Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра мережевих та інтернет технологій

ЗАТВЕРДЖУЮ
завідувач кафедри
мережевих та інтернет технологій

_____ Ю.В. Кравченко

«_____»_____2021 року

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

галузі знань 17 «Електроніка та телекомунікації»
за спеціальністю 172 «Телекомунікації та радіотехніка»

на тему:

РЕАЛІЗАЦІЯ КОНЦЕПЦІЇ ІОТ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ

Виконав: студент групи МІТ -41

Падаленчук Андрій Віталійович _____
(прізвище ім'я по-батькові) (підпис)

Керівник: доцент кафедри мережевих та інтернет технологій

к.т.н. Труш О.В. _____
(посада, прізвище ім'я по-батькові) (підпис)

Київ 2021

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра мережевих та інтернет технологій

ЗАТВЕРДЖУЮ
завідувач кафедри
мережевих та інтернет технологій

_____ Ю.В. Кравченко

«_____»_____2021 року

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Здобувачу вищої освіти Падаленчуку Андрію Віталійович
(прізвище, ім'я, по батькові)

1. Тема роботи:

«Реалізація концепції IoT для підвищення ефективності мереж мобільного зв'язку»

затверджена на засіданні кафедри МІТ «» грудня 2020 р. протокол № 6

2. Термін здачі закінченої роботи «» травня 2021р

3. Вихідні дані до проекту (роботи)

---

4. Зміст пояснювальної записки (перелік питань, що їх потрібно розробити, об'єм – 35-50 стор.)

1. Дослідження концепції інтернету речей та можливостей її використання
2. Аналіз літературних джерел. Аналіз безпроводових технологій для iot
3. дослідження особливостей мультисервісного трафіку
4. Дослідження методів підвищення ефективності використання мережевих ресурсів 4g з іот трафіком

5. Перелік графічного матеріалу 8-10 слайдів

Дата видачі завдання

Керівник роботи к.т.н., доцент кафедри МІТ Труш О.В.
(підпис) (посада, прізвище, ім'я, по батькові)

Завдання прийняв до виконання
(підпис) (прізвище, ім'я, по батькові)

КАЛЕНДАРНИЙ ПЛАН ВИКОНАННЯ РОБОТИ

Номер	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Підготовчий	29.01.2021	
2	Розділ 1	01.03.2021	
3	Розділ 2	01.04.2021	
4	Розділ 3	01.05.2021	
5	Доповідь та слайди	27.05.2021	
6	Пояснювальна записка	30.05.2021	

Здобувач вищої освіти _____
(підпис) (прізвище, ім'я, по батькові)

Керівник _____
(підпис) (прізвище, ім'я, по батькові)

РЕФЕРАТ

Пояснювальна записка: 80с., 40 рис., 3 табл., 20 джерел.

Об’єкт дослідження: процес надавання послуг IoT у стільникових мережах 4G.

Предмет дослідження: розподіл ресурсів мережі 4G / 5G для надавання послуг IoT.

Мета роботи (проекту): вивчення особливостей надавання послуг IoT на базі стільникової мережі НТУ стандарту 4G / 5G і розподіл мережевих ресурсів для забезпечення відповідної якості обслуговування M2M / IoT трафіку.

Методи дослідження: у роботі використані методи теорії інформації, математичні методи системного аналізу, теорії ймовірностей і математичної статистики.

У роботі розглядаються загальні принципи IoT і аналізуються можливості надавання послуг IoT мережами стільникового зв'язку. Досліджено особливості мультисервисного трафіку з урахуванням повідомлень, що генеруються пристроями IoT. Виділено проблеми обслуговування IoT-трафіку у бездротових мережах зв'язку і описані переваги мереж 4G / 5G. Представлена аналітична модель для вивчення імовірнісних і тимчасових характеристик обробки трафіку NB-IoT у присутності конкуруючого трафіку LTE. Представлені можливі стратегії спільного використання ресурсів мультимедіа і сенсорних даних NV у гібридної бездротової мережі LTE / NB-IoT. Проведено порівняння стратегій та надано рекомендації щодо вибору оптимальної стратегії. Проаналізовано процес розподілу частотно-часових ресурсів мережі LTE між UE і M2M / NB-IoT і запропоновано використання технології WI-FI direct для збільшення зони покриття базової станції. Представлені результати моделювання, що підтверджують ефективність даного рішення.

Ключові слова: IOT, M2M, 4G, 5G, LTE, MACHINE-TO-MACHINE, ІНТЕРНЕТ РЕЧІ, ВІРТУАЛЬНА МЕРЕЖА, NB-IOT, LPWN, РАДІОРЕСУРС, WI-FI DIRECT.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІТ – інформаційні технології.

ІС – інформаційна система.

ПК – персональний комп’ютер.

ОС – операційна система.

IoT – Інтернет речей

LTE – стандарт з вдосконалення UMTS для задоволення майбутніх потреб у швидкості.

Wi-Fi – загальновживане найменування для стандарту IEEE 802.11

ВСТУП

Актуальність теми. Концепція Інтернету речей (IoT) є однією з найбільш обговорюваних напрямків розвитку телекомунікаційних мереж та інформаційних систем. Зараз під IoT вже розуміються мільярди фізичних пристроїв по всьому світу, що під'єднані до Інтернету, аналізують і обробляють величезну число даних. Передбачається, що у майбутньому Інтернет речей стане активним учасником ділових, інформаційних і соціальних процесів, вони зможуть взаємодіяти один з одним, обмінюючись інформацією про навколишнє середовище, не вимагаючи втручання людини. Завдяки процесорам і бездротовим мережам все, від планшета до літака, може бути перетворено у частину IoT. Це додає рівень цифрового інтелекту до пристроїв, що в інакшому випадку являлися бнеактивними, дозволяючи їм спілкуватися без втручання людини і об'єднуючи цифровий і фізичний світи.

Швидке зростання як об'єму, так і числа типів даних, що будуть підтримуватися у майбутніх додатках IoT, є однією з ключових особливостей еволюції мереж стільникового зв'язку від 4G до 5G. З огляду на це постачальникам послуг IoT необхідно забезпечити масову передачу мультимедійних даних у поєднанні з повідомленнями машинного типу. Необхідність одночасної підтримки декількох категорій трафіку тягне за собою неоднорідність мереж 5G. Для такого випадку пропонується режим внутриполосного розгортання технології Narrowband IoT (NB-IoT), стандартизованої 3GPP.

Метою дипломної роботи є дослідження особливостей надавання сервісів IoT на базі стільникової мережі 4G / 5G і розподіл мережевих ресурсів для забезпечення належної якості сервісів M2M / IoT трафіку.

Прикладне значення отриманих результатів. Використання розглянутих методів оптимального розподілу мережевих ресурсів дозволяє провайдерам стільникового зв'язку підвищити ефективність планування, адміністрування та експлуатації мереж 4G / 5G, з огляду на зростаючий рівень трафіку M2M / IoT.

І. ДОСЛІДЖЕННЯ КОНЦЕПЦІЇ ІНТЕРНЕТУ РЕЧЕЙ ТА МОЖЛИВОСТЕЙ ЇЇ ВИКОРИСТАННЯ

І.1 Інтернет речей. Визначення основних понять

Зазвичай інтерес людини направлений у якусь одну конкретно сферу суспільного життя. Інформаційна система зберігає інформацію, яка відноситься до конкретної сфери. У ІС інформація про навколишній світ зберігається у вигляді даних.

У попередні роки у області ІКТ з'явився новий напрямок розвитку технологій, що одержало найменування "Інтернет речей" (IoT). Рекомендація МСЕ-Т Y.2060 "Огляд IoT" (06/2012) характеризує "Інтернет речей (IoT)" наступним чином: "Глобальна інфраструктура для інформаційного суспільства, яка дозволяє надавати більш складні сервіси шляхом з'єднання (фізичних і віртуальних) речей друг з одним на основі існуючих і розвиваються сумісних інформаційних і комунікаційних технологій. Використовуючи можливості збору, ідентифікації, передачі і обробки даних, Інтернет речей забезпечує найбільш ефективне використання речей для надавання сервісів для усіх типів додатків при дотриманні вимог безпеки та конфіденційності ".

У 1990 році випускник Массачусетського технологічного інституту Джон Ромки, один із засновників протоколу TCP / IP, створив перший у світі Інтернет. Він підключив до мережі свій тостер.

Термін "Інтернет речей" був введений у 1999 році Кевіном Ештоном. У такому ж році було створено центр Auto-ID Center, що займається розробкою технологій радіочастотної ідентифікації (RFID) і датчиків, завдяки чому ця концепція стала дуже популярною.

У 2008-2009 роках здійснився перехід з "Інтернету людей" до "Інтернету речей", оскільки число підключених предметів перевищило число людей. До 2015 року число підключених пристроїв досягла 25 млрд, а у 2020 році - 500000000.

Таким чином, відбувається еволюційна заміна "Інтернету людей" на "Інтернет речей" (IoT), як проілюстровано на рисунку 1.1.

Більш лаконічно можливо дати наступне визначення:

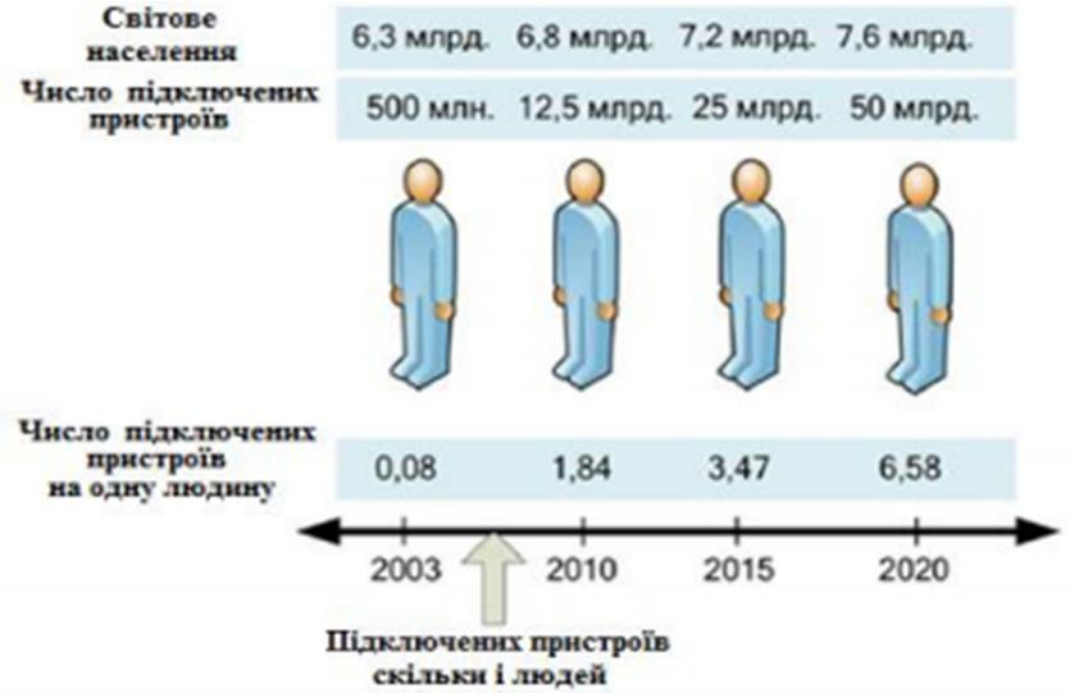


Рисунок 1.1 – часовий масштаб зміни числа людей та пристроїв, що під’єднані до інтернету

Ключові поняття IoT.

"IoT-пристрої": є частиною Інтернету речей і являють собою будь-автономний пристрій, підключений до Інтернету, яким можливо керувати дистанційно.

"Екосистема IoT": містить усі компоненти, що дозволяють підприємствам, урядам і користувачам підключати свої пристрої IoT, включаючи пульти, приладові панелі, мережі, шлюзи, аналітику, безпеку і зберігання даних.

"Фізичний рівень": Являє собою апаратне забезпечення, яке використовується у пристроях IoT, включаючи датчики та мережеве обладнання. Він відповідає за передачу даних, зібраних на фізичному рівні, різних пристроїв.

"Прикладної рівень": містить у себе протоколи і інтерфейси, за допомогою яких пристрої ідентифікуються і взаємодіють один з одним.

"Пульти управління": дозволяють особам використовувати пристрої IoT, підключаючись до них і керуючи ними за допомогою пульта - наприклад, через

мобільні додатки. Пульти включають ПК, смартфони, розумні годинники, телевізори, планшети і нетрадиційні пульти.

"Панелі інструментів": забезпечують відображення відомостей про екосистему IoT для користувачів, надаючи змогу їм управляти (зазвичай віддалено).

"Аналітичний фактор": є програмні системи, що аналізують дані з IoT-пристроїв. Аналітика використовується у значній числа сценаріїв - наприклад, для прогнозування технічного обслуговування.

Аби бути розпізнаним "річчю", всякий пристрій має відповідати певним критеріям:

1. воно повинно передавати дещо сенсорні дані, такі як тиск, температура або вологість.

2. вона повинна мати унікальний ідентифікатор, аби його можливо було ідентифікувати при обміні даними.

3. він зобов’язаний бути здатний обмінюватися інформацією з аналогічними пристроями і мати доступ до провідного Інтернету і Wi-Fi.

Концепція Інтернету речей містить чотири типи мереж, їх можливо класифікувати за масштабом використання:

1. BAN (body area network) - мережу на рівні людини.

2. LAN (local area network) - мережу домашнього рівня. Приватним прикладом такої мережі є концепція "Розумного будинку".

3. WAN (wide area network) - мережа рівня міського району. Це велосипеди, автомобілі, автобуси, підключення до Інтернету.

4. VWAN (very wide area network) - мережу на рівні держави або планети. Це всі державні служби.

Інакше кажучи, Інтернет речей можливо розглядати як мережу мереж, у якій маленькі, малозв’язані мережі утворюють великі, як проілюстровано на рисунку 1.2.

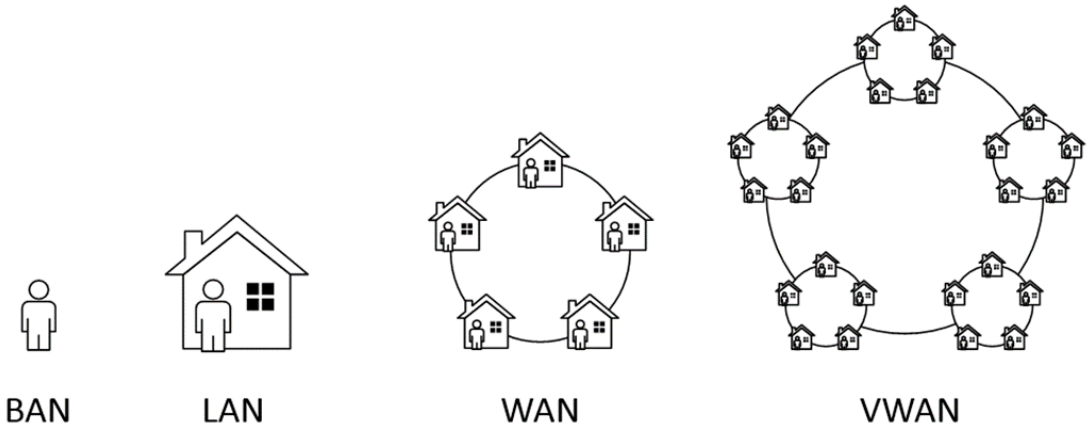


Рисунок 1.2 - Різновиди мереж

I.2 Архітектура Інтернету речей

Стандартизація - важливий момент у будь-якій сфері. Відсутність загальноприйнятих стандартів призвело до створення безлічі систем типу "розумний будинок" розроблених різними компаніями, що призводить до ряду проблем:

1. Формування надлишку стандартів.
2. Надмірне регулювання найпростіших об'єктів і процесів.
3. Велика число організацій і стандартів призводить до лобіювання інтересів окремих компаній у збиток загальним цілям стандартизації.
4. Тривалі терміни розробки стандартів призводять до їх старіння, так як вони не встигають за розвитком технологій, особливо на їх ранній стадії.

Існують різні типи інтерпретації архітектур IoT. Так, Рекомендація МСЕ-Т Y.2060 пропонує чотирьохканальну модель IoT, яка представлена на рис. 1.3.

Рисунок 1.3 - Архітектура Інтернету речей згідно з Рекомендацією MCE-T Y.2060

В моделі MCE-T IoT рівень пристроїв складається як з пристроїв кінцевого користувача, так і з промислових шлюзів. У якості шлюзу точки доступу підключаються до цифрових пристроїв за допомогою різних провідних і бездротових технологій (таких як локальна шина мережі управління (CAN), ZigBee, Bluetooth, Wi-Fi і т.д.).

Ще одна з найбільш загальних трактувань архітектури IoT розроблена IoT World Forum (IWF) і представлена на рис. 1.4.

Центральним моментом цієї архітектури є поділ на ще більш кількісно конкретізіруемая рівні, всередині яких можливо виділити конкретізіруемая технології і стандартні технології, між якими потрібно формалізація взаємозалежності.

Рівень 1 встановлює фізичні пристрої та контролери, що можуть керувати кількома пристроями. Рівень 1 IWF моделі приблизно відповідає рівню у моделі MCE-T. Подібно до моделі MCE-T, елементами цього рівня являють собою не фізичні речі, а пристрої, що взаємодіють з фізичними речами, наприклад, сенсорні і пиктографические пристрою. Серед інших функцій, ці пристрої можуть

виконувати цифро-аналогове і аналого-цифрове перетворення, генерувати дані, а також здійснювати дистанційний опитування і / або дистанційне керування.

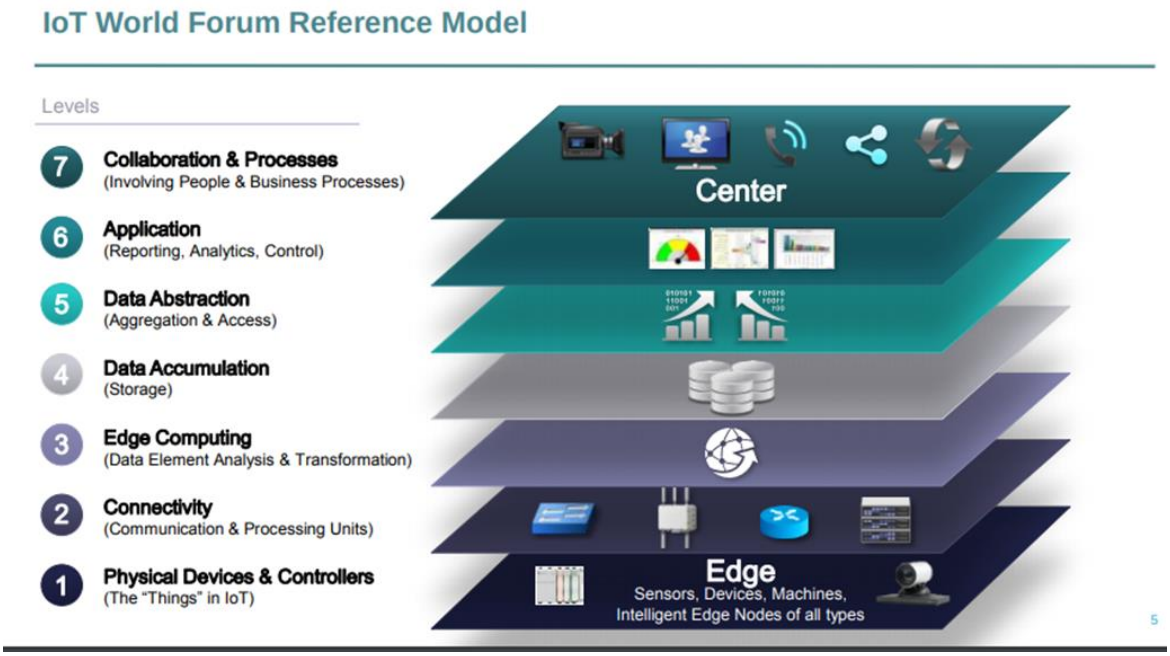


Рисунок 1.4 - Загальна архітектура IoT в межах IoT World Forum

Рівень 2 моделі IWF приблизно відповідає рівню мережі в моделі MCE-T. Основна відмінність полягає у тому, що IWF модель розглядає шлюзи як рівень 2, у той час як модель MCE-T розглядає їх як рівень 1. Оскільки шлюз є об'єднаним і взаємодіє приєднанням, у моделі IWF він розглядається як приєднання рівня 2.

