МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

МОДЕЛЮВАННЯ 5G-МЕРЕЖ ДЛЯ ПІДТРИМКИ ІНТЕРНЕТУ РЕЧЕЙ (IoT)

Виконав:
студент групи 1К-22
спеціальності
123 Комп’ютерна Інженерія
Данило ПОШТОВИЙ

Керівник:
Павло РАТАЙЧУК

Черкаси 2026

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ

Циклова комісія комп’ютерної інженерії та інформаційних технологій

Спеціальність 123 «Комп’ютерна інженерія»

Освітня програма Комп’ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувачка циклової комісії КІ та ІТ

_____ Наталя ФАЛЬЧЕНКО

(підпис)

«_____» _____2026 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Поштовий Данило Олександрович

1. Тема кваліфікаційної роботи Моделювання 5G-мереж для підтримки інтернету речей (IoT)

Керівник роботи Ратайчук Павло Єгорович

затверджені наказом закладу вищої освіти від «6» жовтня 2025 року № 84/1-у.

2. Строк подання студентом кваліфікаційної роботи 08.06.2026

3. Вихідні дані до кваліфікаційної роботи Технічна документація та стандарти щодо архітектури 5G-мереж; концепції та технічні вимоги систем Internet of Things до мережевої інфраструктури (затримка, масштабованість, енергоефективність); параметри IoT-трафіку (телеметричні дані, розмір пакетів, частота передачі); програмне середовище моделювання мереж GNS3.

4. Зміст кваліфікаційної роботи (перелік питань, які потрібно розробити) Дослідження теоретичних основ функціонування 5G-мереж та систем IoT, аналіз протоколів передачі даних та показників якості обслуговування (QoS); аналіз технологій 5G для підтримки IoT-пристроїв та методів оптимізації передачі даних; розробка 5G-мережі для підтримки IoT у середовищі GNS3; визначення показників ефективності мережі; проведення серії перевірок базового навантаження та зміни кількості IoT вузлів

5. Дата видачі завдання 15.09.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів	Примітка про виконання
1	Вступ	14.10.2025	
2	Розділ 1 Теоретичні основи функціонування 5g-мереж та iot	09.12.2025	
3	Розділ 2 Аналіз технологій 5g для підтримки iot-пристроїв	10.03.2026	
4	Розділ 3 Практичне моделювання 5g-мережі для підтримки iot	28.04.2026	
5	Висновки	12.05.2026	
6	Оформлення кваліфікаційної роботи (чистовий варіант)	26.05.2026	
7	Перевірка кваліфікаційної роботи на наявність ознак плагіату (за 10 днів до захисту)	02.06.2026	
8	Подання кваліфікаційної роботи на затвердження завідувачу кафедри (за 7 днів до захисту)	10.06.2026	

Студент _____ Данило ПОШТОВИЙ

(підпис)

Керівник роботи _____ Павло РАТАЙЧУК

(підпис)

АНОТАЦІЯ

Кваліфікаційна робота являє собою дослідження особливостей функціонування мереж п'ятого покоління для підтримки систем з використанням розумних пристроїв та розробці моделі 5G-мережі з оцінкою її ефективності за показниками продуктивності.

Метою роботи є визначення можливостей 5G-технологій для підтримки IoT-систем, розгляд архітектури сучасних мереж, основних технологій та розробка практичної моделі мережі для оцінки її масштабованості і продуктивності.

У роботі було розглянуто теоретичні основи функціонування 5G-мереж та систем IoT, архітектуру мереж п'ятого покоління та ключові технології, такі як Massive MIMO, Network Slicing та Edge Computing. Розглянуто вимоги IoT-систем до мережевої інфраструктури, включаючи показники затримки, масштабованості та енергоефективності, а також протоколи передачі даних та показники якості обслуговування.

Проведено аналіз технологій 5G для підтримки IoT-сенсорів у різних випадках використання, включаючи Smart Industry та Smart Home. Пояснено технології доступу NB-IoT та LTE-M, архітектуру мережевих зрізів, використання Edge Computing для обробки IoT-даних, проблеми масштабування та методи оптимізації передачі даних.

