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

Інститут телекомунікаційних систем

Кафедра Телекомунікацій

До захисту допущено:

Завідувач кафедри

_____ Сергій КРАВЧУК

«___»_____2021 р.

Дипломна робота

на здобуття ступеня <u>бакалавра</u>

<u>Спеціальності 172 «Телекомунікації та радіотехніка»</u>

на тему: «Зв'язок пристроїв IoT без підключення до мережі через мобільні мережі LTE»

Виконав: студент ____4____ курсу, групи _____ТМ-71_____
(шифр групи)

__Кузьменко Катерина Вікторівна_____
(прізвище, ім'я, по батькові) (підпис)

Керівник _д.т.н., професор, завідувач кафедрою. Кравчук С.О_____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _доцент, к.т.н, Правило В.В_____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2021 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Телекомунікацій

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 172 «Телекомунікації та радіотехніка»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Сергій КРАВЧУК
«___»_____2021 р.

ЗАВДАННЯ
на дипломну роботу студенту
Кузьменко Катерині Вікторівні

1. Тема роботи : Зв’язок пристроїв IoT без підключення до мережі через мобільні мережі LTE

керівник роботи Кравчук Сергій Олександрович, д.т.н., професор, завідувач кафедрою телекомунікацій_____
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від 14 квітня 2021 р. № 1007-с

2. Термін подання студентом роботи 7 червня 2021р.

3. Вихідні дані до роботи: використання мобільніх мереж LTE у технологіях Інтернету Речей, задіяння M2M в мережах LTE,

4. Зміст роботи:

1) Введення основних понять про архітектуру LTE

2) Опис масштабованості та впливу M2M/IoT на мобільні мережі

3) Досліждення масштабності M2M

4) Представлення комунікації без підключення над LTE мобільними мережами

5) Представлення експериментальних результатів моделювання без зв’язку

6) Обговорення основних міркувань щодо впровадження та безпеки запропонованої техніки

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

Слайд №1-2: Актуальність та мета роботи

Слайд №3-5: Опис основних понять про архітектуру LTE

Слайд №6: Опис масштабованості та впливу M2M/IoT на мобільні мережі

Слайд №7: Дослідження масштабності M2M

Слайд №8-9: Опис моделі без підключення

Слайд №10-12: Експериментальні результати моделювання без зв’язку

Слайд №13: Вимоги безпеки та впровадження запропонованої техніки

Слайд №14: Загальні висновки по роботі

6. Дата видачі завдання 10.11.2021р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Аналітичний огляд літератури щодо задіяння M2M в LTE	13.11.2020-18.12.2020	
2	Дослідити масштабованість і вплив M2M / IOT на мобільні мережі	07.01.2021-26.02.2021	
3	Розробити модель	06.03.2021-	

	безпідключення комунікацій IOT над LTE мобільними мережами	22.04.2021	
4	Результати запропонованої моделі	24.04.2021- 13.05.2021	

Студент Катерина Кузьменко

Керівник Сергій Кравчук

Реферат

Робота містить 63 сторінки, 16 рисунків, 4 таблиці. Було використано 38 джерела.

Мета роботи: У цій роботі запропоновано та проаналізовано нову техніку для забезпечення невеликого шлицевого ALOHA-подібного каналу зв'язку, вбудованого в кожному LTE eNB, забезпечуючи засоби для зв'язку без обмежень для пристроїв loT. Дослідження системи зв’язку M2M (“машина-машина”). Представлення нової методики передачі даних M2M через безпроводовий доступ LTE без дорогого обміну сигналами на мобільному ядрі.

В ході виконання роботи представлено новий протокол зв'язку без з’єднання для пристроїв loT через мобільні мережі LTE, який не вимагає сигналізації площини управління на EPC.. Проведено моделювання запропонованої моделі.

Ключові слова: Інтернет речей (IoT), довготерміновий розвиток (LTE), система зв’язку “машина-машина” (M2M), безпроводові мобільні мережі.

Abstract

The work contains 63 pages, 16 figures, 4 tables. 38 sources were used.

Goal: This paper proposes and analyzes a new technique for providing a small splined ALOHA-like communication channel embedded in each LTE eNB, providing unrestricted communication means for loT devices. Research of the M2M ("machine-machine") communication system. Introduction of a new M2M data transmission technique via wireless LTE access without expensive signal exchange on the mobile core.

In the course of the work, a new connectionless communication protocol for loT devices via LTE mobile networks was introduced, which does not require control plane signaling on the EPC. The proposed model is modeled.

Keywords: Internet of Things (IoT), long-term evolution (LTE), machine-to-machine (M2M) communication system, wireless mobile networks.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

LTE	Long Term Evolution. Довгострокова еволюція
IoT	Internet of Things - Інтернет речей
M2M	Machine-to-Machine.
RAN	Мережа радіодоступу.
EPC	Evolved Packet Core. Ядро, відповідальне за встановлення та управління IP-з'єднанням "точка-точка" між UE та Інтернетом
UE	User Equipment. Обладнання користувача
SGW	Шлюз обслуговування
MME	Організація управління мобільністю
HSS	Сервер домашнього абонента
PRB	Блок фізичних ресурсів
RB	Блок ресурсів
PBCH	Фізичний широкомовний канал
RACH	Канал довільного доступу.
RAR	Відповідь довільного доступу
TA	Time Advance - область відстеження
RNTI	Тимчасовий ідентифікатор радіомережі
RRC	управління радіоресурсами
QoS	Якість обслуговування
UL	Висхідна лінія зв’язку
DL	Низхідна лінія зв’язку

ВСТУП

Нещодавна еволюція комунікаційних систем представляє велику різноманітність мережевих об’єктів, які взаємодіють між собою та надають широкий спектр нових послуг. За традиційним сценарієм підключених комп’ютерів та портативних пристроїв (наприклад, мобільних телефонів та смартфонів) зв’язок зараз охоплює побутову техніку, машини та транспортні засоби. Зближення Інтернету та стільникових мобільних мереж виробляє нові системи зв'язку «машина-машина» (M2M), визначаючи мобільні мережі як одну з основних платформ для Інтернету речей (loT) [1]. Сплеск вбудованих пристроїв M2M, який протягом найближчих кількох років [2] очікується на мільярди, створить основи loT, сприяючи появі нових послуг зв'язку[3].

Безпроводові мобільні мережі є однією з основних платформ для широкого появи систем M2M. Незважаючи на те, що більшість сучасних систем M2M працюють у мережах 2G та 3G, довготермінова еволюція (LTE) очікується і широко визнана головним фактором, що сприяє появі loT [4], оскільки великі виробники обладнання вже починають фокусувати свої інвестиції в LTO на основі loT [5]. Поєднання запланованого відключення мереж 2G [6] та більшої пропускної здатності та низької потужності LTE зміщує розгортання loT до мобільних мереж LTE.

Відомо, що характеристики трафіку багатьох мережевих додатків M2M істотно відрізняються від характеристик смартфонів [7]. Мобільні мережі були розроблені та оптимізовані для транспортування людського трафіку, і, отже, вони, як відомо, страждають від неефективності використання ресурсів при обробці зв'язку M2M [8]. Вони викликають дедалі більшу стурбованість у галузі для розуміння динаміки зростання M2M у мережах LTE. Визнано, що LTE може бути пригнічений стрибком навантаження як на трафік, так і на

контрольну площину [9-10]. Про випадки впливу такого сплеску навантаження на мобільне ядро повідомлялося протягом останніх років [11-13]. Дослідники безпеки також стверджували, що така неефективність може бути використана під час зловмисних атак. Це призвело до того, що органи стандартизації почали пропонувати рішення [14] для запобігання перевантаженням сигналів та пропонувати вдосконалені системи зв'язку M2M через LTE.

У цій роботі представлена нова методика передачі даних M2M через безпроводовий доступ LTE без дорогого обміну сигналами на мобільному ядрі. Ця комунікація M2M без зв’язку розроблена з урахуванням стандартів 3GPP (Проект партнерства третього покоління). Він використовує низькорівневі канали, зіставлені на фреймі LTE, для кодування даних як у висхідній лінії зв'язку (UL), так і в низхідній лінії зв'язку (DL). Кодуючи дані користувача в певних полях пакетів у цих каналах фізичного рівня (PHY), потенційно можна досягти пропускної здатності близько 16 кбіт / с в DL. і 3,84 кбіт / с в UL. З огляду на характеристики беззв’язкових посилань, метод призначений для додатків M2M з низькою пропускною спроможністю та стійкими до затримки, таких як віддалені камери безпеки, системи перевірки стану, що періодично надсилають повідомлення про неживість, трекери місцезнаходження парку, що періодично звітують про координати тощо.

Запропонований метод визначає альтернативний протокол I рівня, забезпечення невеликого шлицевого ALOHA-подібного зв'язку на кожній базовій станції LTE. Також пропонуються вдосконалення базової системи, які істотно збільшують максимальну досяжну пропускну здатність. Доцільність цієї нової технології демонструється за допомогою системного моделювання. Для того, щоб отримати надзвичайно реалістичні результати, моделювання включає реальне фонове завантаження LTE-трафіку, захопленого найсучаснішим LTE-сніфером на переповненому перехресті центру Манхеттена. Результати вказують на те, що зв’язок M2M без з’єднання через мережі LTE

здійсненний. Вони є потенційною ефективної альтернативою трафіку та сигналізації для розгортання IoT в мережах LTE з майже нульовим впливом на звичайний трафік LTE. Успішне впровадження цієї технології, однак, потребує вирішення ряду наслідків для безпеки, про які також йшлося в статті.

Решта дипломної роботи організована таким чином. Розділ I коротко вводить основні поняття про архітектуру LTE та основні канали, що використовуються в системах зв'язку M2M без зв'язку. У розділі II розглядаються відомі проблеми поширення IoT у мобільних мережах. У розділі III представлені основні результати дослідження масштабованості IoT через мережі LTE. Далі, Розділ IV представляє комунікації без з’єднання в мережах LTE та їх структуру з урахуванням реального захоплення трафіку LTE. У розділі V представлені результати моделювання без зв’язку. Нарешті, розділ VI обговорює основні міркування щодо впровадження та безпеки цієї запропонованої техніки, а розділ VII завершує роботу.

РОЗДІЛ І. LTE МОБІЛЬНІ МЕРЕЖІ

LTE був розроблений з метою забезпечення IP (Інтернет-протоколу) зв'язку між мобільними терміналами та Інтернетом. З цією метою мережа LTE, як правило, оснащена низкою вузлів, які виконують певні завдання. Рисунок 1 робить знімки архітектури мережі LTE. Мережі LTE розділили свою архітектуру на дві основні секції: мережу радіодоступу (RAN) та основну мережу, відому як Enhanced Packet Core (EPC).

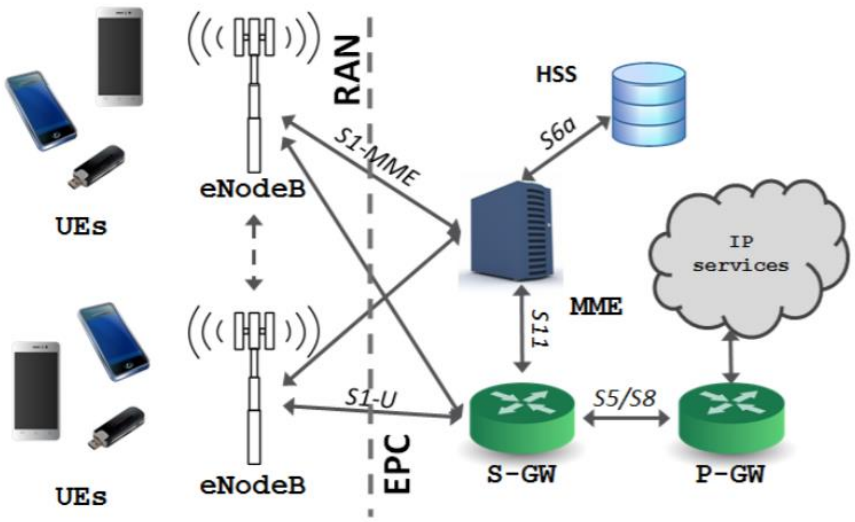


Рис. 1.1 Архітектура мережі LTE

RAN мережі LTE складається з мобільних терміналів, відомих як User Equipment (UE), та eNodeB, або базових станцій LTE. Еволюція мобільних мереж у напрямку LTE дозволила високо ізолювати та спеціалізувати операції RAN та EPC. RAN здатний, незалежно від EPC, призначати радіоресурси для UE, управляти їх використанням радіоресурсів, здійснювати контроль доступу та, використовуючи інтерфейс X2 між eNodeB, керувати мобільністю та передачею обслуговування.

EPC відповідає за встановлення та управління точковим з'єднанням між UE та Інтернетом. Він містить ряд вузлів; Шлюз обслуговування (SGW) і Шлюз

PDN (мережа пакетних даних) (PGW) є двома точками маршрутизації для підключення користувацького трафіку до PDN. Крім того, логістикою встановлення та випуску носія, мобільністю та іншими функціями мережі, такими як аутентифікація та контроль доступу, керує Організація управління мобільністю (MME). Для забезпечення безпеки користувальницького трафіку MME взаємодіє з сервером домашнього абонента (HSS), який зберігає параметри автентифікації, секретні ключі та дані облікового запису користувача всіх UE.

Ряд пристроїв користувацького обладнання (UE) або мобільних терміналів, а також eNodeB або базові станції LTE складають RAN. Ця частина бездротового доступу в мережі LTE контролює призначення радіоресурсів мобільним терміналам, управління їх використанням радіоресурсів, контроль доступу та, у випадку реалізації інтерфейсу X2 між eNodeB, навіть самостійно управляє мобільністю та передачею обслуговування. EPC.