Необхідність у рівні 3 виникає тому, що багато впроваджені системи IoT мають розподілену мережу датчиків, що можуть генерувати великі об’єми даних. Наприклад, нафтові родовища і нафтопереробні заводи, розташовані у Каспійському морі, можуть генерувати до терабайта даних кожен день. Тому рівень Edge computinng полягає у перетворенні потоків даних у інформацію, придатну для зберігання і більше високорівневою обробки. Елементи оздоблення на цьому рівні можуть працювати з великими об’ємами даних і виконувати операції по перетворенню даних, у результаті чого об’єм даних стає набагато менше.

На четвертому рівні, рівні зберігання даних, дані з різних пристроїв, профільовані і оброблені на рівні периферійних обчислень, зберігаються у сховищі, де вони будуть досяжні для вищих рівнів.

Рівень 5, рівень абстракції даних, може агрегувати і форматувати дані таким чином, аби зробити доступ додатків більш ефективним і контрольованим.

Рівень 6, рівень додатків, включає всякий тип додатків, що використовують дані IoT у якості вхідних або управляють пристроями IoT. Як правило, додатки взаємодіють з Рівнем 5 і персистентного даних, тому їм не потрібно функціонувати на мережевих швидкостях. Модель IWF не характеризує строгих вимог до додатків, вважаючи, що цей аспект виходить за рамки обговорення моделі IWT.

Рівень 7, рівень інтероперабельності, з'явився у результаті підтвердження, що Інтернет речей буде корисний тільки у тому випадку, якщо люди зможуть взаємодіяти з ним. Даний рівень може містити у себе декілька додатків та обмін даними або / та керуючої інформацією через Інтернет або корпоративну мережу.

І.3 Сфери застосування IoT

Глобальний IoT та прогноз у цифрах.

За даними глобального аналітичного агентства Gartner, в 2017 році використано IoT-пристроїв на загальний обсяг грошей приблизно $ 8,4 млрд, що на 31% більше, ніж у 2016 році, а вже у 2020 році ця цифра виросла до $ 20,4 млрд.

Загальні витрати на кінцеві пристрої і послуги IoT досягнули приблизно $ 2 трлн у 2017 році, причому дві третини цих пристроїв знаходяться у Західній Європі, Північній Америці та Китаї. Більше 8 мільярдів з усіх пристосувань - це споживчі товари, такі як розумні телевізори і розумні колонки.

Застосування IoT у сільському господарстві.

Аналоговий період у сільському господарстві закінчився, і галузь вступила у цифрову епоху. Інвестиційний банк Goldman Sachs прогнозує, що застосування технологій наступного покоління може підвищити продуктивність світового сільського господарства на 70% до 2050 року.

Використання IoT-датчиків і сенсорів у сільськогосподарських операціях - важливий крок на шляху до створення "розумної" ферми. Розкидані на десятках квадратних кілометрів, вони можуть безперервно передавати по радіоканалах

інформацію про стан контрольованих об'єктів - наприклад, значення таких параметрів, як вологість, температура, рівень здоров'я рослин, резерв палива і т.д. Наприклад, основою системи визначення характеристик грунту є датчики, що встановлюються у контрольних точках і підключаються до систем управління та моніторингу за допомогою технологій LPWAN. Ці датчики призначені для виявлення неоднорідностей (рельєф, тип ґрунту, освітленість, погода, число бур'янів і шкідників). Отримавши необхідні дані, агрономи вирішують, що культури можливо більш ефективно вирощувати на всякому шматку поля.

Вслід виявлення неоднорідностей необхідно грамотно підійти до догляду за рослинами. У цьому можуть допомогти датчики вологості грунту. Датчики, з огляду на тип культури, фазу її зростання та решту чинників, зможуть визначити момент, коли шар грунту досить вологий, і допомогти уникнути ерозії.

Використання IoT у житлово-комунальному господарстві.

Одна зі сфер, в якій у цей час активно впроваджується технологія LPWAN - ЖКГ. Перехід на використання мереж LPWAN дозволяє створювати автономні прилади обліку, здатні працювати роками і збирати інформацію з речей у досяжності 10-50 тисяч метрів від БС у прямої видимості або декількох кілометрів при розміщенні глибоко всередині приміщень або підвалів.

У ЖКГ технології IoT знайшли застосування у інтелектуальних системах диспетчеризації - "розумних" лічильниках ресурсів. Під’єднання до Інтернету, лічильники передають свідчення у хмару, і диспетчер бачить споживання води, електрики і газу. Це дозволяє, не заглядаючи у квартири власників, мати повну картину споживання ресурсів у режимі реального часу, дистанційно керувати лічильниками і оперативно виставляти рахунки мешканцям.

Застосування IoT у транспортній галузі.

Застосування IoT на транспорті містить у собі як системи часткової автоматизації транспорту та безпілотного транспорту, так і різні системи управління транспортними потоками, а також оптимізації роботи громадського транспорту у містах. Ці системи прийнято називати інтелектуальними транспортними системами ITS.

ITC - це системи, що підтримують транспортування вантажів і людей з використанням інформаційних і комунікаційних технологій для ефективного і безпечного використання транспортної інфраструктури і транспортних засобів (автомобілів, поїздів, літаків, суден).

Яскравим прикладом такого додатку є підключена або "розумна зупинка", оснащена як стільникового технологією, так і інтерфейсами пристроїв ближнього радіусу дії (Wi Fi, Bluetooth і т.д.). Ілюстрація "розумної зупинки" зображена на рис. 1.5.

Рисунок 1.5 - Приклад «розумної» автобусної зупинки

Використання IoT у "розумної медицині".

Зростання тривалості життя і хронічні захворювання призводять до того, що лікарняні палати переповнюються, а медперсонал насилу справляється з кількістю пацієнтів. Пристрої, що вимірюють біометричні показники пацієнтів і передають їх у хмару для зберігання і обробки, можуть полегшити роботу медсестер: Їм не доведеться здійснювати регулярні обходи - при необхідності додаток повідомить їх про те, хто зобов’язаний прийти.

Концепція "розумного міста" на основі додатків IoT.

Крім застосування технологій IoT у декотрих галузях, існує можливість отримання синергетичного ефекту від взаємопов'язаного впровадження IoT відразу

у декількох суміжних видах діяльності для отримання ще більшої економії і підвищення ефективності основної діяльності.

Один з найбільш яскравих прикладів можливої значної вигоди від кооперації систем у різноманітних областях спостерігається у міському управлінні. Концепція міського управління, що об'єднує використання технологій IoT у житловому будівництві, охороні здоров'я, транспорті та інших сферах міського життя, одержало найменування "Розумне місто".

У моделі "розумного міста" всі види діяльності та фізичні об'єкти за рахунок підключення до IoT володіють своїм цифровим представленням і підключенням до ІКТ-інфраструктури, на базі якої реалізуються різні сервіси, включаючи використання можливостей різноманітних поміжних галузей та типів діяльності.

I.4 Загрози технології IOT

Фундамент безпеки Інтернету речей складається з чотирьох частин: безпека пристроїв, безпека зв'язку, контроль пристроїв і контроль мережевої взаємодії [6].

На цьому фундаменті можливо створити міцну і просту у побудові організацію безпеки, здатну зменшити негативний вплив більшості загроз безпеки Інтернету речей, включаючи цілеспрямовані атаки. Лінія зв'язку зобов’язана бути безпечною, для цього використовуються технології шифрування, аутентифікації, аби пристрої мали інформацію, чи доцільно довіряти віддаленій системі. Управління ключами також є важливим завданням для перевірки достовірності даних та достовірності каналів для їх отримання [7,8].

Безпека пристроїв - це, перш за все, забезпечення безпеки і цілісності коду. Підписання коду необхідно для підтвердження легітимності його виконання, також необхідний захист під час виконання коду, аби зловмисники НЕ перезаписали його під час завантаження. У кожен пристрій, перш ніж воно потрапить до кінцевого користувача, зобов’язаний бути вбудований контроль "по повітрю" (OTA). Основними компонентами OTA є RFID, NFC і WSNs (бездротові сенсорні мережі) [9].

Найбільш значущими загрозами для системи RFID є десинхронізація, витік інформації і відтворення атак. Атаки десинхронизации дозволяють відстежувати мітки, визначати їх місце розташування, блокувати передачу даних від мітки до зчитувача. Особливо вразлива технологія NFC. Можуть бути проведені атаки типу "відмова у обслуговуванні" (DoS) або "підслуховування". Для підвищення безпеки рекомендується використовувати захищені канали зв'язку [10].

Технологія блокчейн повинна використовуватися для захисту від підробки програмного коду і підміни датчиків.

Блокчейн - це розподілена база даних, у якій пристрій зберігання не підключено до загального сервера. Дана база даних постійно зберігає зростаючий список упорядкованих записів, званих блоками. Кожен блок містить тимчасову мітку і посилання на попередній блок.

Технологія блокчейн забезпечує безпеку на рівні бази даних. Розподілена природа баз даних Blockchain робить вторгнення практично неможливим, оскільки для цього потрібен доступ до дублікатів бази даних на усіх комп'ютерах у мережі одночасно.

Витрати на розгортання і експлуатацію IoT можуть бути знижені при використанні блокчейна, оскільки відсутній посередник. Крім того, до пристроїв IoT можливо безпосередньо звертатися за допомогою блокчейна, надаючи історію підключених пристроїв для усунення неполадок.

II. АНАЛІЗ БЕЗПРОВІДНИХ ТЕХНОЛОГІЙ ДЛЯ IOT ТА ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ МУЛЬТИСЕРВІСНОГО ТРАФІКУ

II.1 Моделі комунікації інтернету речей

З практичного погляду важливо мати уявлення, як інтернет речі підключаються і обмінюються даними відповідно до їх технічних моделей зв'язку. У березні 2015 року Рада з архітектури Інтернету (IAB) випустив керівний документ по архітектурі мережевого підключення інтелектуальних об'єктів (RFC 7452), де визначено концептуальні рамки для чотирьох загальних моделей зв'язку, що використовуються пристроями IoT.

II.1.1 Під’єднання від пристрою до пристрою

Модель зв'язку між пристроями є два або більше пристроїв, що з'єднуються і взаємодіють між собою безпосередньо, а не через проміжний сервер додатків. Ці пристрої обмінюються інформацією через різноманітні види мереж. Проте зазвичай ці пристрої використовують такі протоколи, як ZigBee, Z-Wave або Bluetooth, для прямого контакту від пристрою до пристрою, як зображено на малюнку 2.1.

Рисунок 2.1 – Під'єднання від пристрою до пристрою

Ці мережі зв'язку між пристроями дозволяють пристроїв, що підтримують певний протокол, взаємодіяти і обмінюватися повідомленнями для виконання власних задач. Ця модель зв'язку часто використовується у таких додатках, як

системи домашньої автоматизації, що зазвичай використовують невеликі пакети даних для встановлення зв'язку між пристроями з низькими вимогами до швидкості передачі даних.

Ці пристрої часто знаходяться у прямому зв'язку, часто з вбудованими механізмами безпеки, однак вони також використовують специфічні моделі даних для всякого пристрою, що вимагає додаткових зусиль з розробки.

З погляду користувача, це часто означає, що протоколи даних, що використовуються від пристрою до пристрою, несумісні, і у результаті корпусу доводиться обирати інакші пристрої, що підтримують один і той же протокол. Наприклад, пристрої, що використовують протокол Z-Wave, несумісні з пристроями сімейства ZigBee.

II.1.2 Під’єднання від пристрою до хмари

У моделі зв'язку "пристрій - хмара" пристрій IoT підключається безпосередньо до хмарної службі на базі Інтернету, наприклад, до постачальника послуг оренди додатків, задля управління трафіком повідомлень та обміну даними. Даний підхід зображений на малюнку 2.2.

Рисунок 2.2 - Під’єднання від пристрою до хмари

Ця модель підключення використовується деякими популярними IoT-пристроями, такими як самонавчальний термостат Nest Labs і телевізор Smart TV.

У випадку з самонавчальним термостатом Nest пристрій передає інформацію у базу даних в хмарі, де ця інформація може бути використана для аналізу енергоспоживання будинку. Це хмарне з'єднання дозволяє користувачеві отримати віддалений доступ до свого термостата через смартфон або веб-інтерфейс, а також підтримує оновлення програмного забезпечення термостата. Аналогічним чином, у разі технології Smart TV від Samsung, телевізор використовує інтернет-з'єднання для передачі інформації про програми, що переглядає користувач, у Samsung для аналізу і підключення функції інтерактивного розпізнавання голосу на телевізійному пристрої. В таких умовах модель пристрою, відображена у хмарі, забезпечує додаткову цінність для кінцевого користувача, розширюючи стандартні можливості пристрою.

Однак при спробі інтегрувати вкладення різних виробників можуть виникнути проблеми сумісності. Найчастіше використовуються хмарні сервіси і пристрої одного і того ж виробника. Коли для зв'язку між пристроєм і хмарними сервісами використовуються пропрієтарні протоколи передачі даних, власник або користувач пристрою може використовувати тільки конкретний хмарний сервіс, обмежуючи свої можливості по використанню сервісів інших виробників. Така ситуація позначається терміном "залежність від постачальника", який включає відмінні сторони відносин з постачальником, такі як право власності на дані та доступ до них. У той же час, як правило, користувачі можуть бути впевнені у можливості інтеграції пристроїв, специфічних для конкретної платформи.

II.1.3 Під’єднання від пристрою до шлюзу

У разі моделі підключення пристрою і шлюзу найчастіше пристрій шлюзу прикладного рівня (ALG) підключається через службу ALG як канал для використання хмарної служби. Простіше кажучи, це означає, що прикладне програмне забезпечення функціонує на локальному шлюзовому пристрої, який виступає у якості посередника між пристроєм і хмарної службою і забезпечує безпеку і інші функції, такі як перетворення даних або протоколів.

Ця комунікаційна модель використовується, коли інтелектуальним об'єктів потрібна взаємодія з пристроями, що не підтримують протокол Інтернету IP. Іноді цей підхід використовується для інтеграції пристроїв, що підтримують тільки протокол IPv6, що означає, що для традиційних пристроїв і сервісів, що підтримують тільки протокол IPv4, потрібно шлюз.

Іншими словами, ця модель зв'язку часто використовується для інтеграції нових інтелектуальних пристроїв у традиційну систему з пристроями, що спочатку не можуть з ними взаємодіяти. Недоліком цього підходу є те, що необхідність розробки шлюзу системного і прикладного рівня збільшує складність і вартість системи у цілому.

Ця модель зображена на рисунку 2.3.

Рисунок 2.3 - Під’єднання від пристрою до шлюзу

Існують різні варіації цієї моделі у призначених для користувача пристроях. У багатьох випадках смартфон з додатком використовується у якості локального шлюзу для зв'язку з пристроєм і передачі даних у хмарну службу. Ця модель часто використовується у популярних споживчих пристроях, таких як браслети для вправ. Ці пристрої не мають прямого підключення до хмарного сервісу, тому вони часто використовують додаток для смартфона у якості шлюзу.

Іншим варіантом цієї моделі підключення пристрою до шлюзу є пристрої, що виконують роль концентратора у додатках домашньої автоматизації. Ці пристрої використовуються у якості локального шлюзу між окремими IoT-пристроями і хмарної службою, однак вони також можуть заповнювати прогалини у сумісності між самими пристроями. Наприклад, концентратор Smartthings є окремим шлюзовий пристрій з встановленими прийомопередавачами Z-Wave і Zigbee для підтримки зв'язку з пристроями обох типів. Це пристрій підключається до хмарного сервісу Smartthings, через який користувач може отримати доступ до пристроїв за допомогою програми для смартфона і підключення до Інтернету.

II.1.4 Модель спільного використання даних на сервері

Модель обміну даними на основі сервера відповідає архітектурі, яка дозволяє користувачам експортувати і аналізувати дані інтелектуальних об'єктів з хмарної служби у поєднанні з даними з інших джерел. Ця архітектура підтримує бажання користувачів надати стороннім особам доступ до завантажених даними датчиків. Даний підхід відповідає моделі підключення окремих пристроїв до хмари, що може привести до створення початкової бази даних, у яку IoT-пристрої завантажують дані тільки для одного постачальника послуг з оренди додатків. Архітектура обміну даними на основі сервера дозволяє об'єднувати і аналізувати потоки даних з одного IoT-пристрої.

Рисунок 2.4 - Модель спільного використання даних на сервері

Наприклад, корпоративний користувач, який відповідає за офіс, може бути зацікавлений у консолідації та аналізі даних про фактичне споживання енергії та інших комунальних послугах від усіх IoT-датчиків і підключених до Інтернету комунальних систем. У моделі підключення окремих пристроїв до хмарних сервісів дані від кожного датчика або IoT-системи знаходяться у окремій базі даних. Ефективна серверна архітектура обміну даними повинна дозволяти компанії легко отримувати доступ і аналізувати хмарні дані зі усіх пристроїв у будівлі. Крім того, такий тип архітектури забезпечує переносимість даних. Ефективна архітектура спільного використання даних на основі сервера дозволяє користувачам переміщати свої дані при перемиканні між сервісами IoT, долаючи бар'єри традиційних розподілених баз даних.

Модель спільного використання даних на основі сервера забезпечує федеративний підхід до хмарних сервісів; у інакшому випадку для забезпечення сумісності розміщених у хмарі даних від інтелектуальних пристроїв необхідні хмарні інтерфейси прикладного програмування (API). На малюнку 4 зображено графічне представлення цієї моделі.

Дана модель архітектури є підхід до забезпечення інтероперабельності між цими системами на основі сервера.

Архітектура обміну даними на основі сервера не може повністю компенсувати закритий дизайн системи.

