МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Одарченко Р. С.
“_____”_____2021 р.

ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема: «Сучасні моделі обміну даних M2M, D2D, P2P»

Виконавець: _____ Бібін Д. О.
(підпис)

Керівник: _____ Бахтіяров Д. І.
(підпис)

Нормоконтролер: _____ Бахтіяров Д. І.
(підпис)

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»
(шифр, найменування)

ЗАТВЕРДЖУЮ
Завідувач кафедри

Одарченко Р. С.
“_____”_____2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

Бібіна Дмитра Олексійовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема дипломної роботи: «Сучасні моделі обміну даних M2M, D2D, P2P»
затверджена наказом ректора від «06» квітня 2021 р. №559 / ст
2. Термін виконання роботи: з 17.05.2021 р. по 20.06.2021 р.
3. Вихідні дані до роботи: моделі обміну даними P2P, D2D, M2M, топологія трафіку в мережі передавання даних за даними моделями.
4. Зміст пояснювальної записки: загальна характеристика моделей P2P, D2D, M2M, модель опосередкованого трафіку M2M.
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: реалізація моделі D2D, D2D-комутація, реалізація моделі M2M, реалізація потоку опосередкованого трафіку, узагальнена структурна схема системи спостереження і управління.

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів диплому	27.05.2021 - 30.05.2021	Виконано
2	Вступ	31.05.2021 - 02.06.2021	Виконано
3	ЗАГАЛЬНА ХАРАКТЕРИСТИКА МОДЕЛІ ПЕРЕДАЧІ ДАНИХ P2P	03.06.2021 - 06.06.2021	Виконано
4	ЗАГАЛЬНА ХАРАКТЕРИСТИКА МОДЕЛІ ПЕРЕДАЧІ ДАНИХ D2D	07.06. 2021 - 10.06. 2021	Виконано
5	ЗАГАЛЬНА ХАРАКТЕРИСТИКА МОДЕЛІ ПЕРЕДАЧІ ДАНИХ M2M	11.06. 2021- 14.06. 2021	Виконано
6	ІМІТАЦІЙНА МОДЕЛЬ СТАТИСТИЧНИХ ПОКАЗНИКІВ M2M ТРАФІКУ	14.06. 2021- 16.06. 2021	Виконано
7	Усунення недоліків дипломної роботи та захист	17.06. 2021- 21.06. 2021	Виконано

7. Дата видачі завдання: “14" травня 2021 р.

Керівник дипломної роботи _____ Бахтіяров Д.І.
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Бібін Д.І.
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Дипломна робота складається зі вступу, чотирьох розділів, загальних висновку, списку використаних джерел і має 56 сторінок основного тексту, 16 рисунків. Загальний обсяг роботи 58 сторінок.

Об'єкт дослідження: сучасні моделі обміну даних M2M, D2D, P2P.

Предмет дослідження: дослідження трафіку M2M та визначення його основних статистичних властивостей.

Метою дипломного проекту є дослідження сучасних моделей обміну даних M2M, D2D, P2P та дослідження трафіку M2M, його основних статистичних властивостей.

У першому розділі розглянуто загальні принципи побудови, аналіз, проблематику організації, протоколи і стандарти моделі передачі даних P2P.

У другому розділі розглянуто загальні принципи побудови, аналіз, проблематику організації, протоколи і стандарти моделі передачі даних D2D.

У третьотуму розділі розглянуто загальні принципи побудови, аналіз, проблематику організації, протоколи і стандарти моделі передачі даних M2M.

У четвертому розділі проведено аналіз трафіку моделі передачі даних M2M, виділено основні типи трафіку та змодельовано їх основні статистичні характеритики.

Ключові слова: ІНТЕРНЕТ РЕЧЕЙ, БЕЗПРОВІДНА МЕРЕЖА, M2M, D2D, P2P, ТРАФІК, ТОПОЛОГІЯ, СЕРВІСИ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

БС - базова станція

МС – мобільна станція

СО – система охорони

ЛМ - локальні мережі

ОС - операційна система

СПБ – система протипожежної безпеки

СМ – сенсорна мережа

ARP - Address Resolution Protocol (протокол визначення адрес)

LTE – Long-Term Evolution (глобальний стандарт передачі даних)

CDMA/CD - Carrier Sense Multiple Access with Collision Detection (множинний доступ з контролем несучої та виявленням колізій)

UDP - User Datagram Protocol (це один з найпростіших протоколів транспортного рівня моделі OSI, котрий виконує обмін повідомленнями (датаграмами) без підтвердження та гарантії доставки)

MFTP - Multisource File Transfer Protocol (мережевий протокол передачі файлів.)

TCP - Transmission Control Protocol (один з основних мережевих протоколів Інтернету, призначений для управління передачею даних в мережах і підмережах TCP/IP.)

ВСТУП

На сучасному етапі ровитку телекомунікаційних мереж дуже гостро посало питання, автономності, безпеки, та швидкості передачі даних. Саме тому в наш час винмклт нові моделі передачі даних M2M, D2D та P2P, які характеризуються високим рівнем автономності, технологічності та принципово новим підходом до архітектури мережі.

Дослідження даних моделей є пріоритетним завданням, адже забезпечить в подальшому стрімке впровадження даних технологій в глобальну телекомунікаційну мережу.

Разом з цим існує низка проблем, повзяних із імплементацією даних технологій в сучасну мережу. Також на даний момент ще не вирішені проблеми із забезпеченням безпеки та легалізації підключення.

Саме тому дослідження та глибокий аналіз даних технологій є першим кроком до їх подальшого впровадження на практиці.

У дипломній роботі розглядається тема «Сучасні моделі обміну даних M2M, D2D, P2P».

Метою дипломної роботи є аналіз сучасних моделей обміну даних M2M, D2D, P2P, визначення топології трафіку M2M та його основних статистичних показників.

Актуальність проекту полягає в тому, що на фоні стрімкого розвитку в області телекомунікацій, дослідження із подальшим впровадженням сучасних моделей обміну даних M2M, D2D та P2P дозволить вирішити проблему інформаційних потреб суспільства, які включають в себе необхідність в зв’язку і отриманні різноманітних інформаційних послуг.

РОЗДІЛ 1
ЗАГАЛЬНА ХАРАКТЕРИСТИКА МОДЕЛІ ПЕРЕДАЧІ ДАНИХ P2P

1.1. Аналіз технології P2P

P2P (Peer-to-peer) — варіант архітектури системи, в основі якої стоїть мережа рівноправних вузлів. Комп'ютерні мережі типу peer-to-peer (або P2P) засновані на принципі рівноправності учасників і характеризуються тим, що їх елементи можуть зв'язуватися між собою, на відміну від традиційної архітектури, коли лише окрема категорія учасників, яка називається серверами може надавати певні сервіси іншим [1].

У чистих тимчасових мережах немає концепції клієнта або сервера, тільки схожі вузли, які діють як клієнти і сервери по відношенню до інших вузлів в мережі. Ця модель взаємодії через мережу відрізняється від архітектури клієнт-сервер, в якій зв'язок відбувається тільки між клієнтом і центральним вузлом – сервером. Ця організація дозволяє підтримувати продуктивність мережі при будь-якій конфігурації клієнтського обладнання. Однак існує практика використання мереж P2P, в яких все ще є сервери, але їх роль більше не полягає в наданні послуг, а в збереженні інформації про послуги, що надаються мережевими клієнтами.

В P2P системі автономні вузли взаємодіють з іншими автономними вузлами. Вузли є автономними в тому сенсі, що не існує загальної влади, яка може контролювати їх. В результаті автономії вузлів, вони не можуть довіряти один одному та покладатися на поведінку інших вузлів, тому проблеми масштабування та надмірності стають важливішими ніж у випадку традиційної архітектури [1].

Сучасні P2P-мережі розвивалися завдяки ідеям, що пов'язані з обміном інформацією, які були створені в тому сенсі, що кожен вузол може надавати і отримувати ресурс, наданий іншим учасником.

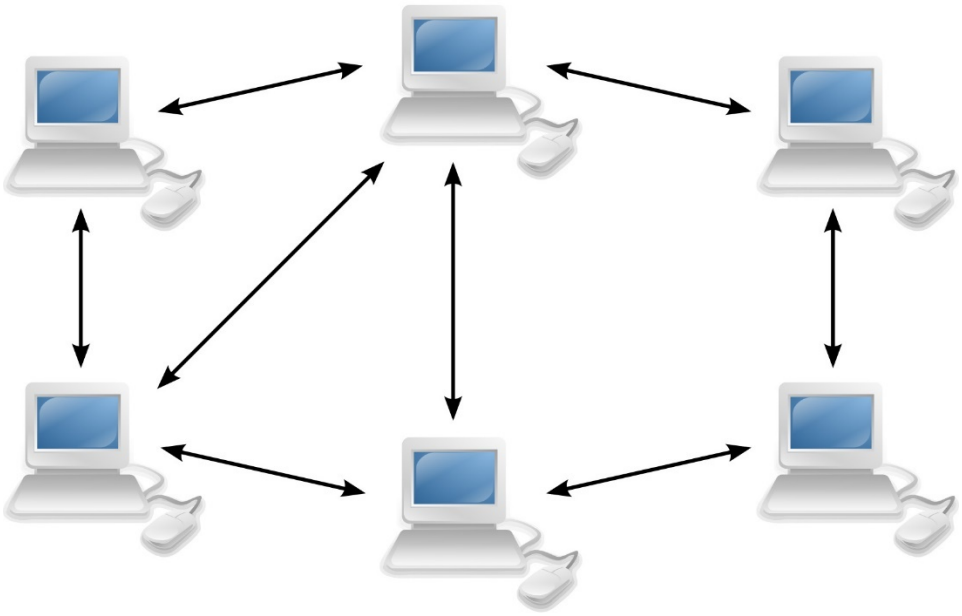

Рис. 1.1. Мережа типу P2P

Однорангові мережі першого покоління характеризуються наявністю виділених центральних вузлів, які можуть, наприклад, виконувати завдання координації баз даних і пошуку. Однак архітектура таких мереж дозволяє здійснювати пряму комунікацію і передачу інформації між будь-яким з її учасників.

Друге покоління тимчасових мереж характеризується відсутністю центральних серверів і, в той же час, фундаментальною можливістю пошуку серед її учасників. Однак алгоритми пошуку в мережах 2-го покоління характеризувалися «хвилеподібним» поширенням запитів та мали низьку ефективність.

Найкращими прикладами є Gnutella, Kazaa або Emule з Kademlia, серед яких лише Kazaa ще має центральний сервер для реєстрації. eDonkey2000/Overnet, Gnutella, FastTrack і Ares Galaxy мають приблизно 10.3 мільйонів користувачів (на квітень 2016 року, згідно зі slyck.com) [2].

Третє покоління P2P-мереж характеризується децентралізованою структурою і принципово новими алгоритмами пошуку, заснованими на ключовій концепції розподілених хеш-таблиць, підтримуваних учасниками мережі.

DHT допомагають вирішити проблему масштабування, вибираючи окремі вузли певних хеш-функцій, що дозволяє використовувати будь-який файл в мережі і він може бути знайдений швидко і ефективно.

Приклад анонімних мереж — Freenet, I2P, ANts P2P, RShare, GNUnet і Entropy. Також прикладом децентралізованої мережі є система анонімної цифрової грошової одиниці BitCoin. Певна ступінь анонімності реалізовується шляхом направлення даних через інших вузли. Це робить важкою ідентифікацію того, хто завантажує або хто пропонує файли [2]. Більшість цих програм володіють вбудованим шифруванням.

Проміжні реалізації цього типу мережі вимагають декількох ресурсів для забезпечення анонімності, що робить їх повільними або важкими у використанні. Однак в країнах з дуже швидким доступом в Інтернет, таких як Японія, анонімні мережі обміну файлами вже стали дуже популярними.

1.2. Поблематика організації зв'язку мережі P2P

У моделі стека мережевих протоколів TCP / IP протоколи P2P відносяться до прикладного рівня. Таким чином, P2P-мережа є накладеною (overlay), що функціонує поверх Інтернету і використовує існуючі транспортні протоколи TCP або UDP.

Клієнтська програма P2P, або просто "клієнт", - програма, що забезпечує функціональність вузла, вона сама є реалізацією лежить в основі мережі P2P-протокола. Клієнт може запитувати сервер або виділені вузли, отримувати відповідь з інформацією про запитані файлах, вузлах, на яких ці файли знаходяться, і далі вже працювати безпосередньо з зазначеними вузлами [2]. Останні реалізації клієнтів наділені повноваженнями обміну службовою інформацією, побудови запитів і пошуку ресурсів у всій мережі без участі серверів.

Node ID - це унікальний визначник вузла, він обчислюється з використанням хеш-функції з IP-адрес і супутньої інформації (Host ID, MAC і т. д.) І призначається при реєстрації в P2P мережі. Ідентифікатор або ключ ресурсу - унікальний ID файлу чи іншого ресурсу, що обчислюється на основі імені файлу і його вмісту за допомогою хеш-функції.

Всі вузли, зареєстровані в мережі протоколу (або на деяких обраних вузлах і / або серверах), разом з ідентифікаторами вузлів, що публікують цей ресурс, забезпечують рівномірний розподіл ключів ресурсів. Завдання пошуку ресурсу зводиться до пошуку ідентифікатора вузла, що зберігає його ключ.

Велике зростання популярності мереж P2P обумовлений привабливістю характеристик даної технології - це децентралізація, розподіленість, самоорганізація мережі. Окреслені принципи **забезпечують такі переваги**, як простота і дешевизна реалізації та підтримки роботи мережі, її відмовостійкість і масштабованість, збільшення швидкості копіювання і колосальна потужність мережі в цілому [2].

Bittorrent, eDonkey2000, Gnutella2, Gnutella – найпоширеніші мережі з великою кількістю подібних вузлів.

BitTorrent. Для ініціалізації вузла в мережі BitTorrent (www.bittorrent.com) клієнт застосовує трекер, який надає інформацію про файли, доступні для копіювання, а також мережеві вузли та надає статистичну інформацію про маршрути. Навіть після ініціалізації сервер «допомагає» вузлам взаємодіяти один з одним, хоча на останніх версій клієнтських програм потрібно сервер тільки на ранній стадії.

При опублікуванні файлу вузлом, програма розбиває цей файл на частини і торрент-файл, що містить інформацією про частини файлу, їх розташування і сервер (необов'язково). Цей файл буде підтримувати поширення. Перший сайт, на якому публікується файл, називається «Сід», а вузол, що копіює файл стає розповсюджувачем за принципом: «чим більше я копіюю, тим більше я дозволяю вам копіювати від мене». Вузли копіюють весь файл і стають розповсюджувачами цього файлу і разом з вузлами повністю переміщують файли, дозволяючи іншим вузлам отримувати частини файлу з декількох джерел, що прискорює копіювання.