Ключові слова: 5g, Інтернет Речей, Iot, Мережева Архітектура, Massive Mimo, Edge Computing, Продуктивність Мережі, Моделювання Мереж, Smart City, Nb-Iot, Масштабованість.

ABSTRACT

This thesis examines the operational characteristics of fifth-generation networks in supporting systems that utilize smart devices and develops a 5G network model to evaluate its effectiveness based on performance metrics.

The aim of the thesis is to identify the capabilities of 5G technologies for supporting IoT systems, examine the architecture of modern networks and key technologies, and develop a practical network model to evaluate its scalability and performance.

The paper examines the theoretical foundations of 5G networks and IoT systems, the architecture of fifth-generation networks, and key technologies such as Massive MIMO, Network Slicing, and Edge Computing. The requirements of IoT systems for network infrastructure are examined, including latency, scalability, and energy efficiency metrics, as well as data transmission protocols and quality of service indicators.

An analysis of 5G technologies for supporting IoT sensors in various use cases, including Smart Industry and Smart Home, is conducted. The paper explains NB-IoT and LTE-M access technologies, network slicing architecture, the use of Edge Computing for IoT data processing, scaling challenges, and methods for optimizing data transmission.

Keywords: 5G, Internet of Things, IoT, network architecture, Massive MIMO, edge computing, network performance, network modeling, smart city, NB-IoT, scalability.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Стрімкий розвиток технологій Інтернету речей та їх широке впровадження у різних сферах життя від розумних міст до промислової автоматизації ставить нові вимоги до мережевої інфраструктури. Вже на початку 2026 року кількість підключених IoT-пристроїв у світі перевищує 25 мільярдів, що створює нечуване навантаження на існуючі мережі зв'язку. Традиційні мережі четвертого покоління 4G/LTE не здатні забезпечити необхідний рівень ефективності для масового впровадження IoT через обмеження у пропускній здатності, високу затримку передачі даних та недостатню масштабність.

Мережі п'ятого покоління 5G розроблені з урахуванням специфічних вимог і пропонують перспективні можливості, наприклад: надвисоку швидкість передачі даних до 20 Гбіт/с, мінімальну затримку менше 1 мс, можливість одночасно підключатися до мільйона пристроїв на квадратний кілометр та високу енергоефективність. Ключові технології 5G, такі як Massive MIMO, Network Slicing та Edge Computing, створюють принципово нові можливості для побудови обсяжних систем з використанням Інтернету речей.

Однак впровадження 5G-мереж для підтримки IoT потребує кілька умов: необхідність оптимізації використання радіоресурсів, забезпечення якості обслуговування QoS для різного трафіку, ефективне управління енергоспоживанням пристроїв та масштабування мережі під велике навантаження. Моделювання 5G-мереж дозволяє побачити ці аспекти в контрольованому середовищі, оцінити ефективність різних архітектурних рішень та оптимізувати параметри мережі.

Таким чином, актуальність теми дослідження пояснюється необхідністю повного аналізу можливостей 5G-технологій для підтримки IoT-систем та розробки практичних рекомендацій щодо проектування та оптимізації таких мереж.

Мета і завдання дослідження. Метою кваліфікаційної роботи є розбір особливостей 5G-мереж для підтримки систем Інтернету речей та розробка моделі мережі з оцінкою її ключових показників продуктивності.

Для хорошого результату поставленої мети необхідно проаналізувати теоретичну складову функціонування мереж п'ятого покоління та систем IoT, вивчити архітектуру 5G та потрібні технології, такі як Massive MIMO, Network Slicing та Edge Computing. Важливим завданням є потреба визначити вимоги IoT-систем до мережевої інфраструктури, включаючи показники затримки та масштабу, а також вивчення протоколів передачі даних у IoT-системах та показників якості обслуговування у 5G-мережах. Необхідно створити сценарії використання 5G для IoT у контексті Smart Industry та Smart Home, а також визначити технології доступу, такі як NB-IoT та LTE-M. Також слід приділити увагу архітектурі мережі та можливостям Edge Computing для обробки IoT-даних. Практична частина роботи буде містити розробку моделі 5G-мережі для підтримки IoT-пристроїв у програмному середовищі моделювання під назвою GNS3, перевірка навантаження з різною кількістю IoT-вузлів та кількістю трафіку, дослідження показників ефективності мережі, включаючи пропускну здатність, затримку передачі пакетів, відсоток втрат. Останнім етапом є підведення підсумків результатів моделювання та оцінка аспектів, 5G-мережі для IoT, про які була мова раніше.