II.1.5 Порівняльний аналіз моделей комуніканції Інтернету речей

Чотири основні моделі зв'язку демонструють стратегії розвитку, що використовуються для забезпечення зв'язку між пристроями IoT. Крім технічних аспектів, застосування цих моделей багато у чому обумовлено відмінностями між невільними і відкритими IoT-пристроями у мережі. І у разі моделі зв'язку між пристроями і шлюзом, її основною характеристикою є здатність подолати обмеження, пов'язані з з'єднанням пропрієтарних IoT-пристроїв. Це означає, що

сумісність пристроїв і відкриті стандарти є ключовими факторами для створення і розвитку взаємопов'язаних систем IoT.

Ці моделі підключення дозволяють краще зрозуміти можливості створення додаткової цінності для кінцевих користувачів за допомогою мережевих пристроїв. Загальна цінність пристроїв підвищується за рахунок надавання користувачам більш легкого доступу до пристроїв IoT і їх даними. Наприклад, у трьох з чотирьох моделей підключення пристрої підключаються до хмарним службам аналізу даних.

Створюючи зв'язку даних з хмарою, користувачі і сервіси можуть швидше і простіше агрегувати дані, виконувати аналіз і візуалізацію великих даних, а також застосовувати методи прогнозної аналітики, аби скористатися перевагами додаткового об’єму даних IoT, отриманих за допомогою традиційних вузькоспеціалізованих додатків баз даних. Іншими словами, ефективні моделі зв'язку є важливим фактором підвищення цінності послуг для кінцевих користувачів, дозволяючи застосовувати нові способи використання інформації. Однак, незважаючи на ці переваги, існують і недоліки.

При виборі архітектури необхідно ретельно продумати питання про додаткові витрати корпорантів при підключенні до хмарним ресурсів, особливо у регіонах з високою вартістю зв'язку.

II.2 Безпровідні технології для IoT

Для забезпечення зв'язку з пристроями IoT можуть використовуватися різні радіо послуги та програми. Однак переважна більшість бездротових мереж для мереж IoT можливо класифікувати у рамках шести основних сегментів, зображених на рисунку 2.9.

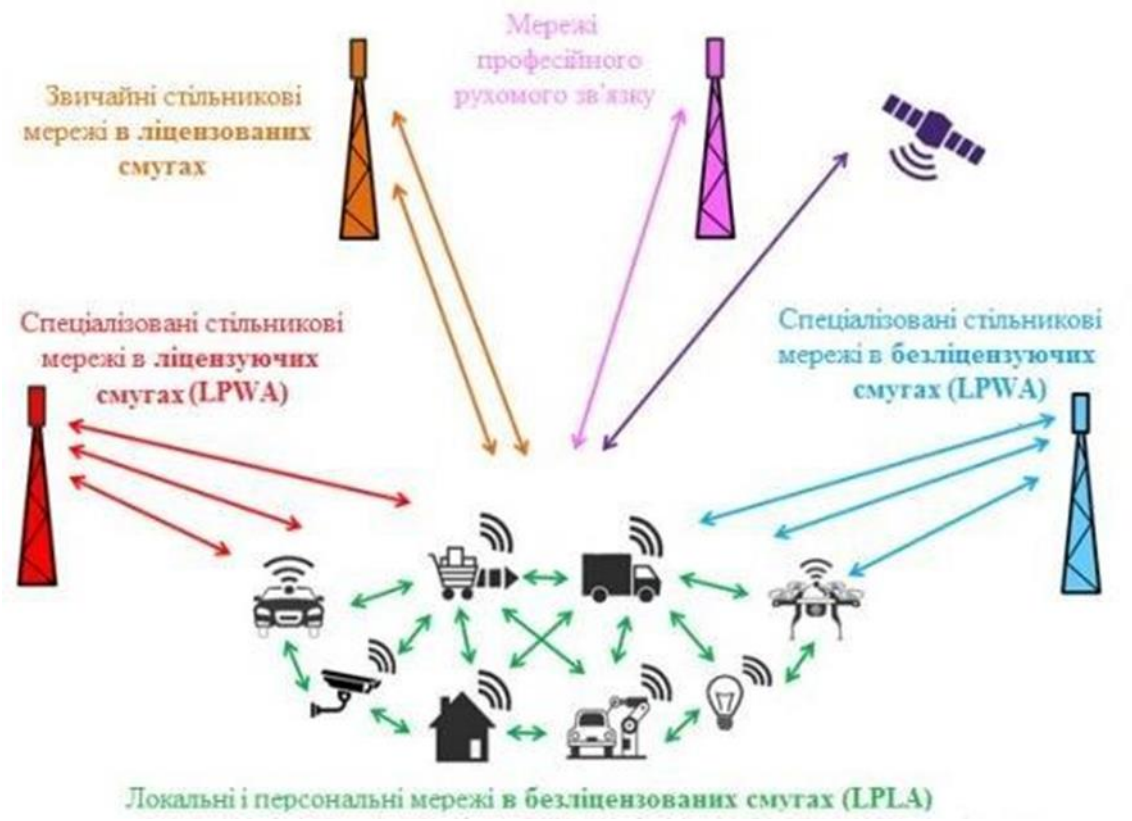


Рисунок 2.9 - Класифікація основних безпроводових технологій для IoT

Дана класифікація виділяє наступні сегменти бездротових технологій:

1. Традиційні стільникові мережі - домінуючі у даний час стільникові модулі на базі GSM / EDGE і інших стандартів стільникового зв'язку покоління 2G, а також додатки на базі звичайних модемів UMTS і LTE без будь-яких спеціальних модифікацій для IWT.

2. Локальні і персональні мережі, як правило, у неліцензованому діапазонах радіочастот або LPLA (Low Power Local-Area Networks). Як приклад можливо привести пристрої малого радіусу дії різних стандартів, таких як ZigBee і Bluetooth. Пристрої цієї категорії не мають прямого підключення до мереж передачі даних, однак можуть використовувати різні шлюзи для розширення зони дії. Наприклад, гібридні рішення mesh-net (чарункова мережа) зі стільниковим шлюзом також відносяться до цієї категорії LPLA.

3. LPWA (Low Power Wide Area Networks) - пристрої широкосмугового стільникового доступу і нові спеціалізовані інтерфейси для широкозонних мереж M2M. Крім спеціалізованих інтерфейсів стільникових мереж, у цю категорію також входять додатки, реалізовані у неліцензованих частотних діапазонах, тобто

пов'язані з пристроїв ближнього радіусу дії, однак розраховані на широку зону покриття. До них відносяться такі стандарти, як LoRa, Weightless і Sigfox.

4. Технологічні мережі на основі професійних стандартів стільникового зв'язку, таких як TETRA або DMR, являють собою нішевий, але, тим не менш, значимий сегмент мереж M2M або IoT. Зокрема, висока надійність мереж таких стандартів і низька затримка виявляються досить затребуваними при автоматизації небезпечних і / або технологічно складних виробництв, таких як хімічна або нафтова промисловість.

5. Супутникові додатки M2M і IoT розвиваються вже давно. Ці системи незамінні у логістиці, де необхідно відстежувати переміщення грузів на достатні відстані, включаючи райони, де відсутні наземні мережі зв'язку.

На даний момент не існує усталеної класифікації додатків IoT по відношенню до вимог до радіотехнологій. Однак розвиток IoT показує, що специфічні вимоги до бездротових технологій можливо розділити на три умовні і дуже широкі категорії:

1) мають більш високі вимоги до надійності або латентності радіоканалів;

2) наявність підвищених вимог до надійності або затримок для каналів радіозв'язку при дуже високій пропускної здатності;

3) наявність вимог до енергоефективності та дешевизні роботи при більш низьких вимогах до затримок і пропускної здатності.

II.3 Аналіз бездротових технологій для IoT у рамках систем IMT

Оскільки у роботі розглядається можливість надавання послуг IoT на базі стільникових мереж, саме цей вид радіотехнологій буде розглянуто більш докладно. Для забезпечення покриття великих територій під вимоги IoT адаптуються сучасні стандарти стільникового зв'язку, а також розробляються нові стандарти. Зокрема, у 2016 р 3GPP завершив роботу над Release 13, який спрямований на реалізацію вимог IoT і створення глобальної екосистеми. У даний час можливо виділити три стандарти: EC-GSM, eMTC (також званий LTE-M або

LTE-MTC) і NB-IoT цього класу. Нижче наведено короткий опис стандартів, адаптованих до вимог IoT, а також їх порівняння у таблиці 2.1.

Радіоінтерфейс EC-GSM.

Група GERAN розробила розширений стандарт GSM для адаптації стандарту GSM до вимог IoT: EC-GSM (також званий EC-GPRS або EC-GSM- IoT).

EC-GSM - це радиоинтерфейс, який дозволяє збільшити число M2M-пристроїв, що працюють у мережі GSM. А за рахунок підвищення радіочутливості модулів досягається збільшення радіусу дії пристроїв при одночасному зниженні їх енергоспоживання. Використання технології EC-GSM не вимагає масштабної заміни комунікаційного обладнання, у деяких випадках можливо обійтися оновленням програмного забезпечення.

EC-GSM можливо використовувати там, де не потрібна висока швидкість передачі даних - технологія підходить для датчиків, детекторів і лічильників систем моніторингу, як на відкритих просторах, так і у приміщеннях.

Для її впровадження у мережу GSM не потрібно модернізація обладнання, усі необхідні зміни вносяться на рівні програмного забезпечення. На відміну від стандартного оператора GSM / GPRS, новий стандарт дозволяє збільшити лінійний бюджет, число підключаються на один сектор базових станцій (БС), а також знизити вартість абонентського пристрою (табл. 2.1).

Адаптація до вимог IoT у частині зниження енергоспоживання забезпечується за рахунок збільшення частоти передачі обов'язкових сигнальних повідомлень, скорочення часових інтервалів прийому і передачі інформації, введення періодів "мовчання" абонентського пристрою тривалістю до 52 хвилин.

Для поліпшення лінійного бюджету на 20 дБ використовуються багаторазові повтори переданої інформації. Крім того, стандарт відмовляється від підтримки сумісності UMTS і LTE, а також покращує механізми аутентифікації і захисту з'єднання абонентських терміналів.

Характеристики	EC-GSM	eMTC	NB-IoT

Діапазон радіочаснтот, МГц	900, 1800	700, 800, 900	450, 700, 800, 900
Ширина частотного канала	200 кГц	1,08 МГц	180 кГц
Число пристроїв IoT на сектор БС, од., не більш того	50000	45000	50000
Швидкість передачі	70 або 240 кбіт/с (GMSK або 8PSK)	1 Мбіт/с (16 QAM)	240 кбит/с (лінія вниз); 240 кбит/с або 20 кбіт/с (лінія вгору)
Тип радіодоступу	TDMA/FDMA	OFDMA (лінія вниз); SC-FDMA (лінія вгору)	OFDMA (лінія вниз); SC-FDMA або FDMA/GMSK (лінія вгору)
Бюджет радіолінії	До 164 дБ або на 24 дБ краще GSM*	До 155 дБ або на 15 дБ краще GSM*	До 164 дБ або на 24 дБ краще GSM*
*3GPP TR36.888/45.820.			

Таблиця 2.1 - Основні характеристики аудиоинтерфейсов IoT, що входять у специфікацію 3GPP Rel.13

Радіоінтерфейс eMTC.

Радіоінтерфейс LTE-eMTC є продовженням адаптації стандартного LTE з урахуванням вимог IoT. Важливою відмінністю технології eMTC є висока пропускна здатність, до 1 Мбіт / с у кожному напрямі (від абонента і до абонента).

eMTC покликана знизити вартість кінцевого пристрою IoT за рахунок відмови від функціональності LTE, яка затребувана і широко використовується у мережах стільникового широкосмугового доступу (MBSA), однак стає надмірною при масовому підключенні пристроїв IoT. Це продовження роботи розпочатна 3GPP у попередньому випуску специфікацій (Release 12), який визначив LTE Cat.0 для IoT. eMTC також додає механізми Extended DRX і PSM для LTE, що вирішують задачу зниження енергоспоживання.

LTE-eMTC має дещо меншу енергоефективність, однак при цьому забезпечує швидкість передачі даних до 1 Мбіт / с у кожному напрямі - від абонента до абонента і від абонента до абонента, і досить низьку затримку на радіоінтерфейсу. Особливістю LTE- eMTC є використання ширини каналу 1,08 МГц (6 ресурсних блоків), а також полудуплексного режиму, що дозволяє максимально знизити вартість кінцевих пристроїв. Слід зазначити, що через більш високої швидкості передачі даних eMTC програє EC-GSM приблизно на 10 дБ у плані поліпшення лінійного бюджету.

З точки зору використання спектру, LTE-eMTC зазвичай не реалізується як окрема несуча. У каналі LTE практично у будь-якій частині виділяється 6 ресурсних блоків, через що транслюються пілотні сигнали LTE-eMTC, і у яких дані LTE-eMTC також мультиплексируются у Тимчасова області. Це дозволяє динамічно перерозподіляти використовувані ресурси (частотний спектр, обчислювальну потужність базової станції і т.д.) у залежності від типу і числа підключених пристроїв і генерується ними трафіку.

У той же час, ці ресурсні блоки відрізняються від ресурсних блоків LTE з точки зору радіоінтерфейсу. Фактично, окрема несуча LTE-eMTC організовується як спеціальна передача даних на окремій ділянці стандартного каналу LTE. А у певні моменти часу ця ділянка може використовуватися і для передачі звичайних даних LTE.

Радіоінтерфейс NB-IoT.

NB-IoT (NarrowBand IoT, вузькосмуговий Інтернет речей) - це стандарт стільникового зв'язку для телеметричних пристроїв з великими об’ємами обміну

даними. Він був розроблений консорціумом 3GPP у рамках роботи над стандартними стільниковими мережами наступного покоління. Перша робоча версія специфікації була представлена у червні 2016 року.

На відміну від двох попередніх, стандарт NB-IoT можливо вважати новою розробкою, а не простий адаптацією стандарту LTE з урахуванням вимог IoT. NB-IoT передбачає інтеграцію з LTE, однак його реалізація змінює не тільки програмне, а й апаратне забезпечення. Стандарт вимагає нового типу радіодоступу, з характеристиками, відмінними від LTE.

Зміни на рівні радіоканалу дозволять знизити вартість пристроїв NB-IoT у порівнянні з eMTC приблизно на 90%. Багато виробників мережевого устаткування і абонентських модулів оголосили про підтримку технології NB-IoT у своїх продуктах: Ericsson, Huawei, Nokia, Intel, Qualcomm. Так що цей стандарт може стати одним з найпопулярніших при реалізації різних IoT-проектів.

Використання смуг радіочастот для цього стандарту передбачається у три можливі варіанти: як окремий частотний канал поза LTE, у захисній смузі радіочастот, необхідної для забезпечення сумісності мереж LTE різних операторів, а також безпосередньо через виділення смуги у каналі мережі LTE. У останньому випадку мережі NB-IoT і LTE повинні належати одному оператору. Для простоти ці режими далі називаються: standalone, guard-band та inband.

Режим in band передбачає заміну одного або декількох блоків ресурсів сигналу LTE на несучу NB-IoT. Причому таке розгортання практично не відрізняється від звичайного блоку ресурсів LTE, як за формою спектру, так і за характеристиками потужності, і не призводить до зміни загальної ширини спектра несучої LTE або збільшення її потужності у межах каналу LTE. Даний варіант розгортання додатково зображений на рис. 2.10. З огляду на це даний режим роботи NB-IoT можливо розглядати як додатковий тип даних, що передаються у сигналі LTE, який повністю вписується у основні тактико-технічні характеристики сигналу LTE.

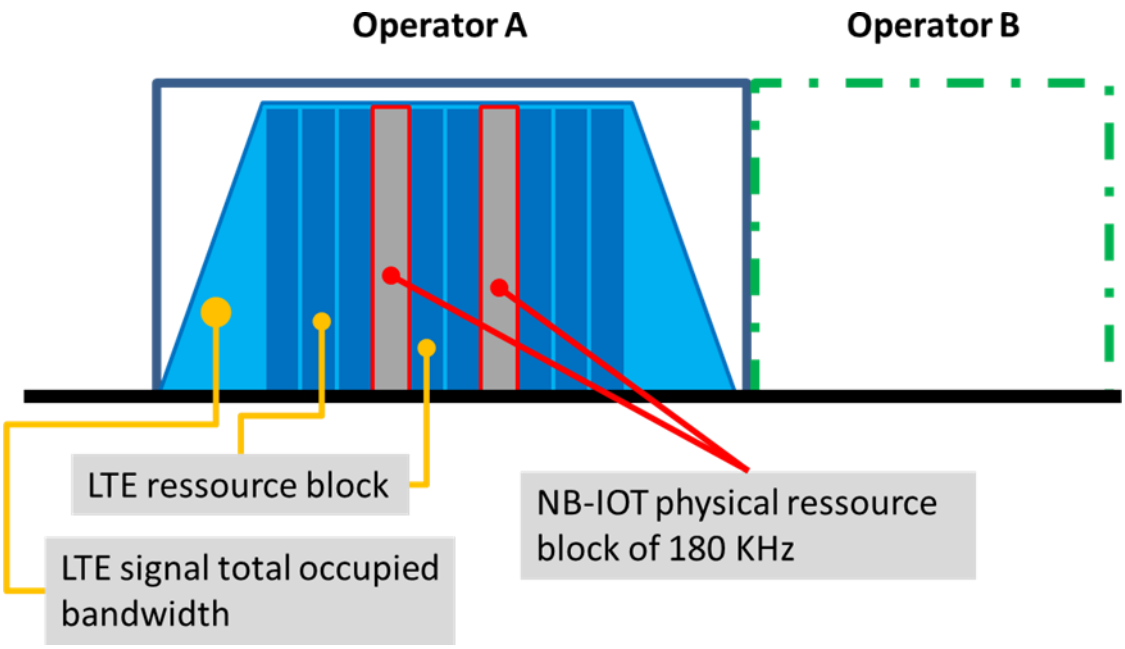


Рисунок 2.10 - Приклад впровадження NB-IoT у внутрішньо сигнальному варіанті (in band)

Внутрішньоканальний (guard-band) режим також використовується тільки разом з несучою LTE, однак вже у вигляді ресурсного блоку поза базової смуги сигналу LTE. У цьому випадку передбачається, що розгортання одного або декількох сигналів NB-IoT у межах кожної захисної смуги (нижньої чи верхньої) має відбуватися при дотриманні вимог до випромінювання незалежного сигналу LTE. Розгортання у захисних смугах шириною менше 5 МГц не визначене у 3GPP. Розгортання внутріканального (в захисних інтервалах) NB-IoT у стандартах 3GPP починається зі шпальт LTE шириною 5 МГц. Для LTE з смугами пропускання 10, 15 і 20 МГц захисна смуга (яка для нижньої і верхньої захисних смуг становить 10% від загальної смуги пропускання каналу) достатня для розміщення декількох несучих NB-IoT. Для захисної смуги необхідно використовувати згладжує фільтр, і у міру збільшення загасання фільтра несуча NB-IoT може бути розміщена ще далі до краю, у залежності від реалізації фільтра базової станції. Приклад реалізації NB-IoT у внутріканального варіанті (захисна смуга) зображений на рис. 2.11.