Вже згадана мережа використовує протоколи BitTorrent і BitTorrent azyrus DHT. Останній заснований на модифікованому протоколі Kademlia і використовується для роботи з файлами метаданих, що не є прив'язаними до серверів, для присвоєння ідентифікаторів і коментарів, а також рейтингових ресурсів для децентралізованого пошуку ресурсів. Замість мережі BitTorrent Azureus для DTH, деякі клієнти з підтримкою протоколу BitTorrent використовують магістраль DHT.

Найпоширенішими є клієнти Azureus, торрент трекер, bitspirit, BitComet, mldonkey.

Gnutella-одна з перших тимчасових мереж, створена в 2000 році. З - за серйозних недоліків алгоритму користувач не може використовувати мережу Gnutella2 (хоча вона все ще працює). www.gnutella2.com). При підключенні клієнт отримує від вузла, з яким йому вдалося підключитися, список з п'яти активних вузлів; на них відправляється запит за ключовим словом. Вузли шукають ресурси за запитом і, якщо не знаходять їх, відправляють запит активним вузлам "дерева" (структура графа типу "дерево" в топології мережі) або перевищив максимальну кількість кроків. Цей пошук називається потоком запитів.

Зрозуміло, що така реалізація призводить до швидкого збільшення кількості запитів і, відповідно, може статися відмова в обслуговуванні на верхніх рівнях "дерева", що неодноразово спостерігалося на практиці. Розробники вдосконалили алгоритм, ввели правила, згідно з якими запити "дерево" можна відправляти тільки декільком вузлам - так званим обраним (ультраперсам), інші вузли (листя) можуть робити тільки наступні запити. Це також введена система кешованих вузлів.

У такому вигляді мережа залишається активною і сьогодні, хоча її популярність знизилася через недоліки алгоритму та слабку масштабованість.

Недоліки «Гутелли» перешкодили розробці нових алгоритмів, які по суті шукають маршрути та ресурси, і призвели до створення набору протоколів DHT (розподілених хеш-таблиць) - конкретно протоколу Chemedia, які широко використовуються в мережах.

У мережі Gnutella запити надсилаються через TCP або UDP, файли копіюються через HTTP. Нещодавно були надані розширення для клієнтських програм, які дозволяють копіювати файли в UDP, щоб робити XML-запити на метаінформацію про файл.

У 2003 р був створений принципово новий протокол Gnutella2 і перші клієнти, які були зворотносумісними з клієнтами Gnutella. Відповідно до нього деякі вузли стають концентраторами, інші ж є звичайними вузлами (leaves). Кожен звичайний вузол має з'єднання з одним-двома концентраторами. А концентратор пов'язаний з

сотнями звичайних вузлів і десятками інших концентраторів. Кожен вузол періодично пересилає концентратора список ідентифікаторів ключових слів, за якими можна знайти публікуються даними вузлом ресурси. Ідентифікатори зберігаються в загальній таблиці на концентраторі [2]. Коли вузол "хоче" знайти ресурс, він надсилає запит ключового слова до свого центру, знаходить ресурс у своїй таблиці та повертає ідентифікатор вузла, який є власником ресурсу, або перераховує будь-які інші концентратори, що просять цю кнопку знову навмання. Цей пошук називається випадковим «пошуком прогулянки».

Примітною особливістю мережі Gnutella2 є її здатність відтворювати інформацію про зображення в мережі для копіювання самого файлу, що дуже корисно при відстеженні вірусів. Пакети, що передаються в мережу, розробляються у власному форматі, подібному до XML, який гнучко покращує функціональність мережі, додаючи додаткову службову інформацію. Запити та списки ID ключових слів пересилаються на концентратори по UDP. Перелік найбільш поширених клієнтських програм для Gnutella і Gnutella2: Shareaza, Kiwi, Alpha, Morpheus, Gnucleus, Adagio Pocket G2 (Windows Pocket PC), FileScope, iMesh, MLDonkey [2].

Мережа EDonkey2000 (www.edonkey.com) з’явилася у 2000 році. Інформація про наявність у ньому файлів публікується клієнтами з використанням унікального ідентифікатора ресурсу у вигляді посилань ed2k на декількох серверах. Серверне програмне забезпечення доступне для встановлення будь-яким користувачем. Сервери надають кнопки пошуку та інформацію. В даний час у мережі є 200 серверів, які одночасно обслуговують близько одного мільйона клієнтів, спільно використовуючи близько мільярда окремих файлів. Загальна кількість зареєстрованих користувачів цієї мережі становить близько 10 мільйонів. Коли мережевий клієнт EDONkey2000 копіює бажаний ресурс, він виконує одночасно з декількох джерел, використовуючи MFTP (протокол передачі файлів з декількох джерел).

Тепер інформацію про доступні файли можна отримати не лише із сервера EDONkey. З 2004 року мережа EDONkey2000 інтегрувала Overnet - повністю

децентралізовану мережу, яка дозволяє здійснювати зв'язок між вузлами без" прив'язки "до серверів, що використовують протокол DHT Kademlia.

Найпопулярнішим клієнтом із закритим кодом (про версія - платний) для мережі EDonkey2000 є програма eDonkey, але вона також має клієнт з відкритим кодом - eMule, крім мережі EDonkey2000, інші мережі P2P - Kad Network (Kademlia) можуть використовувати [2]. Клієнт eDonkey має дуже цікаве розширення, яке дозволяє копіювати високонадійні метадані .torrent, а також забезпечувати перевірку від інших користувачів. Він працює з файлами у вашій власній мережі. У цьому випадку, якщо ви Завантажте файл, який відповідає метаданим, частини файлу, доступні у вашій власній мережі EDONkey2000, також включені до списку джерел для завантаження.

Інтеграція різних можливостей мережі та додаткова перевірка сприяли розвитку мережі EDonkey2000. Користувачі інших мереж почали переходити на неї - наприклад, мережа FastTrace, яка базується на протоколі FastTrace, спеціально реалізується такими популярними клієнтами, як Kaja.

Direct Connect. Розглянемо ще одну мережу – Direct Connect (dcplusplus.sourceforge.net), яка дуже популярна в країнах СНД. Справа в тому, що постачальники мережевих послуг - наприклад, оператори будинкових мереж в Києві, а також мережеві адміністратори компаній до недавнього часу намагалися блокувати на своїх міжмережевих екранах порти, через які спілкуються клієнти мереж Bittorrent, EDonkey2000, Gnutella, Fasttreck, а в тих же випадках, коли екран не допомагав, боролися адміністративними методами [2]. Перешкодами на шляху широкого використання мереж P2P також були велика вартість трафіку і / або дефіцит смуги пропускання каналів.

У цьому питанні у людей є тільки можливість створити локальну однорангову мережу. Технологія прямого підключення виявилася найбільш зручною для цього. У цій мережі клієнт підключається до одного або декількох серверів для пошуку файлів, а сервери не мають підключення. Інформація про кнопку "хочу" для відкриття файлу відправляється на сервер. Файл копіюється безпосередньо між вузлами, як в P2P-мережі.

Клієнт має вбудовану можливість для членів мережі спілкуватися один з одним, список кожного користувача файлу може бути отриманий у вигляді дерева папок, простий механізм для можливості пошуку інформації та копіювання всієї папки. Це зробило технологію прямого підключення – це рішення для P2P-мережі.

1.3. Потоколи і стандарти P2P

Починаючи з версії 4.2.0 офіційного додатка Bitotent, він реалізує функцію операції без слідів на основі протоколу Kadelia. У таких системах трекери доступні децентралізовано у вигляді розподілених хеш-таблиць для клієнтів, які приєднуються до мережі.

У моделі стеку мережевих протоколів TCP / IP протоколи P2P належать до рівня додатків. Отже, мережа P2P - це накладена мережа, яка працює через Інтернет і використовує існуючі транспортні протоколи TCP або UDP.

Мережа Kadelia DHT P2P має такі характеристики. Мережа, здатна підтримувати до 16 вузлів та 16 ресурсів, об’єднаних 7 вузлами, що спільно використовують 12 ресурсів. Вузлам присвоюються відповідні ідентифікатори, а ресурсам - ключі. Другий, з адресами вузлів, що їх публікують, рівномірно розподілений між вузлами мережі.

Припустимо, вузол з ідентифікатором 0 "хоче" знайти ресурс, відповідний ключу 14, для якого він надсилає запит на пошук. Запит проходить певну маршрутизацію і надходить на вузол, що містить ключ 14. Далі, вузол ID 14 перенаправляється на вузол ID 0, відповідний ключу ресурсу 14, який звертається до всіх вузлів.

Під час підключення клієнт отримує список з п’яти активних вузлів від вузла, до якого він може підключитися; їм надсилаються запити пошуку ресурсів ключових слів. Вузли пошуку ресурсів відповідають запиту, і якщо вони не знайдені, переадресуйте запит до "дерева" (графічна топологія "дерева") активним вузлам, якщо ресурс не знайдено або не перевищено максимальну кількість фаз . Такий пошук називається запитом про «затоплення».

ВИСНОВКИ ДО РОЗДІЛУ 1

Зрозуміло, що така реалізація призводить до експоненціального збільшення кількості запитів і, отже, може призвести до відмови в обслуговуванні на більш високих рівнях "дерева", що спостерігалося неодноразово. Розробники вдосконалили алгоритм, запровадивши правила, згідно з якими запити "дерева" можуть надсилатися лише до кількох вузлів - те, що називається ультраперсом, для решти (листя) можуть знадобитися лише останні кнопки. Також була введена система кешованих вузлів.

Недоліки протоколу Gnutella призвели до розробки нових алгоритмів, які, по суті, здійснюють пошук маршрутів і ресурсів, і призводять до створення набору протоколів DHT (розподілена хеш-таблиця) - зокрема, протоколу Kadelia, який зараз широко відомий і використовується майже у всіх мережі.

Коли мережевий клієнт Adonkey 2000 копіює бажаний ресурс, він виконується одночасно з декількох джерел за протоколом передачі файлів MFTP.

РОЗДІЛ 2
ЗАГАЛЬНА ХАРАКТЕРИСТИКА МОДЕЛІ ПЕРЕДАЧІ ДАНИХ D2D

2.1 Аналіз технології D2D

D2D (Device-to-Device) - технологія, в основі якої лежить використання стандартного протоколу бездротового зв'язку, яка дозволяє мобільним пристроям (смартфонам, планшетам, та ін.) зв'язуватися безпосередньо один з одним, минаючи маршрутизацію, що виключає необхідність у базових станціях і точках доступу [3].

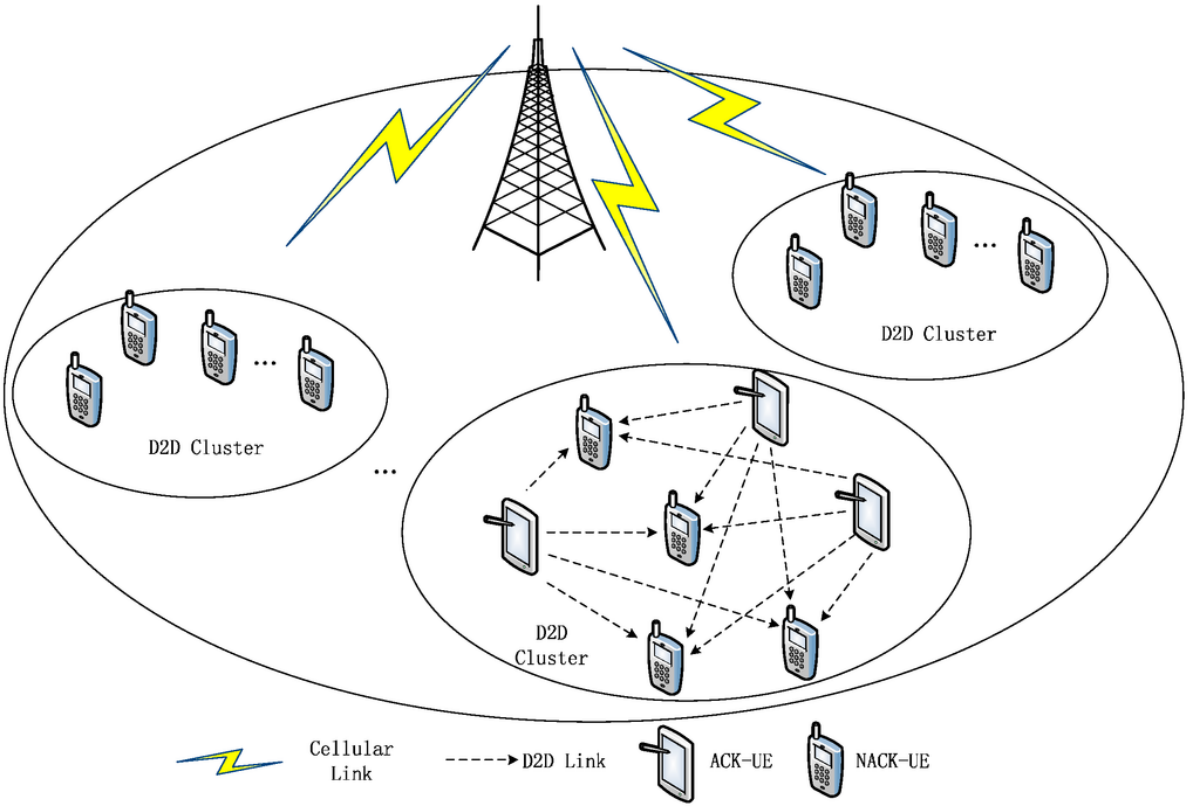

Рис. 2.1. Реалізація моделі D2D

D2D - перспективна технологія поверх LTE. Ця технологія може бути використана при виявленні в зоні доступності бездротового зв'язку мобільних пристроїв і застосовується для соціальних програм, реклами, місцевого обміну інформацією, смарт-зв'язку між транспортними засобами, підтримки громадської

безпеки, коли мобільні пристрої забезпечують підключення до локальної мережі навіть у разі пошкодження існуючої мережі інфраструктури і т.д. (Рис.1) Технологія D2D дозволяє зменшити час очікування встановлення зв'язку між абонентами бездротової мережі, збільшити швидкість передачі даних і знизити енергоспоживання.

