною ліцензією для своїх членів. Semtech вбудовує технологію LoRa у свої набори чіпів. Ці набори мікросхем потім вбудовуються в продукти, пропоновані величезною мережею партнерів IoT та інтегруються в LPWAN від операторів мобільної мережі по всьому світу.

LoRaWAN (Long Range wide-area networks, глобальна мережа великого радіусу дії) - найбільш відомий апаратний протокол LoRa, який призначений для управління зв'язком між LPWAN - шлюзами і кінцевими пристроями.

LoRaWAN базується на топології «зірка» (рис.1.1). Безліч пристроїв по бездротовому з'єднанню передають дані не на один шлюз, а відразу на кілька. Підключення між пристроями і шлюзами здійснюється на двосторонній основі. Зв'язок між шлюзами здійснюється через бездротові рішення, які використовують широкосмугову модуляцію LoRa або FSK. Технологія радіодоступу LoRa використовується в комунікаціях між кінцевим пристроєм і шлюзами. Шлюзи та мережевий сервер підключаються через стандартні IP-з'єднання.

Рисунок 1.1 – Архітектура LoRaWAN

Потім шлюзи, які отримали інформацію, перенаправляють отримані пакети від кінцевого вузла до хмарного мережного серверу, підключеного через мобільний або супутниковий зв'язок, провідний або бездротовий ШПД. Звідти дані надходять на сервери додатків.

Використання декількох шлюзів зручно тим, що кінцеві вузли не мають прив'язки. Це дозволяє гарантувати передачу інформації і контролювати пристрої, що знаходяться в русі. Наприклад, бездротові маячки, прикріплені до вантажних контейнерів, що переміщуються на тривалі відстані, зможуть без проблем обмінюватися даними так як не мають прив'язки до одного шлюзу.

Мережа LoRaWAN складається з наступних елементів: кінцевого пристрою, шлюзу, мережевого серверу і серверу додатків.

Кінцевий пристрій, вузол - об’єкт із вбудованим пристроєм зв'язку малої потужності. Пристрій LoRa End використовується для надсилання невеликої кількості даних на низьких частотах на великі відстані. Його можна використовувати в різних областях, таких як розумне місто, розумне будівництво, автоматизація фабрик, автоматизація ферм та логістика.

Шлюз - антени, які приймають трансляції з кінцевих пристроїв і передають дані назад на кінцеві пристрої через IP-зворотну передачу або 3G / 4G широкосмугові з'єднання.

Мережевий сервер – сервери, які управляють вією мережею, переносять повідомлення з кінцевих пристроїв у потрібну програму та назад. Коли він отримує пакети, він видаляє надмірність пакетів і виконує перевірку безпеки, а

потім визначає найбільш підходящий шлюз для повернення повідомлення підтвердження.

Сервер додатків – це кінцевий сервер, на якому всі дані, що надсилаються кінцевим пристроєм, виконуються після обробки процесів.

Радіоінтерфейс фізичного рівня, який визначає всі аспекти передачі радіосигналів між різними вузлами мережі (шлюзами LoRa) і кінцевими пристроями (сенсорами IoT). Фізичний радіоінтерфейс LoRa заснований на використанні широкосмугових радіосигналів з великою базою. Радіоінтерфейс LoRa встановлює робочі частоти, види модуляції, рівні потужності, сигналізацію і обмін сигналами між передавальними і приймальними пристроями в мережі LoRa.

Ключові характеристики радіоінтерфейсу LoRa:

– використання спектру поширення чіпа на радіоінтерфейсі;

– неліцензійний діапазон 868 МГц для Росії, СНД, країн Близького Сходу і Африки;

– ширина каналу 125 кГц, відстань між центрами сусідніх каналів – 200 кГц;

– підтримка UL і DL;

– модуляція Spread spectrum дозволяє системі працювати на низьких рівнях модуляції (до -20 дБ);

– використання ортогональних SF: якщо два сигналу прийняті одночасно і різниця в рівнях менше 20 дБ, то приймач може обробити обидва сигналу;

– адаптивне призначення швидкості передачі даних в залежності від радіо умов (для нерухомих кінцевих пристроїв) - від 250 кб / с до 5.4 кБ / с для каналу шириною 125 кГц;

– ACK / NAK процедури (в разі якщо в MAC заголовку зазначений тип "confirmed data");

– рандомне використання каналів всередині діапазону для передавання інформації;

– Duty cycle (обмеження часу передачі інформації);

– підтримка мобільності (пакет в UL приймається декількома LoRa шлюзами, пакет в DL відправляється через "кращий" LoRa шлюз;

– визначення місцяположення кінцевого пристрою на основі тріангуляції.

Мережева архітектура LoRa, яка включає абонентські пристрої IoT / M2M, шлюзи LoRa (базові станції), мережеві сервера, підключені по транспортнії мережі до мережі Інтернет та сервера додатків.

Абонентські пристрої IoT / M2M мережі LoRa є, як правило, є пристроями, що включають крім модему датчики або сенсори, які передають дані лише в короткі проміжки часу за заданим графіком.

Шлюзи LoRa (базові станції) призначені для побудови радіальних мережевих архітектур (тип «зірка») великого радіусу дії на базі технології LoRaWAN.

Центральний сервер мережі LoRaWAN, який керує адресно пристроями (кінцевими вузлами), шлюзами мережі і з'єднує мережу доступу LoRaWAN з сервером додатків.

Стек протоколів LoRaWAN представлений на (рис.1.2).

Рисунок 1.2 – Стек протоколів LoRaWAN

LoRa підтримує безліцензійні радіочастотні діапазони субгігагерців, такі як 433 МГц(EU), 868 МГц(EU) та 915 МГц(US). LoRa забезпечує передачу на велику відстань (більше 10 км у сільській місцевості) з низьким енергоспоживанням. Технологія побудована на двох частинах: LoRa, фізичний рівень та LoRaWAN (широкополосна мережа широкого діапазону), верхні шари.

У січні 2018 року було оголошено про нові набори мікросхем LoRa зі зменшеним енергоспоживанням, збільшеною потужностю передачі та зменшенням розміру в порівнянні зі старшим поколінням.

У пристроях LoRa є геолокаційні можливості, які використовуються для тріангулювання позицій пристроїв через часові позначки від шлюзів.

Протокол фізичного рівня LoRa є власником; отже, немає вільно доступної офіційної документації, хоча Semtech надав огляд модуляції та інших відповідних технічних характеристик.

LoRa використовує запатентовану модуляцію з розширеним спектром, схожу на похідну модуляції Chirp з розширеним спектром (CSS). Це дозволяє LoRa торгувати швидкістю передачі даних для чутливості з фіксованою пропускною здатністю каналу, вибираючи кількість використовуваного розповсюдження (вибір радіо-параметра від 7 до 12). Цей коефіцієнт поширення необхідний для визначення швидкості передачі даних та для диктування чутливості радіо. Крім того, LoRa використовує кодування виправлення помилок вперед для підвищення стійкості до перешкод. Високий діапазон LoRa характеризується надзвичайно високими бюджетами бездротового зв'язку, приблизно від 155 дБ до 170 дБ.

Абонентські пристрої IoT / M2M мережі LoRa є, як правило, датчиками або сенсорами, які передають дані лише в короткі проміжки часу по заданому графіку і діляться на три класи. Кожен клас має свої особливості, які визначаються цільовим призначенням:

– Двонаправлені кінцеві пристрої класу A. Такі пристрої LoRa дозволяють організувати двонаправлений обмін і передавати інформацію короткими посилками на шлюз за відповідно заданим графіком. Зв'язок ініціює пристрій, після чого він виділяє два тимчасових вікна, протягом яких очікується відповідь від сервера.Інтервал передачі планується кінцевим пристроєм на основі власних потреб.

Пристрої класу A мають найменшу потужність споживання і застосовуються в додатках, де передача даних від сервера потрібна тільки після

того, як кінцевий пристрій відсилає на нього дані. Передача інформації від сервера кінцевому вузлу здійснюється тільки після того як останній вийде на зв'язок.

– Двонаправлені кінцеві пристрої класу Б. Вони, на додаток до функцій пристроїв класу А, відкривають додаткове вікно прийому по заданому розкладу.

Для того, щоб відкрити вікно прийому, вони синхронізуються по спеціальному опорному сигналу від шлюзу (beacon). Це дозволяє серверу визначити момент часу, коли кінцевий пристрій готовий приймати дані.

– Двонаправлені кінцеві пристрої класу С з максимальним прийомним вікном. Ці пристрої мають вікно прийому майже безперервно відкрите, яке закривається тільки на час передачі інформації. Цей тип кінцевих пристроїв найбільш енергоємний і підходить для задач, коли необхідно отримувати великі обсяги інформації.

Приклад роботи пристрою для кожного класу представлений на на (рис.1.3).

Рисунок 1.3 –Класи пристроїв LoRaWAN

Клас А

– пристрій передає повідомлення в UL і потім "слухає" DL два інтервали часу;

– найменше енергоживлення;

– підтримується всіма пристроями.

Клас Б

– реалізовано аналогічно класу А+;

– підходить для всіх пристроїв які живляться від батарейки;

Клас С

– реалізовано аналогічно класу А+;

– підходить для кінцевих пристроїв, які живляться від постійного джерела.

LoRaWAN працює в неліцензованому радіочастотному спектрі. Це означає, що будь-хто може користуватися радіочастотами, не сплачуючи мільйонних зборів за права передачі. Він схожий на WiFi, який використовує діапазони ISM 2,4 ГГц і 5 ГГц по всьому світу. Будь-хто може встановлювати маршрутизатори WiFi та передавати сигнали WiFi без необхідності ліцензії чи дозволу.

LoRaWAN використовує більш низькі радіочастоти з більшим діапазоном. Той факт, що частоти мають більший діапазон, також має більші обмеження, які часто залежать від країни. Це є викликом для LoRaWAN, який намагається бути максимально рівномірним у всіх різних регіонах світу. Як результат, LoRaWAN визначається для ряду діапазонів для цих регіонів. Ці діапазони досить схожі для підтримки регіонально-агностичного протоколу, але мають ряд наслідків для впровадження резервних систем.

LoRaWAN має офіційні регіональні специфікації, які називаються регіональними параметрами, які ви можете завантажити з веб-сайту альянсу LoRa.

У цих регіональних специфікаціях LoRaWAN також не вказано все. Вони охоплюють регіон лише шляхом визначення загального знаменника.

Крім того, кожен оператор мережевого сервера може вибирати додаткові параметри, наприклад додаткові канали викидів.

LoRaWAN це мережевий стек який знаходиться на фізичному рівні Lora. LoRaWAN має максимальну швидкість передачі даних 27 кбіт / с (50 кбіт / с при використанні FSK замість LoRa) і стверджує, що один шлюз може збирати дані з тисяч вузлів, розгорнутих за кілометри(рис.1.4).