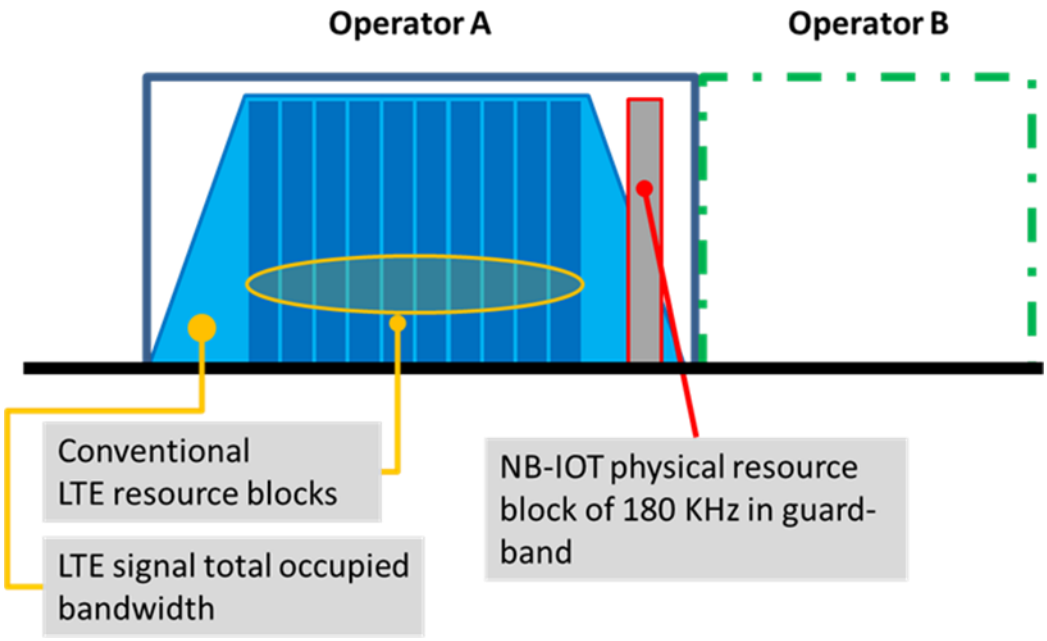


Рисунок 2.11 - Приклад впроваджнення NB-IoT у внутріканнальному варіанті (guard-band)

Варіант автономного розгортання спочатку позиціонується як окрема технологія, призначена у першу чергу для заміни мереж GSM для обслуговування пристроїв IoT. У той же час носій NB-IoT був оптимізований спеціально для можливості роботи у каналі GSM. Так, сигнал NB-IoT у відокремленому (а також у внутріканального варіанті) бачиться як сигнал шириною 200 кГц, з основним випромінюванням, зосередженим у смузі 180 кГц і з двома захисними смугами по 10 кГц, розташованими з боків від основного випромінювання. Ілюстративний приклад розміщення несучої NB-IoT у разі роздільного варіанту розгортання зображений на малюнку 2.12.

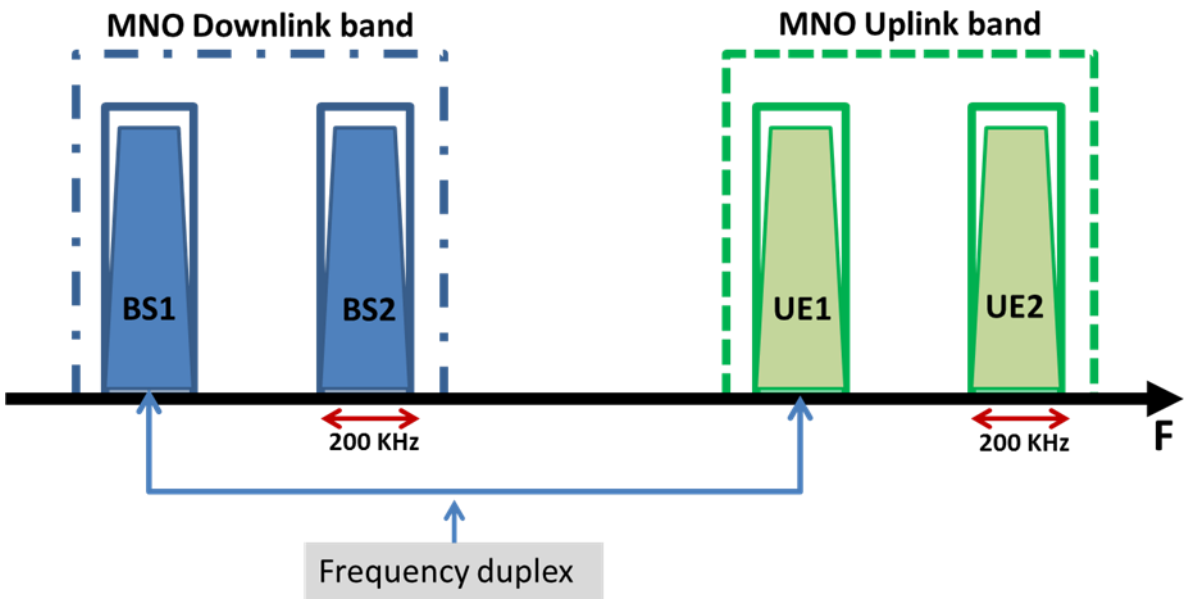


Рисунок 2.12 - Приклад впровадження NB-IoT у відокремленому варіанті (standalone)

Таким чином, варіант автономного розгортання не вимагає розгортання мережі LTE. Хоча режим NB-IoT був спеціально включений у існуючий стандарт LTE для легкої інтеграції у мережі операторів, у даному випадку він виступає як повністю незалежний радиоинтерфейс. Стандарт IMT-2020 (5G) вище 24 ГГц. МСЕ прийняв рішення назвати стільникові мережі п'ятого покоління IMT-2020.

На думку більшості експертів, мінімальний розмір частотного каналу (частотного блоку) для систем IMT-2020 перевищує 200 МГц; проте дещо експерти вважають, що він зобов’язаний бути не менше 500 МГц. Тому для систем IMT-2020 розглядаються смуги частот понад 24 ГГц. Такі високі частотні діапазони, швидше за все, зроблять неможливим виконання вимог IoT у рамках однієї мережі.

Ще до появи технології LPWAN значна число рішень M2M у різних галузях вирішувалося за допомогою технологій узкополосной радіозв'язку, а саме звичайної і транкінгового радіозв'язку з використанням цифрових стандартів. Спочатку створені для вирішення завдань оперативної голосового зв'язку, мережі звичайної і транкінгового радіозв'язку також забезпечують низкоскоростную передачу даних, що виявилося затребуваним для M2M-рішень, особливо з високими вимогами до надійності.

Однак низька затримка і висока надійність забезпечили затребуваність цифровий професійного радіозв'язку у M2M-додатках у хімічній, нафтогазовій

промисловості, телеметрії і т.д. Наприклад, вибухонебезпечні датчики на нафтопереробних і хімічних заводах дуже часто використовують професійний радіозв'язок через складні умови поширення, високих вимог до затримок і доступності радіоканалу.

Незважаючи на досягнення технології LPWAN у плані збільшення дальності зв'язку, існують великі території, де наземна зв'язок недоступна, наприклад, вздовж залізниць у віддалених районах або у відкритому морі. З цієї причини супутниковий зв'язок активно використовується для додатків M2M / IoT. Сегмент M2M не є новим для застосування супутникових технологій.

Однак великий потенціал супутникового зв'язку полягає у підключенні точок доступу LPWAN по супутникових каналах. Для цих цілей вже зараз можливо використовувати VSAT-станції на стаціонарних об'єктах або VS на мобільних платформах, що працюють у ПС. Дані, зібрані точкою доступу LPWAN з локальної території або точкою доступу LPWAN на об'єкті, що рухається (наприклад, з вагонів у поїзді), передаються через супутник на сервер для подальшої обробки. Це дозволяє використовувати прості і малопотужні пристрої LPWAN на кінцевих пристроях без інтеграції з супутниковими терміналами.

II.4 Дослідження особливостей мультисервісного трафіку з урахуванням повідомлень, що генерують пристрої IoT

Телекомунікаційна мережа повинна розвиватися таким чином, аби забезпечувалися усі необхідні умови для практичного застосування концепції Інтернету речей. Одним з таких умов слід вважати обслуговування мультисервісного трафіку з заданими якісними показниками. Даний трафік можливо розглядати як результат складання двох компонентів, що представляють собою потоки IP-пакетів різної природи. Першу складову іноді називають людським трафіком (користувачем, як правило, є людина), другу - трафіком речей, створюваним при реалізації концепції IoT.

Властивості першої складової активно вивчаються фахівцями з теорії телетрафіка на основі теоретичних моделей і результатів вимірювань у діючих мультисервісних мережах. Дослідження другої складової ускладнюється тим, що поки складно передбачити характер зростання трафіку IoT з необхідною точністю. Однак залежність від недостатньої числа статистичної інформації можливо зменшити, використовуючи сценарний підхід [2].

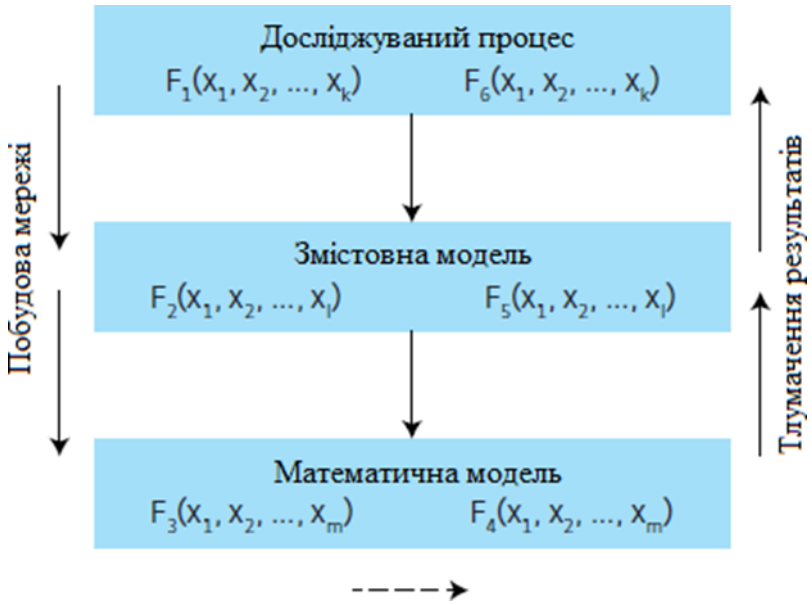


Рисунок 2.13 – Модель для дослідження мультисервісного трафіку

Припустимо, що характеристики руху (атрибути досліджуваного процесу) можуть бути адекватно представлені функцією F1 (x1, x2, ..., xk). Набір змінних xi, i = l, k утворює набір параметрів, адекватно характеризують об'єкт дослідження. При переході до блоку "Модель змісту" ряд змінних зазвичай виключається з подальшого дослідження з об'єктивних і суб'єктивних причин. Це означає, що l> k. Природно, змінюється і вид вихідної функції, що відбиває запис F2 (x1, x2, ..., xl).

При переході до блоку "Математична модель" набір розглянутих змінних також змінюється. Можливі як $l \leq m$, так і $l \geq m$. У результаті дослідження функція F3 (x1, x2, ..., xm) приводиться до вигляду, який позначається як F4 (x1, x2, ..., xm). Різниця цих функцій характеризує помилку, що виникає при дослідженні математичної моделі.

У процесі інтерпретації результатів дослідження моделі формуються дві функції

- F5 (x1, x2, ..., xl) і F6 (x1, x2, ..., xk). Різниця функцій F2 (x1, x2, ..., xl) і F5 (x1, x2, ..., xl), а також F1 (x1, x2, ..., xk) і F6 (x1, x2,. .., xk) служить мірою помилок, що виникають у блоках "Модель вмісту" і "Досліджуваний процес" відповідно.

Кожен IP-пакет, з точки зору теорії телетрафіка, слід розглядати як запит на обслуговування - передачу, прийом або обробку. Вичерпної характеристикою потоку IP-пакетів є функція розподілу тривалості інтервалів між надходженнями запитів. Для ілюстрації, зображеної на малюнку 1, цей розподіл є функцією F1 (x1, x2, ..., xk).

На малюнку 2.14 зображена модель формування потоку IP-пакетів на вході вузла комутації. Операція складання IP-пакетів, що надходять з різних джерел, у цій моделі виконується у гіпотетичному блоці, який позначений символом "Σ". Даний блок можливо розглядати як буферну пам'ять на вході вузла комутації.

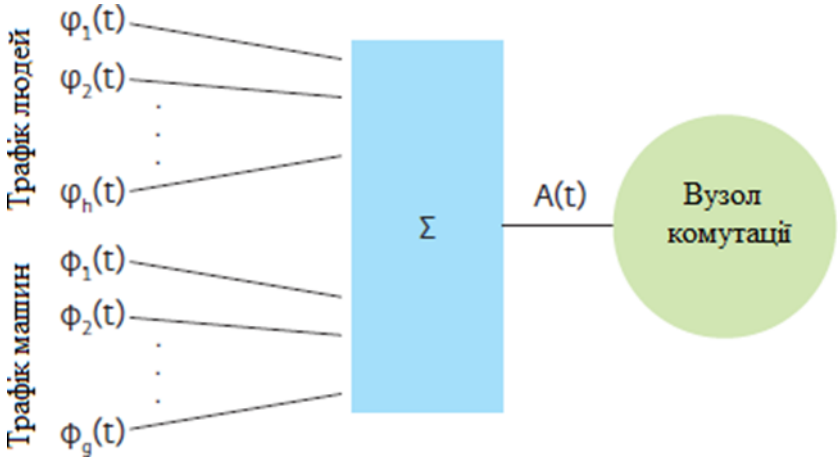


Рисунок 2.14 – Додавання декількох потоків заявок

Передбачається, що для обох класів трафіку (люди і речі) відомі функції розподілу тривалості інтервалів між моментами надходження заявок рівні φi (t), i = l, h, і φj (t), j = l, g, відповідно. На виході підсумовуючого пристрою формується потік заявок, який зобов’язаний бути оброблений вузлом comutacini. Для цього потоку необхідно визначити вид функції розподілу A (t) і її параметри. Це завдання легко вирішується для розподілів φi (t) і φj (t) виду (1), однак вона не представляє практичного інтересу для дослідження моделей мультисервисного трафіку.

Для довільних законів розподілу φi (t) і φj (t) нескладно оцінити інтенсивність вхідного потоку заявок Λ. Якщо для обох класів трафіку відомі значення інтенсивностей вхідних потоків λiφ і λjφ, то виконується така нерівність:

$$\Lambda \leq \sum_{i=1}^{h} \lambda_i^{\varphi} + \sum_{j=1}^{g} \lambda_j^{\varphi} \qquad (2.1)$$

Знак нерівності підкреслює той факт, що дещо програми можуть бути втрачені через обмежений об’єм буферної пам'яті. Сучасні вимоги до значення ймовірності втрати такі, що у співвідношенні (2.1) можливо поставити знак рівності.

Такий підхід представляється розумним ще й тому, що використання у подальших розрахунках значення Λ, як суми усіх значень λiφ і λjφ, дозволить отримати верхню межу необхідної продуктивності вузлів комутації у телекомунікаційній мережі.

Часто вхідні потоки задаються моментами надходження заявок, що зручно висловлювати цілими числами, рівними відношенню поточного часу t до деякого малому періоду x. Це дозволяє знайти діаметрально протилежні закони надходження заявок для загального потоку. Їх можливо назвати "найкращим" і "найгіршим".

Це твердження можливо проілюструвати за допомогою моделі, для якої визначено закони надходження заявок для двох потоків - n1 (t) і n1 (t). У верхній частині малюнка 2.15 зображені відповіді гістограми. Передбачається, що потоки є простими [3]. Нижня частина малюнка ілюструє два закони надходження заявок для загального потоку. Вони відповідають діаметрально протилежним випадків.

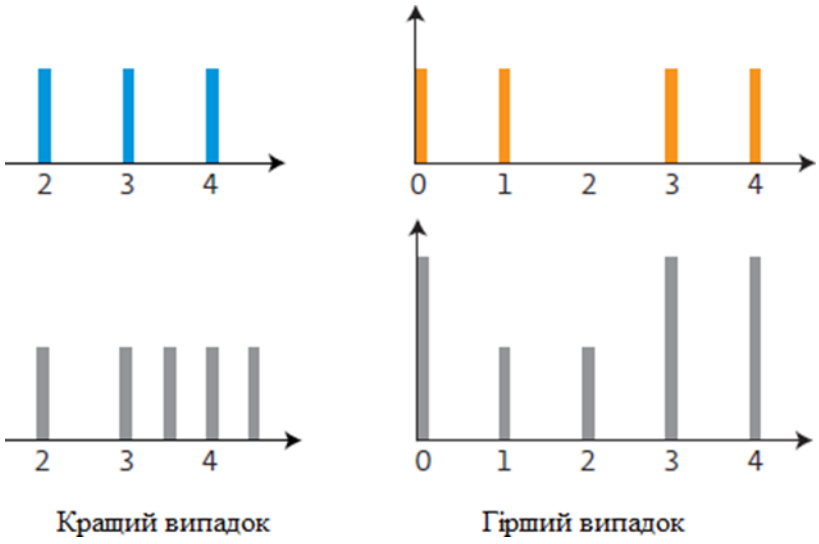


Рисунок 2.15 – Два види функції A(t)

Для "кращого" випадку ординарність зберігається, і сусідні заявки знаходяться на відстані не менше 0,5 один від одного. Для "гіршого" випадку ординальне порушується - у моменти часу 0, 3 і 4 приходять відразу дві заявки. Це відбувається, коли два вхідних потоку ненавмисно "синхронізуються". Визначення "гірше" і "найгірший" використовуються для того, аби підкреслити наступний факт: характеристики якості обслуговування трафіку при заданому значенні пропускної здатності вузла комутації для розглянутих випадків можливо порівнювати за допомогою цих прикметників. На жаль, не завжди вдається встановити залежність між законом входять заявок і відповідним розподілом A (t).

У технічній літературі по трафіку мультисервісних мереж частіше за інших вивчаються розподілу A (t) з так званими важкими хвостами [3]. Ці функції визначені на осі [x0, ∞). Ми також розглянемо приклад розподілу, визначеного на обмеженому інтервалі. Такі розподілу позначаються як Al (t). Нижній індекс "l" - це перша буква у слові "limited", що означає обмежений. Розподілу, для яких область випадку не обмежена, логічно позначати Au (t). Нижній індекс "u" - це перша буква у слові "unlimited", що перекладається як необмежений. Такі ж індекси підходять для середніх значень Al (1) і Au (1) і дисперсій σl2 і σu2, відповідно.