З появою додатків, що використовують великі обсяги переданих даних, таких як сервіси на основі близького взаємного розташування, оператори зв'язку стикаються з постійно зростаючими запитами користувачів. І хоча мережеві технології четвертого покоління, в тому числі LTE (Long Term Evolution), мають вкрай високою ефективністю як на фізичному, так і на MAC-рівні (Media Access Control Layer), вони не можуть впоратися з темпами зростання потреб користувачів. Основною метою все більшого числа досліджень в галузі телекомунікацій стає розробка нового підходу, який дозволив би кардинально змінити методи взаємодії пристроїв в мережах стільникового зв'язку. Одним з таких підходів є встановлення прямих з'єднань між пристроями (D2D, Device-to-Device Communications), при яких передача даних, на відміну від традиційної архітектури, здійснюється без участі базової станції і опорної мережі. Завдяки цьому знижується навантаження на базову станцію а також підвищується ефективність розподілу частотного ресурсу. ще одним перевагою такого типу сполук є можливість організації за допомогою LTE-пристроїв, що підтримують технологію D2D, мереж громадської безпеки, що функціонують там, де стільниковий зв'язок недоступний.

Технологія D2D (пристрій-пристрій) дозволяє пристроям спілкуватися між собою. Але телефони, планшети і тд. вже можуть встановлювати зєднання за допомогою Bluetooth, Wi-Fi і NFC. Однак вони не можуть тримати з'єднання на відстані 500 метрів. Уявімо, скільки пристроїв можна виявити в радіусі 500 метрів. Ви можете з'єднатися з тисячами пристроїв [3].

У цій технології великий потенціал, і поки складно точно передбачити, яку зі сфер нашого життя вона переверне. З одного боку, D2D дозволить вам ділитися інформацією, минаючи оператора стільникового зв'язку. Це дозволить створювати мережі для передачі даних в разі надзвичайних ситуацій. Зрештою, D2D може бути

корисна для бізнесу, з'явиться новий спосіб розповісти про свій бізнес людям неподалік, а інші в свою чергу можуть простіше знайти потрібне їм місце.

Технологія зв'язку між пристроями (device-to-device communications, D2D) вважають по справжньому революційною. Сьогодні, на жаль, мобільні телефони не можуть бути безпосередньо пов'язані один з одним, але технологія D2D розроблена для відправки листів, фотографій або відео друзям, які знаходяться неподалік, за допомогою Bluetooth з низьким енергоспоживанням або Wi-Fi Direct, а не через вишку мобільної мережі. Ймовірно, в довгостроковій перспективі такі базові станції нам будуть просто не потрібні. Для багатьох хто піклується про своє здоров'я людей - це серйозний привід для радості.

D2D є однією з функцій LTE Advanced (більше відома як стандарт зв'язку 4G), який дозволяє обмінюватися інформацією між додатками на пристроях. Основною перевагою цієї технології є зона покриття, яка легко може досягати 500 метрів, тільки уявіть собі, яка кількість гаджетів можна охопити на такій відстані. Завдяки цій технології телефони можуть «говорити» прямо з іншими пристроями і обмінюватися інформацією з маячками [3].

Рис. 2.2. Практична реалізація технології D2D

Нова можливість, яка додається до протокола LTE, допускає можливість зв'язку між двома абонентами в обхід базових станцій. Телефони зможуть «говорити» безпосередньо з іншими мобільними пристроями і обмінюватися інформацією з маячками, розташованими в магазинах та інших підприємствах торгівлі.

Як відомо D2D - ця бездротова технологія має радіус дії 500 метрів, що набагато більше набули широкого поширення Wi-Fi і Bluetooth. Вона включена в оновлення стандарту LTE, яке буде прийнято в цьому році.

Серед інших варіантів застосування, технологія D2D тестується на можливість використання для автоматичного виявлення знаходження поруч людей, організацій та іншої інформації відповідно до заданих критеріїв. Деякі бачать в технології новий перспективний канал для реклами.

Незважаючи на чималу робочу дистанцію D2D споживає відносно малу кількість енергії, тому телефон може постійно відслідковувати пристрої, що знаходяться поруч, без особливого збитку для заряда мобільного акумулятора. Пристрій з включеним режимом D2D зможе виявляти інші телефони, використовуючи технологію або обмінюючись інформацією з маячками - стаціонарними пристроями, встановленими на території організацій або які є частиною інфраструктури аеропортів або залізничних вокзалів.

Маячки, що використовують D2D зможуть передавати корисну інформацію, а також, наприклад, спеціальні пропозиції. Такий пристрій, вмонтований у стійку реєстрації, зможе проінформувати людей, які знаходяться, що купили квиток на рейс, що затримується рейс.

D2D також покликана згладити збої в мережі, які трапляються при напливі абонентів, які намагаються підключитися до однієї і тієї ж базової станції. На даний час розробляється систему, яка дозволить використовувати D2D для обслуговування мільйонів людей, що знаходяться на в центральній частині міста під час культурно-масових заходів та свят.

В теорії, D2D зможе використовуватися для створення комунікаційних додатків, які перенаправляють інформацію від пристрою до пристрою. Деякі месенджери вже можуть використовувати Wi-Fi або Bluetooth для зв'язку з

абонентами, що знаходяться поруч. Але D2D зможе збільшити робочий радіус і розширити можливості таких додатків. Однак, оператори зв'язку зможуть відстежувати, який із пристроїв в їх мережі може використовувати D2D, тому що ця технологія використовує той же радіочастотний діапазон, що і звичайні стільникові канали зв'язку. Таким чином Оператори зможуть навіть отримати нове джерело доходу, обслуговуючи компанії, які хочуть пропонувати сервіси або функції, які залежать нову технологію.

Радіус дії технології розцінюють в 500 метрів, для передачі даних будуть використовуватися ті-ж частоти що і в оператора, тому в деяких випадках він зможе контролювати роботу послуги, що до речі дасть можливість використовувати її як нове джерело доходу. В принципі, використовуючи прямий зв'язок між сусідніми мобільними пристроями дозволить поліпшити використання спектра, загальну пропускну здатність і ефективність використання енергії. D2D з підтримкою LTE пристрої мають потенціал, щоб стати конкурентоспроможними для резервних мереж громадської безпеки, які повинні функціонувати, коли стільникові мережі не доступні або зазнають невдачі.

D2D мобільні користуються набагато вищі швидкості передачі даних, ніж звичайні стільникові мобільні телефони через малої дальності зв'язку. Стільникові мобільні телефони можуть також скористатися D2D, як D2D може допомогти розвантажити трафік від перевантажених мереж стільникового зв'язку.

За словами розробників, в разі розвитку даної технології, в перспективі можна буде повністю відмовитися від стільникових веж в мегаполісах і густонаселених містах. Рівномірно розмістивши по території населеного пункту ретранслятори, можна добитися не тільки поліпшення рівня сигналу, а й створити сервіс для відправки інформаційних повідомлень в радіусі дії LTE Direct.

Наприклад, проходячи повз ресторанно-готельного комплексу, можна буде отримати повідомлення про кількість вільних номерів і діючі знижки, а також дізнатися про концертній програмі, запланованої на вечір в банкетному залі ресторану.

Специфікація LTE Advanced передбачає з періодом 20 секунд невеликі тимчасові слоти тривалістю 64 мс для огляду оточення апарату. Тому такі накладні витрати не дуже великі для терміналів. Але це дозволяє заощадити потужність батареї на відмову від передачі даних з «хмарних» серверів.

Переваги D2D комунікацій

Прямий зв'язок між пристроями може забезпечити ряд переваг для користувачів в різних додатках, де пристрої знаходяться в безпосередній близькості:

- Швидкість передачі даних: Пристрої можуть бути віддалені від стільникової мережі, а отже, будуть не в змозі підтримувати високу швидкість передачі даних, яка може знадобитися.

- Надійний зв'язок. D2D може забезпечити високу надійність зв'язку навіть в при зникненні стільникової мережі наприклад в результаті стихійного лиха.

- Обмін миттєвими повідомленнями: у міру того як D2D зв'язок не залежить від мережевої інфраструктури пристрої можуть бути використані для миттєвого зв'язку між безліччю пристроїв. Це особливо відноситься до двостороннього зв'язку тобто можуть бути використані аварійно-рятувальними службами.

- Використання ліцензованого спектру: на відміну від Wi-Fi, Bluetooth і т.д., D2D використовує ліцензований спектр, тобто частоти, які використовуватися в меншій мірі схильні до появи перешкод, дозволяючи тим самим більш надійний зв'язок.

- Зниження перешкод: не здійснюючи безпосередній зв'язок з базовою станцією, здійснює менше запитів і це впливає на обсяг даних, переданих в межах заданого розподілу спектра. Це зменшує загальний рівень перешкод.

- Економія енергії: Використання D2D для зв'язку між пристроями забезпечує економію енергії по цілому ряду причин. Одним з найважливіших напрямків є те, що якщо пристрої знаходяться в безпосередній близькості, то потрібен набагато нижчий рівень потужності передачі.

Очевидно, що D2D є перспективною технологією і, таким чином, відкриває широкі можливості для операторів стільникового зв'язку. Проте, D2D зв'язок також є складним в тому, що багато технічних проблем повинні бути вирішені перш, ніж вона

могла б бути широко прийняті, такі як якість обслуговування (QoS) гарантії, управління перешкод, розподілу каналів, налаштування сеансу зв'язку і управління, модернізація існуючих інфраструктур, економічна модель ціноутворення і т.д.

Таким чином, спілкування з D2D суспільної свідомості є цікавим ще в значній мірі невикористаними область, яка вимагає інтенсивних дослідницьких зусиль як з боку наукових кіл так і промисловості.

2.2. Проблематика огранізації звязку D2D

В ситуаціях коли користувачі знаходяться близько один від одного, в тому числі коли інформація достатньо специфічна для конкретного місця її використання(наприклад у випадку різноманітних служб близького радіусу дії, коли користувач взаємодіє і обмін.ється інформацією зі своїм безпосереднім оточенням) целесообразно виконувати обмін данними по протоколу D2D, аніж шляхом інфраструктури мережі. Під управлінням мережевого протоколу власне протокол D2D забезпечує локальним службам надійність класу оператора зв’язку оскільки сама мережа може керувати D2D-трафіком. Більше того, D2D-пртокол дозволяє використовувати локальну мережу навіть в разі пошкодження мережевої інфраструктури.

D2D комунікації дозволяють пристроям зв’язуватись між собою без маршурутизаціїї даних через мережеву інфрастурктруру. Можливі сценаріїї застосування D2D включають, серед іншого, локальні послуги, коли D2D пристрої, виявляючи близість, взаємодіють між собою [3-4].

До числа таких послуг належать соціальні додатки, реалізація яких викликана близькістю викликуваного користувача, реклами, місцевого обміну інформацією. Інша додатки включають в себе підтримку інформаційної безпеки, коли D2D-пристрої забезпечують підключення до локальної мережі.

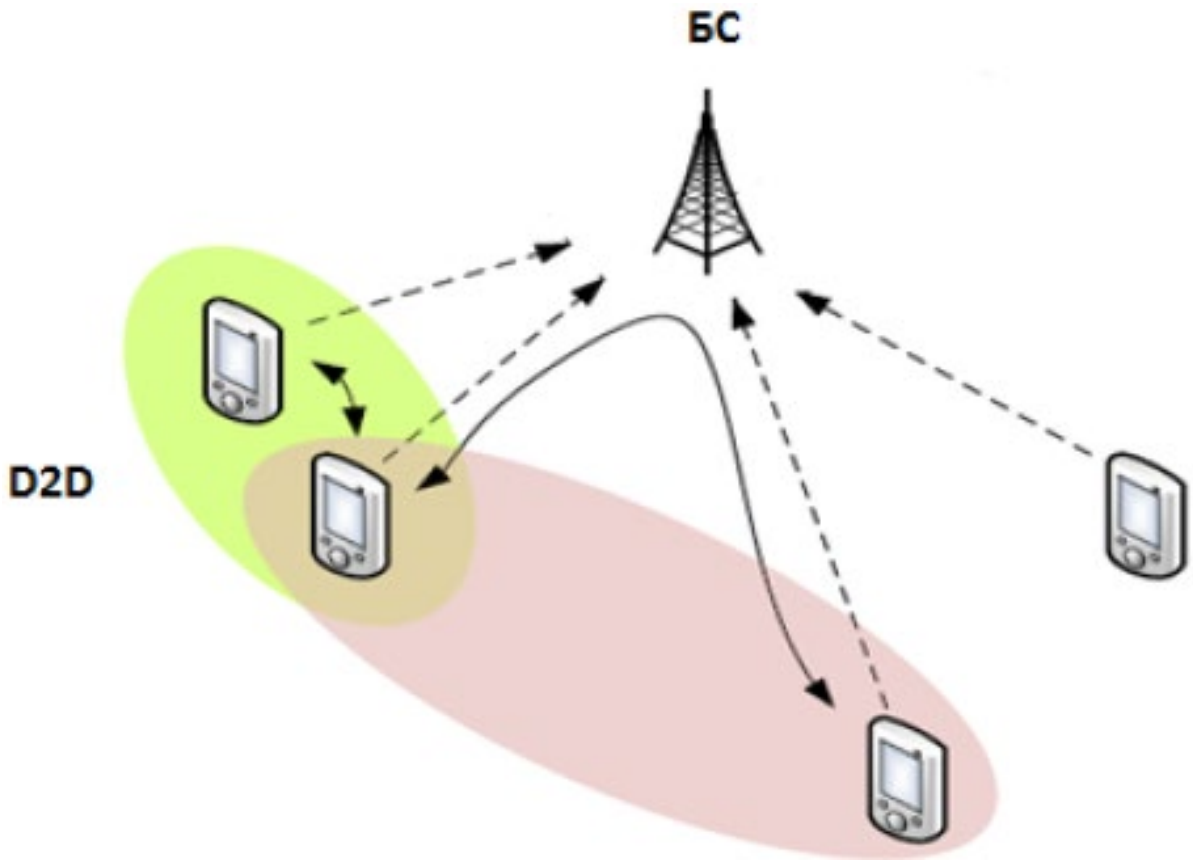

Рис. 2.3. D2D-комутація

D2D- комунікації повинні дати можливість користувачам відчути переваги надщільної мережевої архітектури з точки зору зменшення тривалості затримок, збільшення швидкості передачі даних і скорочення витрат електроенергії. D2D–комунцікація дозволяє вирішувати також такі нові завдання в області проектування та безпеки, керування мобільністю та безпекою. Крім того успіх цієї технології в значній мірі залежить від сценаріїв, в яких користувачі які перебувають у безпосередній близості між собою спілкуються , а також від додатків які будуть розроблені найближчим часом.

Пристрої взаємодіють із базовою станцією через ретрансляцію інформації за допомогою інших пристроїв.Таким чином можливе досягнення виокого рівня QoS. Взаємодія пристрою із ретранслятором характеризується встановленням повного або частокового зєднання.