Рисунок 1.4 – Швидкість в LoRaWAN

Структура кадру протоколу LoRa представлена на рис.1.5.

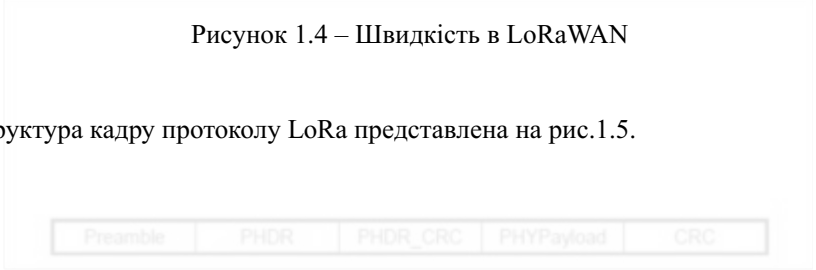

Рисунок 1.5 – Структура кадру протоколу LoRa

Структура кадру LoRa починається з преамбули.

Функція, преамбула визначає схему модуляції пакетів, будучи модульованою тим же фактором розповсюдження як і решта пакету. Зазвичай тривалість преамбули становить 12,25 Цс. За преамбулою слідує заголовок PHY та CRC заголовка, які разом мають 20 біт і кодуються з найбільш надійною швидкістю коду, а решта кадру кодується зі швидкістю коду, визначеною в заголовку PHY. Заголовок PHY також містить таку інформацію, як довжина корисного навантаження та наявність у кадрі 16-бітової CRC завантаження. Зокрема, у мережі LoRa лише кадри висхідної лінії зв'язку містять CRC корисного навантаження. PHY корисне навантаження містить MAC Frame.

Заголовок MAC визначає версію і тип повідомлення даного протоколу, тобто, чи це дані або фрейм управління, чи передається він у висхідній чи низхідній лінії зв'язку, чи має бути визнаний. MAC Header також може повідомити, що це повідомлення, яке залежить від постачальника. У процедурі

з'єднання для активації кінцевого вузла корисне навантаження MAC можна замінити запитом приєднання або повідомленнями про приєднання. Вся частина заголовка MAC та корисного навантаження MAC використовується для обчислення значення MIC за допомогою мережевого ключа сеансу (Nwk_SKey). Значення MIC використовується для запобігання підробці повідомлень та аутентифікації кінцевого вузла.

Пакет шару додатків: корисний набір MAC, який обробляється шаром програми, складається із заголовка кадру, порту кадру та корисного навантаження кадру. Значення Port Port визначається залежно від типу програми. Значення корисного навантаження кадрів шифрується ключем сеансу програми (App_SKey).

LoRa використовує структуру кадру з двома циклічними кодами перевірки надмірності (CRC), що використовуються для виявлення помилкових пакетів, з CRC, що захищає заголовок, а потім кодова послідовність CRC після корисного навантаження для її захисту. Пакети передаються в лінії вгору Uplink використовують режим передачі радіопакет LoRa, в який включені фізичний заголовок LoRa (PHDR) плюс CRC заголовка (PHDR_CRC). Переданий трафік корисного навантаження захищений циклічними кодами перевірки надмірності CRC. PHDR_CRC і поля корисного навантаження вставляються радіопередавачем.

Кожен пакет повідомлення в лінії вниз відправляється сервером тільки на один кінцевий пристрій LoRa і ретранслюється одним мережевим сервером. В пакетах повідомлень в лінії вниз використовується режим передачі радіопакетів, в який включені фізичний заголовок LoRa (PHDR) і циклічний код перевірки надмірності заголовка (PHDR_CRC).

1.2 Робочий цикл (Duty cycle)

Обов'язковий цикл вказує на частину часу, коли ресурс зайнятий.

Коли один пристрій передає по каналу по 2 одиниці часу кожні 10 одиниць часу, цей пристрій має робочий цикл 20% (рис.1.6).

Рисунок 1.6 – Одноканальний робочий цикл

Однак, якщо ми також розглянемо канали, справи стають дещо складнішими. Коли у нас є пристрій, який передає по 3 канали замість одного, кожен окремий канал все ще зайнятий на 2 одиниці часу кожні 10 одиниць часу (тобто 20%). Однак пристрій зараз передає протягом 6 одиниць часу кожні 10 одиниць часу, надаючи йому робочий цикл 60% (рис.1.7).

Рисунок 1.7 – Багатоканальний робочий цикл

У нашому європейському плані частот у нас є канали в різних піддіапазонах, тому, розглядаючи робочий цикл, ми також повинні враховувати їх. Скажімо, 3 канали, якими користувалися раніше, вони перебувають у двох різних піддіапазонах. Кожен окремий канал все ще має робочий цикл 20%, пристрій все ще має робочий цикл 60%, але тепер можна побачити, що смуга 1 використовується для 2 одиниць часу через кожні 10 одиниць часу (20%), тоді як діапазон 2 - використовується для 4 одиниць часу кожні 10 одиниць часу (40%) (рис.1.8).

Рисунок 1.8 – Кілька робочих циклів

Максимальний робочий цикл. Робочий цикл радіопристроїв часто регулюється урядом. Якщо це так, цикл мита зазвичай встановлюється на рівні 1%, але обов'язково потрібно перевіряти правила місцевого самоврядування.

В Європі робочі цикли регулюються розділом 7.2.3 стандарту ETSI EN300.220. Цей стандарт визначає наступні піддіапазони та їхні робочі цикли:

– g(863,0 - 868,0 МГц): 1%

– g1 (868,0 - 868,6 МГц): 1%

– g2 (868,7 - 869,2 МГц): 0,1%

– g3 (869,4 - 869,65 МГц): 10%

– g4 (869,7 - 870,0 МГц): 1%

Крім того, специфікація LoRaWAN диктує робочі цикли для частот приєднання, пристрої частот усіх мереж, сумісних з LoRaWAN, використовують для активації над повітрям (OTAA) пристроїв. У більшості регіонів цей робочий цикл встановлюється на рівні 1%.

Нарешті, у мережі загальнодоступних мереж The Things Network є політика справедливого доступу, яка обмежує ефірний час висхідної лінії зв'язку до 30 секунд на день (24 години) на вузол, а повідомлень низхідної лінії зв'язку - до 10 повідомлень на день (24 години) на вузол. Якщо ви використовуєте приватну мережу, ці обмеження не застосовуються, але ви все одно повинні відповідати урядовим та LoRaWAN лімітам.

Відповідність. Кожен радіопристрій повинен відповідати встановленим обмеженням робочого циклу. Це стосується і вузлів, і шлюзів.

На практиці це означає, що потрібно запрограмувати свої вузли таким чином, щоб вони залишалися в межах. Найпростіший спосіб зробити це - підрахувати, скільки ефірного часу споживає кожне повідомлення, використовуючи один з багатьох калькуляторів ефірного часу, і використовувати цю інформацію для вибору хорошого інтервалу передачі.

Деякі радіомодулі (наприклад, RN2483) також забезпечують обмеження робочого циклу. Якщо перевищити обмеження, модуль подасть скаргу на повідомлення no_free_ch. Зокрема, RN2483 обмежує робочий цикл на основі каналу. Це означає, що якщо налаштований лише 1 канал, модуль почне виконувати робочий цикл після першого повідомлення.

На (рис.1.9) показано виконання ресурсу з обмеженням 20% робочого циклу.

Рисунок 1.9 – Одноканальний робочий цикл без повітря

У європейській смузі передача на каналі в діапазоні частот також впливає на інші частоти в цій смузі.

На (рис.1.10) показано виконання у двох діапазонах, кожен з яких має обмеження 20% робочого циклу.

Рисунок 1.10 – Кілька діапазонів поза повітрям

Оскільки межу робочого циклу на один канал легше реалізувати, то також можна розділити робочий цикл піддіапазону на кількість каналів у цьому піддіапазоні. Так, наприклад, у піддіапазоні з 8 каналами та робочим циклом 1%, кожен канал має робочий цикл 1/8% (тобто 0,125%).

Цей метод також реалізований модулем RN2483, і як результат, замість того, щоб побачити no_free_ch, коли надсилаємо надто швидко після першого повідомлення, можливо надіслати декілька повідомлень до того, як усі 8 каналів будуть "заблоковані" і набуде цикл виконання.

На (рис.1.11) показано виконання цих же двох діапазонів, але примусове виконання на канал.

Рисунок 1.11 – Кілька діапазонів поза повітрям

Пристрій працює відповідно до duty cycle: якщо пристрій передає дані протягом "TimeOnAir", то він не зможе передавати дані протягом "Toffsubband" в цьому діапазоні.

Наприклад, якщо пристрій передає дані протягом 0,5 с в діапазоні 868МГці duty cycle = 1%, то він не зможе передавати дані протягом 49.5 с на всьому діапазоні 868 МГц.

$$Toff_{subband} = \frac{TimeOnAir}{DutyCycle_{subband}} - TimeOnAir \quad (1.1)$$

1.3 Безпека в LoRaWAN мережах

1. Ключі безпеки. LoRaWAN 1.0 визначає ряд ключів безпеки :

NwkSKey, AppSKey та AppKey. Кожна клавіша має довжину 128 біт. Для цього потрібний алгоритм AES-128, аналогічний алгоритму, використовуваному в стандарті 802.15.4.

2. Ключі сесії. Коли пристрій приєднується до мережі (це називається активацією або приєднанням), створюються ключ сеансу для програми AppSKey та ключ сеансу для мережі NwkSKey. NwkSKey ділиться з мережею створеним ключем, тоді як AppSKey залишається приватним. Ці сеансові ключі використовуватимуться протягом тривалості сеансу.

Ключ мережевого сеансу (NwkSKey) використовується для взаємодії між Вузлом та Мережевим сервером. Цей ключ використовується для перевірки цілісності кожного повідомлення за допомогою коду цілісності повідомлення (перевірка MIC). Цей MIC схожий на контрольну суму, за винятком того, що він запобігає навмисному підробленню повідомлення. Для цього LoRaWAN використовує AES-CMAC. У передній частині The Things Network ця перевірка також використовується для зіставлення не унікальної адреси пристрою (DevAddr) до унікальних DevEUI та AppEUI.

Ключ сесії додатків (AppSKey) використовується для шифрування та розшифровки корисного навантаження. Корисне навантаження повністю зашифровано між вузлом та компонентом обробника / сервера додатків мережі The Things (який ви зможете запустити на власному сервері). Це означає, що ніхто, крім вас, не в змозі читати вміст повідомлень, які ви надсилаєте чи отримуєте.