На малюнку 2.16 зображені графіки для двох розподілів з класів Au (t) і Al (t). Як приклади використовуються розподіл Парето і статечна функція довільної форми відповідно. Параметри розподілів Au (t) і Al (t) вибираються так, аби виконувалися умови: Al (1) = Au (1) і σl2 = σu2. Розподіл Al (t) має тільки три зростання, у точках τ, 2τ і 10τ зі значеннями P1 = 0,6, P2 = 0,3 і P10 = 0,1. Тоді для розподілу Парето неважко обчислити параметри положення і форми: x0 ≈ 1,244 і α ≈ 2,302. Для розподілу Al (t) значення τ приймається рівним одиниці.

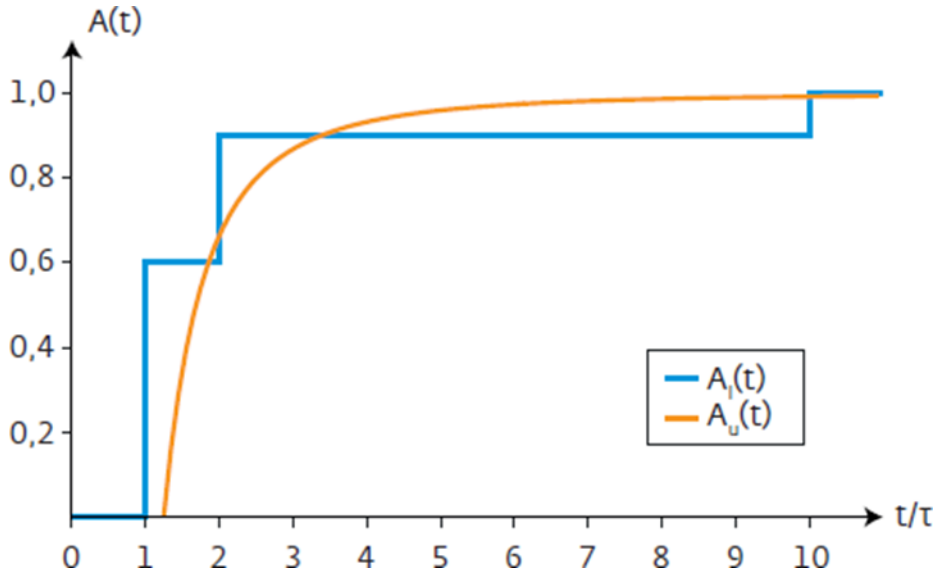


Рисунок 2.16 – Приклади досліджуваних розподілів

Розглянемо однолінійну систему телетрафіка з постійним часом обслуговування заявок. Для навантаження системи, яка дорівнює 0,9, шляхом моделювання були отримані наступні результати:

середній час затримки заявки становить 5,8 і 14,9 для розподілів Au (t) і Al (t)

коефіцієнт варіації часу затримки заявки становить приблизно 0,7 і 0,9 для розподілів Au (t) і Al (t).

Результати моделювання підтверджують, що використання розподілів типу Al (t) дозволяє отримати верхні межі для параметрів часу затримки заявок. Наприклад, у якості такої функції може бути використано бета-розподіл.

III. ДОСЛІДЖЕННЯ МЕТОДІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ МЕРЕЖЕВИХ РЕСУРСІВ 4G З IoT ТРАФІКОМ

III.1 Перспективи використання технологій 4G/5G для IoT

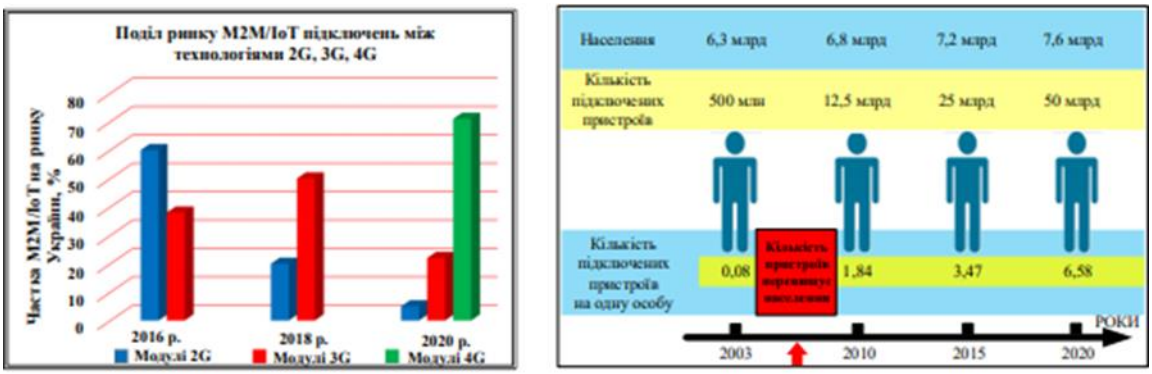
Ринок послуг M2M або Інтернет речей може бути одним із перспективних та динамічних ринків послуг для стільникових операторів [12]. Найбільш важливою перевагою мережі LTE є те, що час відгуку у 10 разів коротший за час відгуку GSM (сигнал від пристрою IoT надходить на сервер і повертається через мережу стільникового оператора). Низька затримка дуже важлива для додатків IoT у режимі реального часу, моніторингу чутливого обладнання та систем управління сигналізацією та промисловим обладнанням.

У мережі TD-LTE завдяки можливості гнучко змінювати розподіл мережевих ресурсів за рахунок гнучкого використання числа часових інтервалів, у мережі TD-LTE з точки зору передачі даних з асиметричним трафіком у мережі IoT, 2G / 3G Мережа має велику перевагу. , Змінити симетрію трафіку низхідної лінії зв'язку.

Оскільки технологія LTE повністю заснована на комутації пакетів і може працювати на протоколі IP, побудова, експлуатація та розширення мережі Інтернет речей на основі LTE є простим і недорогим [2].

Крім того, для мережі LTE призначено 44 смуги частот. Порівняно з технологіями GSM та HSPA (GSM-1-1,5 біт / сек / Гц, HSPA-2,2 біт / сек / Гц, LTE-5 біт / сек), вони мають більше Висока спектральна ефективність / Гц).

Усі ці характеристики знижують капітальні та експлуатаційні витрати на стільникову мережу і, відповідно, вартість одного біта передачі даних. Мережі LTE мають високу масштабованість з точки зору абонентської бази і сьогодні розгортаються з підтримкою адресації IPv6. Це дуже важлива характеристика, оскільки резерв доступних публічних IPv4-адрес швидко скорочується, а число IoT-пристроїв на базі LTE у Україні буде продовжувати рости (рис. 3.1 А).



А) Б)

Рисунок 3.1 - Зростання числа пристроїв, що працюють на основі LTE А) та числа пристроїв у розрахунку на одну людину Б)

Згідно з дослідженням Cisco 2010 року (рис. 3.1В), число смартфонів та планшетів, підключених до Інтернету, на одну людину становить приблизно 2. Однак це не обмеження. У 2020 року ця число становила 6,58 пристроїв на людину, а загальна число комунікаційних пристроїв, що використовують Інтернет, перевищила 50 мільярдів [12].

Хоча трафік, що передається від одного пристрою, невеликий, пристрій M2M все ще генерує відносно великий об’єм службового трафіку (сигналізації) у деяких випадках, що спричиняє перевантаження мережі.

На рис. 3.2 зображені схеми обміну командами у мережі E-UTRAN між eNodeB і MME при управлінні перевантаженням трафіку M2M.

eNodeB, отримавши повідомлення OVERLOAD START (що містить команду "Network Overload Start" для відхилення RRC-з'єднання у мережі радіодоступу E-U TRAN) від модуля управління MME, працюючи з небажаним трафіком, зобов’язаний знизити рівень обслуговування і призначений для користувача трафік.

Після отримання повідомлення OVERLOAD STOP ("Network Overload End") eNodeB відновить роботу з MME без обмежень на згенерований трафік.

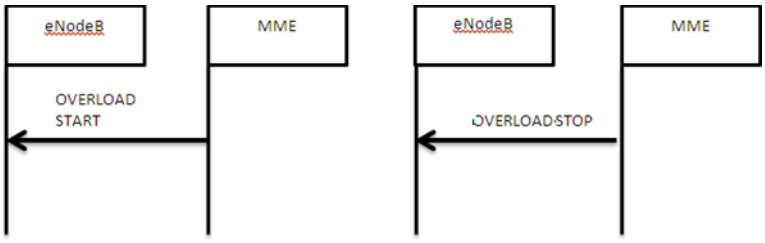


Рисунок 3.2 - Управління перевантаженнями

Rel'13 описує метод розширеного безперервного прийому (aDRX), при якому пейджингового повідомлення може бути відправлено на MME тільки у межах певного часового вікна пейджинга (PTW). Межі PTW визначаються на основі Hyper System Frame Number (H-SFN). Тривалість періоду бездіяльності (або сну) пристрої M2M, яке не відслідковує пейджингові повідомлення про нові події, може досягати 3 годин (рис. 3.3).

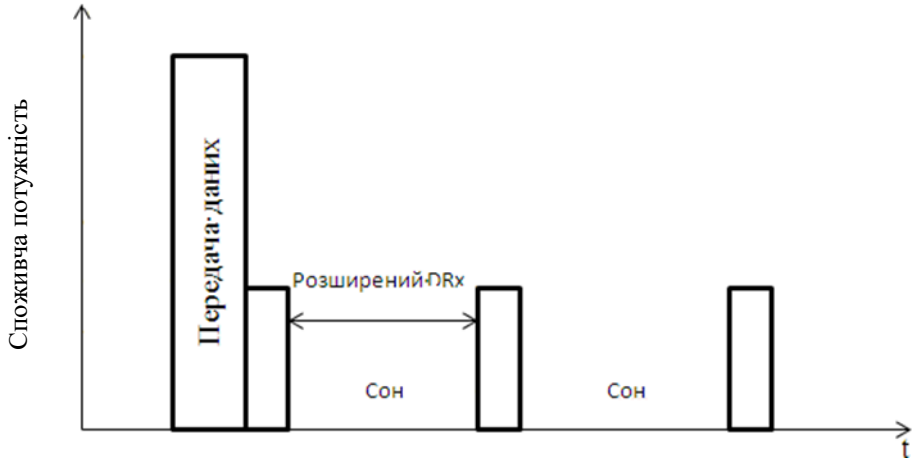


Рисунок 3.3 - Принцип eDRX

Метод PSM

M2M-пристрій отримує інформацію про періоди активації режиму PSM при отриманні заздалегідь налаштованих значень відповідних таймерів. Перший таймер, T 3324 (активний таймер), відповідає за час знаходження пристрою у режимі очікування, протягом якого мережа і M2M-пристрій можуть спілкуватися один з одним. Після закінчення таймера T3324 пристрій переходить у режим PSM до моменту спрацьовування другого таймера T3412, що відповідає за оновлення зони спостереження (TAU) (рисунок 3.4) [2].

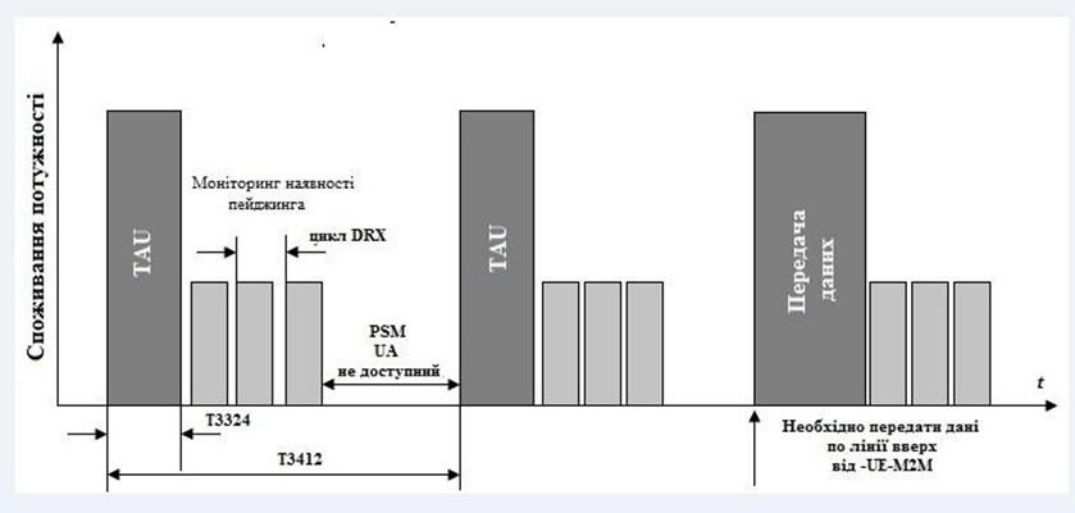


Рисунок 3.4 - Принцип PSM

III.2 Дослідження стратегій розподілу ресурсів

Розпочавшись з низькорівневих систем для дротових сенсорних мереж, технології еволюціонували у великомасштабні стандартизовані бездротові мережі для різних категорій датчиків. Найбільш успішними прикладами систем, призначених для передачі невеликих об’ємів даних, є GSM, LTE-M, LoRaWAN, SIGFOX, GPRS / EDGE і недавно розроблений 3GPP стандарт бездротових вузькосмугових мереж NB-IoT [12]. Останні три з цих технологій характеризуються дальністю покриття у десятки кілометрів, високою енергоефективністю і низькою вартістю обладнання.

Впровадження інтелектуальних пристроїв, таких як системи відеоспостереження, пред'являє принципово нові вимоги до систем збору і доставки інформації.

Об'єднання двох або більше гетерогенних мереж підвищує інтелектуальність і надійність систем прийняття рішень [13]. З огляду на обмежену число радіо ресурсів, вибір стратегії розподілу радіо ресурсів між меншою кількістю високошвидкісних відеокамер і великою кількістю низькошвидкісних інтелектуальних лічильників є важливим завданням для операторів бездротових мереж. У рамках цього завдання необхідно збалансувати ймовірні і тимчасові характеристики (ВХ), такі як ймовірність втрати сеансу для окремих потоків даних.

У даному розділі представлена аналітична модель для дослідження УСН обробки трафіку NB-IoT у присутності конкуруючого трафіку LTE.

За допомогою цього інструменту порівнюються три можливі стратегії розподілу радіо ресурсів: статична, динамічна і динамічна з резервуванням. У якості еталонної моделі розглядається внутрішньо регіональної режим, представлений у LTE Rel. 13 [14 15], де радіостанція LTE ділить частотний спектр з технологією NB-IoT. Ця комбінація була обрана завдяки тому, що:

1. LTE і NB-IoT - це єдині два рішення, що використовують один і той же частотний спектр;

2. Ця комбінація отримує найбільшу підтримку з боку індустрії інтернет-мовлення та, як очікується, стане основним стандартом для збору великих даних у світі інтернет-мовлення.

Модель системи.

Введемо поняття оператора, який реалізує послугу відеоспостереження, використовуючи можливості технологій LTE і NB-IoT. Розглянемо "оператора", який управляє системою зонального спостереження.

Система являє собою гібридне рішення, що складається з:

– деякого числа відеокамер для проведення відеомоніторингу;

– численних датчиків для виявлення вторгнень, пожеж, а також для контролю температури і тиску повітря;

– системи обробки великих об’ємів даних, одержаних як з відеокамер, так і зі смарт-датчиків.

Така комбінація рішень може ефективно співіснувати у рамках однієї мережі. Оскільки обидва рішення працюють на ліцензованих частотах, постачальник послуг, орієнтований на надійність, набуває у оператора мережі певний частотний ресурс через механізм "мережевого зрізу" [16].

Описаний вище сценарій розгортання передбачає поділ наданих ресурсів LTE між двома типами кінцевих точок: камерами спостереження і датчиками NB-IoT, що ставить питання про ефективне розподіл ресурсів. З огляду на це характеристики надійності обох потоків трафіку набувають першорядного

значення, оскільки сервер обробки не може приймати обґрунтовані рішення, якщо частина потоку тимчасово недоступна.

Розглянемо соту LTE з базовою станцією, розташованою у центрі стільникової мережі.

У цьому випадку радіус покриття стільникової мережі для послуг LTE, RL, набагато менше у порівнянні з покриттям технології NB-IoT, RN. Весь набір доступних ресурсів вимірюється у каналах NB-IoT. На це додатково впливає базовий канал. У напрямку висхідного каналу для NB-IoT є C каналів, що можливо розрахувати як C = cS, де S - число ресурсних блоків (RB) c - число базових каналів у одному RB [17]. Вхідний потік від сесій LTE є пуассоновским.

Час надавання послуги LTE розподілено експоненціально із середнім значенням 1 / μ, а мінімальна число ресурсів, на питання встановлення з'єднання на кожному часовому інтервалі висхідного каналу, становить d базових каналів. Нехай a = v / μ пропоноване навантаження LTE.

Запити на з'єднання від NB-IoT накладаються на процес Пуассона з інтенсивністю λ. Кожне надходження даних характеризується експоненціально розподіленим часом обслуговування з параметром θ. Кожна сесія NB-IoT вимагає b базових каналів. Ми позначаємо інтенсивність пропонованої навантаження передачі блоку даних з NB-IoT через λθ. Аналогічно сесій LTE, пристрої NB-IoT вважаються статичними протягом всієї сесії.

Стратегії розподілу ресурсів.

Розглянуті стратегії розподілу ресурсів між камерами LTE і вимірювальними датчиками NB-IoT зображені на рис. 3.5 Зверніть увагу, що максимальна число базових каналів, що можуть бути виділені для NB-IoT і LTE, становить CN = C - RL і LC = C - RN відповідно, де RL і RC - мінімальна число каналів, що завжди доступні і зарезервовані для трафіку LTE і NB-IoT відповідно. Таким чином, у статті представлені порівняння наступних трьох стратегій розподілу ресурсів:

1. статична стратегія (STAT). Ця стратегія відповідає випадку, коли мінімальне і максимальне число базових каналів, виділених для NB- IoT

і LTE, збігаються: RL = SL, RN = CN . Іншими словами, усі ресурси строго розділенні між NB-IoT і LTE;

2. динамічна стратегія (DYN). У цьому випадку мінімальний об’єм ресурсів не призначається NB-IoT і LTE, тобто RL = RN = 0. Однак максимальний об’єм ресурсів і CL = CR = C повністю розділенні між NB-IoT і LTE;

3. динамічна стратегія з резервуванням (DYNRES). У цій стратегії максимальний розподіл ресурсів, доступних для NB-IoT і LTE.

Визначено так, що CN= C - RL> 0 і CL = C – RN. При цьому RN> 0 і RL > 0 визначають мінімальний об’єм ресурсів, призначених для NB-IoT і LTE відповідно. Решта ресурси динамічно розподіляються між двома типами трафіку.

Унікальною особливістю даної системи з двома різнотипними вхідними потоками є той факт, що базові канали будуть послідовно виділятися з урахуванням особливостей внутрішньо смугової технології NB-IoT [18].