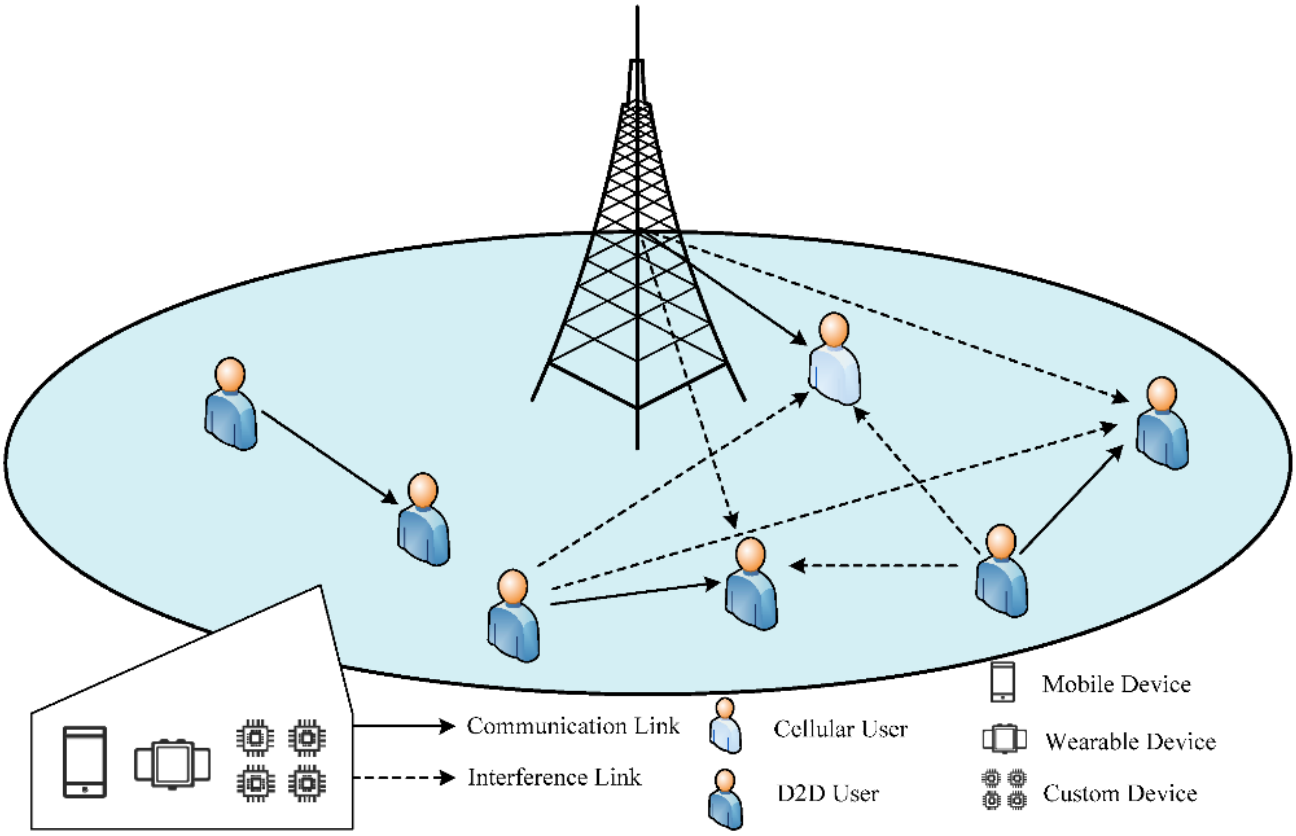

Рис. 2.4. Взаємодія пристроїв із базовою станцією через ретрансляцію інформації за допомогою інших пристроїв

Другий тип пристроїв рівня комутації - пристрої DC-OC (Direct D2D communication with operator controlled link established). Має місце пряма взаємодія D2D-пристроїв, при якій обмін інформацією між джерелом і адресатом може здійснюватись без участі базової станції, але їх взаємодія контролюється оператором [3].

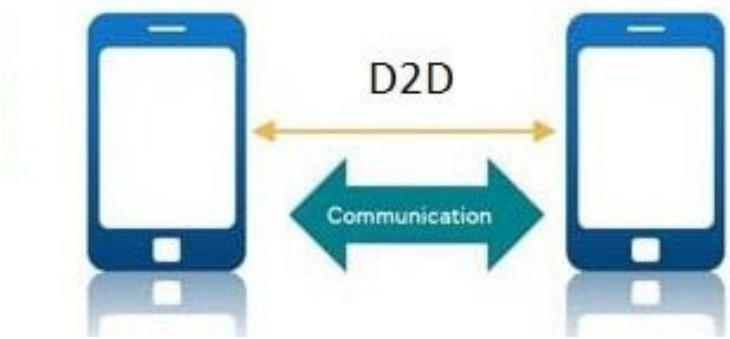

Рис. 2.5. Пряма взаємодія D2D-пристроїв

Третій тип пристроїв рівня комунікації DR-DC. Пристрої джерела та адресата несуть відповідальність за координацію взаємодії з використання ретрансляторів, при цьому оператор не бере учать у процесі встановлення взаємодії.

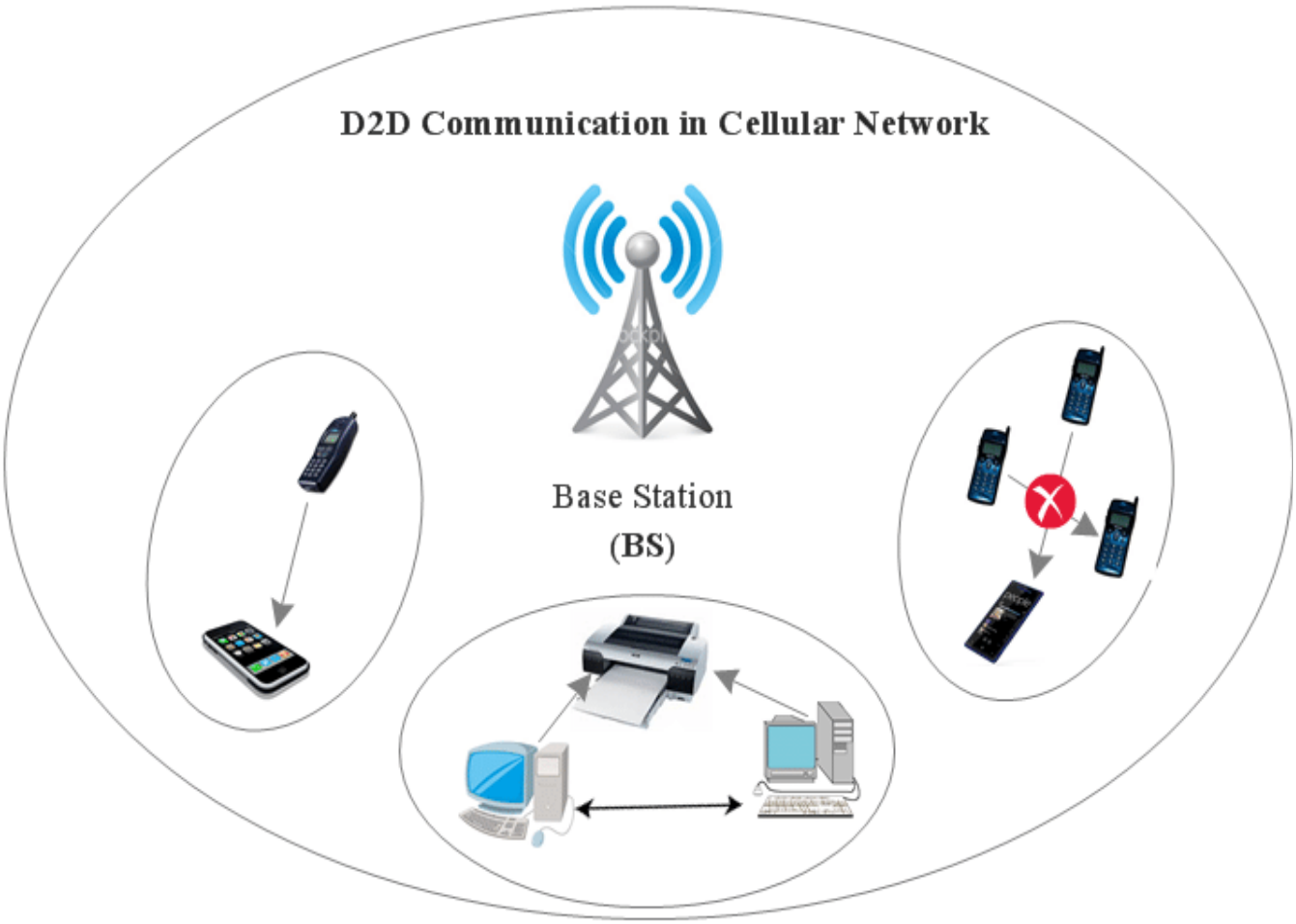

Рис. 2.6. Взаємодія джерела сигналу і адресата через пристрої ретрансляції [3]

Четвертий тип пристроїв рівня комутації – пристрої DC-DC. В цьому випадку пристрої джерела і споживача мають прямий зв'язок один з одним без будь якого контролю зі сторони оператора. Це означає що пристрої джерела ресурсу і призначення повинні використовувати ресурс таким чином щоб забезпечитиобмежений рівень завад для пристроїв одного ж і того самого макрорівня.

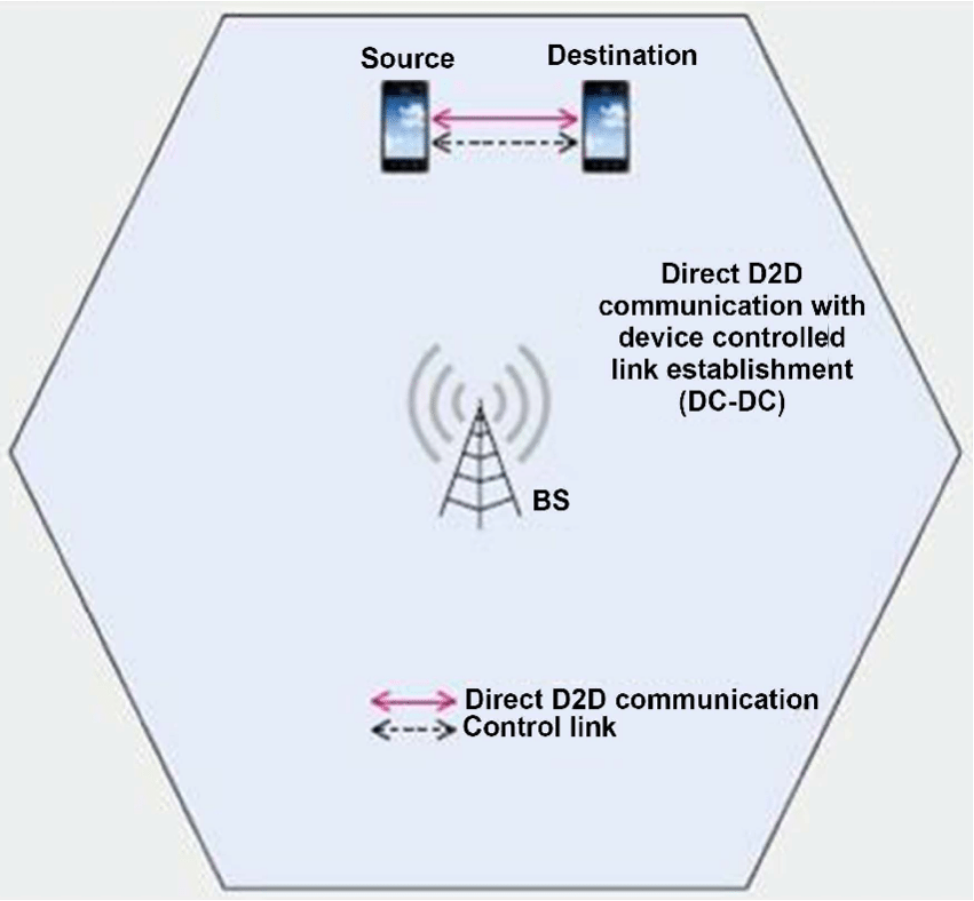

Рис. 2.7. Пряма взаємодія D2D-пристроїв по типу DC-DC

Однак при будь якому із типів взаємодії вагомою проблемою – є проблема безпеки, яка може бути вирішена через список «довірених» пристроїв.

2.3. Потоколи і стандарти D2D

Сьогодні основними бездротовими інтерфейсами для підключення різноманітних пристроїв до Мережі є LTE, Wi-Fi і Bluetooth. Залишаться вони такими і в майбутньому, але для забезпечення стабільної та надійної роботи МОР-інфраструктури, на думку компанії Qualcomm, потрібна значна модифікація всіх цих трьох стандартів бездротового зв'язку.

В якості базової технології при створенні архітектури Інтернету речей буде виступати LTE, але це будуть вже релізи 13 і 14 цього стандарту, в яких пропишуть нові сценарії використання цієї технології. При використанні LTE потрібно вирішити

дві діаметрально протилежні завдання - організувати передачу ресурсоємного контенту, що вимагає збільшення продуктивності мереж, і створити низькошвидкісних і енергоекономічних підключень.

У першому випадку при високому навантаженні може бути задіяна технологія LTE Advanced, що передбачає використання агрегації декількох несучих частот. Подібні рішення вже працюють у 115 операторів в 50 країнах світу - існуючі сьогодні комерційні мережі LTE-A забезпечують низхідну швидкість передачі даних до 450 Мбіт/с при об'єднанні трьох несучих частот.

У тих випадках, коли високі показники не потрібні, наприклад для підключення до Мережі простих пристроїв типу датчиків на швидкості до 1 Мбіт / с, передбачається застосування LTE-M. Очікується, що така можливість (LTE Cat.0) буде прописана вже в наступному, 13-му релізі стандарту. Для організації таких низькошвидкісних підключень буде задіяний напівдуплексний режим роботи у вузькому спектрі з використанням однієї антени. Подібні рішення будуть відрізнятися дешевизною і енергоекономічністю, що має забезпечити їх масове використання.

Також для низькошвидкісних підключень в місцях з високою щільністю розміщення MOP-пристроїв на частотах нижче 1 ГГц передбачається використовувати стандарт Wi-Fi 802.11ah, що забезпечує швидкість від 150 Кбіт/с до 78 Мбіт/с. Розробляються і інші стандарти Wi-Fi, які повинні значно підвищити пропускну здатність бездротових мереж. Той же 802.11ac забезпечує втричі більшу пропускну здатність, ніж 802.11n, і працює в більш вільному діапазоні 5 ГГц [4].