На відміну від попередніх стандартів мобільного зв'язку на основі 3GPP, LTE був розроблений з метою пропонувати лише послуги з комутацією пакетів, забезпечуючи IP-зв’язок між мобільними пристроями та Інтернетом. Мережева архітектура LTE визначає дві частини: мережу радіодоступу (RAN) та ядро стільникового пакету, відоме як Enhanced Packet Core (EPC) [15]. EPC містить вузли, відповідальні за встановлення тунелю, відомого як канал, для передачі трафіку між мобільними пристроями та Інтернетом. Більше того, EPC керує логістикою носія, функціями аутентифікації та шифрування. RAN складається з двох типів вузлів - обладнання користувача (UE) або мобільних терміналів та базової станції eNodeB або LTE. RAN призначає радіоресурси мобільним терміналам та керує їх використанням.

EPC - це ядро, відповідальне за встановлення та управління IP-з'єднанням "точка-точка" між UE та Інтернетом. Більше того, певні операції MAC (Medium

Access Control) в RAN запускаються або контролюються базовою мережею. EPC складається з наступних вузлів мережі. Шлюз обслуговування (SGW) і Шлюз PDN (PGW) - це точки маршрутизації, які закріплюють з'єднання точка-точка, відоме як несуча, між UE та Інтернетом. Орган управління мобільністю (MME) керує логістикою несучої площини управління, мобільністю та іншими функціями мережі. для автентифікації кінцевих користувачів MME взаємодіє з сервером домашнього абонента (HSS), який зберігає параметри автентифікації та секретні ключі всіх UE. Для управління мережею та забезпечення зв'язку мережі LTE виконують низку процесів сигналізації, відомих як функції доступу без доступу (NAS). Такі функції координуються і запускаються за допомогою некористувацьких повідомлень даних між вузлами мережі LTE, відомими на площині управління сигналізацією трафіку.

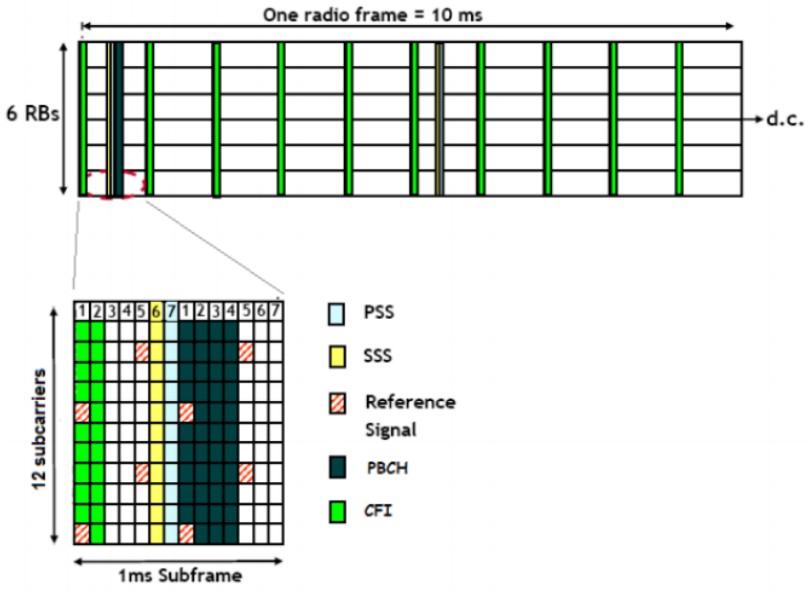


Рис. 1.2. Структура кадру LTE та відображення каналів керування DL

LTE RAN забезпечує пропускну здатність UE за допомогою рівня PHY на основі багаторазового доступу з ортогональним розподілом частоти (OFDMA) [15]. Радіоресурси поділяються як за часом, так і за частотою. Мінімальна одиниця розподілу, відома як Блок фізичних ресурсів (PRB), кодує символи 7x12 у блоці одного блоку ресурсів Ims у часі та Блоку ресурсів (RB) з 12

піднесучих за частотою. Два суміжні блоки ресурсів за часом утворюють підкадр, і, в свою чергу, 10 мс LTE-кадру формується з 10 підкадрів. Стандарт LTE підтримує конфігурації декількох смуг пропускання (BW), від 1,5 МГц (6 RB в частоті на кадр) до 20 MHZ (100 RB в частоті на кадр), причому 10 МГц найчастіше розгортаються. На рисунку 1.2 зображено кадр LTE у випадку конфігурації BW з 6 RB. Набір каналів PHY визначається, відображається та модулюється на фреймі LTE. Вони використовуються для транспортування як сигнального трафіку, так і фактичного спілкування користувачів [16]. Основні PHY-канали в DL наведені на рисунку 1.2. За винятком розподілу та відображення радіоресурсів для користувацького трафіку, відображення PRB для всіх інших каналів є постійним і відомим апріорі, що дозволяє телефону правильно розташуватися та підключитися до eNodeB (базова станція мережі стандарта LTE).

Будь-яке UE, яке бажає отримати доступ до мережі, має спочатку виконати процедуру вибору стільника. Далі UE декодує Фізичний широкомовний канал (PBCH) для вилучення базової конфігурації системи, необхідної для відображення та декодування інших каналів у комірці. На цьому етапі UE може ініціювати фактичне з'єднання за допомогою процедури довільного доступу. Нарешті, через EPC встановлюється носій для передачі та отримання користувацького трафіку.

1.1 Процедура довільного доступу LTE

Канал довільного доступу (RACH) - це канал висхідної лінії зв'язку, який використовується для запиту присвоєння радіоресурсу під час початкового доступу до системи. Перший обмін повідомленнями на цьому каналі також дозволяє UE досягти синхронізації UL. Передача за цим каналом є спільною для всіх користувачів у секторі та слідує протоколу Slotted-ALOHA / CSMA, тому можуть виникнути колізії. RACH мультиплексується за часом і частотою

на кожному кадрі, при цьому кількість ресурсів RACH відображається на кожному кадрі. Існує до 16 різних конфігурацій RACH, що дозволяє вчасно відобразити від 1 до 10 ресурсів RACH у кадрі [27]. Корпус 10, з одним ресурсом RACH у кожному підкадрі, призначений для ситуацій, в яких навантаження RACH є великим.

Процедура довільного доступу LTE, ініційована UE, базується на передачі коротких преамбул, які містять один підпис, вибраний випадковим чином із пулу з 64 доступних підписів. Ця процедура виконується у два етапи, які зображені на рисунку 1.2.1. На першому кроці підпис вибирається випадковим чином і пакет преамбули передається на один із ресурсів RACH. Отримавши преамбулу, eNodeB генерує відповідне повідомлення, відоме як відповідь довільного доступу (RAR), яке включає підпис, використаний у преамбулі, яка створила RAR. У разі зіткнення, виявленого eNodeB, або недоступності радіоресурсів, eNodeB включає поле в RAR-пакеті, що вказує UE на відмову для випадково сформованої кількості кадрів. Мобільний термінал очікує отримати повідомлення RAR протягом заздалегідь визначеного часового вікна. Якщо відповіді не отримано, преамбула повторно передається через мінімум 3 мс.

Повідомлення преамбули не кодує жодної інформації, тому воно має 0-бітове корисне навантаження. Він побудований із послідовностями Задоффа-Чу, що забезпечують покращену ефективність виявлення преамбули. RAR - це 56-бітний пакет, що містить ряд полів: ідентифікатор часово-частотного слота, куди була отримана преамбула, підпис, що використовується в преамбулі, інструкція Time Advance (TA) (для синхронізації UL) та початковий Ресурс UL. RAR також включає призначення довільного 16-бітового тимчасового ідентифікатора мережі для UE, відомого як тимчасовий ідентифікатор радіомережі (RNTI). Рисунок 1.2.1 включає реальне захоплення процедури довільного доступу між смартфоном та комерційною лабораторією Ericsson eNodeB. Захоплення було здійснено за допомогою готового знімача трафіку

Sanjole WaveJudge-Intelijudge 4900 LTE [17]. Усі фіксації руху, представлені в цьому рукописі, були отримані за допомогою того самого інструменту.

1.2 Початкові переходи стану прикріплення та RRC

Після процедури довільного доступу встановлюється підключення управління радіоресурсами (RRC) з кількома повідомленнями, якими обмінюються eNodeB та UE. Якщо UE підключається вперше, виконуються процедури ідентифікації та автентифікації. На цьому етапі встановлюється точковий носій через EPC, і RRC-з'єднання UE переконфігурується відповідно до типу послуги IP та якості обслуговування (QoS), що запитується. Дефіцит спектру та радіоресурсів призводить до суворої політики управління ресурсами. Щоразу, коли UE спостерігається в режимі очікування eNodeB протягом більше декількох секунд (часто від 10 до 15 секунд), RRC-з'єднання для цього UE звільняється, а пов'язані з ним радіоресурси звільняються для повторного використання іншими UE [18]. Незважаючи на те, що достатньо лише одного повідомлення від eNodeB до UE, щоб перевести його вниз у стан очікування RRC в режимі очікування, кожен підключений в режимі очікування і підключеного режиму очікування включає значну кількість сигналів площини управління з великою кількістю повідомлень всередині EPC.

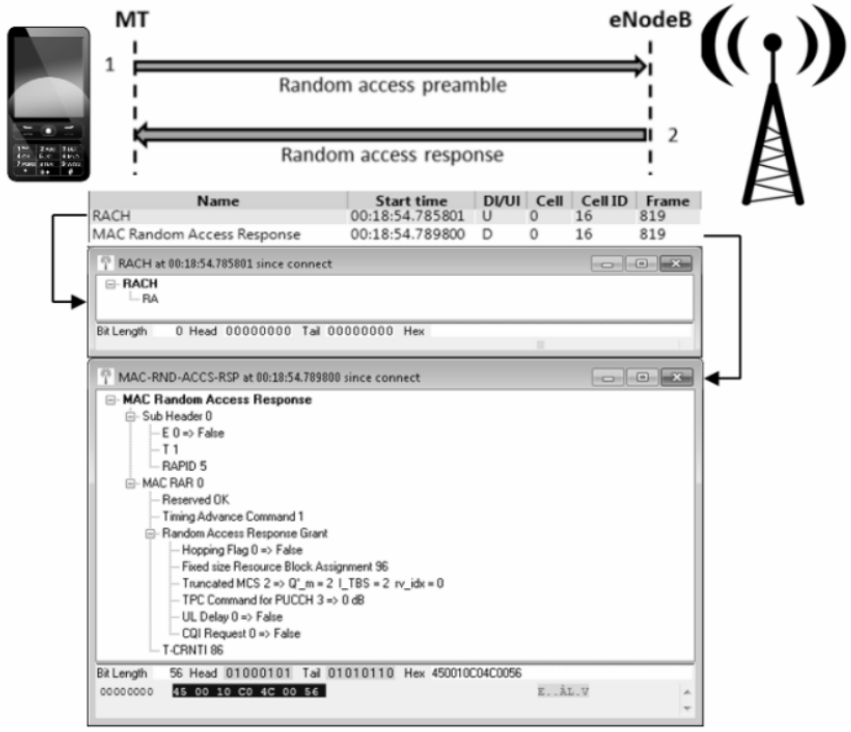


Рис. 1.2.1 Процедура довільного доступу LTE та захоплення з реальної мережі

1.3 Пейджинг

Пейджинг - це процес, який використовується для ініціації мобільного розірваного з'єднання та для запуску переходу стану очікування до підключеного з боку мережі. Всякий раз, коли є вхідне повідомлення, адресоване UE, мережа повинна визначити, в якій комірці знаходиться цей користувач. Якби це місце було відоме апріорі, мобільний термінал повинен був би оновити своє місце розташування за допомогою мережі. Для того, щоб зменшити навантаження сигналізації оновлення місцезнаходження, розташування кожного UE відоме лише з набагато більшою деталізацією, відоме як область відстеження (TA). Отримуючи вхідний трафік для UE, який знаходиться в режимі очікування, EPC запускає трансляцію повідомлення пейджингового зв'язку по кожній комірці в TA, де UE , як відомо, знаходиться [19]. Мобільний термінал відповідає на повідомлення пейджингового

повідомлення, розкриваючи своє точне місце розташування з точки зору комірки або сектора та запускає встановлення носія, ініціюючи процедуру довільного доступу.

1.4 Висновок до розділу

В цьому розділі було коротко описано архітектуру та процедуру вільного доступу мережі LTE. Описано процес пейджингу.

РОЗДІЛ ІІ. МАСШТАБОВАНІСТЬ І ВПЛИВ M2M / IOT НА МОБІЛЬНІ МЕРЕЖІ

M2M – система зв'язку яка відноситься до прямого дротового або бездротового зв'язку між пристроями, що використовують будь-який канал зв'язку, потреба в прямому втручанні людини є необов'язковою.

Така комунікація була спрямована на моніторинг віддалених машин, від яких отримувались дані, оброблялися на центральній станції, за допомогою спеціального програмного забеспечення та, зрештою, передавались назад до тих самих машин із налаштованими параметрами для подальшої роботи.

Хоча системи IoT та M2M мають віддалений доступ до пристроїв інших важливих подібностей немає. Робота системи M2M, як правило, полягає в комутації за принципом «точка-точка», використовуючи вбудовані апаратні модулі та спеціальні протоколи, а робота системи IoT, для передачі даних з пристроїв до хмарних сховищ або проміжного програмного забеспечення, переважно залежить від мережі на базі IP що використовує загальні/відкриті протоколи, для запеспечення максимальної сумісності, а також особливої сумісності між самими приладами.

Стільникові мережі налаштовані на транспортування комунікацій користувачів, що походять від смартфонів, що мають добре зрозумілі характеристики трафіку. Однак динаміки використання мережі та характеристики трафіку систем M2M дуже складні. Трафік M2M істотно відрізняється залежно від типу системи M2M. Наприклад, певні категорії пристроїв мають сильний дисбаланс між UL та DL трафіком, з явним домінуванням UL трафіку на відміну від трафіку смартфонів. Ці

диверсифіковані характеристики трафіку систем M2M є однією з основних проблем для масштабованості IoT в мобільних мережах LTE.