Ці два сеансові клавіші (NwkSKey та AppSKey) є унікальними на кожен присрій за сеанс. Якщо ви динамічно активуєте свій пристрій (OTAA), ці клавіші відтворюються заново при кожній активації. Якщо ви статично активуєте свій пристрій (ABP), ці клавіші залишаються незмінними, поки ви не зміните їх.

3. Ключ програми. Ключ програми (AppKey) відомий лише пристроєм та програмою. Динамічно активовані пристрої (OTAA) використовують прикладний ключ (AppKey) для отримання двох клавіш сеансу під час процедури активації. У

мережі The Things ви можете мати AppKey за замовчуванням, який буде використовуватися для активації всіх пристроїв або налаштування AppKey на кожен пристрій.

4. Рамки лічильника. Оскільки ми працюємо з радіопротоколом, будь-хто зможе фіксувати та зберігати повідомлення. Не можна читати ці повідомлення без AppSKey, оскільки вони зашифровані. Неможливо також підробити їх без NwkSKey, оскільки це призведе до того, що перевірка MIC провалиться. Однак можлива повторна передача повідомлень. Ці так звані атаки відтворення можуть бути виявлені та заблоковані за допомогою лічильників кадрів.

Коли пристрій активовано, ці лічильники кадрів (FCntUp та FCntDown) встановлюються як 0. Кожен раз, коли пристрій передає дані висхідної лінії зв'язку, FCntUp збільшується і кожного разу, коли мережа надсилає дані низхідній лінії зв'язку, FCntDown збільшується. Якщо або пристрій, або мережа отримує сповіщення з лічильником кадрів, нижчим за останнє, сповіщення ігнорується.

Цей захід безпеки має наслідки для пристроїв розробки, які часто є статично активованими (ABP). Виконуючи це, ви повинні усвідомити, що ці лічильники кадрів скидаються на 0 щоразу, коли пристрій перезавантажується (при спалаху мікропрограмного забезпечення або при відключенні його від мережі). Як результат, мережа речей заблокує всі повідомлення з пристрою, поки FCntUp не стане вищим за попередній FCntUp. Тому потрібно перереєструвати свій пристрій у бекенді кожного разу, коли його скидаємо.

5. Поширення спектра. Радіопередач з розширенням спектру традиційно використовувався під час Другої світової війни, щоб ускладнювати моніторинг військових комунікацій - або за допомогою техніки, яка називається "стрибок частоти" (FHSS), – пропускаючи частоту передачі навколо заздалегідь впорядкованим способом, змушуючи ворога постійно наводити порядок (дуже швидко) або "пряма послідовність" (DSSS), де цифрове повідомлення додається до значно більш високої швидкості передачі, псевдослучайності (PR). Код поширює радіосигнал за набагато ширшою смугою пропускання. Насправді настільки широкий, що потужність цілком може бути розсіяна, так що загальний

сигнал падає у фоновий радіошум - і стає непомітним. Отже, відновлення – це питання щоб знати початкову радіочастоту; її псевдовипадковий код та швидкість передачі біту коду PR. Знаючи ці деталі, означає, що синхронізувати приймачі не так складно, як може здатися спочатку. Сигнал просто "вискочить" із шуму, коли буде досягнуто правильних значень.

Техніка, що використовується в LoRa, – це «CHIRP»: стиснутий РЛС імпульс високої інтенсивності. Це ще складніше, але просте з сучасними технологіями. Як випливає з назви, вимога до дизайну фону не використовується для приховування радіосигналу, але застосовується через інші фактори, не просто обробку посилення, але захист від перешкод, обмін каналами та опір радіовідбиттям (серед інших). Тому він використовується як захист від умов експлуатації, а не для опору спостереження. (Хеди Ламарр була співавтором і має патент на FHSS).

Особливістю LoRaWAN є відкритість ідентифікаторів кінцевих пристроїв в радіоефірі, що дозволяє зловмисникові однозначно збирати інформацію, що передається та ідентифікувати пристрої.

LoRa – потік дзвінків для активації пристрою (процедура приєднання) за допомогою OTAA та ABP.

Коли в мережу LoRa додається новий кінцевий пристрій (пристрій LoRa), він повинен пройти процес активації. В процесі активації обидва сеансові ключі діляться між кінцевим пристроєм та мережевим сервером. В даний час LoRa забезпечує наступні два типи методів активації:

– активація на повітрі (OTAA);

– активація персоналізацією (ABP).

Активація в повітрі.У режимі OTAA кінцевий пристрій зв’язується з мережевим сервером для виконання процесу активації, який називається процедурою приєднання. Відповідно до специфікацій LoRa, режим OTAA використовується, коли кінцевий пристрій вже розгорнуто або він скидається. На (рис.1.12) зображено процедуру приєднання.

Рисунок 1.12 – Процедура активації OTTA

Кроки:

1. Повідомлення із запитом приєднання: Кінцевий пристрій запускає процедуру приєднання, надсилаючи повідомлення про запит на приєднання. Він включає DevEUI, AppEUI та DevNonce у запиті на приєднання. DevEUI та AppEUI посилаються відповідно на глобальний ідентифікатор пристрою та додатків. Вони дотримуються формату адресного простору IEEE EUI-64.

DevNonce – це лічильник, що починається з 0, коли спочатку пристрій вмикається та збільшується з кожним запитом приєднання кінцевим пристроєм. Значення DevNonce ніколи не використовуватиметься для заданого значення AppEUI. Якщо кінцевий пристрій може бути задіяний в циклі живлення, то DevNonce повинен бути стійким (має зберігатися в енергонезалежній пам'яті). Скидання DevNonce без зміни AppEUI призведе до того, що мережевий сервер буде відмовлятися від запитів приєднання пристрою. Для кожного кінцевого пристрою мережевий сервер відстежує останнє значення DevNonce, використовуване кінцевим пристроєм, і ігнорує запити приєднання, якщо значення DevNonce не збільшується.

Значення MIC-запиту на приєднання обчислюється кінцевим пристроєм, а ключ програми (AppKey) просувається між кінцевим пристроєм та мережевим

сервером. Повідомлення про приєднання не шифрується. Воно може передаватися за допомогою будь-якої швидкості передачі даних та дотримуючись випадкової частоти стрибків частоти через вказані канали з'єднання (рис.1.13).

Рисунок 1.13 – Поля запиту приєднання до запиту

2. Генерація автентифікації та створення ключових сеансів: після того, як мережевий сервер отримає запит на приєднання, він виконує процес запобігання атаці відтворення, який заснований на DevNonce. Якщо DevNonce у запиті на з'єднання раніше використовувався, мережевий сервер визначає, що повідомлення є недійсним і що процес з'єднання не вдасться. Якщо повідомлення є дійсним, мережевий сервер ідентифікує кінцевий пристрій зі значенням MIC.

Якщо кінцевий пристрій проходить аутентифікацію, мережевий сервер генерує Nwk_SKey та App_SKey. AppNonce – лічильник номерів, створений мережевим сервером. NetID - це 24-бітове поле, його 5 LSB називаються NwkID, яке використовується для розділення адрес географічно дублюваних мереж LoRa. Інші біти NetID можна вільно визначати мережевим сервером.

3. Приєднатися до повідомлення про прийняття: повідомлення про прийняття приєднання містить AppNonce, NetID, DevAddr, DLSettings, RxDelay, та CFList. DevAddr – це 32-розрядний ідентифікатор кінцевого пристрою в поточній мережі (рис.1.14). MSB DevAddr називаються NwkID, який також міститься в NetID. Інші біти можна довільно вибрати мережевим сервером.

DLSettings містить кілька значень, пов'язаних з конфігурацією низхідної лінії зв'язку. RxDelay – це затримка між процесом передачі та прийому. CFList –

необов'язкове поле, яке стосується частоти каналів. Нарешті, все повідомлення про прийняття приєднання шифрується за допомогою AppKey.

Рисунок 1.14 – Приєднання поля прийому повідомлень

4. Передача App_SKey: оскільки App_SKey призначений для захисту кінцевого зв'язку між кінцевим пристроєм та сервером додатків, його слід перенести з мережевого сервера на сервер додатків. Специфікація LoRa не визначає, коли і як обміняти App_SKey з сервером додатків, щоб він міг бути специфічним для реалізації. Це може бути важливою частиною, а тому можливо включати його до процедури приєднання.

5. Генерація сеансового ключа: після отримання повідомлення про прийняття приєднання кінцевий пристрій розшифровує його та генерує сеансові ключі, використовуючи вилучені параметри.

Активація персоналізацією. ABP – це спосіб, яким кінцевий пристрій може належати до певної мережі LoRa, не виконуючи процедуру приєднання за певних умов. У режимі ABP кінцевий пристрій не має DevEUI, AppEUI та AppKey, які є важливими для процедури приєднання. Активація кінцевого пристрою за допомогою персоналізації означає, що DevAddr та чотири сеансові клавіші FNwk_SIntKey, SNwk_SIntKey, Nwk_SEncKey та App_SKey безпосередньо зберігаються в кінцевому пристрої, а не отримуються з DevEUI, AppEUI, AppKey та NwkKey.

Кінцевий пристрій оснащений необхідною інформацією для участі в певній мережі LoRa, як тільки він запускається. Кожен пристрій має унікальний набір F / SNwk_SIntKey, Nwk_SEncKey та App_SKey. Компрометація ключів одного пристрою не повинна загрожувати безпеці зв’язку інших пристроїв. Процес побудови цих ключів повинен бути таким, що ключі не можуть бути отримані

жодним чином з загальнодоступної інформації (наприклад, адреса вузла або DevEUI кінцевого пристрою).

Коли персоналізований кінцевий пристрій вперше звертається до мережі або після повторної ініціалізації, він передає команду Reset Ind MAC у полі FOpt усіх повідомлень висхідної лінії до тих пір, поки не отримає в мережі команду Reset conf. Після повторної ініціалізації кінцевий пристрій має використовувати конфігурацію параметрів за замовчуванням (ідентифікуйте конфігурацію, яка використовувалася під час першого ввімкнення пристрою в мережу).

Технологія LoRa підтримує обробку та конфігурацію запитів на повторне з'єднання для кінцевих пристроїв LoRa. Використовуючи запит на повторне з'єднання, пристрій може просити мережевий сервер повторно активуватися, не відключаючись до отримання активації. Іншими словами, коли він не отримає нову активацію, пристрій продовжить використовувати старий контекст безпеки.

За допомогою запиту на повторне з'єднання можна скинути контекст пристрою, включаючи всі параметри радіо (адреса пристрою, лічильники кадрів, клавіші сеансу, параметри радіо) відновити втрачений контекст сеансу або повторно ввести пристрій (адреса пристрою, сеансові клавіші і рамки-лічильники).

Після активації пристрій може періодично передавати повідомлення із запитом на повторне звернення до звичайних даних програми.