Ще один шлях підвищення продуктивності - використання однієї несучої для передачі даних відразу на три пристрої, що збільшує ємність мережі приблизно в 2,5 рази. Така можливість реалізована в 802.11ac MU-MIMO. Ця модифікація (а потім і 802.11ax) забезпечує швидкость в кілька гігабіт в секунду, що підходить для використання поза приміщеннями (наприклад, на масових заходах).

Також гігабітні потоки здатна забезпечити і технологія 802.11ad, що передбачає залучення неліцензованого діапазону 60 ГГц. Завдяки використанню частини неліцензованого спектра LTE-U, який здатний вдвічі збільшити ємність і дальність сигналу в порівнянні з Wi-Fi. Такі частоти до того ж мають високий коефіцієнт

відбиття від перешкод, наприклад від стін, що робить їх кращими для використання в підвалах і інших складних умовах.

ВИСНОВКИ ДО РОЗДІЛУ 2

Отже, особливе значення надається конвергенції LTE з бездротовими мережами малого радіусу дії (Wi-Fi і Bluetooth), що дозволить розвантажити існуючу телекомунікаційну інфраструктуру та забезпечить більш високий рівень відмовостійкості і безпеки підключень. Сама технологія Bluetooth також зазнає деяких змін - зокрема, в наступному її релізі планується збільшити дальність дії з нинішніх стандартних 7 метрів до 30. МОР передбачає велику різноманітність сценаріїв підключення, тому в багатьох випадках Wi-Fi і Bluetooth органічно доповнювати LTE.

РОЗДІЛ 3
ЗАГАЛЬНА ХАРАКТЕРИСТИКА МОДЕЛІ ПЕРЕДАЧІ ДАНИХ M2M

3.1 Аналіз технології M2M

M2M (Machine-to-Machine або Mobile-to-Machine) – це нова концепція організації мереж, що позначає передачу телеметричних даних від одного пристрою до іншого. Система M2M містить безліч периферійних пристроїв зв'язку та програмне забезпечення. Периферійний вузол, як правило, датчик, що визначає умови робочого середовища фізичного пристрою [5]. Після збору детальної інформації він негайно перетворюється на сигнал. Цифровий сигнал потім передається по мережі. Передача даних в інші програми та вузли створює процедуру прийняття рішення та надсилає командний пристрій на основі аналізу даних, отриманих з використання цих датчиків, що не має багатьох переваг та простіше в управлінні.

Темпи розвитку ринку M2M-обладнання знаходяться під наглядом аналітиків і експертів з багатьох агентств по всьому світу. Їх оцінки і прогнози вкрай оптимістичні, а потенціал розвивається M2M-індустрії просто-таки вражає. Останнє покоління M2M-модулів здатне забезпечити виконання таких базових функцій, як GSM / GPRS, GPS, Bluetooth, ZigBee [5].

На даному етапі технологія M2M продовжує активно розвиватися, системи стали більш високоінтелектуальними, а сфера їх застосування практично безмежно розширилася. Зросли можливості практичної реалізації різних M2M-рішень також завдяки зниженню вартості на технології бездротового зв'язку, підвищення їх продуктивності і функціональності. Здатність управляти віддаленими пристроями за допомогою бездротового сигналу дозволила користувачеві звести до мінімуму залежність від місцезнаходження і часу.

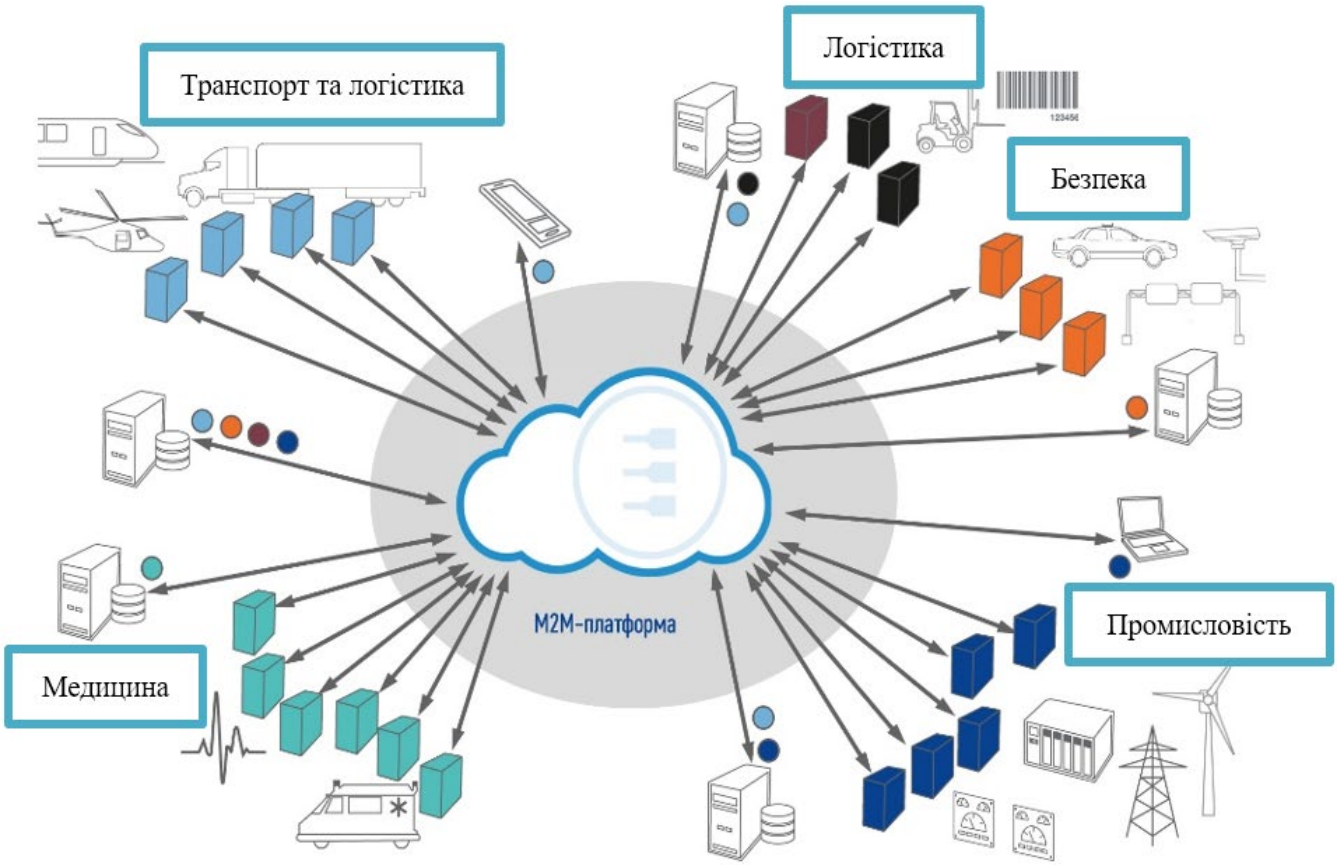

Рис. 3.1. Реалізація моделі M2M [5]

Сьогодні M2M-обладнання дуже широко використовується в протиугінних і охоронних системах, воно стало невід'ємною частиною багатьох правоохоронних структур. Впровадження даної технології дозволяємо забезпечити максимально швидку реакцію спецслужб при спробі угону автомобіля або злому квартири. Сигнал про подію передається по мережі GSM на диспетчерський пульт черговому оператору у вигляді SMS-повідомлення або голосового сигналу, одночасно можливо сповіщення власника. Особливо відчутна підтримка M2M систем в погано телефонізованих районах.

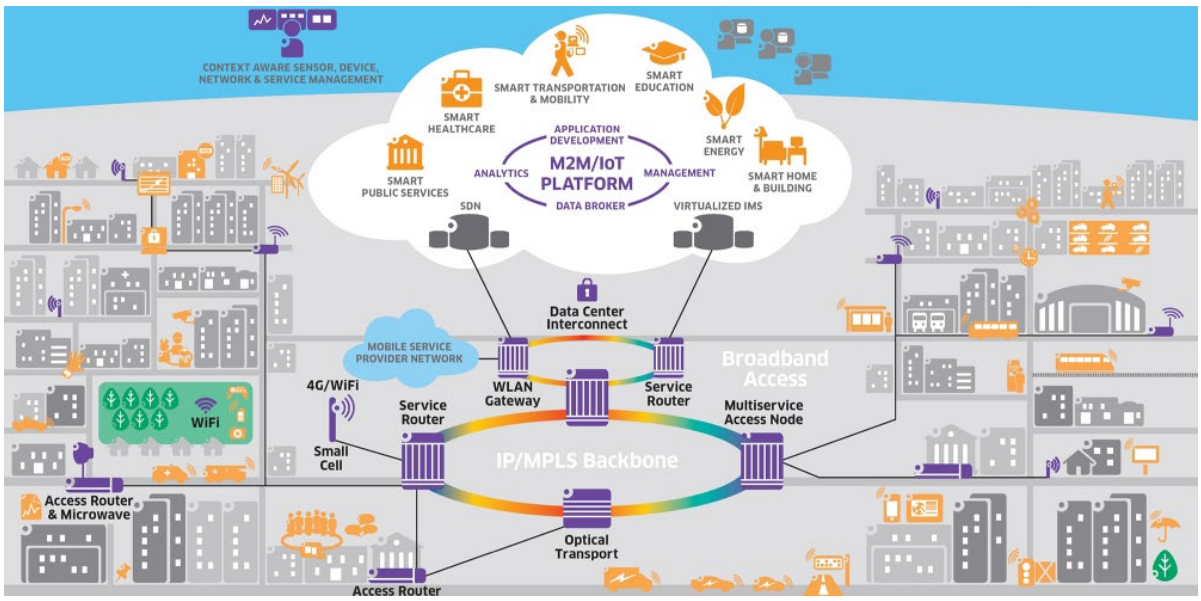

Рис. 3.2. Реалізація концепції «Розумне місто» через модель M2M

Якщо ще зовсім недавно на цьому можливості нової технології закінчувалися, то зараз вона проникла і в інші сфери, наприклад, банківську. Тепер банки впроваджують M2M модулі з SIM-картами в свої банкомати. Технологі. M2M можна застосовувати і в аграрному комплексі, датчики моніторингу вологості грунту дозволять зробити витрату води максимально економічною і ефективною. А система «розумний будинок» давно перетворилася з мрії в реальність, її численні переваги може оцінити кожен бажаючий. Модулями зв'язку постачаються безліч різних датчиків контролю температури, рівня освітленості, механічної напруги мостів, тиску в трубопроводах, датчиків вогню і диму і т.д. Подальшим етапом в розробці M2M систем телеметрії буде досягнення максимальної чутливості детектора GPS-сигналу і стабільності роботи M2M модулів в найскладніших умовах.

На ринку технологічних рішень для M2M свої розробки пропонує не один десяток компаній, в тому числі і такі світові лідери як компанії Nokia, Sony Ericsson, Siemens.

Не так давно цікаве M2M рішення представила американська компанія MaxStream. Фахівцями було розроблено пристрій XBee Xtender, який дозволяє об'єднувати машини, що використовують мережу ZigBee / 802.15.4., Але при цьому усунений головний недолік ZigBee-мереж. Якщо раніше пристрої мали невелику

покриття зони (30-100 м), то дане рішення здійснює зв'язок між машинами знаходяться на відстанях до 60 км. Вартість цього дива складає 400 доларів [5].

Інше цікаве рішення - Motorola G24 модулі. Виробники завжди намагалися створити пристрій здатний працювати навіть в найжорсткіших кліматичних умовах, ці радіомодулі здатні працювати в рекордному температурному діапазоні - від -30 до +85° С.

Як бачимо, ринок M2M технологій розвивається в різних напрямках і вже в найближчому майбутньому розробники і виробники M2M модулів зможуть нас порадувати новими досягненнями в цій галузі.

Система M2M складається з декількох елементів:

- Периферійні вузли;
- Комунікаційне обладнання;
- ПЗ.

Периферійні вузли, як правило, є датчиками, що визначають умови навколишнього середовища та умови роботи фізичних пристроїв. Після збору детальної інформації вона негайно перетворюється в цифровий сигнал, який потім передається по мережі. Передача даних у програми та інші вузли забезпечується пристроєм зв'язку. Програмне забезпечення засноване на аналізі даних, отриманих від датчика, прийняття рішень та передачі команд на пристрій. Використання таких бездротових технологій незаперечне. Використання обладнання M2M економить витрати на утримання кабельної інфраструктури та економить дорогоцінний час, зменшуючи кількість працівників, роблячи бізнес більш ефективним та простішим в управлінні.

Застосування M2M:

1. Системи доступу

Дають можливість певної групи людей за допомогою свого смартфону заходити в певні приміщення, відкривати електронні замки, двері і т.д. Такі дії здійснюються за допомогою звичайного телефонного дзвінка або посилкою певного коду.

2. Системи охорони приміщень

Дозволяють здійснювати дистанційну бездротову охорону приміщень. Дає можливість користувачам систем самостійно дистанційно ставити-знімати з охорони такі приміщення. Так само додаткові сервісні функції, як сигналізація і паніка.

3. Системи безпеки

Бездротові системи безпеки (пожежна, аварійна, персональна і т.д.). Дозволяє незалежно і дистанційно відстежувати стан об'єктів і при необхідності повністю автономно посилати сигнали тривоги або інформацію про стан об'єктів.

4. Дистанційний контроль і управління "домашнім" обладнанням

Дає можливість за допомогою мобільного телефону дистанційно здійснювати контроль "домашнього" обладнання, підтримувати певні умови в приміщеннях, дистанційно керувати таким обладнанням (обігрівачі, кондиціонери, насоси, сауни і т.д.).

5. Автомати з продажу, кавові автомати, обмінні машини, автоматичні бензоколонки і т.д.

Дистанційно контролювати стан, здійснювати контроль працездатності, дистанційна охорона, дистанційний збір інформації про наявність "запасів" і їх кількості, статистика. Телефонні апарати, встановлені вздовж автомобільних трас, паркувальні автомати, управління вуличними табло.

6. Ліфти, ескалатори тощо

Дистанційний контроль працездатності, передача сигналу тривоги і т.д.

7. GSM відео

Надає можливість здійснювати дистанційну передачу зображення (охорона, контроль стану і т.д) через GSM мережу.

Важливою проблемою сучасного ринку M2M є безпека такого типу взаємодії. На жаль, про неї творці подібних пристроїв думають далеко не в першу чергу, ставлячи на перше місце практичність і зручність застосування.