Мережі мобільності LTE розроблені для забезпечення збільшення ємності та ефективності спектру для підтримки великої кількості підключених пристроїв. Хоча в даний час значний відсоток нинішніх стільникових екосистем M2M базується на застарілих мережах другого та третього поколінь (2G та 3G), LTE визнано основною платформою для появи IoT. Більше того, застарілі мережі GSM вже заплановано припинити до кінця 2016 року. Паралельно, характеристики трафіку багатьох додатків IoT, що суттєво відрізняються від трафіку зі смартфонів та планшетів, є потенційним джерелом неефективності використання мережевих ресурсів. Як наслідок, існує занепокоєння щодо потенційного впливу систем M2M на регулярну роботу мереж LTE, які можуть бути пригнічені сплеском як трафіку, так і сигнального навантаження.

Поява IoT також призводить до сигнальних наслідків для EPC. На основі жорстких механізмів контролю за вступом потрібно оптимізувати використання мережі мобільності. Кожна транзакція або потік трафіку з / на пристрій M2M призводить до сигналізації на EPC для встановлення необхідних радіоресурсів. Непотрібні установи зв'язку можуть потенційно перевантажити основну мережу. Цей негативний вплив сигнального навантаження вже спостерігався в дикій природі у певних операторів мобільного зв’язку. Враховуючи очікуваний сплеск кількості підключених пристроїв M2M, результуюче зростання сигналізації може потенційно перевантажити EPC, що підтверджується спільнота стандартизації як потенційна загроза мережам LTE.

Поява IoT має прямий вплив на сигнальне навантаження в EPC. Перед розгортанням безпроводових вбудованих пристроїв, які використовують пакетні послуги, слід врахувати деякі особливості мобільного ядра. Кожен окремий потік трафіку між UE і зовнішнім хостом часто призводить до сигналу площини

управління про перехід між станами RRC. Широко визнано, що непотрібний сигнальний трафік може потенційно перевантажити основну мережу, і дослідники теоретизують, що це може бути використано в атаках безпеки. Негативні наслідки перевантаження сигналів у мобільній мережі вже спостерігалися в дикій природі [11]-[13], [21]-[23]. Така велика кількість відомих випадків сигнальних штормів у дикій природі є чіткою мотивацією для розробки нових методів передачі, які не вимагають сигналізації на площині управління. У зв'язку з цим очікуваний сплеск такої сигналізації через розширення систем M2M визнається потенційним загроза LTE [14].

2.1 Висновки до розділу

В цьому розділі було розглянуто основні проблеми поширення IoT у мобільних мережах. Зроблено висновок, що використання мережі мобільності слід оптимізувати, щоб мінімізувати співвідношення навантаження сигналізації на трафік даних користувача.

РОЗДІЛ ІІІ. ДОСЛІДЖЕННЯ МАСШТАБНОСТІ M2M

Усі результати моделювання, представлені в цьому дослідженні, були створені на спеціальному тестовому полі досліджень безпеки. Він має середовище моделювання OPNET Modeler [32]. Він розроблений як повністю сумісний із стандартами інструмент, спеціально розроблений для великих масштабів. Усі результати моделювання, представлені в цьому дослідженні, були розроблені, впроваджені та закодовані з нуля щодо масштабованості та аналізу безпеки реальних мереж LTE. Тестовий стенд дозволяє швидко впровадити, протестувати та проаналізувати вплив великих розгортань системи M2M в дуже реалістичному середовищі. На рисунку 3.1 показано знімок екрана тестового зразка досліджень безпеки LTE.

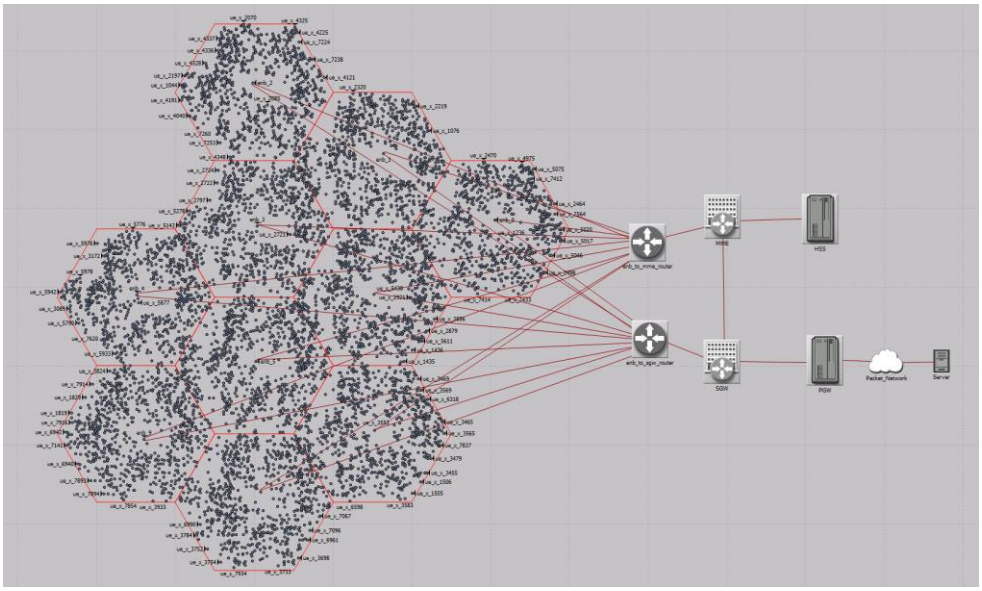


Рисунок 3.1 Тест для моделювання LTE для дослідження масштабованості M2M

Для проведення широкомасштабного імітаційного аналізу тестовий стенд використовує функцію System-in-the-Loop в OPNET [33]. На основі цього інструменту довільно велика мережа може бути розподілена по ряду віртуальних машин (ВМ) на хмарній інфраструктурі. Кожній ВМ призначено запустити частину повномасштабного моделювання, причому ВМ обмінюються даними через Інтернет - або, в нашому випадку, Локальну мережу (LAN). Це забезпечує засоби для імітації довільно великої мережі з мільйонами мобільних пристроїв, базових станцій та великої базової інфраструктури. Більше того, розподіл моделювання на декількох віртуальних машинах забезпечує великі переваги, із значним часом моделювання та необхідним обчислювальним зменшенням потужності, порівняно з базовим моделюванням, що виконується на одній машині з обмеженими ресурсами [35].

Для того, щоб отримати дуже точні результати взаємодії систем M2M, що обмінюються даними через мережу LTE, змодельований трафік законних пристроїв (як вбудованих пристроїв M2M, так і смартфонів) базується на високореалістичних статистичних моделях трафіку. Ці моделі отримані на основі повністю анонімних спостережень за реальними слідами трафіку LTE від одного з основних операторів першого рівня в США. Обидва повністю анонімні

записи детальної інформації про дзвінки (обробляється IP-трафік LTE для отримання статистичних моделей трафіку даних через LTE для типових смартфонів та пристроїв M2M. Розподіл ймовірностей формулюється на основі спостережуваних характеристик трафіку, таких як кількість висхідної / низхідної лінії зв'язку. пакети, час між пакетами, розмір пакета, час між сеансами та sessioCDR) та повністю анонімізовані метадані потоку IP-трафіку від розміру exn.

Для того, щоб генерувати реалістичні моделі з популярних смартфонів, ми обробляємо анонімізовані дані з останніх моделей телефонів від чотирьох основних виробників смартфонів. Паралельно ми аналізуємо анонімізовані дані для шести типових типів пристроїв M2M: відстеження активів, інтелектуальна мережа, персональні пристрої відстеження, телемедицина, GPS-навігатори, системи дистанційного оповіщення та електронні книги.

Це дозволяє реалістично моделювати зв’язок пристроїв LTE та взаємодію з мережею мобільності порівняно з іншими простішими та довільнішими статистичними моделями трафіку, що використовуються в літературі для подібних робіт. Етикетка для кожної категорії M2M була узагальнена, щоб не надавати конкретної інформації про фактичний тип вкладених пристроїв, що аналізуються, однак ми групуємо трафік для конкретних пристроїв на основі відомих IMEI та IP-адрес. При проведенні цього дослідження не було зібрано та використано жодної інформації, що ідентифікує особу. Наскільки будь-які дані були проаналізовані, це були анонімні та / або зведені дані.

3.1. Методологія аналізу

Важливо підкреслити, що мета аналізу полягає не в реалістичному моделюванні абсолютного впливу M2M на конкретне розгортання мережі LTE, а в тому, щоб представити цінну інформацію про потенційний вплив та

масштабованість IoT над LTE. Мета полягає в тому, щоб надати аналіз потенційних проблем масштабованості IoT, а не надати реалістичні результати, що вказують на те, як велика кількість пристроїв M2M буде насичувати мережу, і який буде конкретний вплив. Як результат, представлений тут аналіз керується дуже базовою, але суворою методологією.

Усі сценарії популяції мереж і пристроїв є суто загальними і не стосуються жодної заданої архітектури мережі. Конфігурація з точки зору обчислювальної потужності, пропускної здатності каналів та фактичної архітектури є довільною, спрямована на загальні результати. Тим не менше, тестовий стенд безпеки відповідає стандартам і точно імітує продуктивність та поведінку реальної мережі LTE. Експерименти чітко демонструють потенційний вплив масштабованості трафіку M2M і, що ще важливіше, потенційні вузькі місця або теплові точки в мережі. Однак абсолютно ніякої конкретної інформації не можна зробити з фактичного навантаження M2M, яке можна побачити в конкретному реальному комерційному впровадженні LTE.

Усі результати в Розділі 3.3 нормуються тим самим довільним скаляром, щоб надати порівняльний аналіз, а не кількісний аналіз. Мережа LTE кожного оператора налаштована по-різному і зібрана з безліччю постачальників та архітектур. Тому наша мета не кількісно визначити точний вплив сигналізації великої сукупності пристроїв, підключених до M2M, з певної категорії, а скоріше визначити, як би збільшився цей вплив, якби кількість пристроїв M2M збільшилась у коефіцієнт, наприклад, 10. Додатковим результатом є порівняльне визначення того, які зв’язки або вузли EPC переживають найбільший стрес дорожнього руху. Ці результати можуть бути дуже цінними для дослідницької спільноти для розробки стратегій управління радіоресурсами, оптимізованих для систем M2M, та для визначення мобільних архітектур наступного покоління для IoT.

Результати жодним чином не можуть бути використані для отримання та визначення фактичного навантаження трафіку та сигналізації в існуючому розгортанні LTE для заданого розміру популяції M2M.

Імітована мережа є загальною, з одним екземпляром EPC (MME, SGW, PGW та HSS), що обробляє IP-зв'язок між UE та зовнішнім сервером. Ємність сервера вважається безмежною, щоб не заважати вимірюванням на EPC. LTE RAN змодельований з ємністю та специфікаціями стандартного 10MHz розгортання LTE і складається з 10 комірок.

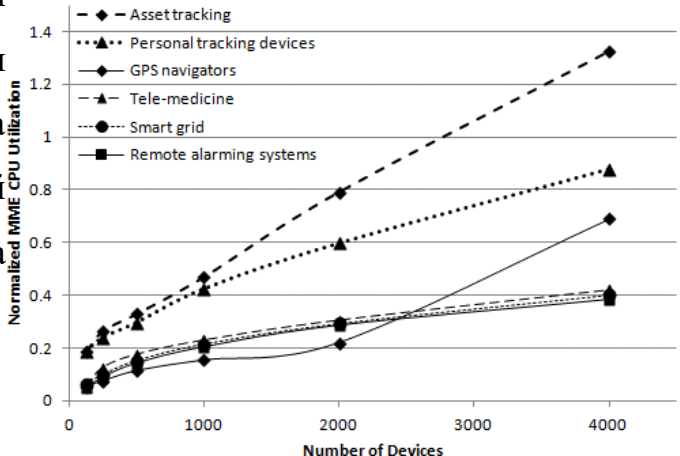
3.2. Результати

Проводиться серія симуляційних експериментів, в яких декілька мобільних терміналів M2M відправляють і приймають трафік відповідно до статистичних моделей трафіку, реалізуючи пристрої M2M з кожної категорії M2M. Кількість пристроїв збільшується і становить від 125 до 4000 UE. Різноманітна статистична інформація реєструється та складається для того, щоб проаналізувати, як масштабується кожна категорія пристроїв з точки зору як сигналізації, так і навантаження даних на EPC. Подальші експерименти проводяться, щоб отримати уявлення про те, як масштабованість систем M2M може потенційно вплинути на QoS користувачів смартфонів.

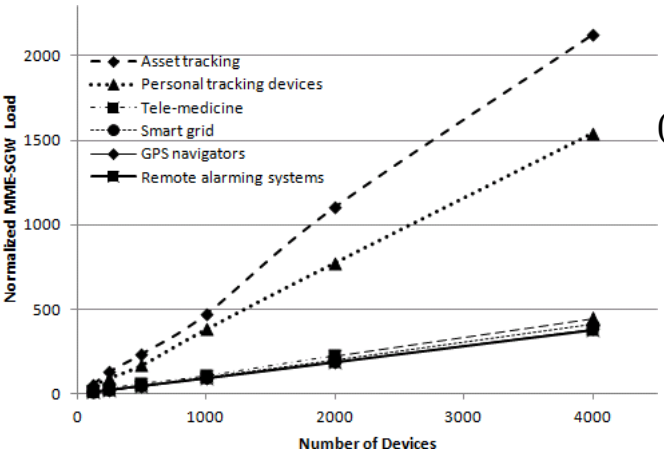
1) ***Сигнальне навантаження***: Потоки трафіку між пристроєм і хостом вимагають встановлення ресурсів у випадку пристрою, який спочатку перебуває в режимі очікування RRC. Протягом сеансу або потоку мобільний пристрій може залишатися у підключеному стані або може перемикати стан вперед-назад, залежно від часу між пакетами. Співтовариство стандартизації визнає збільшення трафіку сигналізації, спричинене системами M2M, як потенційну загрозу для мереж LTE [36]. Значне збільшення популяції M2M може потенційно створити напругу для EPC за допомогою цього сигналізаційного стрибка трафіку.