Повідомлення повторного запиту періодично надає серверам можливість ініціалізації нового контексту сеансу для кінцевого пристрою.

Запит на повторне з'єднання може використовуватися для передачі кінцевого пристрою між двома мережами або для повторної клавіші та / або зміни devAddr пристрою в певній мережі.

Мережевий сервер також може використовувати можливість повторного запиту, щоб скинути параметри прийому пристрою, якщо між пристроєм та мережевим сервером існує десинхронізація стану рівня MAC.

Типи запитів на повторне з'єднання. Існує три типи повідомлень про повторне з'єднання, які можуть передаватися кінцевим пристроєм. Попереднє повідомлення байта Rejoin Request вказує тип повторного з'єднання.

Повторне повідомлення із запитом. Повідомлення повторного запиту типу 0 або 2 містить NetID (ідентифікатор домашньої мережі пристрою) та DevEUI кінцевого пристрою з подальшим 16-бітовим лічильником (RJcount0). RJcount0 - це лічильник, що збільшується з кожним переданим кадром типу 0 або 2. RJcount0 ініціалізується до 0 кожного разу, коли кінцевим пристроєм успішно обробляється Join-Accept(рис.1.15).

Рисунок 1.15 – Повторне приєднання запиту 0 або 2

Для кожного кінцевого пристрою мережевий сервер повинен відслідковувати останнє значення RJcount0 (зване RJcount0_last), яке використовується кінцевим пристроєм. Він ігнорує повторні запити, якщо (Rjcount0 <= RJcount0_last) RJcount0 обов'язково ніколи не загортається. Якщо RJcount0 досягає 2^16-1, пристрій припиняє передавати ReJoin-запит типу 0 або 2 кадри. Пристрій може повернутися до стану приєднання.

Повідомлення повторного запиту не шифрується. Пристройний цикл передач Rejoin-Req типу 0 або 2 передач завжди повинен бути <0,1%

Повідомлення повторного запиту типу 0 призначене для передачі від одного разу на годину до одного разу на кілька днів, залежно від випадку використання пристрою. Це повідомлення також може бути передано за командою ForceRejoinReq MAC. Це повідомлення може використовуватися для підключення мобільного пристрою до відвідуваної мережі в роумінгових ситуаціях. Він також може бути використаний для повторної переробки або зміни devAddr статичного

пристрою. Мобільні пристрої, які очікують роумінг між мережами, повинні передавати це повідомлення частіше, ніж статичні пристрої.

Повідомлення повторного з'єднання-запиту типу 2 призначене лише для того, щоб увімкнути повторну перевірку кінцевого пристрою. Це повідомлення можна передавати лише після команди MAC ForceRejoinReq.

Тип повторного приєднання-запит 1 аналогічно до запиту приєднання, повідомлення типу повторного вступу-запиту 1 містить JoinEUI та DevEUI кінцевого пристрою(рис.1.16). Повідомлення типу "Зворотний зв'язок" типу 1 може бути перенаправлено на сервер приєднання кінцевого пристрою будь-яким мережевим сервером, який його отримує. Запит на повторне з'єднання типу 1 може бути використаний для відновлення з'єднання з кінцевим пристроєм у разі повної втрати стану мережевого сервера. Рекомендується передавати повідомлення повторного запиту типу 1 мінімум раз на місяць.

Рисунок 1.16 – Повторне приєднання запиту 1

RJcount1 для повторного запиту типу 1 - це інший лічильник від RJCount0, який використовується для типу Rejoin-request. RJcount1 - це лічильник, що збільшується з кожним переданим кадром типу "Зворотне з'єднання" 1. Для кожного кінцевого пристрою сервер приєднання відслідковує останнє значення RJcount1 (зване RJcount1_last), яке використовується кінцевим пристроєм. Він ігнорує повторні запити, якщо (Rjcount1 <= RJcount1_last).

RJcount1 ніколи не обертається для даного JoinEUI. Періодичність передачі типу 1 Reinoin-Request типу 1 повинна бути такою, щоб це обертання не могло відбуватися протягом усього пристрою протягом певного значення JoinEUI.

Повідомлення Rejoin-request type 1 не шифрується. Зарядний цикл передач пристрою Rejoin-Req типу 1 завжди повинен бути <0,01%.

Повідомлення про повторний запит типу 1 призначене для передачі від одного разу на день до одного разу на тиждень. Це повідомлення використовується лише у випадку повної втрати контексту на стороні сервера. Ця подія є дуже малоймовірною, а затримка для повторного підключення пристрою вважається затримкою від 1 дня до 1 тижня.

Повторний запитат обробки повідомлень. В будь-який час мережевий сервер обробляє Re-Join-Request (тип 0,1 або 2) та генерує повідомлення Join-accept (рис.1.17) . Він повинен підтримувати як старий контекст безпеки (ключі та лічильники, якщо такі є), так і новий, поки не отримає перший успішний кадр висхідної лінії з використанням нового контексту, після чого старий контекст може бути безпечно відкинутий.

У всіх випадках обробка повідомлення про повторний запит мережевим сервером аналогічна обробці стандартного повідомлення про приєднання, оскільки мережевий сервер, який спочатку обробляє повідомлення, визначає, чи слід його переслати на сервер приєднання для створення а у відповідь приєднати повідомлення про прийняття.

Рисунок 1.17 – Повторний запитат обробки повідомлень

Мережевий сервер відповість повідомленням про приєднання, якщо він хоче змінити ідентифікацію мережі пристрою (роумінг або повторну клавішу). У такому випадку RJcount (0 або 1) замінює DevNonce в процесі виведення ключа. Мережевий сервер також надсилає звичайний кадр низхідній лінії зв'язку, необов'язково містить команди MAC. Ця низхідна лінія передається по тому ж

каналу з тією ж швидкістю передачі даних і тією ж затримкою, що і замінює повідомлення приєднання-прийняття.

1.4 Переваги стандарту LoRaWAN

Серед незаперечних переваг у порівнянні з іншими стандартами LoRaWAN:

– найбільш динамічно розвивається загальносвітова екосистема (понад 500 учасників TheLoRaAlliance. А це означає, що в усьому світі значно більше виробників датчиків, програмних рішень і мережевого устаткування в порівнянні з іншими стандартами.

– дуже низьке споживання енергії (наприклад, датчик для контролю житлово-комунального господарства може без заміни батареї пропрацювати до 10 років. Пристрої в мережі LoRaWAN асинхронно обмінюються даними тільки тоді, коли їм є, що передати. Можна задати передачу даних за розкладом або поза залежністю від конкретного часу.

У звичайних мобільних мережах пристрої часто змушені «прокидатися» для синхронізації з мережею і перевірки повідомлень для отримання і / або відправки.

Така синхронізація призводить до значної витрати енергії і скорочує автономний термін роботи пристрою від акумулятора. Аналітики GSMA провели безліч досліджень мереж LPWAN, в результаті чого прийшли до висновку: автономність LoRaWAN-пристроїв в 3-5 разів вище в порівнянні з іншими технологіями.

– велика територія покриття однієї базової радіостанції (до 12 км - в умовах міста і понад 25 км - в сільській місцевості)

– ємність мережі.

Для забезпечення нормальної роботи мережі LPWAN шлюз повинен мати дуже високу пропускну здатність або можливість отримувати повідомлення з дуже великою кількістю кінцевих пристроїв. Висока ємність мережі LoRaWAN досягається за рахунок використання адаптивної швидкості передачі даних і

використання багатоканального приймача в шлюзі, що гарантує одночасне отримання повідомлень на кількох каналах.

Шлюзи дозволяють одночасно по одному каналу отримувати інформацію з пристроїв, які використовують різні швидкості для передачі даних. Адаптивна швидкість для передавання даних також оптимізує час роботи акумулятора обладнання.

Мережі LoRaWAN можуть бути розгорнуті з мінімальною кількістю інфраструктури. У міру необхідності, в залежності від кількості пристроїв в мережі, можна змінювати швидкості передачі даних або збільшити кількість шлюзів.

На мережі IoT Ukraine вже реалізовані всі ключові рішення широкої палітри Інтернету речей і працюють сотні підключених пристроїв. Тепер всі великі міста, промислові підприємства і агрофірми отримали можливість, динамічно розвивати свої розумні екосистеми, скорочувати витрати і підвищувати ефективність. Перша Національна мережа для розумних девайсів будується на обладнанні та програмному забезпеченні компаній - лідерів світового ринку телекомунікацій і IT, Cisco (США) і Actility (Франція).

Завдяки такому загальнонаціональному інфраструктурному проекту, Україна повинна вже за рік, перестати бути позаду в розширені прогресу технології Інтернету речей від усього теперішнього світу та стане однією з найбільших центрів досліджень та впроваджень програмних продуктів, необхідного обладнання та дослідження новітніх рішень як для внутрішнього ринку України, так і для ринків усього світу.

Мережі LoRaWAN розгортаються в діапазоні частот, які не потребують ліцензування. Одна базова станція здатна обслуговувати кілька десятків тисяч пристроїв, що обумовлено великим охопленням сигналу і високою завадостійкістю. Крім того, термін служби акумулятора може досягати десяти років. При використанні сонячних батарей пристрій буде працювати автономно до тих пір, поки не закінчиться його ресурс.

1.5 Варіанти застосування LoRaWAN

Можливі такі варіанти застосування LoRaWAN:

– автоматичне зчитування показань із лічильників споживання різних ресурсів (вода, газ, електрику і т.д.);

– моніторинг розумних електромереж;

– відстеження транспорту і вантажів;

– контроль стану ємностей з небезпечними речовинами на виробництві;

– оцінка промислового обладнання;

– контролювання паркувального простору;

– системи розумного вуличного освітлення;

– прогноз погодних умов;

– пожежні і охоронні сигналізації;

– контролювання рівня забруднення повітря;

– переробка сільського господарства;

– відстеження тварин;

– виявлення вогню;

– відстеження флоту;

– домашня безпека;

– контроль якості забруднення повітря в будівлях;

– промисловий моніторинг температури;

– управління активами;

– виявлення витоку радіації;

– поводження з відходами;

– автоматизація будівель.

2 ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ LORAWAN РІЗНИХ ПАРАМЕТРІВ

2.1 Продуктивність параметрів технології LoRaWAN

У цій роботі було проведено спостереження та пояснення ефекту різних параметрів LoRaWAN. Крім того, ми показали, наскільки значні показники вигоди можна отримати, розумно встановивши параметри системи.