3.2. Проблематика організації звязку M2M

Технології передачі даних M2M може бути 2 видів[5]:

- стабільний M2M забезпечує використання різних рішень: управління процесами, нагляд за безпекою, платіжні термінали, лічильники, роздрібні машини;
- Mobile M2M дозволяє управляти автопарком і надавати велику кількість автомобільних додатків. Автомобільний ринок пропонує безліч можливостей

використовувати M2M як пристрій в транспортному засобі, здатний контролювати, діагностувати, навігацію, статус, безпеку і мобільний зв'язок.

Способи реалізації технології M2M[4-5]:

- DTMF - дозволяє надсилати зашифровані повідомлення за допомогою звичайних голосових каналів. Його можна ефективно використовувати в цілях безпеки (формати DTMF передають інформацію, таку як ідентифікатор контакту), найпростіший пульт дистанційного керування, контроль особистої інформації, наприклад, у голосовій пошті. Зазвичай автовідповідач вимагає пароль, щоб дозволити доступ в меню. Це основна можливість M2M, яка використовується в більшості мереж.
- SMS - це невелика послуга обміну повідомленнями. Оскільки оператори мобільних мереж надають цю послугу, технологія M2M відкриває широкі можливості для користувачів. Головна перевага SMS полягає в тому, що повідомлення можуть передаватися за мілісекунди і містити великий обсяг інформації. SMS відкриває двері для більшості стаціонарних та мобільних додатків M2M, таких як роздрібні автомати, платіжні термінали, комунальні послуги тощо.
- модем, який здійснює зв'язок за допомогою даних. Використання комутованих каналів для передачі інформації обмежується даними "постійно увімкненими", що нижче, ніж швидкість зв'язку. Доступна система передачі пакетної інформації GPRS або CDPD, яка дозволяє інтерактивно спілкуватися в режимі реального часу. Дані "Завжди увімкнено" є основним стандартом зростання M2M. Віддалене лікування та розваги стали можливими з розвитком GPRS та CDPD.
- WAP-IP був розроблений для рішень "людина-машина" і почав будуватися для електронного замовлення, придбання та оплати, поєднуючи інформаційні послуги та програми для управління та моніторингу. Для роздрібних машин WAP-IP може створити основу мережевої безпеки та розробити антивандальні системи.
- 4G покоління мобільного зв'язку пропонує необмежені можливості в телекомунікаційному середовищі, де всі машини та пристрої, що створюють мережу, відповідають одному протоколу.

3.3. Протоколи та стандарти M2M

З M2M тісно пов'язане поняття пористих мереж, а методика встановлення комунікацій більше схожа на передачу естафети. Нова архітектура включає в себе різні типи з'єднань, а її суть полягає в змішуванні існуючих апаратних рішень в самих незвичайних комбінаціях.

Розглянемо потенційні складові M2M. Перша - Wi-Fi. Технологія отримала найбільшого поширення, незважаючи на недоліки: значне енергоспоживання, висока вартість адаптерів і мала зона покриття. Для її збільшення використовуються різні методи, наприклад комбінація спеціальних антен і способів доступу до середовища (Space Division Multiple Access - SDMA).

Другий за важливістю компонент M2M систем - Bluetooth. Його плюси: невеликі розмір і маса адаптерів, низька ціна обладнання. Максимальна зона покриття практично еквівалентна 802.11 [5]. Однак максимальна кількість одночасно працюючих в одній зоні пристроїв Bluetooth обмежена, а мережева функціональність мізерна.

Bluetooth Альтернатива - UWB, або Ultra Wide Band - зв'язок, що відрізняється високим ступенем утилізації ширини спектра радіочастот для передачі сигналів на невеликі відстані (кілька метрів). Передбачається, що максимальна швидкість передачі може досягати 500 Мбіт. ,

Ще один ймовірний учасник мереж M2M - ZigBee. Ця технологія орієнтована на мережу, яка обслуговує імені не комп'ютерні пристрої. Адаптери ZigBee будуть недорогими і маленькими, з невисоким енергоспоживанням. Залишається тільки питання щодо фізичного рівня: ZigBee, адже досі не запроваджено жодного протоколу зв’язку даної технології.

В даний момент для бездротової Wi-Fi характерна "стільникова" архітектра , прийнята операторами мобільного зв'язку: безліч точок доступу, що мають кабельне з'єднання. Відповідно, якщо ви хочете покрити більшу зону, то вам буде потрібно чимале число точок доступу і розгалужена дротова мережа. Фактично це зводить

нанівець перевагу бездротового доступу. Найчастіше у великих інсталяціях левову частку бюджету поглинає опорна провідна інфраструктура.

У M2M роль базової інфраструктури, що з'єднує точки доступу, відводиться бездротових комунікацій, які побудовані на базі Wi-Fi. Щоб така опорна мережа справлялася з потоком даних, що генеруються клієнтськими пристроями, кожна точка доступу повинна відводити для опорних комунікацій більше одного каналу Wi-Fi. Але численні передавачі, що працюють одночасно, засмічують ефір, і якщо їх зони дії перекриваються (а це буває практично завжди), то ємність мережі буде зменшуватися з кожним новою точкою доступу.

Ідеально підходить для стаціонарної базової мережі технологія поділу каналів в просторі - SDMA Wi-Fi. Вона забезпечує підвищену дальність і пропускну здатність у разі фіксованого розташування вузлів, в той час як кінцеві користувачі будуть як і раніше мати Wi-Fi доступ.

Втім, невгамовний енергетичний апетит бездротових адаптерів не дає можливості використовувати Wi-Fi для підключення компактних мобільних пристроїв. Більш доречним в стільниковому, портативному IP-телефоні, наладоннике або планшетному ПК буде адаптер Bluetooth. Він економно витрачає електроенергію, недорогий і забезпечує високу пропускну здатність на відносно невеликих відстанях. Це хороша заміна Wi-Fi для застосування всередині приміщень. У випадках, коли пристрій знаходиться в безпосередній близькості від точки доступу, можна вдатися і до Сніп, чия продуктивність повністю задовольнить навіть потреби відеомагазину або відеокамери спостереження. Для простих сенсорів або офісної / побутової техніки (холодильники, кондиціонери, системи освітлення та безперебійного харчування) ZigBee підійде.

Симбіоз Bluetooth і Wi-Fi в рішенні представлений від Cisco, призначеному для лікарень. Датчики пацієнтів, компактні та економічні, не здатні підтримувати протокол 802,11, але кишенькові комп'ютери медсестер - можуть. Тому КПК, обладнані як адаптером Wi-Fi, так і інтерфейсом Bluetooth, виконують роль сполучної ланки між лікарняному бездротовою мережею та сенсорами пацієнтів. У тому ж напрямку працюють шведські дослідники з університету Упсала, які застосовують

для віддаленого спостереження за хворими дітьми комбінацію з сенсорів Bluetooth і Wi-Fi, GSM і мереж GPRS. Маленькі пацієнти перебувають в комфортній домашній обстановці, з батьками і, тим не менше, знаходяться під пильним наглядом кваліфікованих лікарів спеціалізованої клініки.

Також пісутствует рішення у вигляді комбінованих точок доступу, оснащених адаптерами Wi-Fi і Bluetooth. Доступ систем One Network залежить від набору підключених модулів. Вихід на опорну ячеистую бездротову мережу забезпечують модулі під назвою Network Connect, а за динамічну реконфігурацію і маршрутизацію відповідають модулі мережевого сервера. Клієнт Connect Модулі, що забезпечують клієнтські з'єднання, існують у безлічі варіантів, що підтримують 802.11a /B/G і Bluetooth. Також передбачається, що в майбутньому асортимент поповнять компоненти, що працюють з технологіями UWB і 802.16a. Модулі мережевого підключення проводяться як в дротовому варіанті - підключення до опорної мережі за допомогою Ethernet 10/100, так і в бездротовому - 802.11a / p

ВИСНОВОК ДО РОЗДІЛУ 3

Отже, головною проблемою пористих бездротових мереж і M2M був і залишається брак стандартів, які дозволили б взаємодіяти продуктам різних компаній. Відсутність впрвадження стандартизації в обалсті бездротового зв'язку, стає серйозною перешкодою для широкого поширення подібних технологій. Те, що прекрасно працює в одній країні, в іншій вимагає законодавчого врегулювання.

РОЗДІЛ 4
ІМІТАЦІЙНА МОДЕЛЬ СТАТИСТИЧНИХ ПОКАЗНИКІВ M2M ТРАФІКУ

4.1 Классификація трафіку M2M

Трафік M2M зявився в мережах зв’язку із появою перших телеметричних пристроїв. В мережах зв’язку із комутацією каналів до недавнього часу найбільш широкого застосування отримали системи сигналізації (контролю доступу, пожежної, аварійної сигналізації) і системи телеметрії. Ці системи виконують функції контролю над технологічними процесами або спостереження за навколишнім середовищем.

Використання ресурсів цього трафіку і мережі зв'язку не так важливо, як вплив на якість обслуговування інших видів трафіку. Наприклад, ресурси мережі доступу абонентів (абонентні лінії) використовуються майже виключно для охоронної сигналізації. Дистанційний потік даних телеметрії контролю технічних процесів, таких як різні труби, електромережі, залізниці і т.д., комунікація, як правило, обслуговуються виділеними ресурсами мережі. Інших форм розгортання мережі M2M (від машини до машини) не так вже й багато, тому істотних проблем з якістю обслуговування інших послуг немає.

Нинішній рівень розвитку комп'ютерних і комунікаційних технологій призводить до проникнення інформаційних технологій в сферу експлуатації, яка раніше не включувалася в мережу зв'язку. Розвиток USN (Ubiquitous Sensor Networks) відкриває дуже широке поле застосування інформаційних технологій в більшості сфер людської діяльності.

Розвиток мережі дорожнього руху VANET та інших телекомунікаційних систем, призначених у багатьох випадках для передачі даних між машинами, істотно впливає на швидкість трафіку M2M в мережі зв'язку, і тим самим збільшує вплив на якість послуг зв'язку.

Дії зарубіжних дослідників забезпечили оцінку потенціалу розвитку USN і трафіку, що генерується цими мережами зв'язку, визначаючи самозйомний характер

USN трафіку і значення параметрів Hurst для різних USN -додатків. USN Network є одним з видів розгортання мережі M2M. Остання реалізація відбувається швидко і сьогодні стоїть нагальне завдання вивчення впливу M2M трафіку на існуючі мережі зв'язку.

Сьогодні наочним прикладом сильного зростання трафіку M2M є розвиток комунікаційної структури житла. Можна припустити, що результатом цього процесу є те, що мережа буде створена шляхом об'єднання різних датчиків керованих об'єктів. Як мінімум, кількість таких датчиків визначається кількістю лічильників за обсягом послуг споживання (електроенергія, водопостачання тощо). Тому кількість комбінованих датчиків тільки в процесі може перевищувати кількість мешканців. Ще одним пріоритетним напрямком розвитку мережі M2M є розвиток систем моніторингу навколишнього середовища, а також розробка систем управління громадським порядком і систем безпеки.

Ці системи можуть використовувати як дротові, так і бездротові мережі зв'язку для передачі даних. Кількість терміналів мережі M2M незабаром може перевищити чисельність населення, а отже і фактичну кількість клієнтів мережі зв'язку. Це підтверджує загальну концепцію розвитку, відому як Інтернет речей (IoT).

Трафік M2M істотно впливає на якість обслуговування в мережах бездротового зв'язку та на їх роботу. Наприклад, короткі сеанси зв'язку M2M ускладнюють або повністю усувають контроль якості каналу за допомогою оцінки часу зайняття (розмови), який традиційно використовується медіа-операторами.

Специфіка галузі застосування подібних систем контролю може виражатися в специфічних особливостях виробленого трафіку. Зокрема, поведінка ряду пристроїв може бути взаємозалежною, що може призводити до їх масової активності, що виражається в неконтрольованому зростанні трафіку.

Тому тепер необхідно вміти оцінювати його вплив на трафік M2M і якість послуги зв'язку, а також визначити способи організації систем M2M, що забезпечать «гармонійні» взаємодії та інтеграцію з традиційними мережами зв'язку.

Прогноз зростання трафіку M2M. Є багато прогнозів щодо зростання трафіку M2M у світі. Водночас акцент зроблено на експоненціальному характері розвитку трафіку M2M, що характерно для розвитку нових телекомунікаційних технологій.

Використовуючи метод прогнозування посилань, ви можете отримати прогноз фіксованого і загального зростання трафіку M2M в мобільних і бездротових мережах доступу, показаний в статистиці на рис. 4.1.

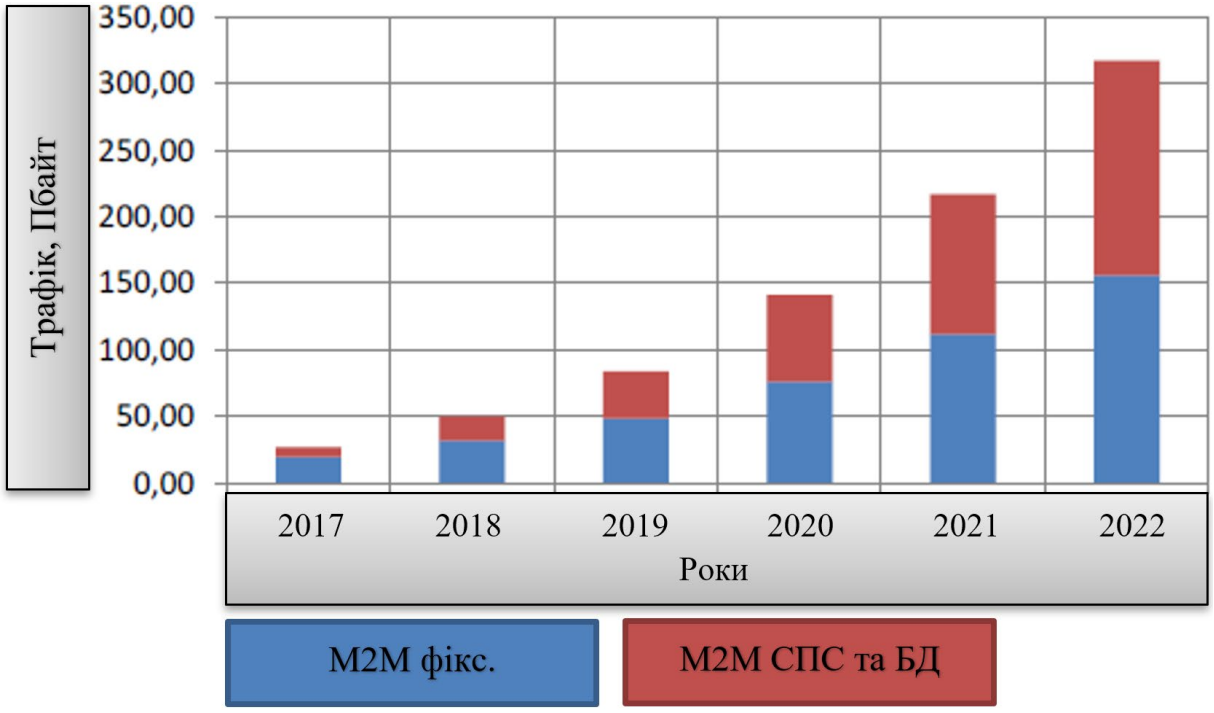

Рис. 4.1. Прогнозування зростання сумарного навантаження M2M в мережах фіксованого і рухомого зв'язку і бездротового доступу [6]

З наведеної діаграми видно оцінювання M2M навантаження в мережах рухомого зв'язку, бездротового доступу і фіксованого зв'язку близькі за значенням, що пояснюється схожими значеннями загальної величини навантаження в цих мережах. Як бачимо, сумарний обсяг прогнозованого трафіку M2M на 2022 рік перевищує 300 Пбайт, що вимагає проведення детальних досліджень характеристик цього трафіку. Варто відзначити, що частка трафіку M2M складе при цьому близько 5% від сумарного трафіку мереж зв'язку. Крім того, слід очікувати, що трафік M2M може мати істотно інші характеристики, ніж трафік традиційних мереж зв'язку [6].