Перший експеримент досліджує навантаження каналу MME-SGW та використання центрального процесора MME для розпізнавання сигнального впливу масштабування пристроїв M2M, а результати наведені на рисунку 3.2.1 (a) та (b). Інтуїтивно зрозуміло, що категорії M2M, які мають найбільший вплив на використання каналів MME-SGW, відстеження активів та особисті пристрої відстеження, також найбільше напружують використання процесора MME. Зосереджуючись на цих двох категоріях пристроїв, можна помітити, що, хоча вони генерують приблизно однакове навантаження сигналізації MME-SGW для 125 пристроїв, навантаження зростає набагато швидше для відстеження активів із збільшенням кількості пристроїв. Згідно з рисунком 3.2.1 (a), 2000 пристроїв відстеження активів виробляють на 42,6% більше сигнального навантаження, ніж, наприклад, така ж кількість персональних пристроїв відстеження. Трохи схожа картина спостерігається для процесора MME. Зокрема, 125 персональних пристроїв відстеження виробляють приблизно таку саму завантаженість процесора MME, як 125 пристроїв відстеження активів, але 2000 пристроїв відстеження активів мають 32,5% більше навантаження, ніж така ж кількість персональних пристроїв відстеження. Для пристроїв 4000 M2M відстеження активів на 50,5% вище. Цікаво також помітити різке збільшення використання процесора MME, оскільки кількість GPS-пристроїв перевищує 2000. При збільшенні кількості пристроїв у 8 разів з 250 до 2000, використання CPU MME збільшується в 1,99 рази, проте коли подвоївши їх з 2000 до 4000, навантаження збільшується в 2,14 рази.

Загалом, результати вказують на чіткий стрибок навантаження сигналу в міру збільшення кількості популяції пристроїв M2M. Однак збільшення сигналізації видається лінійним і, за винятком GPS-пристроїв, постійним. Цей результат, хоча і базується на



моделюванні, може розглядатися як хороша новина, оскільки більше збільшення навантаження сигналів може свідчити про велику проблему для мобільних мереж впоратися з масштабованістю систем M2M.



(a)

(b)

Рисунок 3.2.1. Вплив сигналізації масштабованості M2M: (a) нормалізоване навантаження MME-SGW та (b) нормалізоване використання CPU MME

Щоб кількісно визначити категорію пристрою M2M, яка генерує найбільше збільшення сигналізації, у таблиці 1 перелічені коефіцієнти використання центрального процесора MME та градієнти навантаження каналу MME-SGW. Градієнт для кожної категорії був усереднений, оскільки кількість пристроїв масштабується від 125 до 4000. Згідно з результатами, пристрої для відстеження активів та персонального відстеження викликають збільшення використання процесора MME приблизно в 1,5-2,5 рази швидше, ніж пристрої, що належать до інших категорій . Що стосується посилання MME-SGW, навантаження від відстеження активів зростає в 17,88 рази швидше, ніж інші.

Ці результати вказують на те, що пристрої відстеження активів загалом потенційно можуть бути однією з найскладніших комунікаційних систем через мобільні мережі LTE, особливо якщо кількість пристроїв M2M, що відповідають категорії відстеження активів, значно зросла до мільйонів або навіть мільярдів нових з'єднань.

Сигнальне навантаження, що виникає внаслідок роботи пристроїв M2M, частково пов'язано з частими переходами стану RRC. Для багатьох категорій

систем M2M характерні невеликі імпульси передачі даних, як у висхідній, так і в низхідній лінії зв'язку, через часті інтервали. Проміжок часу між спалахами даних та сеансами зв'язку безпосередньо впливає на навантаження сигналів на EPC. Наприклад, якщо сеанси передачі даних повторюються з інтервалом трохи довшим, ніж таймер очікування RRC мережі, EPC буде нести набагато більше сигнального навантаження, оскільки пристрої постійно переходять між режимами очікування та підключенням для кожного спалаху трафіку. Теоретично відомо, що це може становити потенційну загрозу мережі [37].

Для того, щоб дослідити масштабованість систем M2M через LTE, важливо визначити, наскільки ефективно використовуються мережеві ресурси. Для цього ми досліджуємо середню кількість переходів стану RRC, які індукуються кожною системою M2M для передачі фіксованого обсягу даних. У таблиці 2 перелічено кількість переходів в режимі очікування на нормалізовану одиницю завантаження даних (додавання висхідної та низхідної ліній) у сценарії з 1000 пристроями. Результати обчислюються для кожної категорії трафіку M2M. Незважаючи на те, що інтелектуальні мережі та пристрої віддалених сигналізацій виробляють менше навантаження на сигнали в MME, ніж пристрої для відстеження активів та персонального відстеження, як показано на рисунку 5, через їх невеликий обсяг транзакцій, що відбувається через рідкісні проміжки часу, вони використовують мережу найбільш неефективно з усіх розглянуті нами категорії пристроїв.

Таблиця 3.2.1

Середнє використання ЦП MME та градієнти навантаження MME-SGW

Категорія M2M	**Середній градієнт ЦП MME**	**Середній градієнт навантаження MME-SGW**
Відстеження активів	0,00035	1,66893

Розумна сітка	0,00015	0,24562
Особисте відстеження	0,00024	0,30330
Телемедицина	0,00020	0,34757
GPS-навігатори	0,00014	0,1277
Дистанційна тривога	0,00016	0,09333

Таблиця 3.2.2

Кількість підключених до незаходжених державних переходів на M2M навантаження

Категорія M2M	**Переходи, пов’язані з режимом очікування на нормовану одиницю руху**
Відстеження активів	0,15593
Розумна сітка	45,67325
Особисте відстеження	5,37232
Телемедицина	9.22127
GPS-навігатори	23.63992
Дистанційна тривога	54,96471

2) ***Навантаження даних***: Системи M2M дуже різноманітні за обсягом даних, які вони передають і отримують, і часто виникає дисбаланс в обсязі трафіку висхідної та низхідної ліній [8]. Це є складним завданням для проектування архітектур мобільних мереж, які повинні ефективно боротися з неоднорідністю IoT. Як частина цього аналізу, ця робота також має на меті надати уявлення не лише про масштабованість трафіку даних, що виробляється кожною категорією пристроїв, а й про непрямий вплив, який стрибок обсягу трафіку даних може потенційно надати на конкретні елементи мережі.

Подібно до аналізу масштабованості навантаження сигналізації M2M, ми отримали результати, щоб визначити швидкість, з якою збільшується трафік даних із збільшенням сукупності M2M кожної категорії. На рисунку 3.2.2 розглянуто нормоване навантаження в зв'язку SGW - PGW для цієї ситуації. Зверніть увагу, що це посилання агрегує всі дані, як висхідну, так і низхідну, для всіх пристроїв в модельованій мережі. Як і у випадку масштабованості сигналізації, зображеної на рисунку 3.2.1 (а), пристрої відстеження активів та персонального відстеження, здається, генерують потенційно найбільше збільшення навантаження на трафік даних. Це додатково вказує на неоднорідність IoT, оскільки деякі вбудовані категорії пристроїв масштабують як сигналізацію, так і навантаження даних набагато швидше, ніж інші, в яких навантаження зростає дуже незначно.

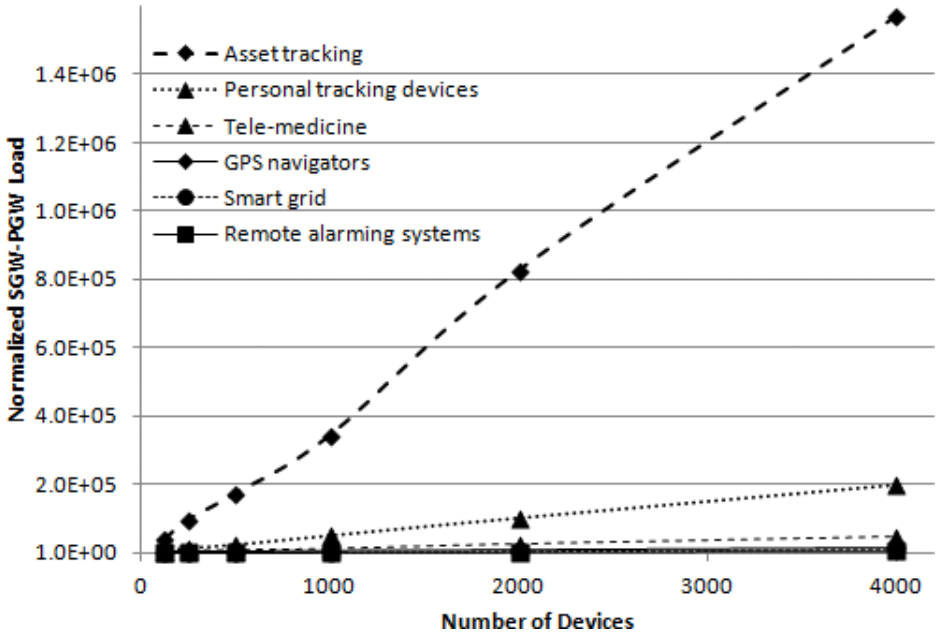


Рисунок 3.2.2 Масштабованість навантаження трафіку даних M2M

У таблиці 3.2.3 узагальнено результати збільшення навантаження трафіку даних висхідної та низхідної ліній зв'язку для кожної категорії M2M. Подібно до таблиці I, градієнт збільшення навантаження даних усереднюється, коли кількість населення масштабується від 125 до 4000 UE. Результати показують, що пристрої відстеження активів збільшують навантаження на трафік даних на два-два порядки швидше, ніж більшість інших категорій. Зауважте, що масштабованість трафіку даних також свідчить про те, що відстеження активів потенційно може бути однією з найскладніших систем M2M, оскільки воно масштабується через мобільні мережі LTE. Збільшення навантаження відстеження активів дещо збалансовано у висхідній та низхідній лініях, на відміну від персональних пристроїв відстеження, які мають значне збільшення, особливо в висхідній лінії зв'язку.

Таблиця 3.2.3

Навантаження трафіку даних висхідної та низхідної ліній зв'язку для кожної категорії M2M

Категорія M2M	**Середній градієнт трафіку UL**	**Середній градієнт трафіку DL**
Відстеження активів	191.187	201.247
Розумна сітка	1,565	0,646
Особисте відстеження	43,973	6.279
Телемедицина	11.284	0,590

GPS-навігатори	2.287	1.355
Дистанційна тривога	0,689	0,908

Масштабованість IoT через мобільні мережі LTE представляє додаткові виклики, засновані на цьому в основному незбалансованому співвідношенні між трафіком висхідної та низхідній лінії зв'язку деяких вбудованих пристроїв. На відміну від смартфонів, з переважним навантаженням по низхідній лінії зв'язку різні типи систем M2M працюють із сильно збалансованим трафіком даних вгору або вниз. На рисунку 3.2.3 зображено приклад цього різноманіття в дисбалансі між трафіком висхідної та низхідної ліній. У цьому прикладі можна спостерігати відстеження активів як систему з дещо збалансованим трафіком порівняно з персональними пристроями відстеження, які мають в 16 разів більше трафіку в висхідній лінії зв'язку. Цей дисбаланс обумовлений нормальною роботою персональних пристроїв відстеження, які в основному передають періодичні повідомлення висхідної лінії зв'язку з оновленням місцезнаходження.

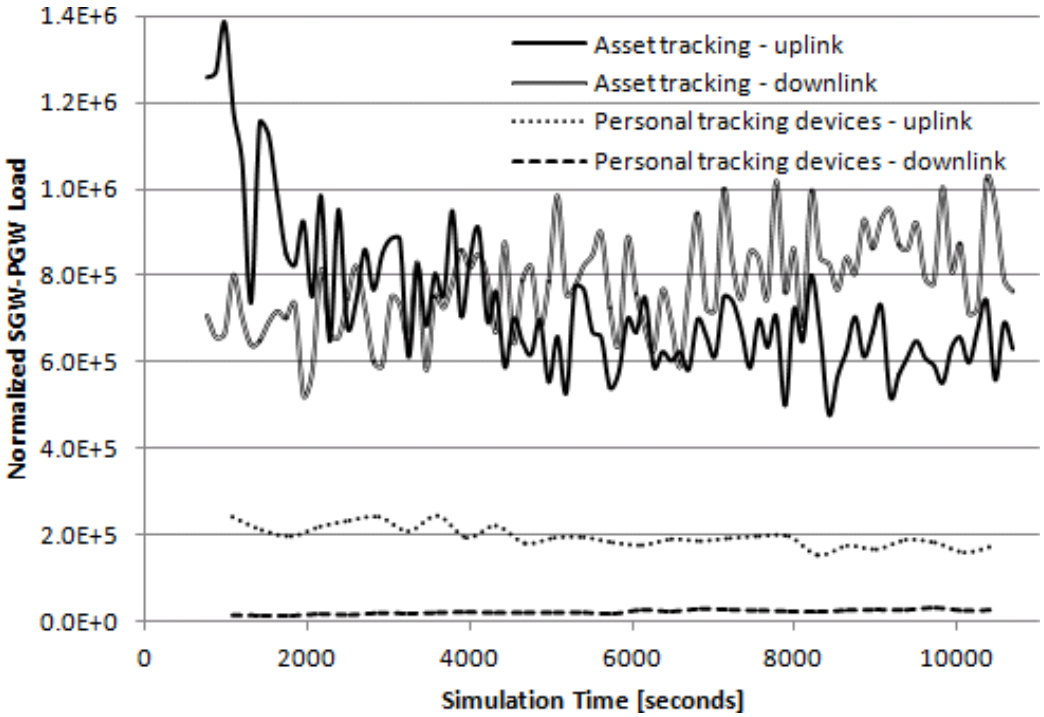


Рис. 3.2.3 Нормалізоване навантаження UL проти DL SGW-PGW для персональних пристроїв та пристроїв відстеження активів

3) ***Вплив на QoS***: вузли EPC, обтяжені великою кількістю сигналів, спричинених масштабуванням пристроїв M2M, можуть мати негативні наслідки для інших мобільних користувачів. Однією з цілей цього документу є визначити, яким чином на якість обслуговування користувачів смартфонів може впливати зростаюча кількість пристроїв M2M. Рисунок 3.2.4 ілюструє середню затримку, яка спостерігалася під час переходів стану RRC для невеликого набору користувачів смартфонів, зайнятих діяльністю одночасно з пристроями 1000 M2M. Той самий експеримент проводиться для кожної з шести аналізованих категорій M2M. Зверніть увагу, що завдяки впровадженню тестового стенду, всі UE, присутні в моделюванні, повинні зробити початкове прикріплення перед початком спілкування. Тому ми починаємо збирати результати для QoS для смартфонів через сім хвилин після моделювання, щоб на результати QoS ненавмисно не вплинув стрибок навантаження сигналу на початку моделювання, коли пристрої 1000 M2M підключаються до мережі. Також зауважте, що спочатку метричні піки QoS, оскільки всі смартфони підключаються одночасно, починаючи з сьомої хвилини.