Востанні кілька років Інтернет речей (IoT) викликає величезний інтерес з боку наукових та промислових громад, завдяки неабиякому потенціалу, практично кожен об'єкт може мати віддалений доступ і керування ним відбуватиметься через з'єднання з Інтернетом. Таке повсюдне підключення дозволило б надавати різні послуги у широкому спектрі. Наприклад, міста могли
б мати вигоду від розумного управління освітленням, більш ефективного відходу управління та постійний моніторинг інфраструктури. В промисловості підключені датчики можуть допомогти постійно контролювати виробничий процес, роблячи це можливим швидко виявляти або навіть прогнозувати збої, перебуваючи в сільськогосподарському секторі широкого збору екологічних даних, оскільки температура та вологість ґрунту можуть покращити кількість та якість виробництва ґрунту, зменшуючи при цьому витрати. Здоров'я, моніторинг, безпека та автоматизація дому - це також приклади можливого застосування. Взагалі потреби комунікацій значно відрізняються від класичної високої пропускної здатності та низької вимоги до затримки, які до цих пір зумовили проектування традиційних систем зв'язку. Наприклад, важливіший довгий діапазон зв'язку та низьке споживання енергії ніж високі бітрейти і підтримка передачі коротких пакетів від величезної кількості пристроїв буде більше важливо, ніж забезпечення стабільних високопропускних з'єднань для небагатьох користувачів.

Одне хороше рішення – це LoRaWAN, відкритий стандарт, який рекламує LoRa Alliance, який визначає середній контроль доступу (MAC) та протоколи управління мережею на верхній частині дальності (LoRa) фізичний (PHY) шар.

Топологія мережі дуже проста: радіосигнали передані кінцевими пристроями приймаються одним (або декількома) шлюзи, які потім пересилають пакети до мережі Сервер (NS) для подальшої обробки. Набір мікросхем LoRa розроблений як енергоефективний, і він обіцяє активізацію до 10 років енергетичної автономності для пристроїв з акумулятором. Крім того, було доведено, що діапазон передачі досягає до 1,5 км у міських сценаріях та 15 км у сільській місцевості. Рівень PHY заснований на частотній модуляції і підтримує множинні коефіцієнти розповсюдження. Крім того, сигнали, передані з різних коефіцієнтів розповсюдження майже ортогональні, що потенційно дозволяє багатопакетний прийом на шлюзі. Ще одна вигода полягає в тому PHY працює в галузі промисловості, науки та медицини (ISM) діапазони в МГц, що знижує вартість розгортання технології. В додаток, стандарт LoRaWAN пропонує велику гнучкість мережі конфігурації, що є ще одним привабливим фактором. Дійсно мережевий сервер може вибирати коефіцієнти розповсюдження, використовувані різними вузлами, тривалість вікон прийому, каналів передачі / прийому, пріоритет пакетів даних про підтвердження і так далі. При правильному встановленні цих параметрів, можливо підтримувати надійні / двосторонні комунікації та змінити баланс між надійністю зв'язку, затримкою, енергоефективністю та потужністю системи. Однак поки що ефект певних параметрів можна передбачити в застосуваннях з відносно низькою кількістю вузлів взаємодії між різними механізмами системи.

2.2 Особливості модуляції та мікросхеми LoRa та огляд стандарту LoRaWAN

Модуляція LoRa. LoRa – схема модуляції, запатентована Semtech та на основі частотного спектру розповсюдження. Дальність зв'язку, що досягає 15 км в оглядовій сільській місцевості райони та 1,5 км у міських застосуваннях на відкритому повітрі. Чутливість (і, таким чином, покриття) можна покращити ціною нижнього бітрейту, змінюючи параметр коефіцієту розповсюдження, який

приймає цілі значення від 7 до 12. Вищим значенням коефіцієту розповсюдження відповідають більш низькі бітрети передачі, але вимагають отримання більш низького сигналу, потужність для правильного прийому, що перетворюється на більш тривале покриття дальності. Для кожного значення параметра коефіцієнтів розповсюдження, в таблиці.2.1 зображено пов'язаний індекс швидкості передачі даних, номінальна швидкість передачі даних, рівень чутливості та час передачі.

Час передачі пакетів визначається для PHY корисного навантаження 32 байти, явний режим заголовка, швидкість коду, що дорівнює 2 та каналу 125 кГц пропускна здатність.

Таблиція 2.1 – Основні характеристики передачі для різних значень параметрів коефіцієнтів розповсюдження

Коєфіцієнт розповсюдження	Індекс швидкості передачі даних	Швидкість передачі даних (кбіт\с)	Чутливість(дБ)	Час передачі пакетів (с)
7	5	5,470	-130,0	0,740
8	4	3,125	-132,5	0,136
9	2	1,760	-135,0	0,247
10	2	0,980	-137,5	0,493
11	1	0,440	-145,0	0,888
12	0	0,250	-142,5	1,777

Ключовою особливістю модуляції LoRa є те, що пакети використання різних коефіцієнтів розповсюдження, майже ортогональні: передачі перекриття за часом та частотою все ще можуть бути правильно розшифровані приймачем за умови, що сила потужності сигналу досить більша, ніж у перешкод.

Стандарт LoRaWAN. Стандарт LoRaWAN [14] визначає MAC та мережу протоколів управління для пристроїв, що використовують модуляцію LoRa. Мережева топологія - це зірка, утворена трьома видами пристроїв:

– Кінцевий пристрій (ED): периферійний вузол, як правило, датчик або привід, який здійснює зв'язок лише через LoRa PHY;

– Мережевий сервер (NS): централізований об'єкт, який управляє мережевими параметрами, пересилає повідомлення програмам і надсилає відповіді до кінцевого пристрою через шлюз (и);

– Шлюз (GW): проміжний вузол, який передає повідомлення між ED та NS. ED і GW спілкуються за допомогою модуляції LoRa, в той час як зв'язок між GW та NS здійснюється за допомогою застарілої технології IP. Зазвичай шлюзи обладнані з чіпсетами LoRa, дозволяють паралельний прийом кількох сигналів. Комерційні мікросхеми радіо LoRa мають 8 паралельних шляхів прийому (або ланцюгів), кожен з яких може слухати до певної частоти і демодуляції сигналів, що перекриваються, використанням квазі-ортогональності різних коефіцієнтів розповсюдження.

Пристрої LoRaWAN працюють у неліцензованих смугах ISM, в конкретних частотах, які залежать від регіонального регулювання: у цьому розділі ми розглянули європейський (868 МГц) діапазон частот, який стандарт ділить на чотири канали, орієнтовані на 868,1 МГц, 868,3 МГц, 868,5 МГц і 868,625 МГц. Як описано в таблиці.2.2, згідно з LoRaWAN специфікаціями, перші три канали можна використовувати як для передачі висхідної лінії зв'язку (UL) та низхідної лінії зв'язку (DL), при цьому канал передачі 868.625 МГц зарезервований для комунікацій DL.

Таблиця 2.2 – Канали LoRaWAN за замовчуванням та обмеженням постійного струму

Частота (МГц)	Напрямок	Постійний струм	Межа потужності (Вт)
868,1	DL, UL	1%	14
868,3	DL, UL	1%	14
868,5	DL, UL	1%	14
869,525	DL	10%	27

Більше того, канали регулюються різними обмеженнями потужності передачі та робочим циклом (DC). Зокрема, три двонаправлені канали належать до одного піддіапазону і, отже, колективно підпадають під загальне обмеження постійного

струму 1%, так що передача UL (відповідно DL) в будь-якому з таких канали будуть споживати UL (відповідно DL) постійного бюджету всіх три канали. Натомість канал лише для DL на частоті 869,525 МГц належить до іншого піддіапазону, який дозволяє постійний струм 10% і більшу потужність передавання. Зауважемо, що швидкість передачі інформації у таблиці.2.1, зазвичай використовується для позначення пари коефіцієнту розповсюдження значення пропускної здатності. Обмежуючи нашу увагу 125 кГц для широких каналів, індекс швидкості передачі інформації поєднується з одним коефіцієнтом розповсюдження, як показано в таблиці.2.1.

Стандарт також визначає три класи кінцевих пристроїв, а саме Клас-А (усі), Клас-В (маяк) та Клас-С (безперервні), які відрізняються в управлінні передачами DL: Пристрої класу А можуть отримувати пакети DL лише негайно після передачі UL; Клас-В може розкладати ping-інтервал, протягом якого вони можуть приймати пакети DL; нарешті, Клас -С завжди можеуть отримувати пакети, якщо вони їх самі не передають.

У цій роботі ми зупинимося на пристроях класу А, які є найбільш популярними та складними, враховуючи більшь обмежені можливості спілкування. Вони отримують живлення від акумулятора і можуть отримувати лише протягом двох прийомів вікна (RX1 і RX2), які відкриваються відповідно 1 с і 2 с після закінчення кожної висхідної лінії передачі. Радіоінтерфейс відключається до наступної UL для економії енергії. RX2 відкривається лише в тому випадку, якщо жодне повідомлення DL не отримано успішно під час RX1.

Відповідно до стандартних установок, мережевий сервер може дати відповідь на передачу UL, надіславши пакет DL в RX1, використовуючи той самий канал і коефіцієнт розповсюдження пакету UL або в RX2, з використанням виділеного каналу (на 868,625 МГц в Європі) та коефіцієнт розповсюдження 12 (тобто найнижчий бітрейт) для максимального діапазону покриття. Ці параметри за замовчуванням можуть бути змінені мережевим сервером до кінця відповідні команди MAC. Передачі UL можуть бути не підтверджені або підтверджені. У першому випадку повідомлення передається лише один раз і не очікується, що

визнає мережевий сервер підтвердження, тоді як в останньому випадку, повідомлення передаються повторно до підтвердження (ACK) пакет повертається приймачем, максимум спроб передачі, з m ∈ {1,... , 8}. Зауважемо, встановлення m = 1 збігається з непідтвердженим випадком (загальна кількість передач не може перевищувати m в обох випадках), але у випадку підтвердженого повідомлення, одержувач повинен буде: генерувати ACK.

Для підтвердженого трафіку також передбачений стандарт LoRaWAN механізм адаптивної швидкості передачі даних (ADR), за допомогою якого мережевий сервер може керувати параметрами передачі кінцевих пристроїв та оптимізувати продуктивність будь-якого пристрою або самого пристрою глобальної мережі.

2.3 Сучасні технології моделювання та дослідження ефективності LoRaWAN

В останні роки технологія LoRaWAN є найсучаснішою. Предмет багатьох досліджень, в яких проаналізовано її ефективність та особливості емпіричних вимірювань, математичний аналіз та імітаційні інструменти.

Деякі роботи з LoRaWAN, такі як, перевіряють тестування діапазону покриття та коефіцієнт втрат пакетів за допомогою емпіричного вимірювання, але без дослідження впливу налаштування параметрів на продуктивність. Інші роботи, такі як, вивчають вплив параметрів модуляції на зв’язок між кінцевим пристроєм та його шлюзом, не враховуючи складніших мережевих конфігурацій.