Особливості трафіку M2M. Для опису трафіку в сучасних мережах зв'язку існують різні теоретичні моделі, як правило, побудовані на основі теорії масового обслуговування. Завданням побудови моделі, є опис властивостей трафіку (потоку), і параметрів його обслуговування мережею зв'язку [6].

Потік M2M - це потік даних, що може перемикати пакети або мережеві канали в мережі передачі даних. Основна його відмінність у порівнянні з трафіком від однієї людини до іншої полягає в тому, що ініціатор передачі інформації - це автоматизований інструмент. Залежно від обміну даними системи розгортання (взаємодія протоколу) передача події відбувається в таких ситуаціях:

1) передача даних через вплив зовнішніх факторів (зміна фізичних параметрів, що контролюється датчиком);

2) кінець фіксованого періоду часу (як правило, тривалість інтервалу не може бути випадковим значенням);

3) технічні причини - передача даних телеметрії (пов’язаних з ініціалізацією пристрою, перезавантаженням пристрою, тощо), не пов’язаної із зазначеними вище умовами.

Відповідно до перерахованих умов передачі даних, 3 типи трафіку, які можна виділити, є умовами в системі M2M.

Перший тип трафіку здійснюється непрямою системою, автоматично використовує активний пристрій (передача даних може бути ініційована). Цей трафік можна розглядати як реакцію на випадкові події окремо (наприклад: отримати значення, виміряне протягом певного періоду, яке активує аварійний сигнал або інший сигнал тривоги, тощо). У цьому випадку властивості трафіку залежать від природи процесу, що контролюється. Але якщо така система призначена для управління випадковими подіями, які трапляються рідко (системні аварійні тривоги, контроль доступу тощо), то загалом інтенсивність спостережуваних подій може дорівнювати або навіть менше інтенсивності пристроїв контролю відмов. Щоб забезпечити необхідну надійність для виявлення спостережуваних подій, необхідність контролю за технічним станом датчика. Для цього потреба, обсяг послуг

передачі даних може бути набагато більшим, ніж обсяг корисної інформації, а характер трафіку визначається специфікаціями процесу діагностики стану датчика.

Другий тип - псевдодетермінований трафік, виробляється автоматизованою системою датчиків. В даний час набули поширення системи збору даних та контролю моніторингу SCADA. У цих системах датчик знаходиться під контролем (пасивні пристрої) і передає дані про вимоги головних пристроїв. Як правило, у поточній системі медіанний інтервал генерації трафіку не обумовлений в будь-який час. Цей тип трафіку також включає трафік, генерований різними автоматизованими системами планування (дані, що оновлюються відповідно до загальних графіків тощо).

Третій - це тип службового трафіку, який характерний для системи роботи датчика. Він здійснюється, коли відбуваються зовнішні (часто випадкові) події, які призводять до необхідності виконувати дії для підтримання роботи операційної системи, а також для діагностики стану датчика. Це спричиняє широкий спектр збоїв у програмному забезпеченні транспортних послуг, усуваючи процес, необхідний для підключення, передачу параметрів для налаштування датчиків тощо. Як правило, службовий трафік призводить до генерації трафіку сигналізації, який досить добре досліджений для мереж USN.

4.2. Модель опосередкованого трафіку M2M

Опосередкований трафік. Даний тип трафіку породжується у системі з активними пристроями під зовнішнім впливом системних процесів. Залежно від конкретного застосування системи моніторингу характер цих процесів може відрізнятися. Розглянемо найбільш поширені процеси, які можуть виникнути в найбільш масивних додатках, таких як:

- аварійна сигналізація (пожежна сигналізація, сигналізація, що демонструє цілісність конструкцій будівель та споруд, несправність систем технічного забезпечення життєдіяльності, ознаки незаконного проникнення на об’єкти, що охороняються), наприклад, у житлово-комунальних зонах;

- контроль загроз навколишнього середовища (контроль за забрудненням навколишнього середовища, погодних умов, сейсмічних і кліматичних загроз), що реалізується структурами Міністерства з надзвичайних ситуацій;

- догляд за здоров`ям людини (контроль серцевого ритму, артеріального тиску, структури крові та інших показників), який застосовується в медичних установах в терапевтичних і профілактичних цілях.

Кожен з перерахованих вище процесів може мати свої особливості, які будуть відображені в трафіку, генерованого системою. Однак загальною рисою цих додатків є те, що події, які ведуть до трафіку, відносно рідкі. Інтенсивність цих подій відповідає інтенсивності збоїв технічного оснащення, тому необхідно стежити за станом пристроїв для роботи цих систем, що вимагає трансляції службових повідомлень. Властивості трафіку сервісних повідомлень залежать від методу моніторингу технічного стану. Наприклад, контрольний пристрій може періодично використовуватися сервером для моніторингу стану. У цьому випадку період запитів може бути обраний на основі вимог в залежності від надійності (фактора готовності) системи.

Коефіцієнт готовності розраховується за формулою:

$$Кг = \frac{Тс}{Тс+Тн+Тв}, \quad (4.1)$$

де Тс - час справного стану (напрацювання на відмову) (годин);

Тн - час виявлення несправності (год);

Тв - час відновлення (год).

Припустимо, що відмови пристрою випадкові і різновірогідні на протязі періоду опитування, то необхідний період опитування може бути отриманий і дорівнюватиме:

$$to = \frac{2}{Кг}(Тс - Кг(Тс + Тв)), \quad (4.2)$$

Наприклад, при вимозі Кг= 0,9999, часу відновлення Тв=2 год і напрацювання на відмову 50 000 годин, необхідний період запиту дорівнює 6 годин. Отже, при реальному значенні надійності інженерних систем інтенсивність телеметрії є низькою, і лише велика кількість подібних систем має необхідне значення в обслуговуванні.

Складність у підтримці трафіку, що генерується такими системами, полягає в тому, що "поведінка" пристроїв цього типу може бути взаємозалежною. Наприклад, якщо певні пристрої, які контролюють стан об’єкта або процесу, змінюються таким чином, що більшості контрольних пристроїв доведеться передавати інформацію про ситуацію (аварійний рівень, при якому всі параметри перевищують допустимі межі). Ця ситуація може спричинити широкомасштабне повідомлення (дзвінок). У цьому випадку інтенсивність трафіку буде визначатися кількістю пристроїв управління і буде залежати від кількості надісланих повідомлень та можливості спрацьовування пристрою та інтенсивності подій, що спричинили подію. Активація пристрою.

Для аналізу такого потоку була створена імітаційна модель, яка робить такі припущення:

- ожен n застосунків може перебувати в неактивному та активному стані.

- у пасивному стані пристрій генерує лише технічний потік (контроль стану), який є певним процесом у часі, з часом Ті. Величина Ті вибирається випадково при ініціалізації моделі, як рівномірно розподілена випадкова величина в межах від T_{min} до T_{max}.

- коли відбувається певна подія і зупиняється там на короткий час, пристрій переходить в активний стан, протягом якого генерує випадкову кількість трафіку, а потім повертається в пасивний стан. Потік, що генерується пристроєм в активному положенні, пов'язаний і має рівномірний розподіл V_{min} до V_{max} із середнім значенням V.

- подія виникає в незалежні випадкові моменти часу. Припустимо, що інтервал часу між цільовими подіями випадковий і має експоненціальний розподіл ймовірності і середнім значенням t_E.

Вихідні дані для моделювання: t_E=100, T_{min}=0, T_{max}=1, V_{max}=1000 (повідомлень), V_{min}=0, n=10.

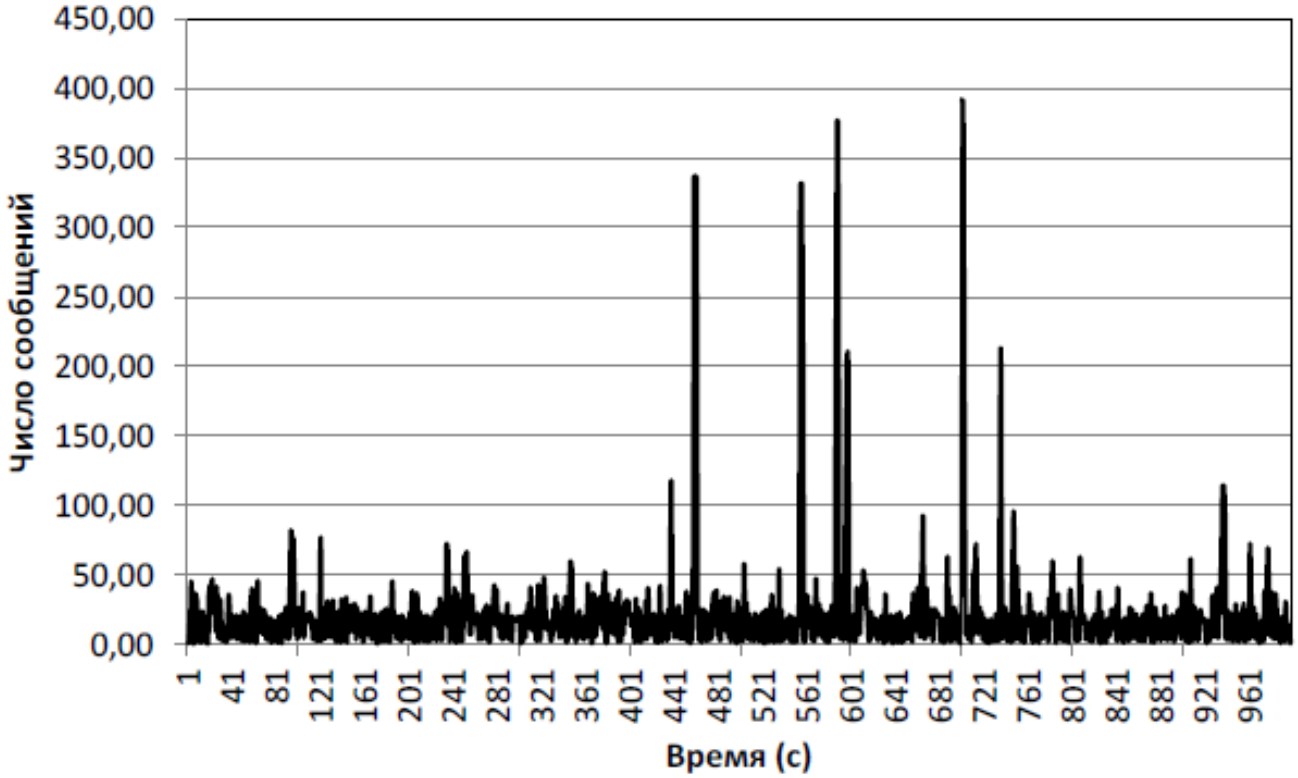

Рис. 4.2. Реалізація потоку опосередкованого трафіку

На рис. 4.2 показано, що існують суттєві піки при пульсації трафіку в процесі надходження, які значним чином перевершують середнє значення.

На рис. 4.3 представлено графічну залежність оцінки зміни дисперсії при оцінці показника Херста. Також на графіку представлено три прямі для значень ймовірності [7] p=0,1; 0,5; 1,0. Показник Херста відповідно становить H= 0,451; 0,375; 0,292.

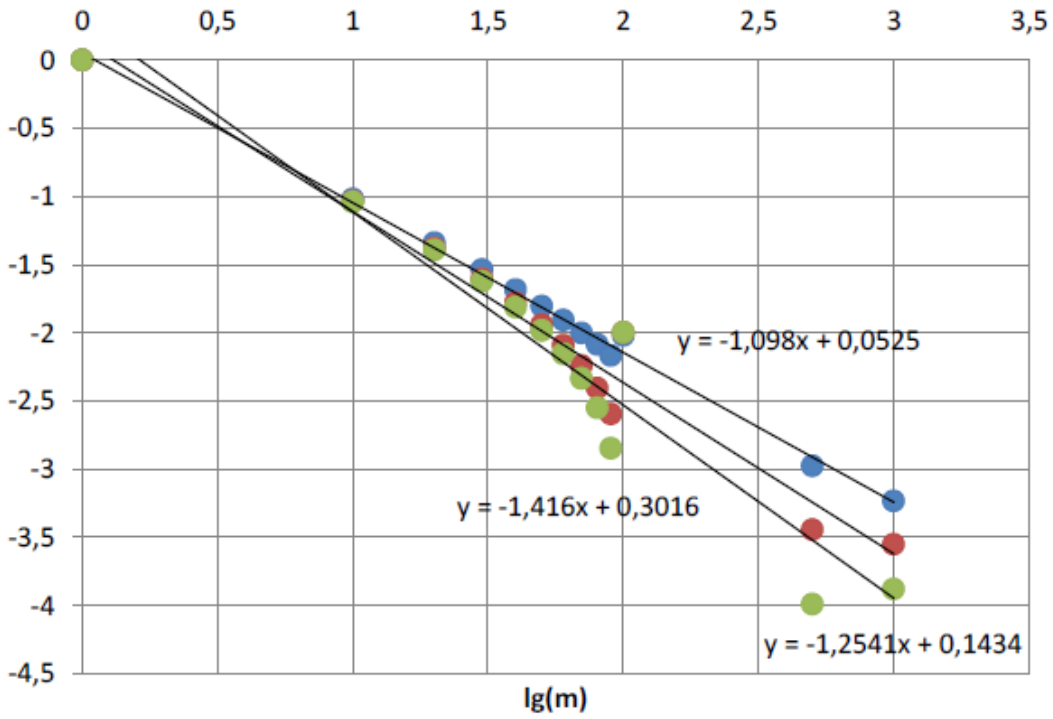

Рис. 4.3. Показник Херста при зміні дисперсії

Отже, сгенерований трафік, в залежності від окремих параметрів може мати властивості антиперсистентного потоку (H<0,5) або найпростішого потоку (H≈0,5). Раніше антиперсистентні властивості спостерігалися для потоку втрат пакетів UDP.