Кожна категорія трафіку M2M по-різному впливає на затримку переходу до стану смартфона, причому категорія відстеження активів має найбільший вплив. Як тільки затримки досягнуть стійкого стану, пристрої відстеження активів накладають затримку, яка більше ніж удвічі перевищує затримку, яку виробляють GPS-навігатори, категорії з найменшим впливом. Незважаючи на те, що затримка переходу стану RRC істотно зростає, значення, досягнуті під впливом навантаження пристроїв 1000 M2M, все ще залишаються низькими і, швидше за все, не призведуть до помітного погіршення якості обслуговування. Однак QoS користувачів смартфонів може суттєво погіршитися завдяки більшій

кількості вбудованих пристроїв M2M, особливо якщо досягнуто прогнозів про мільярди з'єднань.

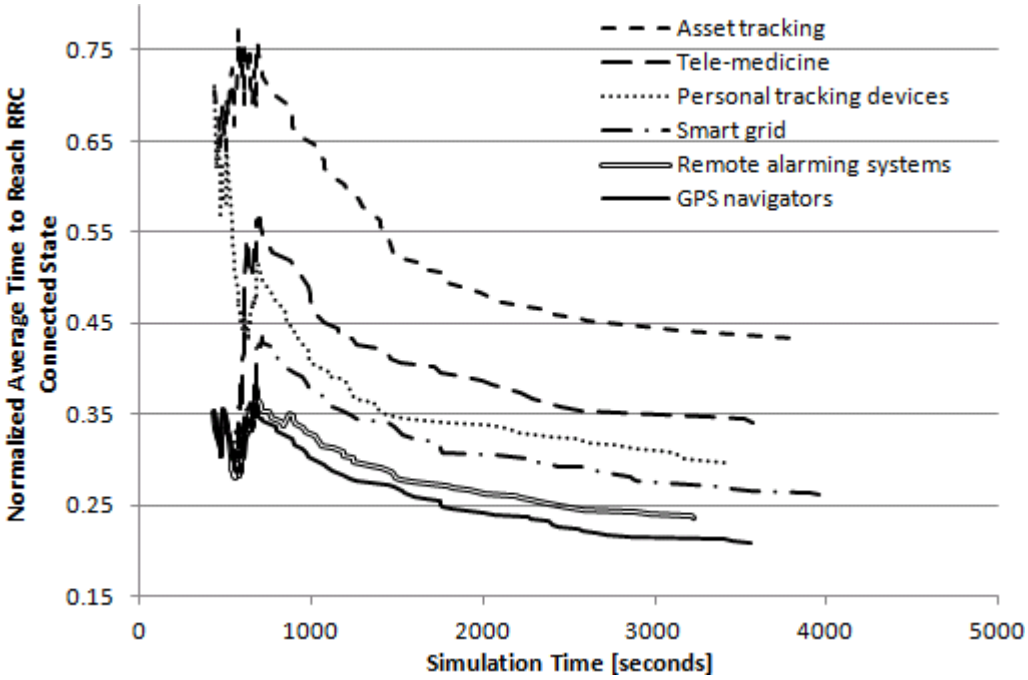


Рис. 3.2.4 Нормалізована середня затримка для досягнення стану підключеного RRC для смартфонів під час трафіку пристроїв 1000 M2M

Для того, щоб зрозуміти, як масштабування M2M-пристроїв впливає на QoS користувачів смартфонів, у таблиці 3.2.4 відображається середня нормована затримка пакетів висхідної лінії зв'язку, які зазнають 50 смартфонів, оскільки кількість пристроїв M2M постійно подвоюється, коливаючись від 500 до 2000 року. середній градієнт затримок у діапазоні масштабування. Завдяки сильному впливу, який пристрої для відстеження активів накладають на центральний процесор і пропускну здатність вузла EPC, як ми вже бачили пропускну здатність у цій статті, ця категорія також спричиняє найвищий приріст затримки пакетів висхідної лінії зв'язку для смартфонів серед усіх розглянутих нами категорій. У порівнянні із затримкою, спричиненою навігаторами GPS, затримка від пристроїв відстеження активів збільшується в 10 разів швидше. Як і при затримці переходу стану RRC, значення затримки пакетів висхідної лінії зв'язку, вироблені з пристроїв 2000 M2M, не особливо високі для цієї кількості пристроїв, однак вони значно зростають із

збільшенням кількості пристроїв M2M. Отже, досить великий обсяг трафіку M2M може потенційно спричинити затримки, що перевищують поріг допуску програм, особливо тих, що мають суворі вимоги до затримки.

Таблиця 3.2.4

Середня нормована затримка пакетів висхідної лінії зв'язку

Категорія трафіку M2M	**Нормалізована середня затримка пакетів висхідної лінії зв'язку**			**Середній градієнт**
	500	**1000**	**2000**	
Відстеження активів	0,00141	0,00516	0,00697	0,00020
Розумна сітка	0,00146	0,00147	0,00157	0,00006
Особисте відстеження	0,00144	0,00145	0,00158	0,00007
Телемедицина	0,00144	0,00146	0,00194	0,00015
GPS-навігатори	0,00484	0,00486	0,00152	0,00002
Дистанційна тривога	0,00150	0,00148	0,00174	0,00011

3.3 Висновок до розділу

У цьому розділі представлені основні результати дослідження масштабованості loT через мережі LTE. Основною метою є широке розуміння потенційного впливу сплеску пристроїв M2M як на мережу, так і на QoS користувачів смартфонів. Обговорюються як тестовий стенд моделювання, так і методологія, що застосовується для отримання та побудови результатів.

На підставі отриманих результатів визначено, що навантаження сигналів і трафіку даних збільшується лінійно, оскільки кількість підключених пристроїв

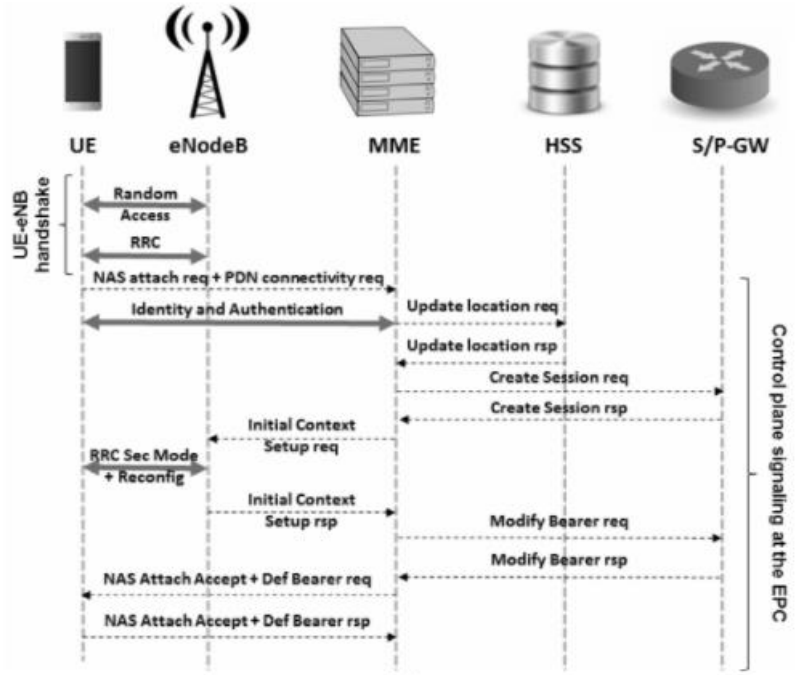
збільшується. Це хороша новина, оскільки це означає, що не слід очікувати сигнальної бурі. Тим не менше, деякі категорії пристроїв M2M, такі як відстеження активів, демонструють набагато швидшу сигналізацію та збільшення навантаження на трафік даних. Це вказує на те, що певні системи зв'язку M2M представлять більший виклик для мобільних мереж LTE.

РОЗДІЛ IV. КОМУНІКАЦІЇ БЕЗ ПІДКЛЮЧЕННЯ НАД LTE МОБІЛЬНИМИ МЕРЕЖАМИ

Цей документ представляє новий протокол зв'язку без з’єднання для пристроїв loT через мобільні мережі LTE, який не вимагає сигналізації площини управління на EPC. Ця техніка спеціально розроблена для вбудованих пристроїв M2M з низькою пропускною здатністю та допустимим затримкою трафіку, які часто є найгіршим сценарієм з точки зору сигнального навантаження на EPC. Наприклад, камера безпеки, що повідомляє про зображення кожні 5 хвилин, викликає два переходи стану RRC (в режимі очікування до підключеного та підключеного до простою) кожні п’ять хвилин. Для того, щоб досягти нульової цілі сигналізації, комунікація без з'єднання відображає дані користувача на початкових повідомленнях рукостискання між UE та eNB. Це повідомлення, якими обмінюються до повідомлення про запит на приєднання від UE, вбудованого в повідомлення RRCConnectionSetupComplete. спрацьовує сигналізація площини управління на EPC . Для ілюстрації цього рукостискання повідомлення на рисунку 4.1.1 (a) зображено процедуру приєднання LTE, як визначено стандартами 3GPP. Зверніть увагу, що для спрощення фігури певні рукостискання об’єднані в одну стрілку. Для випадку процедури RACH та зв'язку RRC між UE та eNB, рисунок 4.1.1 (b) представляє реальне захоплення окремих повідомлень, задіяних в обох рукостисканнях. Можна спостерігати повідомлення Artach Request, включене до пакету RRCConnectionSetupComplete UL.

Ще однією метою протоколу без з’єднання є повністю сумісна з стандартами конструкція, яка не вимагає стандартних модифікацій для роботи. У зв'язку з цим протокол вбудовується у стандарти 3GPP, хоча вимагає

користувальницьких стільникових модемів для пристроїв IoT та нових функціональних можливостей eNB.



(a)

Name	Start time	DI/UI	Cell ID	Frame
RACH	00:02:24.862663	U	16	607
MAC Random Access Response	00:02:24.866663	D	16	607
RRCConnectionRequest	00:02:24.872663	U	16	608
RRCConnectionSetup	00:02:24.887663	D	16	609
RRCConnectionSetupComplete	00:02:24.921663	U	16	613
Security Protected NAS Message	00:02:24.921663	U	16	613
Attach Request	00:02:24.921663	U	16	613
PDN Connectivity Request	00:02:24.921663	U	16	613

(b)

Рис. 4.1 Процедура приєднання NAS: a) сигналізація площині управління та b) реальне захоплення початкового рукостискання UE-eNB (RACH + RRC)

4.1. Трафік висхідної лінії зв'язку

IoT-пристрій, що здійснює зв'язок по беззв’язковому каналу, відображає свій UL-трафік на преамбулах RACH. Вибір даного підпису з пулу з 64 підписів призводить до кодування 6 бітів інформації. Припускаючи кількість k ресурсів RACH, відображених на кожному 10-секундному кадрі LTE, загальна пропускна спроможність, яку можна захистити всіми пристроями loT, складе 1

біт на секунду. Цю здатність також слід було б розподілити з фактичними преамбулами RACH, що передаються смартфонами та іншими мобільними пристроями в контексті процедури довільного доступу. Розділ 4.4 обговорює, як це не буде проблемою, оскільки навантаження RACH дуже низьке навіть у міському густонаселеному районі.

RACH може бути відображений у 16 різних конфігураціях, з k в діапазоні від 1 до 10, тобто 10 у випадку, коли в кожному підкадрі виділяється ресурс RACH. У частотній області дослідження демонструють, що оптимальна ефективність виявлення преамбули в eNB має сигнали преамбули та 12 RB BW, що відповідає 1,08 МГц та 2,16 МГц відповідно. Тому теоретично можна відобразити до 8 ресурсів RACH за частотою в межах 10MH2 кадру. Однак не рекомендується конфігурація з кількома одночасними частотними ресурсами RACH, щоб уникнути обробки стрибків на eNB, які повинні будуть виявляти та декодувати кілька сигналів преамбули одночасно. Виходячи з цього, діапазон можливих значень для k дорівнює k = 1, .., 10 · 8. Зверніть увагу, що випадок k = 80 передбачає, що весь кадр присвячений передачі преамбул, без місця для фактичної передачі даних. Цей випадок мав би сенс лише у сценарії eNB, призначеного виключно для трафіку без зв'язку, можливо, охоплюючи склад у приміщенні або іншу територію без трафіку на смартфонах. Також зауважте, що k = 80 також призведе до обробки шипів.