Для отримання більш загальних результатів використовується стохастична модель геометрії для спільного аналізу втручань у часі та частотні домени. Помічено, що при впровадженні стратегії повторення пакетів, тобто передача кожного повідомлення багаторазово ймовірність відмови зменшується, але середня пропускна здатність зменшується через введену надмірність. В роботі автор пропонує закриті форми для ймовірностей зіткнення та втрат пакетів, де показано припущення про досконалу ортогональність між SFs, показано що

розподілений процес Пуассона не точно моделює зіткнення пакетів у LoRaWAN. Пропускна здатність мережі, затримка та швидкість зіткнення для передачі висхідної лінії аналізуються в, використовуючи теорію черги та розглядаючи канал Aloha протокол доступу та регуляторні обмеження у використанні різних піддіапазонів, вказує на важливість на розумне розщеплення трафіку на доступних піддіапазонах для покращення роботи мережі. В математичній моделі продуктивності мережі, враховано такі фактори, як ефект захоплення та реалістичний розподіл SFs в мережі. Однак модель так і не включає деякі важливі мережеві параметри, запобігаючи вивченню їх впливу на мережеву ефективність.

А крок далі робиться де автори розробляють: модель, яка дає можливість враховувати різні параметри конфігурації, такі як кількість ACK, надіслані GW, SF, що використовуються для передач низхідній лінії зв'язку, і DC обмеження, накладені регламентом. Однак у цій роботі багаторазова повторна передача не розглядалася.

Дослідженн містить аналіз системного рівня LoRaWAN та дає значну інформацію про вузькі місця та поведінку мережі при наявності трафіку низхідної лінії зв'язку. Однак, крім того, щоб вказати на деякі недоліки в дизайні у схемі доступу середнього доступу LoRaWAN ця робота не відповідає, для того щоб запропонувати будь-який спосіб поліпшення продуктивності технології. У роботі знову використовуються моделювання на рівні системи для оцінки ефективності підтверджених та непідтверджених повідомлень та показують згубний вплив підтвердження трафіку на загальну пропускну здатність мережі. Єдиним запропонованим рішенням є використання декількох шлюзів, без глибокого дослідження особливостей LoRaWAN стандарту. В запропонований модуль для тренажера ns-3 і використовується для аналогічної сфери, порівнюючи сценарії одиночного та багатобічного руху та використання непідтверджених та підтверджених повідомлень. У цьому випадку автори правильно реалізують кілька шляхів прийому GW, але не враховують їх їх асоціацію до конкретної частоти UL, яка зазвичай відбувається під час налаштування мережі: дійсно, кількість пакетів які можуть бути прийняті одночасно на заданій частоті не повинні перевищувати

кількість шляхів прийому, які є на цій частоті. Також у цьому випадку дослідження зосереджується на аналізі ефективності, не пропонуючи жодного поліпшення.

Автори орієнтуються на оригінальний алгоритм ADR запропонований, що передбачає можливі поліпшення. Як правило, модифіковані алгоритми дають збільшення мережі, масштабованість, рівномірність між вузлами, коефіцієнт доставки пакетів та стійкість до змінних умов каналу. В автори розрахували оптимальний розподіл SFs, щоб мінімізувати ймовірність зіткнення та запропонувати схему для підвищення рівномірності для вузлів, віддалених від станції, шляхом оптимального призначення SF та передавати значення потужності на вузли мережі, щоб зменшити показник помилки пакетів.

У роботі показано, як використання стійкого носія MAC-протоколу множинного доступу (p-CSMA) при передачі UL-повідомлень може покращити коефіцієнт прийому пакетів. Однак слід звернути увагу на те, що маючи багато EDs, які відкладають передачу через низький рівень значення p може призвести до недостатнього використання каналу. Автори досліджують за допомогою моделювання вплив обмеження постійного струму у застосуваннях LPWAN, де показують можливості адаптації курсу які є основними для підтримки розумного рівня продуктивності, коли діапазон покриття та навантаження комірки збільшити. Однак вплив налаштування інших параметрів на продуктивність мережі не враховується.

У цьому дослідженні ми відрізняємось від існуючої літератури, ми орієнтуємося на великі мережі з двостороннім трафіком, застосування яких дає можливість спостерігати якісь непередбачені ефекти, що виникають внаслідок взаємодії декількох обслуговуваних вузлів одним єдиним GW та NS. Крім того, в аналізі ми вивчаємо по черзі роль, яку відіграють настроювані мережеві параметри, виділяючи таким чином деякі підводні камені, які можуть вплинути на продуктивність мережі. Були запропоновані можливі протидії, які потребують невеликих змін на рівні MAC, і ми оцінюємо їх ефективність у деяких застосуваннях.

2.4 Налаштовані параметри і сценарії моделювання

Аналіз, проведений у цій роботі, використовує ns-3 модуль lorawan. Модуль був вдосконалений для підтримки різних конфігурацій мережі з метою отримання та розуміння ролі, яку відіграє кожен налаштований параметр та виявлення непередбачених поведінок. Модуль підтримує підтверджені та непідтверджені повідомлення, конфігурацію декількох мережевих параметрів і реалістичну модель мікросхеми GW, що враховує вісім доступних паралельних шляхів прийому. З цього розділу ми навели докладну інформацію про доступні функції що будуть використано для аналізу мережі.

Доступні налаштування мережі. Ознайомлення із параметрами конфігурації мережі, які доступні в тренажері та які створені для контролю поведінки та особливості обох GW та EDs - Шлюз: в тренажері ми маємо можливість включення або вимкнення обмеження постійного струму на GW для аналізу його впливу на продуктивність мережі.

– Пріоритет передачі / прийому: оскільки GW не може приймати та передавати одночасно, цей параметр визначає відносний пріоритет передачі (TX) над прийомом (RX), у разі конфлікту. Якщо надається пріоритет до RX, тоді передача пакетних передач DL буде відкладена до завершення заходів прийому (за умови, що буде відкрито відповідне вікно прийому). І навпаки, якщо пріоритет віддається TX, то прийом будь-якого вхідного сигналу буде негайно перервано для запуску передачі DL. Зауважимо, що на сьогоднішній день передача пріоритетності - єдиний доступний варіант у комерційних GWs.

– Пріоритетність піддіапазону: необхідний стандарт LoRaWAN, RX1 відкривається на тому ж каналі, де і відповідна UL була отримана, а RX2 відкрито на виділений канал DL, який також є в Європі більш м'які обмеження постійного струму (10% замість 1% дозволено на інших каналах). У тренажері ми увімкнули режим, який перемикає це налаштування, роблячи його можливо відкрити RX1 на виділеному каналі DL, і RX2 на каналі, використовуваному для зв'язку UL.

– Підтвердження швидкості передачі даних: специфікації LoRaWAN рекомендуємо використовувати ACK, передані на RX1 той же SF для передачі UL, при передачі на RX2 використовують найнижчу доступну швидкість передачі даних (SF = 12). Модуль моделювання був модифіковано, щоб забезпечити використання більш високих швидкостей передачі даних для обох вікон прийому. Цей параметр передбачає компроміс між надійністю та ефективним використанням наявного постійного струму і часових ресурсів. Зауважемо, що такий варіант насправді може бути впроваджено в LoRaWAN за допомогою спеціалізованого MAC командування.

– Кількість спроб передачі: для підтвердженого трафіку, максимальна кількість m спроб передачі для налаштованого повідомлення може приймати значення в множині {1, 2, 4, 6, 8}. - Повний дуплекс GW: як уже згадувалося, в даний час GW не можуть передавати і приймати одночасно. Однак це може бути цікавим, щоб дослідити потенційну ефективність виграшу, отриманого реалізацією повного дуплексного GW. Ця функціональність може бути реалізована шляхом розміщення двох GW або поєднання GW з простим чіпсетом LoRa, який слід використовувати тільки для передач, залишаючи GW вільним для прийому повідомлення. Щоб перевірити цю функціональність, ми додали: новий режим для модуля lorawan в тренажері ns-3 що дозволяє ідеально повноцінне дуплексне спілкування.

– Кількість шляхів прийому: число r паралельних шляхів прийому в GW - це параметр, який може бути змінений в тренажері. Крім стандартного значення r =8, ми також розглядали значення r = 3 та r = 16 для вивчення як можуть паралельні можливості прийому GW впливати на загальну продуктивність системи.

Довідкові сценарії. Було досліджено два основні сценарії моделювання. Оскільки ми зацікавлені в оптимізації параметрів шару MAC, ми припускаємо що один GW, який обслуговує кілька EDs, які генерують пакети періодично, з рівним періодом, але випадковими фазами. Крім того, трафік, генерований пристроями, може бути або підтверджений, не підтверджений, або змішаний, тобто з

половиною пристроїв, які вимагають підтвердження та іншою половиною надсилання непідтверджених пакетів.

У першому сценарії ми припускаємо, що EDs є випадковим чином розподілені в межах покриття GW, і ми враховуємо лише втрату шляху.

Другий сценарій складається з більш реалістичного міського розгортання, де EDs випадково розташовані зовні або всередині будівлі, що мають різну висоту та ширину стін. Тут розповсюдження каналу впливає на втрати шляху, просторово корельоване затінення та ослаблення через наявність будівель. Щоб отримати реалістичну настройку, потрібно врахувати трафік моделі, описаний в мобільній автономній звітності (MAR) звіти, згідно з якими пристрої надсилають пакети в періоди, що змінюються від 30 хвилин до 24 годин. Кількість пристроїв також змінюється для оцінки потужності (у перерахунку на кількість активних пристроїв), які можуть підтримуватися GW в реалістичному сценарії.

Щоб полегшити інтерпретацію результатів, ми нехтуємо короткочасними згасаючими явищами, які можуть вплинути на отриманий сигнал потужності. Вплив моделі каналу на розподіл SFs (і, отже, DRs) можна спостерігати на рис. 2.1, де крапки показують положення випадково розміщених EDs навколо центрального GW, тоді як кольори використовуються для представлення бітрейта для кожного пристрою, тобто його значення DR (табл. 2.1.). Бітрейт – це найбільша дозволена потужність сигналу, що приймається на ГВт, відповідно до порогів чутливості в табл. 2.1. Зауважимо, що розподіл швидкості стає все більш хаотичним за наявності тривалого затінення та факторів ослаблення стінок, які впливають на поширення.

Рисунок 2.1 – Розподіл тарифів даних для різних моделей каналів

Показники ефективності. Передача пакетів на рівні PHY може мати п'ять можливих результатів:

– Успіх (S): пакет правильно отриманий GW.

– Втрачено через чутливість (U): пакет надходить на GW з потужністю, меншою за чутливість, і GW не може заблокувати його.

– Втрачено через перешкоди (I): пакет правильно заблокований GW, але його отримання не вдається через достатню кількість інтерфейних пакетів, з достатньою потужністю для зриву ортогональних сигналів.