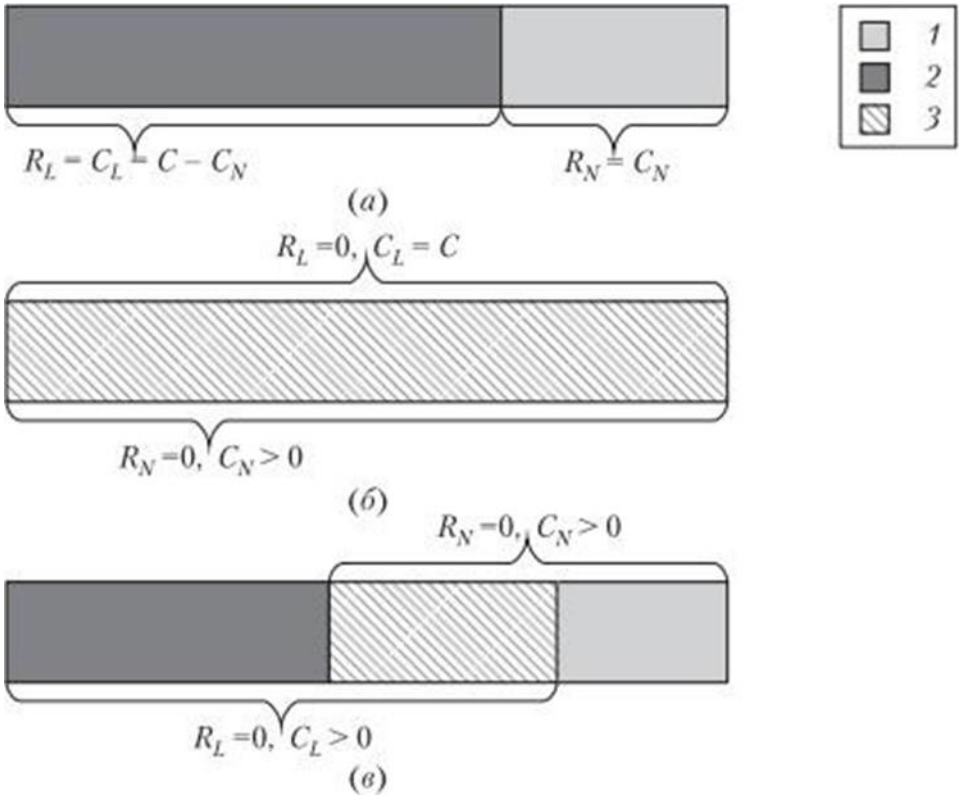


Рисунок 3.5 - Пропоновані стратегії розподілу ресурсів: (а) STAT; (б) DYN; (в) DYNRES; 1 - NB-IoT; 2 LTE; 3 - NB-IoT + LTE

Процес управління ресурсами зображений на рисунку 3.6.

Розглянемо систему без активних сесій і припустимо, що поступає нова сесія від NB-IoT. У цьому випадку RB стає доступним для NB-IoT, де кожен запит на прийом даних вимагає рівно b базових каналів NB-IoT.

Таким чином, нова сесія NB-IoT займає базові канали у цьому RB. При наступному встановленні сесії NB-IoT усі канали у цьому РБ вже будуть зайняті, тоді буде виділений наступний RB, доступний для послуг NB-IoT.

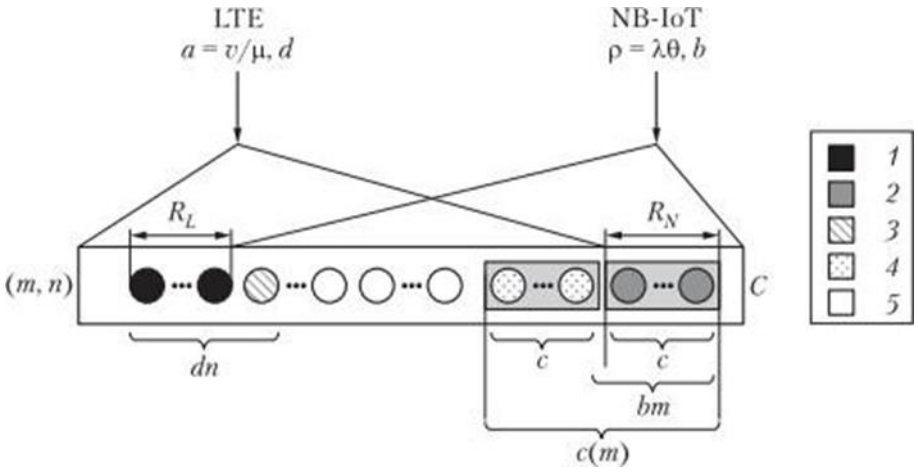


Рисунок 3.6 - Схема послідовного розподілу ресурсів стільники мережі LTE: 1-зарезервовані ресурси для LTE; 2 -зарезервовані ресурси для NB-IoT; 3-ресурси, використовувані LTE; 4 - ресурси, використовувані NB-IoT; 5 -вільні ресурси для LTE і NB-IoT

Описана вище система може бути представлена як система масового обслуговування з двома вхідними потоками, що мають різні дисципліни обслуговування з виділенням блоків ресурсів.

Визначимо стан системи. Відзначимо, що запит на обслуговування від LTE приймається, якщо на момент його надходження є не менше d каналів з CL = C - RN, що зменшує число доступних базових каналів на величину d і число RB на [d / c]. Число сесій LTE [d / c] завжди є цілим числом [d / c] ≥1. Якщо, приймаючи запити на з'єднання від NB-IoT число базових каналів у поточному РБ більше 6, то сесія NB-IoT приймається у цьому РБ. Якщо число доступних базових каналів менше b і новий РБ доступний для трафіку NB-IoT, то цей РБ приймає запит від NB-IoT на обслуговування, тим самим зменшуючи число базових каналів у цьому РБ на b. У інших випадках сесія NB- IoT втрачається.

Нехай m (t) і I n (t)> 0, визначають число активних сесій NB-IoT і LTE, відповідно. Таким чином, стан системи стільникового мережі LTE, яка обслуговує трафік NB-IoT і LTE, може бути описано двовимірним випадковим процесом {m (f), n (t), t> 0}, за яким слід простір станів:

$$\chi = \{m \geq 0, n \geq 0 : nd \leq C - R_N, c(m) \leq C - R_L, nd + c(m) \leq C\},$$

де c (m) = c [bm / m] - число базових каналів, зайнятих сесіями NB-IoT; M = [c / b] - максимальна число сесій NB-IoT, що можуть бути обслужені у одному РБ.

Відзначимо, що {m (t), n (t), t> 0} - це марковский процесс. Нехай p (m, n) (t), {m, n} ∈ X, - стаціонарний розподіл ймовірності m сесій NB-IoT і n сесій LTE у системі у момент часу t:

$$p(m,n) = \lim_{t\to\infty} p(m,n)(t), \{m,n\} \in \chi.$$

Аби отримати рівняння локального балансу, розглянемо довільний контур на діаграмі переходу станів. Стаціонарний розподіл вірогідності випадкового процесу {m (t), n (t), t> 0} задовольняє наступному рівнянню локального балансу:

$$p(m,n)\frac{c(m)}{\theta} = p(m-1,n)\lambda, m > 0, (m,n) \in \chi;$$

$$p(m,n)\mu n = p(m,n-1)\nu, n > 0, (m,n) \in \chi;$$

і представлені таким виразом:

$$p(m,n) = G^{-1}(X)\left(\frac{\rho}{Mb}\right)^m \left(\prod_{i=1}^{m}\left[\frac{i}{M}\right]\right)^{-1}\frac{a^n}{n!}, \qquad (3.1)$$

Де константа G (X) має такий вираз:

$$G(X) = \sum_{(m,n)\in X}\left(\frac{\rho}{Mb}\right)\left(\prod_{i=1}^{m}\left[\frac{i}{M}\right]\right)^{-1}\frac{a^n}{n!}, \qquad (3.2)$$

Отримання формул для ймовірностей блокування сеансів є трудомістким обчислювальним процесом, так як простір станів системи досить велика і число станів може досягати декількох десятків тисяч. Для усунення цього обмеження був розроблений спеціальний чисельний алгоритм, який заснований на зворотному співвідношенні між можливостями ненормованих макросостояніе і коротко описаний нижче.

Визначимо розбиття простору станів X

$$X = \cup_{s=0}^{S} Xs, \qquad (3.3)$$

де Xs = {(m, n) X: c (m) = sc}

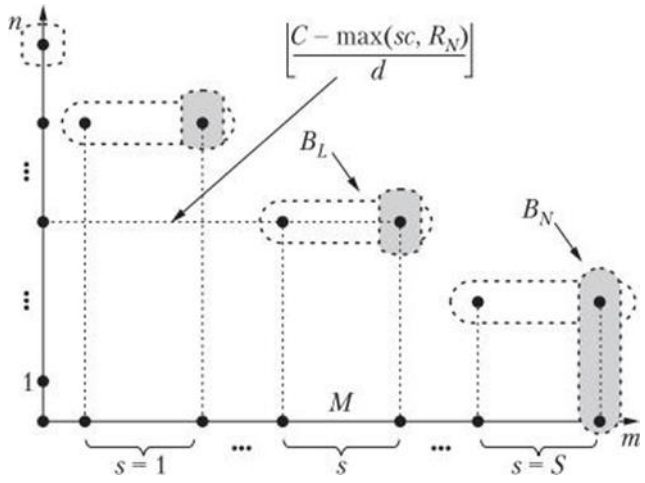


Рисунок 3.7 - Розбиття простору X на макростани

Розбиття простору станів на макросостоянія зображено на рис. 3.7. Тут також зображені підпростору, що відповідають станам блокування сеансів LTE і NB-IoT. Знайшовши стаціонарний розподіл станів системи, представлене у (3.1) і (3.2), і діючи над (3.3), можливо легко отримати необхідні ймовірності блокування. Зокрема, використовуючи (3.3), ми отримуємо ймовірність блокування сеансів LTE:

$$p_L = p(0, [\frac{C - R_N}{d}]) + \sum_{s=1}^{[(C-R_L)/c]} \quad \sum_{m=[s-1]M+1}^{sM} \quad p(m, [\frac{C - max[sc, R_N]}{d}]).$$

Аналогічні обчислення проводяться для підмножини блокуючих сесій NB-IoT, що у підсумку дає вираз для розрахунку ймовірності блокування сесій NB-IoT у покрокової формі:

$$p_N = \sum_{n=0}^{[R_L/d]} \quad p\left(\left[\frac{C-R_L}{c}\right] M, n\right) + \sum_{s=[R_N/c]}^{[(C-R_L)/c]-1} \quad \sum_{n=[(C-(s+1)c)/d]+1}^{[(C-max(scR_N))/d]} \quad p(sM, n).$$

Середня тривалість сеансу набуває вигляду:

$$E[T_N] = \frac{\sum_{m=0}^{[(C-R_L)/b]} \quad \sum_{n=0}^{\left[\left(C-max([m/M]c, R_N)\right)/d\right]} \quad [m/M]p(m,n)}{\lambda(1-p_N)}.$$

Середня число базових каналів, зайнятих на одну сесію NB-IoT, має вигляд:

$$E[b_N] = M \sum_{m=0}^{[(C-R_L)/b]} \quad \sum_{n=0}^{\left[\left(C-max([m/M]c, R_N)\right)/d\right]} \quad \left[\frac{m}{M}\right] p(m, n).$$

Середнє число каналів, займаних ete-сесіями, має вигляд:

$$E[b_L] = d \sum_{m=0}^{[(C-R_L)/b]} \sum_{n=0}^{[(C-max([m/M]c,R_N))/d]} np(m,n).$$

Середня число базових каналів, зайнятих обома типами трафіку, розкривається через E [bNL] = E [bN] + E [bL].

Для того аби отримати кількісну і якісну оцінку поведінки цієї системи, проводиться чисельний аналіз запропонованих стратегій розподілу ресурсів. Вхідні параметри для чисельного аналізу представлені у таблиці.

На малюнку 3.8 зображено значення ймовірності блокування сеансу LTE у залежності від загальної числа з'єднань датчиків NB-IoT при обраної статичної стратегії розподілу ресурсів STAT, при якій загальні радіоресурс строго розділені між двома типами трафіку. Для цієї стратегії вводиться коефіцієнт розподілу ресурсів 7, який характеризує число ресурсів, зарезервованих для NB-IoT. Зверніть увагу, що у результаті суворого поділу ресурсів між LTE і NB-IoT ефективність стратегії STAT залежить тільки від обраного значення 7.

Причина цього полягає у тому, що стратегія STAT створює дві незалежні віртуальні бездротові системи, одну для LTE і одну для NB-IoT. Хоча ця стратегія є найпростішою з точки зору реалізації, її можливо рекомендувати тільки для систем, де середнє навантаження від усіх сервісів працює паралельно::

1) рідко змінюється у часі;
2) відома заздалегідь;
3) може бути добре передбаченим;

Така поведінка системи рідко спостерігається на практиці.

Значення ймовірності блокування у стратегії DYN, коли загальні ресурси доступні для обох трафіків, сильно залежить від поточного навантаження від сегмента NB-IoT. Для менших значень числа підключених пристроїв NB-IoT стратегія DYN перевершує STAT, оскільки дозволяє переключити всю смугу пропускання на доступність пристроїв LTE при відсутності трафіку NB-IoT.

Параметр	Опис	Значення

C	Число базових каналів у СОТС LTE Число базових каналів у RB	100
$c\ R_N\ R_L$	Число каналів для NB-IoT Число каналів для LTE	4
$b\ d$	Число каналів для сесій NB-IoT Число каналів для LTE-сесій	{0,…100}
θ	Середня швидкість сесій NB-IoT Середня тривалість LTE-сесій	{0,…100} 1
$1/\mu$	Інтенсивність вхідного потоку NB-IoT Інтенсивність вхідного	4
λ	потоку LTE	100 кбіт 10с
ν		10/хв 1/хв

Таблиця 3.1 - Параметри системи для чисельного аналізу

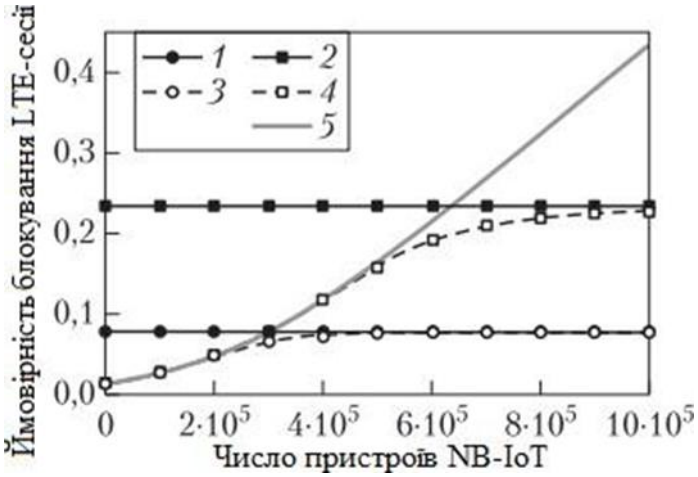


Рисунок 3.8 - Можливість блокування LTE у залежності від запропонованого навантаження NB-IoT: 1 - STAT, У = 0.8; 2 - STAT, У = 0.6; 3- DYNRES, RL = 0.8; 4 - DYNRES, Rl = 0.6; 5 – DYN

Зростання трафіку NB-IoT супроводжується збільшенням значень ймовірності блокування для стратегії DYN, оскільки трафік NB-IoT починає конкурувати за ресурси з постійним навантаженням, що надходить від трафіку LTE. Нарешті, поява великої числа пристроїв NB-IoT призводить до того, що трафік NB-IoT починає домінувати у загальному діапазоні. У результаті ймовірність блокування буде вище, ніж у стратегії STAT, незалежно від обраного значення коефіцієнта розподілу ресурсів. Стратегія розподілу ресурсів DYN може бути рекомендована для систем, у яких можливо порівняти середні навантаження, необхідні для кожного потоку (вимірювані у Гц / с). У той же час стратегія DYN залишається адекватним рішенням для нестабільних систем, де навантаження може сильно змінюватися у часі.

Перейдемо до третьої стратегії, DYNRES, де певна число ресурсів резервується для кожного типу трафіку, а ресурси, що залишилися динамічно

розподіляються між ними. Значення RL вибирається еквівалентним відповідному значенню 7 у раніше розглянутій стратегії розподілу ресурсів STAT, а RN вважається рівним нулю. Іншими словами, порівнюються статичний і динамічний варіанти розподілу. Відзначимо, що для меншого числа пристроїв NB-IoT характеристики стратегії DYNRES ідентичні характеристикам стратегії DYN. Однак збільшення значень ймовірності блокування для DYNRES зростає повільніше, ніж для DYN. Це пояснюється тим, що частина ресурсів, що могли б бути зайняті трафіком LTE, зайняті динамічним розподілом. Крім того, при більш високому навантаженні трафіку NB-IoT ймовірність блокування LTE для DYNRES ніколи не перевищить відповідного значення для системи зі стратегією STAT. Для надзвичайно великого числа вкладень NB-IoT крива для DYNRES асимптотично наближається, однак не перетинає криву для системи STAT.

Уявімо у ортогональному розрізі рис. 3.6, на якому зображена ймовірність блокування сесії NB-IoT у порівнянні із загальним числом підключених LTE-пристроїв. Як і у попередньому випадку, ми підберемо параметри для стратегії DYNRES таким чином, аби об’єми ресурсів, зарезервованих для NB-IoT у STAT і DYNRES, були рівні. Важливо відзначити, що у даному випадку RN дорівнює (1 - γ), а не γ. Значення RL вважаються рівними нулю. Таке ж якісне поведінку спостерігається для цього симетричного випадку і на рис. 3.8. Однак між рис. 3.8 і 3.9 є помітні кількісні відмінності. Значення ймовірності блокування для NB-IoT на порядок нижче, ніж для LTE. Це пов'язано з більш низькими вимогами до ресурсів окремої сесії NB-IoT, що, у свою чергу, призводить до збільшення шансів на отримання послуг навіть у приблизно повністю завантаженої системі. Крім того, спосіб розподілу каналів NB-IoT у режимі in-panel також відповідає самому режиму сенсорного трафіку.

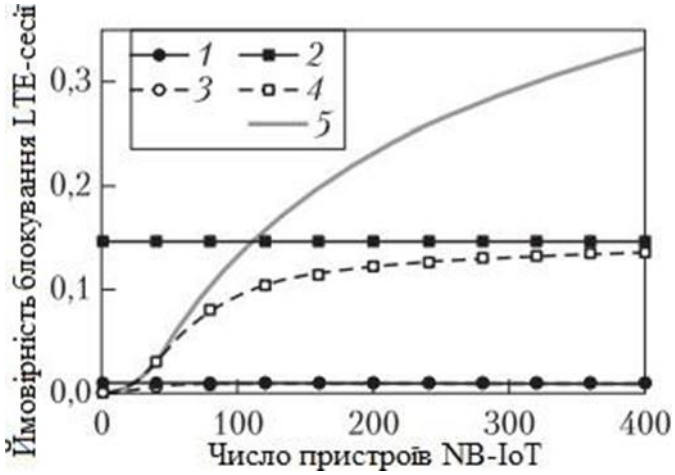


Рисунок 3.9 - Ймовірність блокування NB-IoT у залежності від запропонованого навантаження LTE: 1 — STAT, У = 0.8; 2 — STAT, У = 0.6; 3 — DYNRES, Rl = 0.8; 4 — DYNRES, Rl = 0?6; 5 — DYN

Сеанси LTE займають весь РБ, у той час як трафік NB-IoT отримує повний РБ, хоча один сеанс не займає його повністю. Тому наступні декілька сесій NB-IoT гарантовано будуть обслужені, так як залишок вже виділеного RB не може бути зайнятий ніяким трафіком LTE. Незалежно від числа трафіку LTE, система DYNRES завжди перебуває у виграшному становищі.