Припускаючи ймовірність зіткнення $p_1 collision^{\uparrow} UE = 1^{"} \backslash \%$ (що включає зіткнення RACH, помилки декодування тощо), k = 10 частотно-часових ресурсів RACH на кадр і 64 підписи, RACH може обробити навантаження до $R_{RACH}^{\max}$ = -10·64·ln(1-$p_{collision}^{UE}$ =6,432 преамбули на кадр. Це призводить до максимальної пропускної здатності UL без трафіку $R_{UL}^{\max}$ = $\frac{6 \cdot 432 \cdot 6}{0.01}$ = 3,86 кбіт / с. Зверніть увагу, що ця необроблена максимальна ємність буде розподілена між усіма пристроями loT без зв'язку, що знаходяться в комірці. Ресурси RACH також

спільно використовуються з трафіком преамбули від смартфонів та інших підключених пристроїв, які нормально спілкуються через LTE.

Ємність для трафіку без з’єднання UL потенційно може бути збільшена різними способами. Найбільш основним є збільшення кількості ресурсів RACH на кадр. Паралельно eNB потенційно може приймати кілька преамбул у слоті RACH. Тривалість сигналу преамбули істотно коротша за фактичний слот, в якому він передається, запобігаючи затримці розповсюдження в результаті зіткнення з наступним слотом. Тому розумний планувальник може дозволити двом або більше пристроям IoT передавати преамбулу в одному слоті якщо вони знаходились на досить різній відстані від eNB, наприклад у сценарії, зображеному на рисунку 4.1.1.

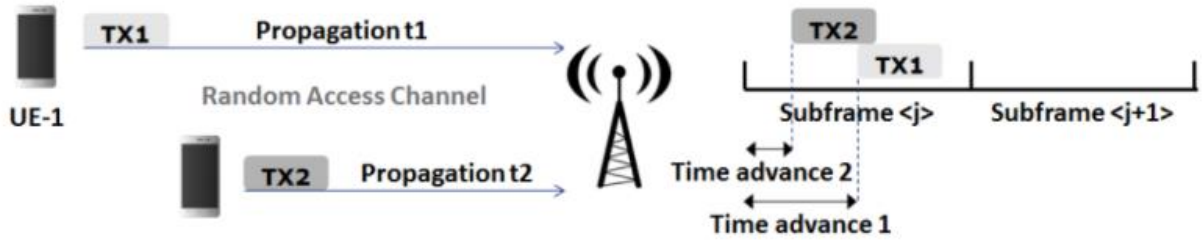


Рис. 4.1.1 Попередній час довільного доступу LTE вимірювання та передача двох преамбул в межах одного підкадру

4.2 Трафік по низхідній лінії зв'язку

DL-трафік передається у відповідь на заданий UL-зв'язок від пристрою, що не потребує зв'язку, або як мережевий DL-трафік. У будь-якому випадку дані кодуються в полі RNTI. Цей довільний ідентифікатор, не потрібний у режимі без підключення, дозволяє кодувати 16 біт DL-трафіку в кожному повідомленні RAR. Незалежно від того, чи є на RACH зіткнення або помилки декодування, цей канал спроектований таким чином, що повідомлення RAR

може передаватися в DL-прийому преамбули в даному слоті RACH. Отже, максимальна кількість RAR-повідомлень, які можна передавати на кадр, становить одне на кожен ресурс RACH, що відображається на кадрі LTE. Припускаючи конфігурацію, з присвоєними 10 ресурсами RACH на кадр, максимальна пропускна здатність, яка може бути доставлена пристроям без підключення в DL $R_{DL}^{max} = \frac{10 \cdot 16}{0.01} = 16kbps.$ Як і у випадку з пропускною здатністю UL, необмежена пропускна здатність цього каналу повинна бути спільною для всіх пристроїв IoT без з'єднання в комірці, а також повідомлення RAR, що передаються на звичайні мобільні пристрої. Результати дослідження цього базового навантаження RACH обговорювались у Розділі 3.4.

Потенційний спосіб підвищення пропускної здатності DL використовує той факт, що поле TA у повідомленні RAR не є необхідним для пристроїв, що не потребують з'єднання, оскільки вони не потребують UL-синхронізації для кодування та передачі даних. Отже, eNB може кодувати додаткові дані в цьому 11-бітному полі, досягаючи максимальної пропускної здатності DL $\frac{10 \cdot (16 + 11)}{0.01} = 27kbps.$ В якості альтернативи, частина 11-бітового поля TA може бути використана як поле ідентифікатора призначення, так що передбачуваний IoT-пристрій може ідентифікувати відповідний DL-трафік.

Враховуючи конструктивні та передавальні характеристики RACH, можна правильно декодувати кілька преамбул в межах одного слота, або через різні сигнатури, або через досить несхожі затримки розповсюдження. У разі трафіку DL без з'єднання, що передається у відповідь на UL-трафік, всі зіткнені UE отримають одне і те ж повідомлення RAR. За допомогою перевірки підпису, закодованого одним із полів у RAR, передбачуваний одержувач буде ідентифікований, а інші UE відкинуть повідомлення. Якби два або більше UE обрали один і той самий підпис, це призведе до зіткнення, яке слід виявити та

вирішити на вищих шарах, або із згаданим полем ідентифікатора призначення, закодованим частково, або сукупністю 11-бітного поля TA.

4.3. Запуск режиму без з’єднання

Для того, щоб мати можливість передавати дані по беззв’язковому каналу, як UE, так і eNB повинні виконати рукостискання таким чином, щоб обидві сторони знали, що дані UL та DL будуть кодовані відповідно в підписах преамбули та полі RNTI. Це рукостискання має бути спроектовано таким чином, щоб воно могло спрацьовувати через UE (мобільний трафік) та eNB (трафік, який припиняється мобільним телефоном).

У разі сплеску мобільного припиненого трафіку eNB запускає активацію режиму без з’єднання за допомогою пейджингового повідомлення. Цей тип повідомлення включає в себе хвіст із 3 бітів доповнення, які завжди встановлюються на нуль. Захоплення реального пейджингового повідомлення з мережі LTE показано на рисунку 4.3.1. Не порушуючи роботу та зв’язок звичайних мобільних пристроїв LTE, eNB кодує в цих 3 бітах інструкцію для активації режиму без з’єднання. У цьому випадку поле TMSI (Тимчасовий ідентифікатор абонента мобільного телефону) у повідомленні *пейджингового повідомлення* відповідатиме ідентифікатору конкретного пристрою, присвоєному кожному вбудованому пристрою без з’єднання.

Ємність PCH (пейджинговий канал) розподіляється як для пристроїв IoT без з’єднання, так і для регульованих мобільних пристроїв LTE, розташованих в одній камері. Експерименти в розділі 4.4 показують, що поточне навантаження в PCH є досить низьким, щоб дозволити відобразити тригер для мобільного завершеного потоку без зв'язку.

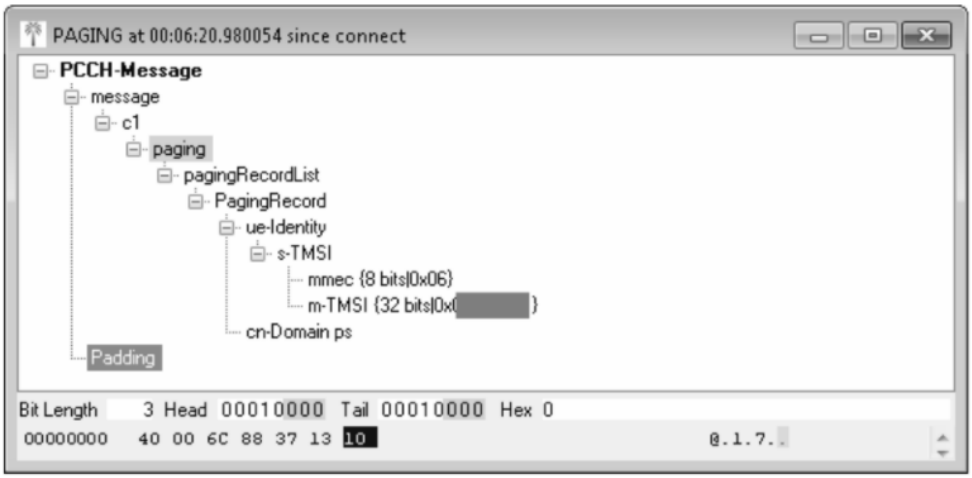


Рис. 4.3.1 Повідомлення пейджингового виклику LTE, захоплене з реальної мережі з 3 бітами доповнення

У разі ініційованого мобільним потоком даних UE ініціює режим без з'єднання. Простота повідомлення преамбули робить таку дію дуже складною. Тим не менше, дуже важливо мати можливість ініціювати комунікацію без підключення від UE, оскільки це переважний напрямок потоку трафіку в багатьох додатках M2M з допускною затримкою та низькою пропускною здатністю. Це випадок, наприклад. камери безпеки та сигналізація періодично.

Найпростіший спосіб ініціювати потік без з'єднання UL - зарезервувати для цього один із 64 підписів RACH. Це призведе до незначного погіршення максимальної пропускної здатності UL. У випадку, якщо звичайний термінал LTE передає преамбулу із зарезервованим підписом, eNB обробляє її як як звичайну преамбулу, так і без з'єднання, відповідаючи повідомленням RAR на

перший. У випадку звичайного пристрою LTE, повідомлення UL RRCConnectionRequest вказувало б eNB, що це справді звичайна преамбула. Відсутність такого повідомлення означало б протилежне.

Як альтернатива спрацьовуванню режиму без з'єднання може бути визначення послідовності M підписів $S = [s_1, s_2, \ldots, s_M]: s_i \in 64 RACH signatures$. Передача M преамбул у суміжних кадрах, з його підписами, що відповідають послідовності S, вказувала б eNB на початок потоку без з'єднання UL.

4.4 Фоновий мобільний трафік LTE на каналах RACH та пейджингових каналах

Як обговорювалося в попередніх підрозділах, повідомлення, що використовуються при передачі даних без зв'язку (преамбули RACH, RARS та пейджингові повідомлення), використовують ті самі ресурси, що і дуже важливі канали управління на рівні LTE PHY. Для того, щоб оцінити можливість безсистемного зв'язку, слід дослідити навантаження на ці канали в поточних мобільних мережах LTE.

30-хвилинне захоплення реального трафіку LTE по повітрю було зроблено в п'ятницю, 24 жовтня 2014 року, в обідню перерву. Захоплення було здійснено на жвавому перехресті в центрі Манхеттена, одного з найбільш густонаселених районів США. Зафіксовано рух транспорту для двох камер. Важливо чітко підкреслити, що весь трафік через ефірний інтерфейс LTE зашифрований, тому жодне передавання даних користувача не може бути вилучене із захоплення трафіку. Більше того, для захоплення застосовувались специфічні фільтри, щоб реєструвались лише повідомлення площини сигналізації.

Преамбули RACH, повідомлення RAR та трафік підкачки аналізувались індивідуально. У випадку преамбул RACH та відповідних відповідей RAR, як

слоти, так і підписи перевірялись для виявлення будь-яких потенційних зіткнень. Результати можна узагальнити наступним чином:

• Навантаження RACH: трафік довільного доступу на клітинку дуже низький, з відсутністю трафіку RACH у більшості кадрів і, щонайбільше, спроби преамбули на кадр. Застосовуючи основні статистичні інструменти, навантаження RACH було апроксимовано та змодельовано як випадкову величину Бернуллі з параметром p = 0,0580826 (ймовірність мати одну преамбулу в одному кадру 10 мс).

• Random Access Responses(Відповіді довільного доступу): Враховуючи низьке навантаження RACH, спостерігалася лише одна відповідь RAR на преамбулу, що призвело до такої ж кількості та частоти повідомлень RAR DL, як спроби преамбули RACH в UL.

• Пейджинг: спостерігається в середньому 2,55 пейджингових повідомлень за секунду, що призводить до 0,0255 пейджингових повідомлень на кадр.

4.5. Покращення та обмеження системи

Вкрай важливо, щоб eNB завжди надавав абсолютний пріоритет регулярному LTE-трафіку на RACH і пейджингових каналах. Отже, початок потоку без з’єднання DL, ініційований повідомленням пейджингового повідомлення, буде відкладений, поки в черзі не буде передано регулярних повідомлень пейджингового повідомлення. Враховуючи навантаження на пейджингове спостереження, що спостерігається в Розділі 4.4, затримка, яку це введено, буде незначною, не впливаючи на стійкий до затримок трафік підключення.

Повідомлення DL RAR, які транспортують трафік без з’єднання DL, також можуть використовуватися для підтвердження (ACK) повідомлень UL. Наприклад, з 16 біт даних, які можуть бути закодовані повідомленнями DL RAR, які транспортують трафік без з’єднання DL, також можуть використовуватися для підтвердження (ACK) повідомлень UL. в полі RNTI кількість бітів може бути використана для передачі хешу з 6 бітів, переданих в UL. В якості альтернативи, біти ACK можуть кодуватися в 11-бітовій команді TA RAR, що не потрібно в режимі без з’єднання. У будь-якому випадку eNB не повинен передавати ACK без підключення у відповідному ресурсі DL в слот RACH, в якому була отримана звичайна преамбула LTE RACH. Система надає пріоритет повідомленням RAR з довільним доступом, що надсилаються на стандартні мобільні пристрої LTE.

У разі кількох преамбул, переданих в одному і тому ж слоті RACH з різних пристроїв IoT без підключення, зіткнення не може бути вирішено, якщо дві або більше преамбул мають однаковий підпис. Зважування команди TA як повідомлення ACK забезпечує спосіб такого дозволу зіткнення.