– Втрачено через насичений приймач (R): пакет надходить на GW з достатньою потужністю, але весь паралельний прийом шляху, налаштований на канал передачі пакету, вже зайнятий прийомом інших пакетів.

– Втрачено через передачу GW (T): прийом пакетів порушується при передачі пакету DL (яка може бути тривалою в час приходу пакету, розпочинається під час прийому пакетів, якщо GW віддає пріоритет передачі).

У випадку непідтвердженого трафіку позначаємо пакет як успішний, коли він успішно отриманий на GW, що, у свою чергу, пересилає його до NS через надійне з'єднання.Для підтвердженого трафіку ми розрізняємо два випадки в залежності про те, чи несуть пакети DL інформацію (наприклад, UL пакет - це запит до NS, і відповідний пакет DL відповідь), або просто ACK, який використовується для зупинки повторної передачі пакетів UL. У першому випадку

передача є успішною, коли і UL, і послідовний пакет DL успішно приймаються NS та ED відповідно, в рамках доступних спроб передачі. У другому випадку замість цього, ми припускаємо, що передача є успішною, якщо в щонайменше один з генерованих пакетів UL доставляється в NS, незалежно від того, чи приймається ACK пристроєм.

Відповідно, ми визначаємо два показники ефективності:

– Підтверджений показник успішності пакету (CPSR): ймовірність підтверджений пакет UL, і відповідний пакет DL правильно отримано в одному з доступних спроб передачі;

– Коефіцієнт доставки пакетів висхідної лінії зв'язку (UL-PDR): ймовірність пакет UL отриманий правильно (незалежно від того, чи є ACK запитується).

3 ФУНКЦІОНУВАННЯ КАНАЛУ ЗВ'ЯЗКУ ТЕХНОЛОГІЇ LORA

3.1 Огляд фізичного шару

LoRa – це модуляція широкого спектру чирпу, в якій використовуються частотні чирпи з лінійною варіацією частоти в часі з метою кодування інформації. Зважаючи на лінійність імпульсів сигналу, зміщення частоти між приймачем і передавачем еквівалентно тимчасовим зміщенням, які легко усуваються в декодері. Це також робить цю модуляцію несприйнятливою до ефекту Доплера, еквівалентного зміщенню частоти. Зсув частоти між передавачем і приймачем може досягати 20% пропускної здатності, не впливаючи на продуктивність декодування. Це допомагає знизити ціну передавачів LoRa, оскільки кристали, вбудовані в передавачі, не потрібно виготовляти з надзвичайною точністю.

Оскільки тривалість символу LoRa довша, ніж типові сплески AMinterference, що породжуються системами спектра частотного стрибкового розширення (FHSS), помилки, породжені подібними перешкодами, легко виправляються за допомогою коду виправлення помилок вперед (FECs). Типова позаканальна селективність (максимальне співвідношення потужності між перешкодою в сусідній смузі та сигналом LoRa) та відхилення спільного каналу (максимальне співвідношення потужності між втручальником у тому ж каналі та сигналом LoRa) приймачі LoRa відповідно становлять 90 дБ та 20 дБ. Це перевершує традиційні схеми модуляції, такі як частотна модуляція (FSK), і робить LoRa добре придатною для передачі малої потужності та передачі дальнього радіусу дії.

3.2 Параметри фізичного шару

Для налаштування модуляції LoRa доступно декілька параметрів: пропускна здатність (BW), коефіцієнт розповсюдження (SF) та швидкість коду (CR). LoRa використовує нетрадиційне визначення коефіцієнта розповсюдження як

логарифму у базі 2 кількості сигналів на символ. Ці параметри впливають на ефективний бітрейт модуляції, її стійкість до перешкод і простоту розшифровки.

Ширина смуги пропускань є найважливішим параметром модуляції LoRa. Символ LoRa складається з сигналів 2SF, які охоплюють весь частотний діапазон. Починається з серії верхніх сигналів. Коли максимальна частота смуги буде досягнута, частота загортається, і збільшення частоти починається знову з мінімальної частоти. На рис. 3.1, наведено приклад передачі LoRa в коливанні частоти в часі. Положення цього розриву в частоті - це те, що кодує передану інформацію. Оскільки в символі є сигнали 2SF, символ може ефективно кодувати SF біти інформації.

Рисунок 3.1 – Коливання частоти в часі зразкового сигналу, що випромінюється передавачем LoRa, де fc - центральна частота каналу, а BW-пропускна здатність

У LoRa швидкість сигналу залежить лише від пропускної здатності, швидкість сигналу дорівнює пропускній здатності (один сигнал в секунду на Герц пропускної здатності). Це має декілька наслідків для модуляції: збільшення одного з коефіцієнта розповсюдження розділить частотний діапазон сигналу на два (оскільки 2SF сигналу покривають всю пропускну здатність) і помножить тривалість символу також на два. Однак він не розділить швидкість передачі бітів на два, оскільки в кожному символі буде передано ще один біт. Більше того, швидкість передачі символів і швидкість передачі бітів при заданому коефіцієнті розповсюдження пропорційні частотній смузі частот, тому подвоєння пропускної здатності ефективно подвоює швидкість передачі. Це представлено в формулі

(3.1), яка пов'язує тривалість символу (TS) з пропускною здатністю та коефіцієнтом поширення.

$$T_s = \frac{2^{SF}}{BW} \tag{3.1}$$

Крім того, LoRa включає прямий код виправлення помилок. Швидкість коду (CR) дорівнює 4 / (4 + n), при n ∈ {1, 2, 3, 4}. Враховуючи це, а також той факт, що SF-біти інформації передаються за символ, формула (3.2) дозволяє обчислити корисну швидкість передачі бітів (Rb).

$$R_b = SF \cdot \frac{BW}{2^{SF}} \cdot CR \tag{3.2}$$

Наприклад, установка з BW = 125 кГц, SF = 7, CR = 4/5 дає швидкість передачі біт Rb = 5,5 кбіт / с. Ці параметри також впливають на чутливість декодера.

Зниження швидкості коду допомагає знизити швидкість помилок пакету (PER) при наявності коротких сплесок перешкод, тобто пакет, переданий із кодовою швидкістю 4/8, буде більш толерантним до перешкод, ніж сигнал, що передається з кодовою швидкістю 4/5. Цифри в табл. 3.1 взяті з таблиці даних SX1276.

Таблиця 3.1–Чутливість приймача LoRa Semtech SX1276 LoRa в дБм при різній пропускній здатності та коефіцієнтах розповсюдження

SF / BW	7	8	9	10	11	12
125кГц	-123	-126	-129	-132	-133	-136
250кГц	-120	-123	-125	-128	-130	-133
500кГц	-116	-119	-119	-125	-128	-130

Інший параметр модуляції LoRa, реалізований у приймачах Semtech, – це низька оптимізація швидкості передачі даних. Цей параметр є обов'язковим у LoRa при використанні коефіцієнтів розповсюдження 11 і 12 з пропускною здатністю 125 кГц або менше. Ефект цього параметра не задокументований; однак формула (3.2) показує, що воно зменшує кількість бітів, переданих на символ, на два.

3.3 Формат фізичного кадру

Хоча модуляція LoRa може використовуватися для передачі довільних кадрів, фізичний формат кадру задається та реалізується у передавачах та приймачах Semtech. Ширина смуги пропускання та коефіцієнт розповсюдження є постійними для кадру.

Кадр LoRa починається з преамбули. Преамбула починається з послідовності постійних підйомів, які охоплюють весь діапазон частот. Останні два підняття кодують слово синхронізації. Слово синхронізації - це однобайтове значення, яке використовується для диференціації мереж LoRa, які використовують однакові смуги частот. Пристрій, налаштований на задане слово синхронізації, перестане слухати передачу, якщо декодоване слово синхронізації не відповідає його конфігурації. За словом синхронізації слідують два та чверть нижніх сигнали, тривалістю 2,25 символу. Загальна тривалість цієї преамбули може бути налаштована між 10,25 та 65,539,25 символами. Структуру преамбули можна побачити на рис. 3.2.

Після преамбули з'являється необов'язковий заголовок. Коли він присутній, цей заголовок передається зі швидкістю коду 4/8. Це вказує на величину корисного навантаження (у байтах), швидкість коду, що використовується для кінця передачі, та чи є 16-бітна CRC для корисного навантаження в кінці кадру. Заголовок також включає CRC, щоб дозволити приймачу відкидати пакети з недійсними заголовками. Розмір корисного навантаження зберігається за допомогою одного байта, обмежуючи розмір корисного навантаження до 255 байт.

Заголовок не є обов'язковим, це дозволяє його відключити в ситуаціях, коли це не потрібно, наприклад, коли довжина корисного навантаження, швидкість кодування та наявність CRC відомі заздалегідь. Корисне навантаження надсилається після заголовка, а в кінці кадру - додаткова CRC. Схематичне узагальнення формату кадру можна побачити на рис. 3.2.

Рисунок 3.2 – Структура кадру LoRa n ∈ {1..4}

Формула (3.3), отримана з таблиць даних Semtech , дає кількість символів, необхідних для передачі корисного навантаження ns, як функцію всіх цих параметрів. Це число слід додати до кількості символів преамбули, щоб обчислити загальний розмір пакета в символах. У цьому рівнянні PL - розмір корисного навантаження в байтах, CRC = 16, якщо CRC увімкнено, а нуль інакше, H = 20, коли заголовок увімкнено, і нуль в іншому випадку, а DE = два, коли включена низька оптимізація швидкості передачі даних і нуль інакше . Ця формула також показує, що мінімальний розмір пакету становить вісім символів.

$$n_s = 8 + max\left(\left\lceil \frac{8PL - 4SF + 8 + CRC + H}{4 \cdot (SF - DE)} \right\rceil \cdot \frac{4}{CR}\right) \quad (3.3)$$

3.4 Загальна ємність та завантаження каналу

Загальна потужність мережі не лише пов'язана з розміром корисного навантаження. Оскільки дві передачі на одній частоті, але при різних коефіцієнтах розповсюдження, можуть декодуватись одночасно, то далі логічний канал визначається парою (смуга частот, коефіцієнт розповсюдження).

Загальна пропускна спроможність мережі LoRaWAN – це сума потужностей усіх логічних каналів. У діапазоні частот 125 кГц є шість можливих факторів розповсюдження (від 7 до 12), що приводить загальну ємність каналу 125 кГц до 12,025 біт / с.

Набір обов'язкових каналів містить три канали 125 кГц, які складають мінімальну загальну ємність мережі 36 кбіт / с. Оператори мереж можуть додавати більше каналів (надсилаються на пристрої за допомогою команд NewChannelReq), тим самим збільшуючи ємність мережі.