III.3 Розподіл частотно-часових ресурсів мережі LTE між UE та M2M/IoT

У технології LTE механізми планування канальних ресурсів не визначені стандартним чином, залишаючи вибір за виробниками обладнання базових станцій. Використання рішень щодо розподілу мережевих ресурсів дозволяє ефективно реагувати на зміни стану і умов роботи бездротової мережі, що можуть бути викликані, наприклад, відмовою або перевантаженням її елементів, коливаннями трафіку, що надходить у мережу, динамікою зміни сигнальної і помеховой обстановки і т.д. До таких ресурсів відносяться, перш за все, символи (часовий ресурс) і частотні поднесущие (частотний ресурс). Найменшою структурною одиницею радіоресурсу, який може бути виділений мобільної станції або M2M-пристрою, є блок ресурсів (Resource Block, RB). На малюнку 3.10 зображена структура кадру для частотних дуплексів.

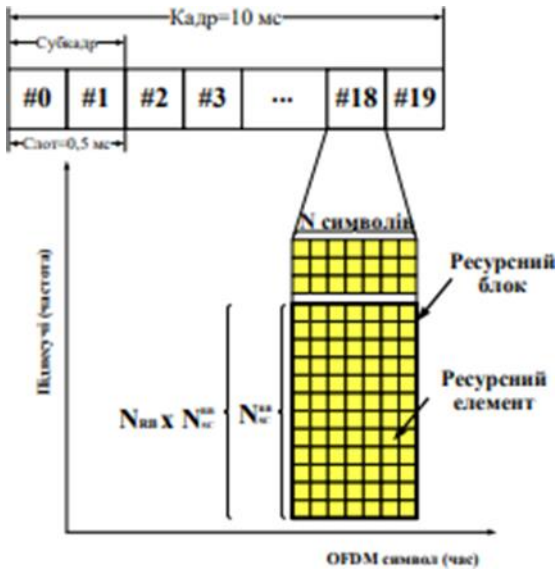


Рисунок 3.10 - Структурная кадру LTE при частотному дуплексі

Один ресурсний блок (РБ) складається з 12 піднесучих, рознесених на 15 кГц (разом займають 180 кГц) і 7 символів OFDM зі звичайним циклічним префіксом. Блок фізичних ресурсів (PRB) містить 2 RB, що разом доставляють 168 ресурсних елементів (RE) за 1 мс. RE може передавати 2, 4, 6, 8 біт при наступних видах модуляції: QPSK, 16QAM, 64QAM, 256QAM, відповідно. Для збільшення пропускної здатності використовується технологія агрегації спектра [19]. При цьому на швидкість передачі даних впливає число виділених ресурсних блоків (NRB), число ресурсних елементів (12·7, де 12 - число тих, що піднесуть, 7 - число символів), число антен MIMO, кодова швидкість (KodRATE), позиційні модуляції (log 2 (Module)).

$$R = \frac{N_{RB}^{'} \cdot 12 \cdot 7 \cdot MIMO \cdot Kod_{RATE} \cdot log2(Modul)}{0.5\text{мс}} \qquad (3.4)$$

де 0,5 мс – тривалість одного ресурсного блоку.

При розробці нових алгоритмів функціонування планувальника бездротових мереж 4G / 5G необхідно враховувати ряд особливостей M2M-трафіку. У специфікаціях консорціуму 3GPP сформульовані основні властивості M2M-трафіку.

Перш ніж перейти до алгоритму оптимального розподілу ресурсів, виділимо особливості функціонування гетерогенної мережі LTE. Встановлено, що найчастіше блоки даних M2M мають вкрай малий розмір і генеруються великою кількістю різних M2M-пристроїв. З огляду на це доцільно виділення

планувальником базової станції eNodeB одного RB (мінімальна число) для передачі даних від одного M2M-пристрої.

Для вирішення цієї проблеми ми пропонуємо проводити кластеризацію для локалізації M2M-трафіку всередині кластера, з подальшою агрегацією і класифікацією при передачі у ядро мережі LTE, що дозволить планувальником оптимально використовувати радіоресурс і знизити сигнальну навантаження на eNodeB. Також таке рішення дозволяє агрегувати повністю або частково ідентичні повідомлення з метою зменшення об'єму даних, переданих M2M-пристроями. Слід зазначити, що рішення планувальника про виділення мережевих ресурсів у першу чергу грунтується на вимогах QoS. Тому завдання розподілу частотно-часових ресурсів у технології LTE повинна бути сформульована як задача розподілу мережевих РБ між UEs і M2M-пристроями у залежності від заявлених вимог до смуги пропускання і параметрів QoS [20].

Ми пропонуємо визначати клас, до якого належить конкретний трафік UE, на основі параметрів QCI (QoS Class Identifier). У роботі пропонується розділити трафік від M2M-пристроїв на 4 пріоритети з різними вимогами до E2E QoS (t). Пріоритет даних до шлюзу від дочірніх вузлів через основні вузли і до шлюзу фіксується у поле ToS (Type of Service) пакета IPv6.

Максимальне значення допустимої затримки для трафіку I класу становить 100 мс, для II класу - 1 с, для III класу - 100 с, для IV класу - 1000 с. Передача інформації у мережі LTE здійснюється за допомогою частотно-часових ресурсів, у яких розташовуються керуючі сигнали і корисні дані. Розташування спектра для стільникових користувачів, пристроїв IoT і M2M у висхідному і низхідному каналах зображено на малюнку 3.11.

Таке розташування спектра дозволяє застосовувати агрегацію спектра для стільникових користувачів і M2M-пристроїв.

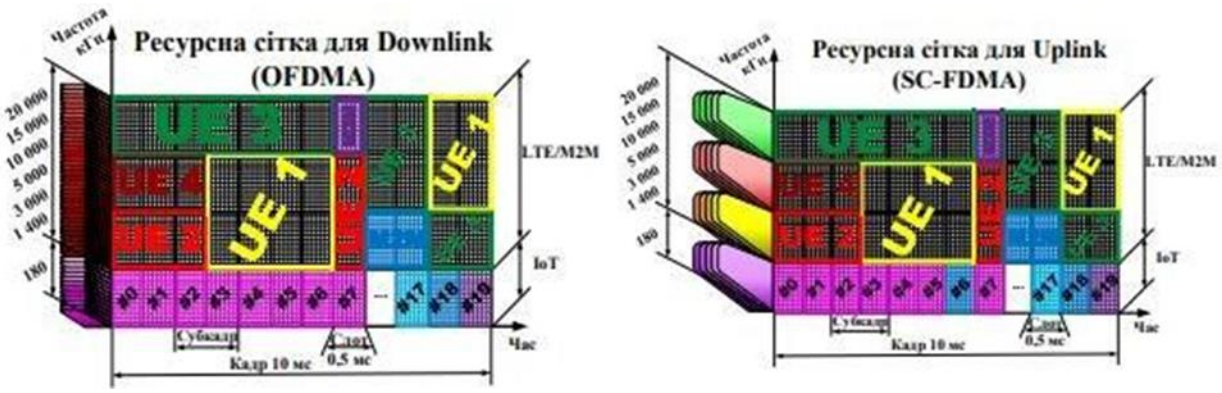
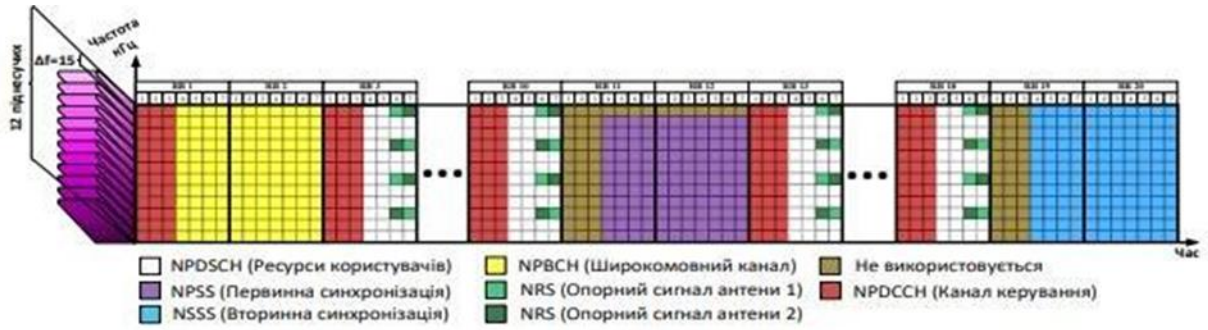


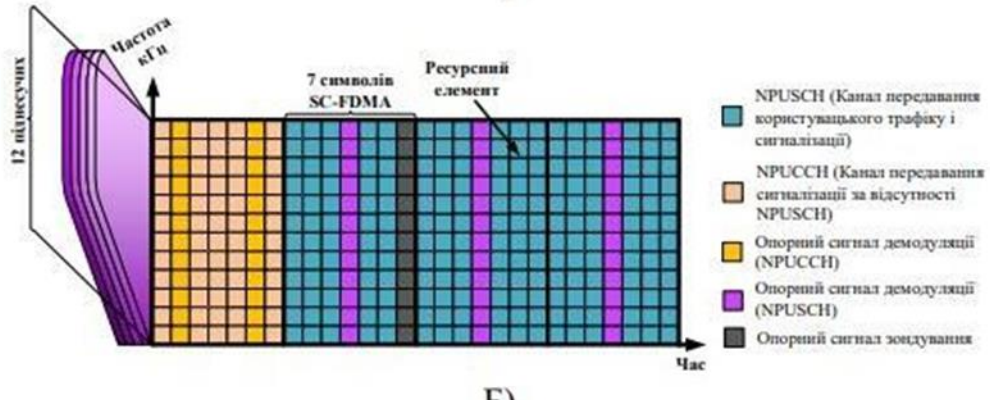
Рисунок 3.11 - Виділення ресурсів для користувачів у висхідному (зліва) та висхідному каналах (справа)

При передачі інформації з пристрою користувача на базову станцію і назад використовуються різні типи потоків (сигнальні і корисні). Їх розміщення для низхідного і висхідного потоків по-різному.

На малюнку 3.12 (А) зображено розташування корисного навантаження висхідного каналу і сигнальних даних у кадрі з частотного дуплексу для пристроїв M2M, що генерують низкоскоростной трафік у реальному часі. Кадр направляється eNodeB по каналу LTE на шлюз, який, у свою чергу, направляє дані на відповідне M2M-пристрій.



А)



Б)

Рисунок 3.12 - Розташування каналізаційних та корисних даних від M2M пристроїв у низхідному каналі А) та висхідному Б)

У сітці ресурсів для пристроїв використовуються наступні канали: - NPDSCH, по якому передаються призначені для користувача ресурси M2M пристроїв; - NPSS передає первинну синхронізацію, необхідну для фіксації номера кадру; - NSSS відповідає за вторинну синхронізацію, що відповідає за номер підкадрів; - широкомовний канал представлений:

– канал NPBCH, що відповідає за набір параметрів (ідентифікатори осередків і параметри управління доступом), необхідних для початкового доступу до середовища передачі;

– NRS несе опорний сигнал від антен, необхідний для визначення стану каналу;

– NPDCCH - канал управління, у якому базова станція вказує число і розташування у блоках ресурсів каналу для розширень M2M, також у цьому каналі вказується часовий інтервал для випадкового доступу. Для передачі інформації від шлюзу M2M до базової станції використовуються наступні канали (рис. 3.12 В):

– PUSCH - канал для користувача трафіку і сигналізації.

– PUCCH - канал управління призначеним для користувача трафіком і сигналізації при відсутності PUSCH;

– SRS - зондує опорний сигнал.

Впровадження шлюзу M2M у архітектуру мережі LTE для агрегації, приоритизации і балансування трафіку.

Весь зібраний трафік відправляється провідними вузлами на шлюз, де він диференціюється на чотири класи (Малюнок 3.13) відповідно до пріоритетів пристроїв. Відправлення повідомлення на базову станцію про виділення радіоресурсів у ній враховує допустимий час обслуговування, передбачене для кожного класу M2M-пристроїв.

З огляду на, що ці M2M-пристрої повинні бути оброблені на шлюзі і у черзі $t_{\text{черги і}}$, а після цього ще очікують виділення базовою станцією радіоресурсів у

частотно-часової області $t_{BS\,i}$, необхідно дотримуватися умов гарантійного обслуговування трафіку $t_{\text{обсл.i}}$

$$t_{\text{обсл.i}} \geq t_{\text{черги i}} \geq t_{BS\,i} \qquad (3.5)$$

У разі, коли трафік від M2M-пристроїв першого класу знаходиться у черзі часу, що призводить до порушення умови (3.5) він переміщається у чергу нижчого порядку. Шлюз обслуговує цей трафік негайно, а дані, що вже знаходяться у цій черзі, в'януть у обслуговуванні з урахуванням максимально допустимого значення QoS.

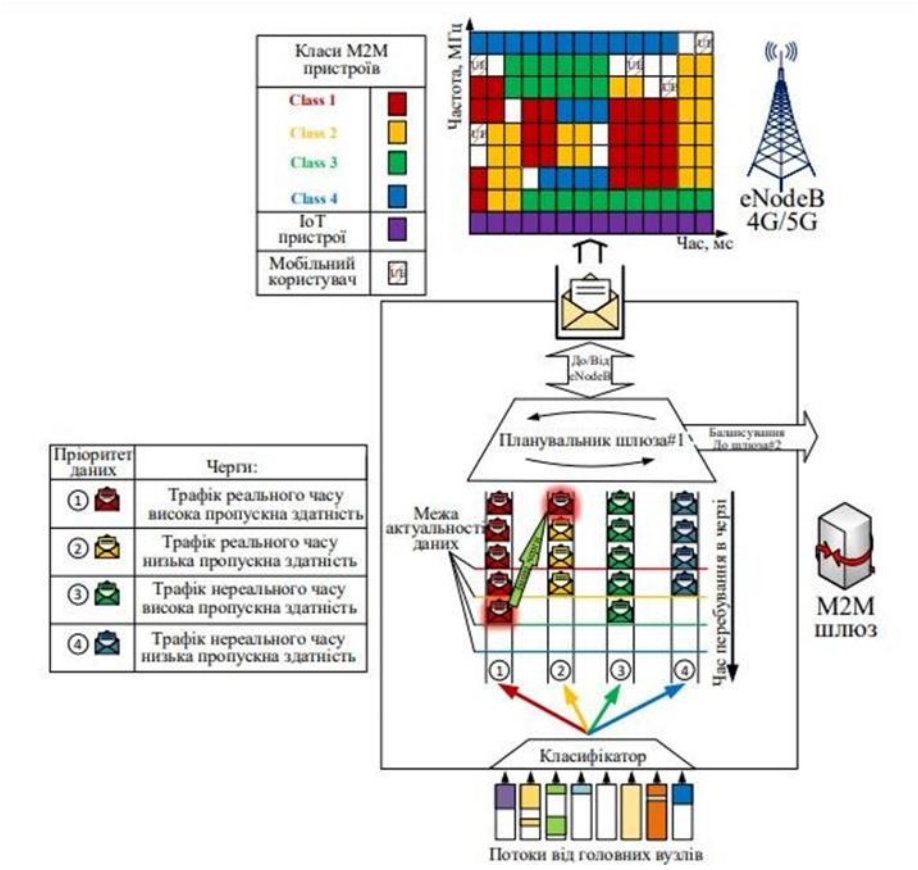


Рисунок 3.13 - Принцип обслуговування шлюзом мультисервісного трафіку із застосуванням черг 4 пріоритетів та фіксацією часу перебування часу у них

III.4 Збільшення зони покриття базової станції за рахунок використання технології WI-FI direct

Wi-Fi Direct - це стандарт бездротової передачі даних, який дозволяє пристроям підключатися один до одного безпосередньо без додаткового проміжної ланки у вигляді маршрутизатора.

Wi-Fi Direct покликаний зняти обмеження і зробити можливим пряме підключення пристроїв.

У разі відсутності вільних радіоресурсів у ресурсної мережі базової станції для виконання умови (3.5), про це повідомляється шлюзу, який, використовуючи технологію Wi-Fi Direct, перенаправляє M2M-трафік для обслуговування на інший шлюз, що знаходиться у зоні обслуговування малої стільники (фемто- стільники).

Таким чином, відбувається розподіл навантаження між шлюзами для гарантованого обслуговування пристроїв. У умовах, коли пристрій не має можливості встановити зв'язок через базову станцію, однак поруч знаходиться інший пристрій (див. Рис. 3.14), яке має хороший стан каналу, воно може виступати у якості ретранслятора. Таким чином, зона покриття базової станції збільшується.

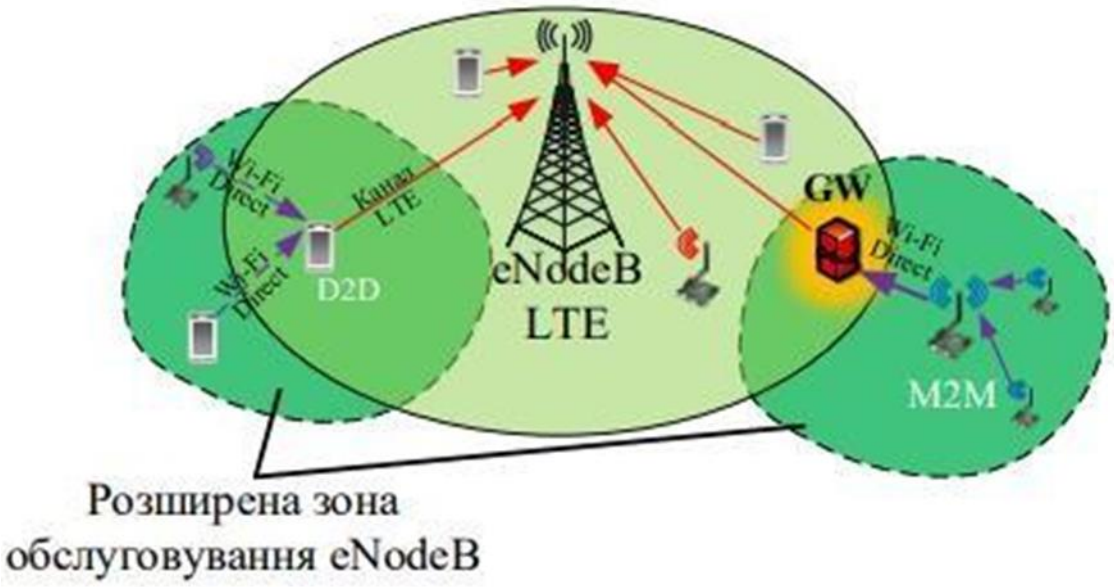


Рисунок 3.14 - Збільшення зони покриття базової станції

Для комбінації стеків протоколів слід вибрати протокол конвергенції пакетних даних (PDCP), що знаходиться між Wi-Fi Direct MAC і LTE. Відповідно до нього обмін даними відбуватиметься у три етапи:

LTE-пакети шифруються і перевіряються на цілісність у PDCP з використанням ключів, відомих тільки клієнту і eNodeB (evolved NodeB). Таким чином, інші абоненти не можуть розшифрувати пакети LTE, що проходять через мережу Wi-Fi;

Новий шлюз може обробляти блок пакетних даних (PDU) на рівні PDCP;

MAC-рівень Wi-Fi Direct забезпечує надійну і безпечну передачу даних і може виконувати повторну передачу кадрів на MAC-рівні.