4.3. Модель псевдодетермінованого потоку M2M

В даний час набули широкого поширення системи моніторингу та диспетчерського управління (SCADA). Подібна система являє собою систему майстер-підлеглий, в якій роль майстра виконує сервер збору даних, а підлеглого контролер або датчик (сенсор), встановлений на контрольованому об'єкті. Передача даних здійснюється через мережу зв'язку. У загальному випадку, в мережі зв'язку може функціонувати безліч таких систем. Основний принцип побудови даної системи зображений на малюнку 4 [8].

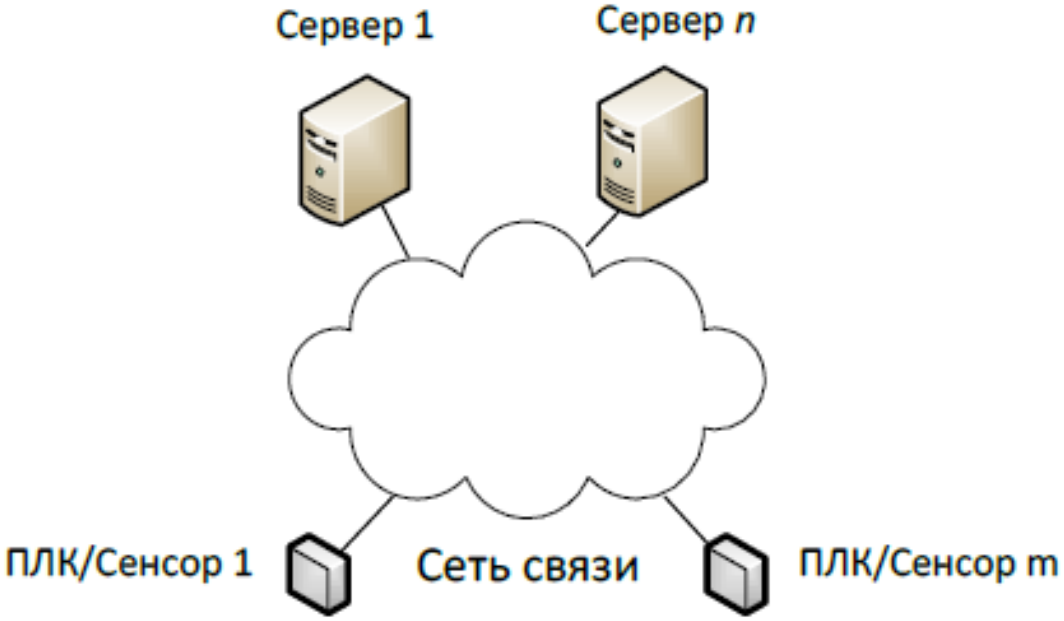

Рис. 4.4. Узагальнена структурна схема системи спостереження і управління

Відомо, що навантаження між сервером та j-пристроєм є детермінованим потоком даних (пакетів): запитів сервера і відповідей контролера (датчика). Мінливі параметри трафіку системи, можуть бути визначені, в загальному випадку, розподілом і мають певний цикл повторень T_i.

Якщо в мережа складається з *n* систем спостереження, то при постійній фазі між моментами надходження заявок (відповідей) φ_i=1…n, загальний трафік також буде представляти собою детермінований процес з періодичним повторенням рівним найменшому спільному кратному всіх періодів опитування Ts=lcm{Ti} i=1…n (рис. 4.5).

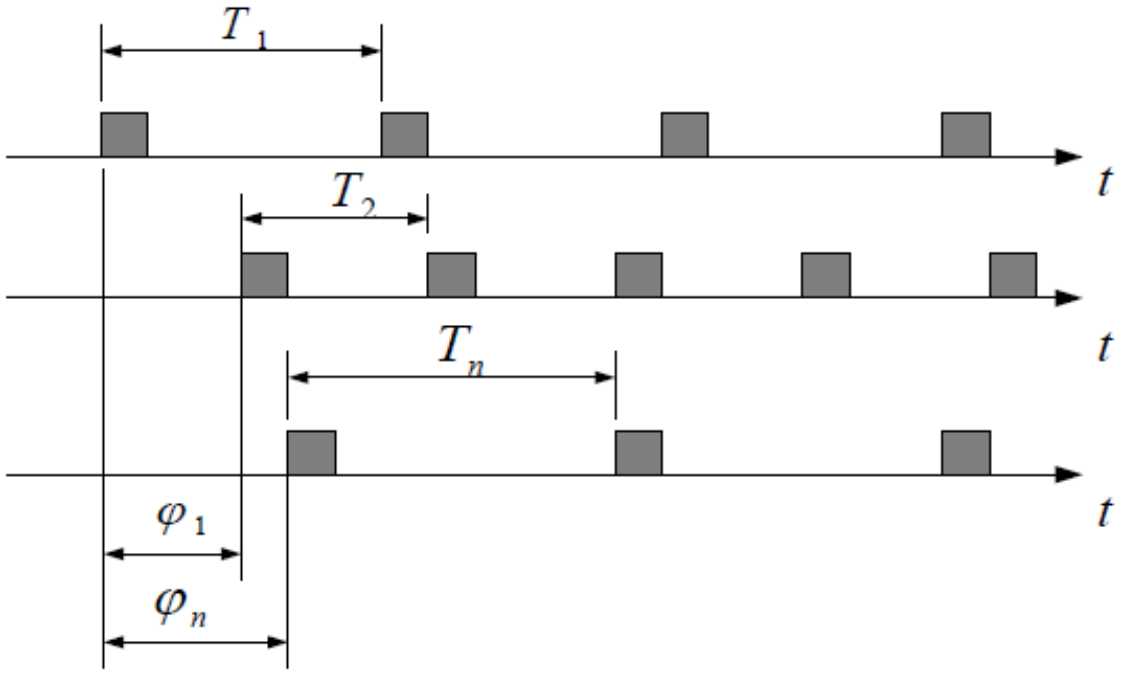

Рис. 4.5. Модель трафіку систем моніторингу

Якщо крокові переходи є нестатичними та випадковими (через асинхронне перемикання та перезапуск окремих систем), загальний трафік також отримує атрибути випадкового процесу (фальшивий трафік). За допомогою змоделювальних систем трафіку, що складаються з декількох систем моніторингу (n = 10) та генерують періодичні потоки (у встановленому режимі). Фаза Ti i=1 .... n випадково вибирається в діапазоні від 1 до 60 секунд (значення часу відповідають рівномірному закону розподілу). Кожна з систем спостереження може перезапускатися в випадковий момент часу, тобто величина фазового зсуву φi=1…n може змінюватися випадковим чином. Інтервал часу між рестартами системи випадковий і підпорядкований експоненціального закону розподілу ймовірності з середнім значенням 0,6 перезапусків на год. Реалізації трафіку наведено на рис. 4.6.

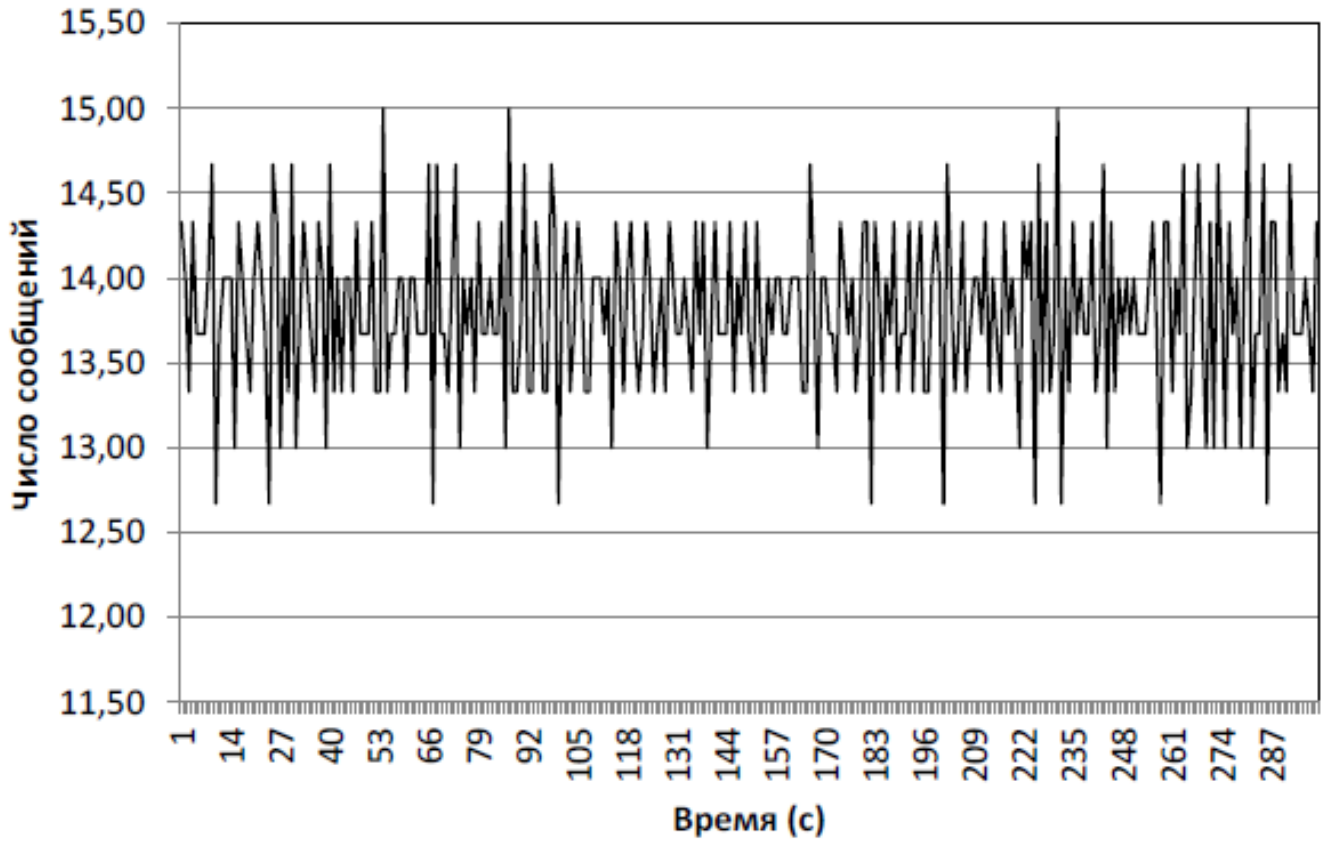

Рис. 4.6. Реалізація потоку детермінованого трафіку

ВИСНОВОК ДО РОЗДІЛУ 4

Отже, статистичні властивості потоку опосередковано визначаються такою особливістю, як залежність вихідного трафіку, що призводить до масштабної роботи пристрою в разі настання якоїсь певної події, а, отже, пікового трафіку випадкового. Аналіз статистичної природи цього розділу доводить, що він є антиперсистентним. Статистичні властивості псевдодетермінованного трафіку повинні визначатися кількістю і тривалістю роботи ланцюгового обладнання для моніторингу, а також інтенсивністю перезавантаження. Аналіз статистичної природи цього Трафіку показує, що він самоподібний з рівнем самоподібності однаково високим.

ВИСНОВКИ

В ході даної дипломної роботи було проведено аналіз сучасних моделей обміну даних M2M, D2D, P2P. Наведені основні проблеми організаці зв'язку та методи їх вирішення, наведено приклади протоклів і стандартів завдяки яким реалізується дані мережі.

Також проведено аналіз трафіку M2M. На основі аналізу виникнення несанкціонованих подій в мережах M2M, що вимагають здійснення передачі інформації, виділені основні типи трафіку M2M.

Розроблено моделювання опосередкованого, псевдодетермінірованного і службового трафіку в мережах M2M. Завдяки яким визначено статистичні властивості потоку опосередкованого трафіку.

Визначено його головну особливістю - залежність джерел трафіку, яка при настанні відповідних подій призводить до масової активності пристроїв і, як наслідок, призводить до випадкових піків трафіку. Результати імітаційного моделювання даного потоку довели, що він є антиперсистентним.

Охаракетризовані статистичні властивості псевдодетермінованного трафіку, які визначаються числом і періодами послідовностей опитування пристроїв, а також інтенсивністю перезапусків. Результати імітаційного моделювання даного потоку доводять, що він є самоподібним з високим ступенем самоподібності.

Таким чином на основі проведених дослідів в подальшому можна розробити модель керування трафіком M2M на основі чіткого розпорядку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Рошан, Педжман, Ліері, Джонатан "Основи побудови бездротових локальних мереж стандарту 802.11": Пер. англ. - М .: "Вільямс", 2004. - 304с.

2. Аджемов, А.С. Від електронної Росії до U-Росії: напрямки розвитку телекомунікацій / А.С. Аджемов, А.Е. Кучерявий // Інноваційна економіка Росії. - 2016. – 260 с.

3. Бабков, В.Ю., Системи мобільного зв'язку / Бабков, В.Ю., Вознюк, М.А., Дмитрієв, В.І. - М..: СПб ГУТ, 1999. - 330 с.

4. Бельков, Д.В. Аналіз втрат пакетів при передачі UDP-трафіку / Д.В.Бельков, Е.Н.Едемская, Л.В.Незамова, Т.А.Едемская // Зб. матеріалів Всеукраїнської науково-технічноі конференціі "Інформаційні системи та комп'ютерний моніторінг", Донецьк, ДонНТУ. - 2011.- 11-13 квітня. С. 249-253.

5. Булгак, В.Б. Нові методи прогнозування розвитку телекомунікацій та їх застосування в галузі / В.Б. Булгак, Л.Є. Варакин, І.І. Каледіна, В.Д Москвітін, Л.Ф. Шамаєва. - М.: МАС, 2017. - 105 с.

6. Пятилетний прогноз развития сетевых технологий [Електронний ресурс] // Беспроводные технологии. – 2017. – Режим доступу до ресурсу: https://wireless-e.ru/market/prognoz-razvitiya-setevyh-tehnologij/.

7. Вентцель, Е.С. Теорія ймовірностей / Вентцель, Е.С. - М.: Наука, 1969. - 576 с.

8. Гольдштейн, Б.С. Мережі зв'язку пост-NGN / Б.С. Гольдштейн, А.Е. Кучерявий. - Санкт-Петербург: БХВ-С. Петербург, 2013. - 160 с.