Оскільки швидкість передачі бітів залежить від коефіцієнта розповсюдження, не всі логічні канали мають однакову ємність. Навантаження для логічного каналу визначається середнім часом кількості пристроїв LoRa, які намагаються надсилати дані.

3.5 Оцінка коефіцієнта зіткнення

Відповідно до поточної специфікації, пристрої та шлюзи можуть передавати в будь-який час. Немає прослуховування перед розмовою або CSMA механізмом. Це робить LoRaWAN дуже схожим на ALOHA , але всупереч ALOHA зі змінною довжиною пакету.

Через обмеження в 1% робочого циклу, 100 пристроїв знадобилося б для імітації навантаження одного, і це число зросло б пропорційно максимальному навантаженню зв'язку, яке ми хотіли перевірити. . Оскільки таких пристроїв було не так багато, моделювання використовуються для оцінки поведінки LoRaWAN під навантаженням.

Для моделювання випадкових процесів викидів пакетів був побудований тренажер. Для кожної точки даних було змодельовано п'ятсот тисяч пакетів. Якщо час передачі двох пакетів перекривається, ми вважаємо, що відбувається зіткнення і що жоден з двох пакетів не доходить до шлюзу. Коефіцієнт зіткнення

– це кількість пакетів, що зіткнулися, поділене на загальну кількість пакетів,

відправлених під час моделювання. Використання пропускної спроможності каналу обчислюється як обсяг даних, який успішно передається під час моделювання, поділений на теоретичний максимальний обсяг даних, який міг бути відправлений у канал, на ємність каналу, помножену на тривалість моделювання. Навантаження каналу таке, як визначено в попередньому розділі 3.6, або еквівалентно, сума тривалості всіх пакетів, відправлених під час моделювання, поділена на тривалість моделювання.

Тривалість пакетів для різних розмірів корисного навантаження була обчислена за допомогою калькулятора LoRa Semtech, для коефіцієнта поширення семи, пропускної здатності 125 кГц, частоти коду 5/4 та шести символів у преамбулі.

Якщо припустити, що прихід пакетів дотримується закону Пуассона та рівномірного розподілу довжини корисних навантажень між одним і 51 байтом, можна намітити очікуване використання потужності та швидкість зіткнення залежно від навантаження для одного логічного каналу. Результат показаний на рис. 3.3.

Рисунок 3.3 – Використання потужності посилання та швидкість зіткнення пакетів для мережі LoRaWAN та порівняння з мережею ALOHA

Змінна довжина пакету не сильно впливає на продуктивність LoRaWAN, спостережувана поведінка дуже близька до поведінки ALOHA. Максимальне

використання потужності становить 18% від ємності каналу і досягається при завантаженні каналу 0,48. Однак при такому навантаженні близько 60% переданих пакетів скидаються через зіткнення.

Це може бути проблемою, оскільки якщо пристрої не використовують підтверджені повідомлення, деякі повідомлення будуть втрачені (і збільшення кількості разів, яке кожне повідомлення надсилає пристроями, є поганим рішенням, оскільки це збільшить навантаження на посилання), і якщо пристрої використовують підтверджені повідомлення, їм доведеться повторно передаватибільшість пакетів кілька разів, що додатково вплине на термін служби акумулятора пристроїв.

Повідомлення, підтверджені LoRaWAN, надіслані пристроями, повинні бути розпізнані пакетом, відправленим під час одного з двох вікон прийому після передачі, тоді як підтверджені повідомлення, надіслані шлюзом, будуть підтверджені під час наступної передачі висхідної лінії зв'язку. Підтвердження - це лише прапор у заголовку пакету, а налаштування цього прапора визнає останнє отримане повідомлення. Таким чином, при використанні підтверджених повідомлень новий пакет не повинен надсилатися до отримання підтвердження попереднього пакету; інакше буде неможливо дізнатися, на який пакет буде посилатися наступне підтвердження.

Недолік цього механізму полягає в тому, що підтверджене повідомлення потребує двох послідовних передач, щоб досягти успіху, таким чином збільшуючи ймовірність зіткнення з іншими повідомленнями та кількість необхідних повторних передач. Шлюз не надсилає команди MAC на пристрій, тому повідомлення про підтвердження завжди використовує 13-байтовий MAC-заголовок і не має корисного навантаження. Ми також враховуємо ці повідомлення під час обчислення навантаження, тобто коли сума тривалості всіх повідомлень та їх підтверджень дорівнює тривалості моделювання, значення навантаження дорівнює одиниці. Результат показаний на рис. 3.4.

Рисунок 3.4 – Використання потужності посилання та швидкість зіткнення пакетів для мережі LoRaWAN при використанні підтверджених повідомлень

Як і очікувалося, рівень успішності значно нижчий, ніж без підтверджених повідомлень. Однак це відносно ефективний спосіб реалізації цієї функціональності, оскільки в будь-якому випадку необхідні дві успішні передачі. Результати показують, що LoRaWAN надзвичайно чутливий до навантаження каналів, подібно до ALOHA. Рішення, реалізоване звичайними мережевими протоколами, такими як 802.11 або стільникові мережі, для усунення цієї проблеми є CSMA. Для забезпечення масштабованості LoRaWAN може бути цікаво вивчити доцільність впровадження механізму CSMA в LoRaWAN. Можливою проблемою є обмеження робочого циклу, яке застосовується в шлюзі,і це заважає надто часто надсилати повідомлення; інша - це потенційна неперехідність каналу (тобто кінцевий пристрій може або не може «відчути носій», якщо інший кінцевий пристрій передає на той самий шлюз). Якщо збережена поточна архітектура, механізм CSMA повинен був би контролювати мережевий сервер, що поставило б на нього ще більше навантаження. На жаль, механізм CSMA також може зняти ризик зіткнення підтвердження підтверджених повідомлень, зробивши це в період, що не має суперечок.

Поточна специфікація LoRaWAN не має жодних засобів для забезпечення якості обслуговування, і, таким чином, вона не повинна використовуватися для критичних додатків. Регулювання кількості разів, коли пристрій надсилає свої пакети, може збільшити ймовірність проходження цих пакетів, але це робиться за

рахунок більшої кількості зіткнень з передачами від інших вузлів і не дає жодної жорсткої гарантії.

В даний час LoRaWAN використовує групи ISM, які мають перевагу в тому, що вони безкоштовні і не вимагають ліцензії. Однак ці групи все більше використовують конкуренти LoRaWAN. Навіть якщо LoRa дуже стійкий до перешкод, ці смуги мають обмежену ємність, і не гарантується, що ємність цієї смуги достатня. Використання фірмового частотного діапазону матиме перевагу для видалення більшості перешкод.

3.6 Роль мережевого сервера

LoRaWAN визначає поведінку пристроїв, але не поведінку мережевого сервера. Як показано в розділі 3.5, важливо тримати навантаження на мережу низькою, а мережевий сервер повинен це виконувати, надсилаючи команди MAC на пристрої. Правильну поведінку мережевого сервера важко оцінити.

Мережевий сервер може легко погіршити продуктивність мережі. Наприклад, він може використовувати команду LinkADRReq для налаштування кількості разів, коли пристрій надсилатиме кожен кадр даних. Цей параметр рекламується як спосіб контролю якості обслуговування пристрою.

Більше того, рекламуються мережі LoRaWAN, які можуть працювати з мільйонами пристроїв. Мережевий сервер буде відповідати за оптимізацію всіх цих вузлів. Навіть якщо частота подій у сенсорних мережах значно нижча, ніж у традиційних мережах, продуктивність мережевого сервера повинна бути ретельно оцінена мережевими операторами, щоб забезпечити масштабування мережі.

3.7 Роль шлюзу

У поточній специфікації зазначено, що шлюз є лише реле. Це пов’язано з тим, що пакети, що надсилаються пристроями, не мають адреси призначення (що зберігає кілька байтів) і що немає зв'язку між пристроєм і шлюзом. Дійсно,

оскільки кілька шлюзів можуть отримувати одне і те ж повідомлення від пристрою, лише один з них повинен відповідати на нього. На мережевий сервер потрібно вибрати кращий шлюз.

Єдине завдання, яке повинні вирішувати шлюзи, - це терміни передачі повідомлень низхідної лінії зв'язку. Цей термін повинен бути точним, щоб пристрій отримував повідомлення у вікні отримання. Не вказано, чи отримують шлюзи повідомлення для відправки разом із сервером, а також час, в який воно повинно бути надіслане, або якщо шлюз надсилає повідомлення, отримане з сервера, як тільки він його отримує, і незрозуміло, яке рішення реалізоване в існуючих шлюзах. Оскільки час зворотного ходу інтерфейсного інтерфейсу шлюзів неможливо контролювати, перше рішення слід реалізувати. Це також дозволить синхронізувати передачі різних шлюзів, уникаючи зіткнень між ними.

У поточній специфікації кожен шлюз присвячений певному мережевому серверу. Це означає, що і шлюзи, і зібрані дані є "власністю" суб'єкта господарювання, який працює єдиним мережевим сервером. Надалі було б цікаво розширити функцію шлюзів, щоб вони могли пересилати пакет на певні мережеві сервери, як показано на рис. 3.5. Це може ефективно зменшити витрати пристроїв та розгортання мережі.

Рисунок 3.5 – Приклад спільних шлюзів у LoRa

Схожість

Джерела з Бібліотеки 28

1	Студентська робота	ID файлу: 1011186488	Навчальний заклад: Taras Shevchenko National Universit	7 Джерело	1.36%
2	Студентська робота	ID файлу: 1008364254	Навчальний заклад: Poltava National Technical Yuri Kondratyuk U...		0.65%
3	Студентська робота	ID файлу: 8289674	Навчальний заклад: Lviv Polytechnic National University	5 Джерело	0.64%
4	Студентська робота	ID файлу: 1007934726	Навчальний заклад: National Technical University of Ukra	2 Джерело	0.56%
5	Студентська робота	ID файлу: 1010296840	Навчальний заклад: Kharkiv National Air Force University named ...		0.45%
6	Студентська робота	ID файлу: 6000204	Навчальний заклад: National Technical University of Ukraine “Kyiv Po...		0.42%
7	Студентська робота	ID файлу: 1004051731	Навчальний заклад: National Aviation University	5 Джерело	0.31%
8	Студентська робота	ID файлу: 1000734732	Навчальний заклад: Lviv Polytechnic National University		0.26%
9	Студентська робота	ID файлу: 1013097468	Навчальний заклад: Yuriy Fedkovych Chernivtsi National University		0.1%
10	Студентська робота	ID файлу: 1003903029	Навчальний заклад: National Technical University of Ukraine “Kyi...		0.08%
11	Студентська робота	ID файлу: 1011568986	Навчальний заклад: Vasyl Stus Donetsk National Universi	3 Джерело	0.08%