Три невикористані біти заповнення пейджингового повідомлення дозволяють використовувати до 8 різних режимів без підключення. Режим без підключення визначає кількість слотів RACH на кадр, який буде намагатися використати потік. Посилання без з’єднання може бути налаштоване для відображення даних, наприклад, лише на одному слоті RACH на кадрі або лише в непарних номерах. Це призведе до нижчого навантаження на RACH та меншої кількості зіткнень за рахунок меншої пропускної здатності. Це також дозволить синхронізувати трафік без з’єднання з декількох пристроїв.

Подальше обмеження ліній зв'язку без зв'язку - це те, що як альтернативний протокол передачі рівня 1, він обходить усі протоколи LTE

вищого рівня, таким чином не забезпечуючи засобів для безперебійної мобільності. Тому ця технологія призначена лише для немобільних додатків.

4.6. Наскрізна архітектура

Комунікації IoT без з’єднання призначені лише для забезпечення рівня I зв'язку між пристроями M2M та базовими станціями LTE з архітектурою PHY, яка не впливає на стандартизовану LTE PHY. Таким чином, цей новий тип підключення забезпечує вузьку лінію доступу ALOHA з прорізом на кожному eNB. Для взаємодії цієї технології з мережею пакетних даних 3 рівня (PDN) пропонуються дві альтернативи.

З одного боку, eNB може бути надійно безпосередньо з'єднаний з PDN, таким чином, що трафік, що не потребує з'єднання, перенаправляється безпосередньо в Інтернет. Цей варіант, хоча і здійсненний, не рекомендується через проблеми масштабування. Для забезпечення безпечного з'єднання кожен eNB повинен бути обладнаний захищеним шлюзом, який реалізував кілька функцій безпеки, таких як функціональність брандмауера, на відміну від поточної мережевої реалізації функцій безпеки.

З іншого боку, поточний EPC може альтернативно встановити та підтримувати постійний носій між eNB та P-GW. Весь трафік без з’єднання, що надходить або закінчується на підключених пристроях M2M, розташованих на даній комірці, буде потім направлений через цей постійний носій до PGW, де брандмауер, NAT (переклад мережевих адрес) та інші.

4.7 Висновок до розділу

Цей розділ представляє комунікації без з’єднання в мережах LTE та їх структуру з урахуванням реального захоплення трафіку LTE. В цьому розділі

описано трафіки по висхідній та низхідній лініях зв’язку, а також запуск режиму без зв’язку.

Новий метод PHY Layer для передачі даних в основному розроблений і призначений для дуже низької пропускної здатності та терпимих до затримок додатків loT. Теоретично посилання без з’єднання можуть також використовуватися для додатків loT з високою пропускною здатністю і навіть для забезпечення посилань для смартфонів, подібних до таких для Універсальної системи мобільного зв'язку (UMTS) Cell-FACH RRC. Цей параметр не рекомендується, однак через велике навантаження трафік без з’єднання буде спричиняти основні канали управління LTE PHY, що може призвести до погіршення обслуговування звичайних мобільних пристроїв. У зв’язку з цим існують певні ключові міркування щодо безпеки та впровадження, які слід врахувати.

На підставі результатів у підрозілі 4.4 можна помітити, що навантаження на трафік як на RACH, так і на PCH дуже низьке, навіть у дуже густонаселеному районі під час доби, в обідню перерву, коли користувачі зазвичай перевіряють соціальні мережі, читають новини та загалом генерують сплеск трафіку мобільної мережі. Це підтримує можливість розгортання посилань без підключення, накладених на поточні розгортання LTE, не помітно впливаючи на фоновий RACH і трафік підкачки з мережі LTE.

РОЗДІЛ V. ЕКСПЕРИМЕНТАЛЬНІ РЕЗУЛЬТАТИ

Для того, щоб оцінити доцільність запропонованого протоколу, в Python та на інструменті моделювання мережі OPNET Modeler побудовано дві системні моделі лінії без зв'язку . Сценарій моделювання складається з одного eNB LTE 10 МГц. Змінне число k ресурсів RACH відображається на кожному кадрі, при цьому k знаходиться в діапазоні від I до 20. Також імітується особливий випадок виділеної комірки без з'єднання з N = 80. Під час моделювання кількість N пристроїв M2M розташовується в комірці з постійним потоком UL-трафіку, що доходить до їх модему. Кожен пристрій M2M намагається передати одну преамбулу в кожному кадрі. У DL також передбачається постійний потік трафіку на UE, що відображає дані про повідомлення RAR, що надсилаються до пакетів ACK UL. Таким чином, передається максимум один пакет DL на UE на кадр.

Для того, щоб забезпечити реалістичні результати, до моделювання додається фонове RACH, RAR та навантаження на пейджингове повідомлення. Це фонове навантаження моделюється з тих самих 30 хвилин за повітряним захопленням реального трафіку LTE, описаного в Розділі 4.4. Зверніть увагу, що це навантаження мережі, яке спостерігається під час обідньої перерви в робочий день на жвавому перехресті в центрі Манхеттена. Моделювання призначене для випадку навантаження RACH та PCH у 10 разів вище, ніж у центрі Манхеттена. Виконується 20 повторень кожного моделювання, а їх результати усереднюються.

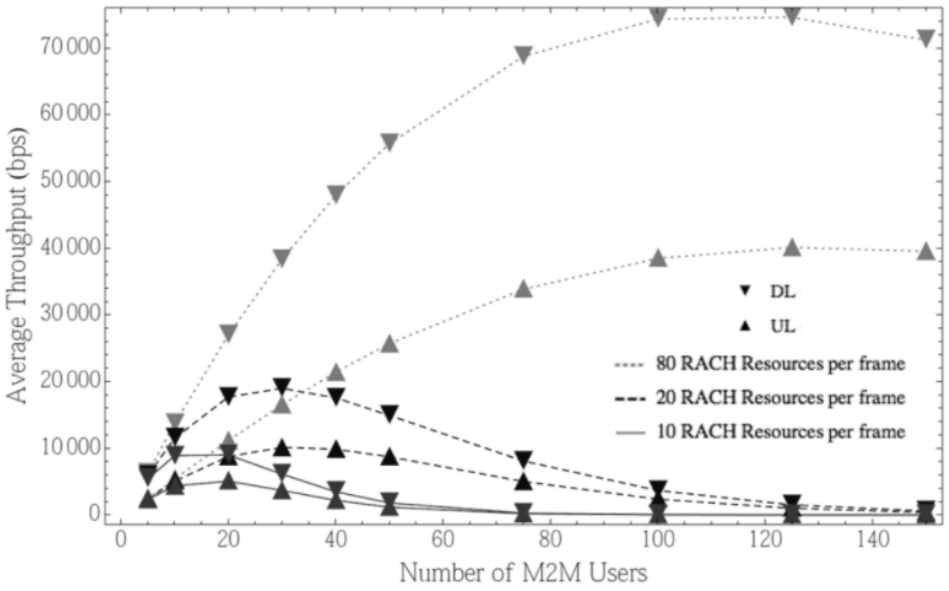


Рис. 5.1. Пропускна здатність без з’єднання UL та DL з різним розподілом ресурсів RACH у фреймі LTE

На рисунку 5.1 зображено вихідну пропускну здатність, як у UL, так і в DL, для трьох різних конфігурацій ресурсів RACH, зіставлених у фреймі LTE (k). Випадок, коли k = 80 ресурсів RACH у межах 10 МГц, є випадком повністю виділеної соти без зв’язку. Як і слід було очікувати, суперечливий характер лінії зв'язку без зв'язку призводить до значного погіршення пропускної здатності в міру збільшення навантаження. Зауважте, що це погіршення також серйозно вплине на роботу звичайної мережі LTE.

Наступним кроком цього аналізу є визначення бездоступного зниження пропускної здатності через фонове навантаження LTE на RACH. Це досліджено на рисунку 5.2, на якому зображено пропускну здатність із конфігурацією 10 ресурсів RÄCH на кадр. Результати збираються у випадку відсутності фонового навантаження із зазначеним вище навантаженням у центрі Манхеттена та, нарешті, з гіпотетичним навантаженням у 10 разів більшим.

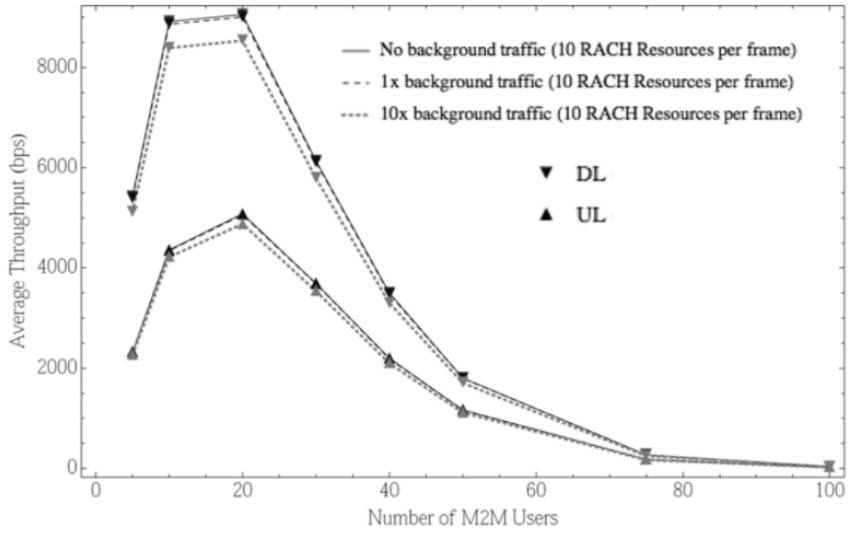


Рис. 5.2. Пропускна здатність без з’єднання UL та DL з фоновим навантаженням LTE RACH

Результати вказують на те, що фонове навантаження RACH однієї з найбільш густонаселених областей США не вплине на ефективність зв'язку без зв’язку. Як результат, за умови контрольованого розгортання M2M та відсутності суперечливих UE, вплив лінії без зв’язку на звичайні комунікації LTE буде майже нульовим. У гіпотетичному випадку фонового навантаження RACH в 10 разів інтенсивніше, ніж у центрі Манхеттена, пропускна здатність даних без з’єднання потенційно може погіршитися на 5% у DL та 4% у UL. У цьому сценарії як стільниковий оператор, так і постачальник послуг M2M повинні ретельно планувати та розгортати UE без з’єднання, щоб запобігти погіршенню продуктивності LTE в цій стільниковій мережі. Хоча можна стверджувати, що 10-мегагерцовий стільник з 10-кратним збільшенням кількості користувачів ніж у центрі Манхеттена в жодному разі не було б гарячої точки високого рівня якості (QoS) без накладання пристроїв без з’єднання.

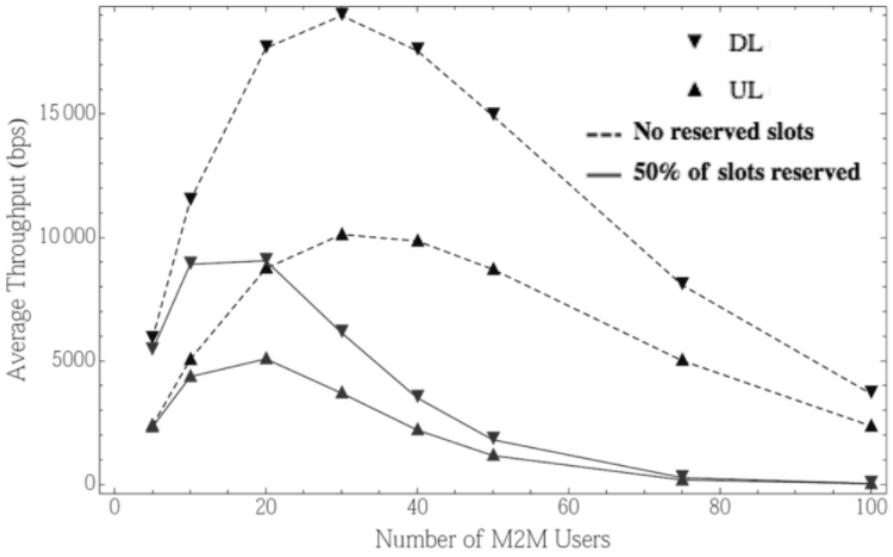


Рис. 5.3. Аналіз пропускної здатності без з’єднання UL і DL при резервуванні слотів RACH

Нарешті, ми прагнемо дослідити вплив трафіку без з’єднання на процедуру довільного доступу пристроїв LTE. З цією метою ми реалізуємо повне моделювання eNodeB та його каналу RACH. Ряд звичайних мобільних пристроїв LTE підключаються та обмінюються даними з цим eNB, генеруючи те саме навантаження RACH, що і з повітряного захоплення, проаналізованого в Розділі 3.4. Змінна кількість пристроїв без з’єднання накладається з однаковою схемою постійного трафіку, реалізованою в попередніх результатах. Визначено два типи зіткнень. Відновлюване зіткнення відбувається, коли преамбула LTE RACH надсилається в тому ж ресурсі RACH, що і будь-яке повідомлення UL без з’єднання. Незважаючи на зіткнення, різний підпис у преамбулі LTE RACH дозволяє eNB декодувати його та відповісти відповідним повідомленням RAR. Невідновлюване зіткнення визначається як відновлюване зіткнення з додаванням того, що преамбула LTE вибирає той самий підпис, що й будь-яке повідомлення UL без з’єднання, з яким вона стикається. У цьому випадку eNB не зможе декодувати преамбулу LTE, що призведе до невеликого негативного внеску на затримку доступу до мережі користувачів LTE.

На рисунку 5.4 зображено середній відсоток обох типів зіткнень. Результати вказують на те, що, хоча оптимальний розмір розгортання без з’єднання M2M (як визначено на рисунку 3.2.2) призведе до приблизно 50% відновлюваних зіткнень, кількість невідновлюваних зіткнень близька до нуля. Цей результат є інтуїтивно зрозумілим, оскільки невідновлювані колізії відбуватимуться лише в тому випадку, якщо преамбула без з’єднання відповідає ресурсу RACH та підпису з преамбулою LTE.