Малюнок 3.15 ілюструє проходження пакетів у висхідному і низхідному напрямках. У результаті комбінації LTE і Wi-Fi дозвіл операцій передачі даних.

Шлюз використовує ACK / NACK для забезпечення відправки всього трафіку LTE на базову станцію, тому операції ARQ / ARQ виконуються тільки менеджером кластера eNB.

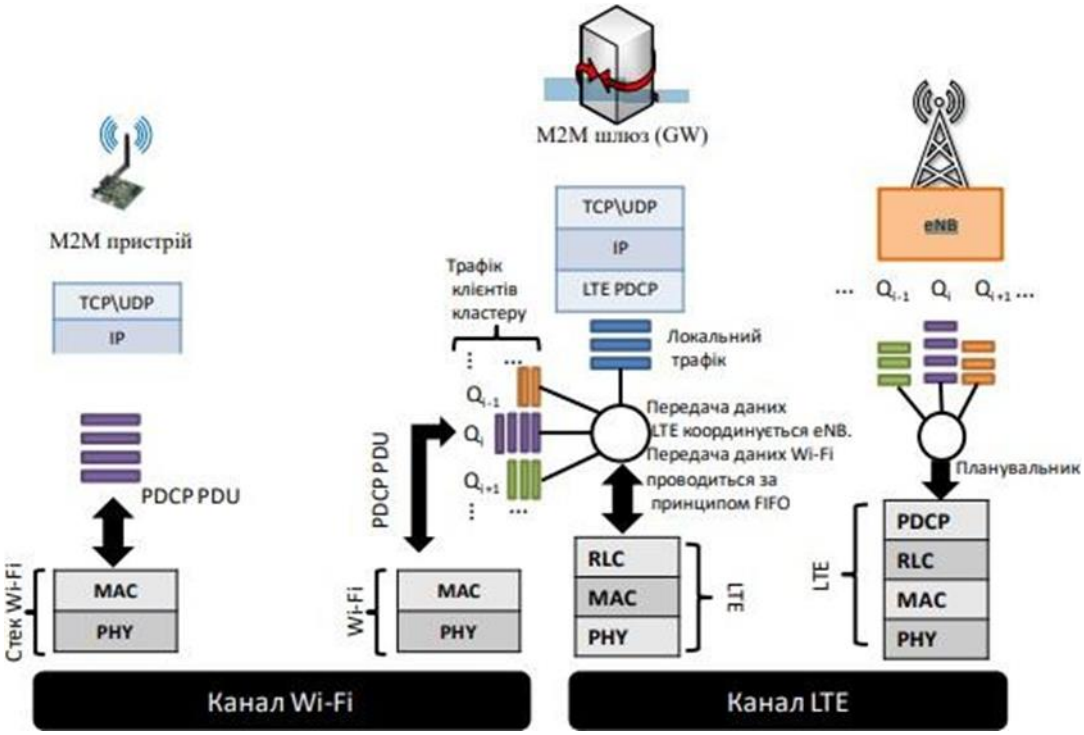


Рисунок 3.15 - Проходження даних між абонентами і eNodeB

На рисунку 3.16 зображена вдосконалена архітектура гетерогенної мережі LTE, яка призначена для обслуговування великої числа пристроїв M2M.

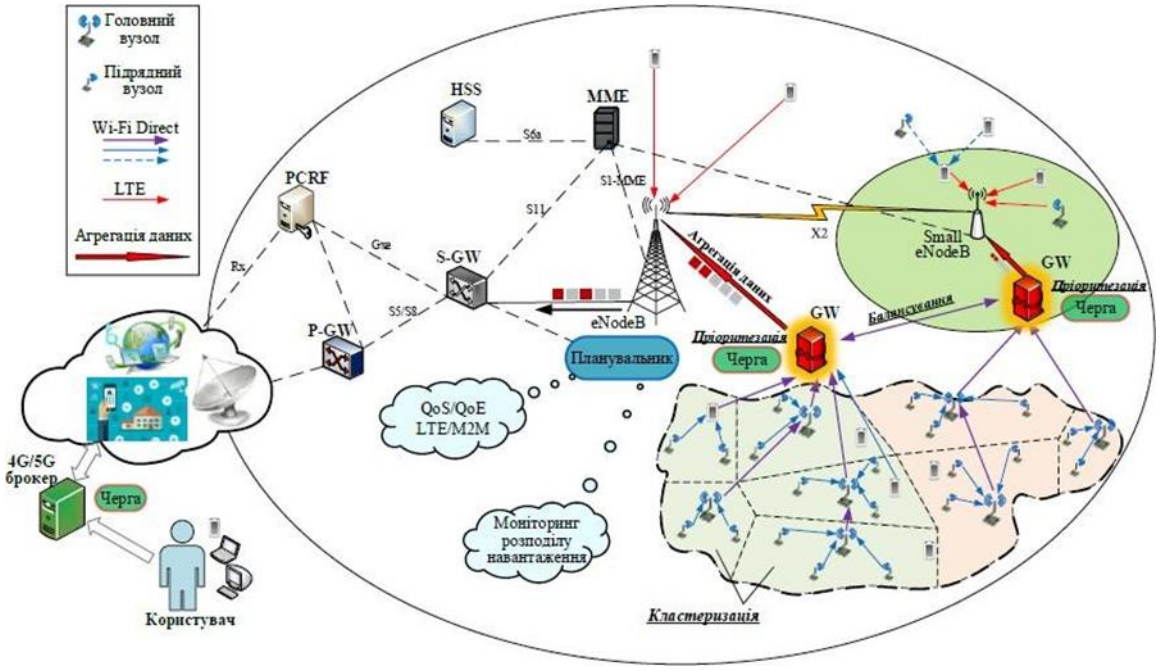


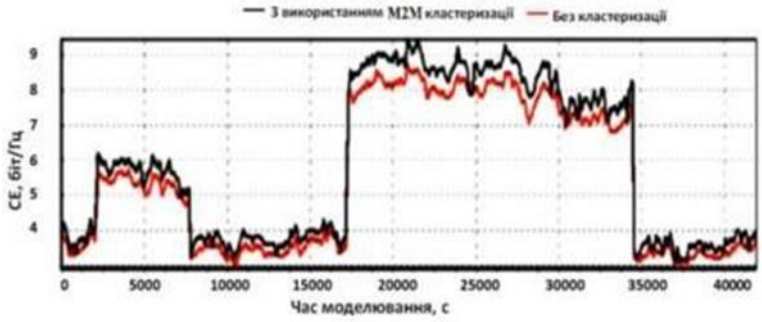
Рисунок 3.16 - архітектура гетерогенної мережі 4G/5G

Для оцінки ефективності даного методу було проведено порівняння режимів роботи мережі з використанням і без використання M2M-кластерів. У області виводу результатів кількісного моделювання були розміщені графіки, що показують зміну параметрів мережі у залежності від навантаження. Для моделювання було обрано такі параметри:

Радіус макро комірки	1200 м
Число макро комірок	3
Режим MIMO	4x4
Радіус M2M домену	50 м
Вид модуляції DL (в каналі LTE)	64 Q
Вид модуляції UL	16 AM
Зміна параметрів абонентів	Кожної ітерації з імовірністю 0,1
Генерація абонентського навантаження	Згідно нормального закону розподілу, послуги відповідно QCI
Смуга пропускання каналу LTE	1.4; 3; 5; 10; 15; 20 Мгц (в залежності від послуги)
Генерація числа абонентів	Згідно нормального параметричного закону розподілу
Середня число абонентів	120
Відсоток суміжного трафіку	5%

Таблиця 3.2 - Параметри моделювання

А)



Б)

Рисунок 3.17 - Навантаження на мережу при використанні M2M – доменів Wi-Fi Direct і без них (А) та системна спектральна ефективність (Б)

Перший графік показує завантаження мережі при використанні доменів M2M - Wi-Fi Direct і без них. Другий показує зміну спектральної ефективності у залежності від того, чи використовується домен M2M. У області параметрів моделювання зображені основні параметри моделювання, а саме: число базових станцій, діапазон частот на одну станцію, режим обходу, тип і порядок модуляції і середня число абонентів.

При застосуванні запропонованого рішення ефективність використання мережевих ресурсів підвищується. Зокрема, знижується частка сигнальних даних при ширині каналу 1,4, 3, 5, 10, 15, 20 МГц. Частка сигнальних даних зменшилася приблизно на 10%, як зображено на рис. 3.18.

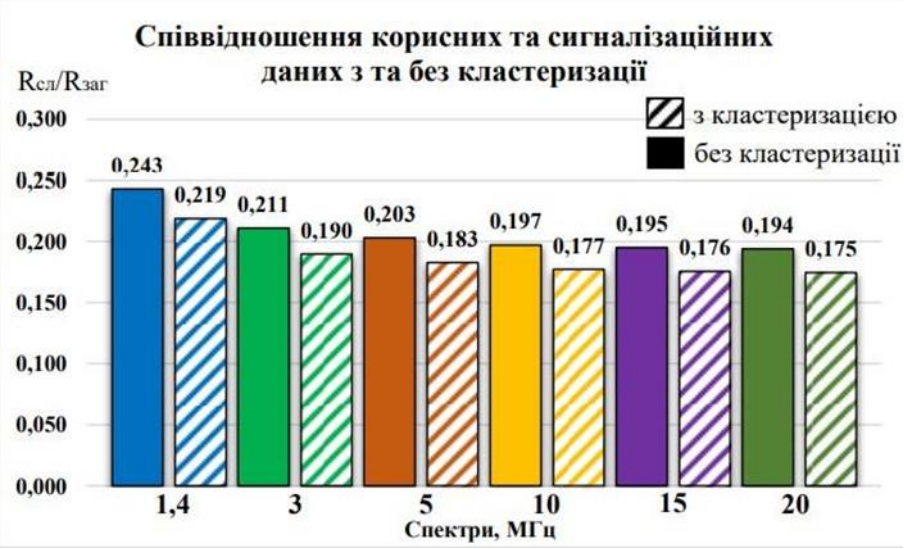


Рисунок 3.18 - Підвищення використання ресурсів за рахунок зменшення числа сигналізаційних даних

Можемо зробити висновок, використання M2M дозволяє розвантажити мережу у умовах високого рівня перевантаженості. Розвантаження мережі відбувається за рахунок двох основних факторів: сусіднього трафіку і зниження необхідної пропускної спроможності за рахунок агрегації каналів обслуговування керівником групи. Таким чином, можливо зробити висновок, що застосування технології M2M Wi-Fi Direct у стільникових мережах дозволяє завантажити мережу у середньому на 10%, а також збільшити середню спектральну ефективність на 6% за рахунок суміжного трафіку і агрегації сигнальних каналів.

ВИСНОВКИ

У роботі вивчені і визначені основні особливості мереж IoT. Аналізується функціонування гетерогенної мережі 4G / 5G і можливість надавання послуг зв'язку стільниковим користувачам або пристроям M2M / IoT з наскрізним якістю обслуговування.

У роботі представлені методи ефективного збору різнорідних даних бездротовою мережею Інтернету речей. Основна увага приділяється передачі високошвидкісних відеопотоків з підключених до LTE камер спостереження і низькошвидкісних сенсорних даних, зібраних з декількох пристроїв, підключених до технології NB-IoT. Розглядається аналітична модель для оцінки ефективності розподілу радіоресурсів. Модель дозволяє досліджувати особливості спільного використання ресурсів LTE і NB-IoT. Три альтернативні стратегії спільного використання ресурсів стільники LTE з підтримкою технології NB-IoT були оцінені на прикладі прикладного оператора спостереження, що реалізує систему моніторингу.

Чисельне дослідження показало, що стратегія STAT дуже чутлива до пропонованого навантаження і вимагає точної інформації про рівень вхідного навантаження. Також зображено, що стратегія DYN з повністю динамічним розподілом ресурсів досягає високої пропускної здатності системи, однак не може гарантувати необхідну надійність обслуговування. Запропонована стратегія динамічного розподілу ресурсів з резервуванням, DYNRES, задовольняє вимогам надійності, зберігаючи коефіцієнт використання ресурсів на високому рівні. Стратегія DYNRES рекомендується для майбутнього розгортання IT у стільникових мережах 5G, а запропонована аналітична модель може бути застосована для оцінки ефективності майбутніх рішень.

Пропонується вдосконалити архітектуру мережі LTE шляхом впровадження шлюзу, який взаємодіє з базовою станцією по каналу LTE і суперсілантірует на неї дані пристроїв M2M / IoT, перенаправляє головними вузлами з дочірніх вузлів по каналу Wi-Fi. Для оцінки ефективності методу кластеризації та використання Wi-

Fi Direct було проведено порівняння режимів роботи мережі з використанням і без використання кластеризації M2M. У ході дослідження було розглянуто, що використання M2M-кластеризації дозволяє розвантажити мережу у умовах високого рівня перевантаженості. Розвантаження мережі відбувається за рахунок двох основних факторів: суміжного трафіку і зниження необхідної пропускної спроможності за рахунок агрегування каналів обслуговування. Тому зроблено висновок, що застосування технології Wi-Fi Direct у якості основи для M2M / IWT у стільникових мережах дозволяє завантажити мережу у середньому на 10%, а також збільшити середню спектральну ефективність на 6% за рахунок суміжного трафіку і агрегації сигнальних каналів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Höller J. From machine-to-machine to the internet of things : introduction to a new age of intelligence / Jan Höller. – Amsterdam: Academic Press, 2014. – 330 с.
2. Центр керування M2M [Електроний ресурс]– Режим доступу: https://kyivstar.ua/uk/la/products/mobile/services/control/m2m (16.11.18)
3. F. Ghavimi and H. Chen, "M2M Communications in 3GPP LTE/LTE-A Networks: Architectures, Service Requirements, Challenges, and Applications," in IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 525-549, Secondquarter 2015, doi: 10.1109/COMST.2014.2361626.
4. J. Chen, K. Hu, Q. Wang, Y. Sun, Z. Shi and S. He, "Narrowband Internet of Things: Implementations and Applications," in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 2309-2314, Dec. 2017, doi: 10.1109/JIOT.2017.2764475.
5. Rekhissa HB, Belleudy C, Bessaguet P. Energy Efficient Resource Allocation for M2M Devices in LTE/LTE-A. Sensors. 2019; 19(24):5337. [Електроний ресурс]– Режим доступу: https://doi.org/10.3390/s19245337
6. M. Raza, M. Fiorani, A. Rostami, P. Öhlen, L. Wosinska, and P. Monti, "Dynamic Slicing Approach for Multi-Tenant 5G Transport Networks [Invited]," J. Opt. Commun. Netw. 10, A77-A90 (2018).
7. Che D., Safran M., Peng Z. From Big Data to Big Data Mining: Challenges, Issues, and Opportunities. In: Hong B., Meng X., Chen L., Winiwarter W., Song W. (eds) Database Systems for Advanced Applications. DASFAA 2013. Lecture Notes in Computer Science, vol 7827. Springer, Berlin, Heidelberg.
8. Kim, S. Effective crowdsensing and routing algorithms for next generation vehicular networks. Wireless Netw 25, 1815–1827 (2019).
9. Jung Y-A, Shin D, You Y-H. A Computationally Efficient Joint Cell Search and Frequency Synchronization Scheme for LTE Machine-Type Communications. Symmetry. 2019; 11(11):1394.
10. Alam, Tanweer, Blockchain and its Role in the Internet of Things (IoT) (June 30, 2019). Tanweer Alam. " Blockchain and its Role in the Internet of Things (IoT).", International Journal of Scientific Research in Computer Science, Engineering and Information Technology. Vol 5(1), 2019. DOI: 10.32628/CSEIT195137
11. Півнева, О. А. Проблеми безпеки екосистеми Інтернету речей (IoT) / О. А. Півнева, О. В. Мнушка // Синергетика, мехатроніка, телематика дорожніх машин і систем у навчальному процесі та науці : зб. наук. пр. за матеріалами II міжнар. наук.-практ. конф. – Харків : ХНАДУ, 2018. – С. 85–87.
12. Войтович О. П. Дослідження безпеки системи розумного будинку / О. П. Войтович, В. В. Вишньовський, К. В. Савченко // Тези доповідей Шостої Міжнародної науково-практичної конференції "Методи та засоби кодування, захисту й ущільнення інформації", Вінниця, 24-25 жовтня 2017 р. – Вінниця : ВНТУ, 2017. – С. 67-70.
13. Базилевич, В. М. Захищена система розумного будинку з використанням Internet of Things / В. М. Базилевич, М. В. Мальцева, Т. А. Петренко, Л. Г. Черниш // Технічні науки та технології. - 2020. - № 2 (20). - С. 218-228.

14. Belova, A., & Onischenko, V. (2019). МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РОЗУМНОГО БУДИНКУ. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 2(6), 134-141.

15. Сторожева Анастасия Андреевна. "Анализ угроз информационной безопасности системы "умный дом"" Научный журнал, no. 1 (35), 2019, pp. 39-41.

16. Лупенко С. А. Обгрунтування методів теорії телетрафіка для проектування систем управління заявками у комп'ютеризованих систмах обслуговування користувачів сервісних центрів / С. А. Лупенко, М. А. Побережний // Збірник тез доповідей VII Міжнародної науково-технічної конференції молодих учених та студентів „Актуальні задачі сучасних технологій", 28-29 листопада 2018 року. — Т. : ТНТУ, 2018. — Том 2. — С. 147. — (Комп'ютерно-інформаційні технології та системи зв'язку).

17. Дугінець Г. В. Концепція "Інтернет речей" у глобальному виробництві:досвід для України / Г. В. Дугінець // Економіка і регіон. - 2018. - № 1. - С. 127-133. - Режим доступу: http://nbuv.gov.ua/UJRN/econrig_2018_1_18.

18. Yatskiv, N., & Yatskiv, S. (2016). ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У МЕРЕЖІ ІНТЕРНЕТ РЕЧЕЙ. Науковий вісник НЛТУ України, 26(8), 381-387.

19. Хижняк, С. П. ., & Правило, В. В. . (2021). ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ. Збірник матеріалів Міжнародної науково-технічної конференції «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ», 143–145.

20. Gershenfeld, N., Krikorian, R., & Cohen, D. (2004). The Internet of Things. Scientific American, 291(4), 76-81.