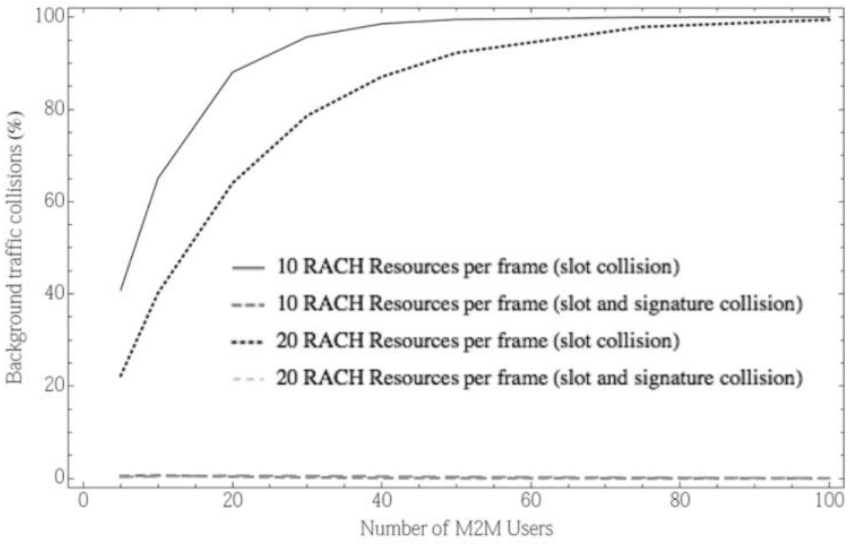


Рис. 5.4. Зіткнення у стандартному трафіку RACH через трафік без з’єднання M2M

5.1 Висновок до розділу

В цьому розділі представлено експериментальні результати моделювання без зв’язку. Проведено аналіз пропускної здатності без з’єднання UL та DL з різним розподілом ресурсів RACH у фреймі LTE. Наступним кроком було визначення бездоступного зниження пропускної здатності через фонове навантаження LTE на RACH. Результати даного аналізу були представлені на рисунку 5.2. Досліджено вплив трафіку без з’єднання на процедуру довільного доступу пристроїв LTE. В результаті, враховуючи те, що мережа завжди надавала б пріоритет трафіку LTE RACH, вплив ліній, що не мають з'єднання, на продуктивність LTE RACH було б майже нульовим.

РОЗДІЛ VI. ВИМОГИ БЕЗПЕКИ І ВПРОВАДЖЕННЯ

Незважаючи на потенційну функціональність та результати зв’язку без з’єднання для IoT з низькою пропускною здатністю, що допускає трафік через лінії LTE, слід розглянути кілька важливих аспектів. Як основний протокол передачі даних рівня 1, ця технологічна документація не забезпечує ніяких засобів для аутентифікації та шифрування. Ця функціональність, яка зазвичай реалізується в LTE Mobility Management Entity (MME) та Home Subscriber (HSS), обходить в системі без з’єднання. Тому і аутентифікацією, і шифруванням слід керувати на верхніх шарах.

Постачальник послуг, що розгортає нову систему IoT без підключення, повинен впровадити шифрування трафіку, щоб зловмисник не підслуховував трафік даних. Взаємна аутентифікація також повинна бути чітко реалізована для запобігання атакам "Людина посередині" (MitM). У партнерстві з оператором стільникової мережі провайдери послуг можуть впровадити аутентифікацію та шифрування в eNB. Однак для цього потрібні будуть суттєві зміни в eNB, а також послуга M2M та забезпечення абонентів на базових станціях, що може бути складним. У будь-якому випадку, важливо зазначити, що такі явні накладні витрати на шифрування та автентифікацію зменшать максимальну досяжну пропускну здатність для каналу даних без з’єднання.

Основною проблемою запропонованого протоколу є мінімізація його впливу на регулярну роботу терміналів LTE. UE-модем без підключення буде вводити навантаження на канал LTE RACH, щоб встановити лінію передачі даних. Незважаючи на те, що ретельне планування та контрольована кількість loT-пристроїв на осередок будуть тримати навантаження RACH під контролем, як виробник оригінального обладнання M2M (OEM), так і оператор стільникового зв'язку повинні дотримуватися суворої політики, щоб запобігти

перевантаженню радіодоступу. Доведено, що насиченість каналу RACH призводить до повної відмови в обслуговуванні перевантаженої комірки.

На рівні протоколу можна застосувати ряд ресурсів для запобігання насиченню RACH. Наприклад, для звичайного трафіку LTE можна зарезервувати ряд підписів. Імпортуючи методи керування навантаженням RACH з UMTS, можна визначити ймовірність стійкості p, наприклад, що пристрій loT без зв'язку з даними для передачі надсилатиме преамбулу в заданому кадрі з ймовірністю p. Імовірність 1-p, передача буде відкладена до наступного кадру.

Необхідний подальший рівень захисту, оскільки відомі випадки атак, які, взаємодіючи з драйверами модему або прошивкою, реалізують порушення поведінки протоколу в CSMA-подібних мережах доступу. Пристрої M2M без з'єднання повинні мати апаратне збезпечаення (HW) таким чином, щоб перешкоди трафіку LTE RACH були мінімізовані. Наприклад, передня частина радіочастотних частот (RF) таких пристроїв може бути спроектована таким чином, щоб ефективна потужність пристрою складала лише від 1,5 МГц до 3 МГц, тим самим не даючи вузлам M2M вводити навантаження в ресурси RACH, що відображаються в найвіддаленіших RB кадру. Як і у випадку зі схемами протоколів без з'єднання для регулювання навантаження RACH, зменшення ВЧ-частоти відбуватиметься за рахунок зменшення максимальної досяжної пропускної здатності.

6.1 Висновок до розділу

Незважаючи на вищезазначені міркування безпеки, посилання без зв'язку все одно слід ретельно планувати та розгортати.

РОЗДІЛ VII. ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

У цій роботі запропоновано та проаналізовано нову техніку для забезпечення ALOHA-подібного каналу зв'язку, вбудованого в кожному LTE eNB, що повинен забезпечити засоби для зв'язку без обмежень для пристроїв loT. Цей новий тип бездротового каналу розроблений для додатків loT з низькою пропускною здатністю, які часто є найменш ефективними з точки зору відношення навантаження трафіку сигналізації до фактичного трафіку даних. Ця нова технологія використовує певні канали LTE рівня PHY, щоб вбудувати як UL, так і DL-трафік даних в початкове рукостискання мобільних пристроїв з eNB, що не призводить до сигналізації площини управління на EPC.

На підставі результатів, і припускаючи контрольоване розгортання без шкідливих або неправильних пристроїв IoT, 20-30 пристроїв IoT можуть бути розгорнуті в комірці без впливу на регулярний трафік LTE та максимальної пропускної здатності UL приблизно від 4 кбіт до 8 кбіт / с. Хоча невелика, ця кількість підключених пристроїв була б достатньою для типових додатків M2M, таких як камери безпеки та віддалена сигналізація в офісі / на складі чи в комерційному центрі під охопленням декількох осередків. Спеціальний eNB без з’єднання може вмістити близько 120 вбудованих пристроїв.

З метою дослідження впливу трафіку без з’єднання на процедуру довільного доступу пристроїв LTE було реалізовано повне моделювання eNodeB та його каналу RACH. Результати вказують на те, що, хоча оптимальний розмір розгортання без з’єднання M2M (як визначено на рисунку 3.2.2) призведе до приблизно 50% відновлюваних зіткнень, кількість невідновлюваних зіткнень близька до нуля. Враховуючи дуже низьке навантаження преамбул LTE RACH, ймовірність зіткнень, що не підлягають відновленню, дуже низька.

Отримані результати моделювання, включаючи фонове навантаження, яке спостерігається в реальній мережі LTE, свідчать про доцільність використання

запропонованої техніки. Такий підхід може потенційно забезпечити, за типової конфігурації RACH, як визначено стандартами 3GPP, максимально досяжну пропускну здатність близько 4 кбіт/с в UL і 9 кбіт/с в DL. Представлений тут аналіз показує, що вплив лінії без зв'язку на поточні мережі LTE буде незначним, тоді як потенційні вигоди значні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] A. Iera, C. Floerkemeier, J. Mitsugi, and G. Morabito, “Special Issue on the Internet of Things,” in IEEE Wireless Communications, vol. 17, December 2010, pp. 8–9.

[2] “More than 50 billion connected devices,” Ericsson, Ericsson White Paper, February 2011, http://goo.gl/Xi7dE1.

[3] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. Johnson, “M2M: From mobile to embedded internet,” Communications Magazine, IEEE, vol. 49, no. 4, pp. 36 –43, april 2011.

[4] D. Lewis, “Closing in on the Future With 4G LTE and M2M,” Verizon Wireless News Center, September 2012, http://goo.gl/ZVf7Pd.

[5] “Sierra Wireless invests in LTE-M future for lower power and better coverage in the Internet of Things,” M2M NOW, July 2014, http://goo.gl/NFs33w.

[6] “M2M Industry Faces Call to Action with 2G GSM Sunset,” Aeris, January 2014, http://goo.gl/mBMkq6.

[7] M. Shafiq, L. Ji, A. Liu, J. Pang, and J. Wang, “Large-scale measurement and characterization of cellular machine-to-machine traffic,” Networking, IEEE/ACM Transactions on, vol. 21, no. 6, pp. 1960–1973, December 2013.

[8] T. Petsch, S. Khan Marwat, Y. Zakit, and C. Gorg, “Influence of Future M2M Communication on the LTE system,” in Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP. IEEE, 2013, pp. 1–4.

[9] A. Prasad, “3GPP SAE-LTE Security,” in NIKSUN WWSMC, July 2011.

[10] M. Jaber, N. Kouzayha, Z. Dawy, and A. Kayssi, “On cellular network planning and operation with m2m signalling and security considerations,” in Communications Workshops (ICC), 2014 IEEE International Conference on. IEEE, 2014, pp. 429–434.

[11] M. Dano, “The Android IM app that brought T-Mobile’s network to its knees,” Fierce Wireless, October 2010, http://goo.gl/O3qsG.

[12] C. Gabriel, “DoCoMo demands Google’s help with signalling storm,”Rethink Wireless, January 2012, http://goo.gl/dpLwyW.

[13] “Signal storm caused Telenor outages,” Norway News in English, June 2011, http://goo.gl/pQup8e.

[14] 3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects, “Study on Core Network Overload and Solutions. 3GPP TR 23.843,” vol. v0.7.0, 2012.

[15] S. Sesia, M. Baker, and I. Toufik, LTE, The UMTS Long Term Evolution: From Theory to Practice. Wiley, 2009.

[16] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network, “Physical layer aspects for Evolved Universal Terrestrial Radio Access (UTRA). 3GPP TR 25.814,” vol. v7.1.0, 2006.

[17] Sanjole, “WaveJudge 4900A LTE analyzer,” http://goo.gl/ZG6CCX.

[18] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network, “Evolved Universal Terrestrial Radio Access (EUTRA) - Radio Resource Control (RRC) - Protocol Specification. 3GPP TS 36.331,” vol. v8.20.0, 2012.

[19] ——, “Evolved Universal Terrestrial Radio Access (E-UTRA) – User Equipment (UE) procedures in idle mode. 3GPP TS 36.304,” vol. v9.11.0, 2012.

[20] P. Lee, T. Bu, and T. Woo, “On the Detection of Signaling DoS Attacks on 3G Wireless Networks,” in INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, May 2007.

[21] M. Donegan, “Operators Urge Action Against Chatty Apps,” Light Reading, September 2011, http://goo.gl/FeQs4R.

[22] S. Corner, “Angry Birds + Android + ads = network overload,” iWire, June 2011, http://goo.gl/nCI0dX.

[23] S. Decius, “OTT service blackouts trigger signaling overload in mobile networks,” Nokia Networks, September 2013, http://goo.gl/rAfs96.

[24] C. Ide, B. Dusza, M. Putzke, C. Muller, and C. Wietfeld, “Influence of M2M communication on the physical resource utilization of LTE,” in Wireless Telecommunications Symposium (WTS), 2012. IEEE, 2012, pp. 1–6.

[25] S. Duan, “Congestion control for M2M communications in LTE networks,” University of British Columbia, 2013.

[26] S.-Y. Lien and K.-C. Chen, “Massive Access Management for QoS Guarantees in 3GPP Machine-to-Machine Communications,” Communications Letters, IEEE, vol. 15, no. 3, pp. 311–313, March 2011.

[27] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network, “Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Physical channels and modulation. 3GPP TS 36.211,” vol. v10.3.0, 2011.

[28] H. Holma and A. Toskala, HSDPA/HSUPA for UMTS: high speed radio access for mobile communications. John Wiley & Sons, 2007.

[29] “OPNET Modeler,” http://goo.gl/GW7WGo.

[30] D. Spaar, “A practical DoS attack to the GSM network,” in In DeepSec, 2009, http://tinyurl.com/7vtdoj5.

[31] A. L. Toledo and X. Wang, “Robust detection of mac layer denialofservice attacks in csma/ca wireless networks,” Information Forensics and Security, IEEE Transactions on, vol. 3, no. 3, pp. 347–358, 2008.

[32] “OPNET Modeler,” http://goo.gl/GW7WGo.

[33]“OPNET System in the Loop,” http://goo.gl/NvBcP7.

[35] J. Jermyn, R. P. Jover, M. Istomin, and I. Murynets, “Firecycle: A scalable test bed for large-scale lte security research,” in Communications (ICC), 2014 IEEE International Conference on. IEEE, 2014, pp. 907– 913.

[36] 3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects, “Study on Core Network Overload and Solutions. 3GPP TR 23.843,” vol. V0.7.0, 2012.

[37] P. Lee, T. Bu, and T. Woo, “On the Detection of Signaling DoS Attacks on 3G Wireless Networks,” in INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, May 2007.

https://uk.wikipedia.org/wiki/LTE