Об’єкт і предмет дослідження. Об'єктом дослідження є мережі п'ятого покоління та системи Інтернету речей.

Предметом дослідження є процеси передачі даних у 5G-мережах при підтримці IoT-пристроїв, показники швидкості обслуговування та методи оптимізації мережевої інфраструктури.

Методи дослідження. Для вирішення поставлених у роботі завдань буде використовуватися наукова література та технічна документація щодо стандартів 5G та IoT, ознайомлення з архітектурою мереж п'ятого покоління та їх компонентів, порівняння технологій доступу та протоколів передачі даних. Відбуватися це буде у вигляді комп'ютерного моделювання мережі у

спеціалізованому програмному середовищі GNS3, розглядаються випадки з різними параметрами мережі та навантаження. Для обробки отриманих даних використовується аналіз результатів моделювання та побудова графічних залежностей, а також здійснюється оцінка мережі за допомогою QoS.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ФУНКЦІОНУВАННЯ 5G-МЕРЕЖ ТА IoT

1.1 Концепція та архітектура мереж п’ятого покоління

Мережі п'ятого покоління 5G представляють собою якісно новий етап розвитку технологій, що забезпечують сучасні можливості для передачі даних, підключення пристроїв та надання послуг. На відміну від попередніх поколінь мобільного зв'язку, які в основному робили акцент на покращенні швидкості передачі даних для користувачів мобільних телефонів, то 5G розроблялися з урахуванням потреб різноманітних галузей суспільства, таких як Інтернет речей, автономний транспорт, автоматизацію промисловості, розумні міста та звісно ж медицину.

Еволюція мобільних мереж зв’язку. Розвиток мобільних мереж зв'язку пройшов кілька ключових етапів. Перше покоління 1G з'явилося у 1980-х роках та використовувало аналогову технологію передачі голосу і забезпечувало лише базові можливості мобільного зв'язку. Друге покоління (2G), представлене стандартами GSM та CDMA у 1990-х роках, перейшло на цифрову передачу даних, що дозволило не тільки покращити якість голосового зв'язку, але й надати базові послуги передачі даних, такі як SMS та доступ до Інтернету з дуже малою швидкістю.

Третє покоління 3G, яке стало стандартом на початку 2000-х років значно підвищило швидкість передачі даних до кількох мегабіт на секунду, що зробило можливим мобільний доступ до Інтернету, відеодзвінки та мультимедіа. Четверте покоління 4G або LTE почало активно з’являтися з 2010 року та забезпечило швидкість передачі даних до 100-300 Мбіт/с, низьку затримку та

високу якість мобільного доступу, що стало основою для розвитку мобільних додатків, можливості транслювати події у реальному часі та соціальних мереж.

П'яте покоління мобільного зв'язку виходить за межі простого збільшення швидкості передачі даних. Концепція 5G базується на трьох основних сценаріях використання, визначених міжнародним союзом електрозв'язку ITU:

- Enhanced Mobile Broadband (eMBB) - покращений мобільний широкосмуговий доступ з швидкістю до 20 Гбіт/с для завантаження та до 10 Гбіт/с для відправлення даних;
- Ultra-Reliable Low-Latency Communications (URLLC) - дуже надійний зв'язок з низькою затримкою менше 1 мс для критичних ситуацій;
- Massive Machine-Type Communications (mMTC) - масове підключення обладнання з можливістю обслуговування до 1 мільйона пристроїв на квадратний кілометр.

Ключові характеристики 5G-мереж. Мережі п'ятого покоління характеризуються набором технічних параметрів, що значно перевершують можливості попередніх поколінь. Максимальна швидкість передачі даних у 5G може досягати 20 Гбіт/с для завантаження, що у 20 разів більше, ніж у 4G. Реальна швидкість для користувачів становить від 100 Мбіт/с до кількох гігабіт на секунду залежно від умов та навантаження мережі.

Затримка передачі даних у 5G-мережах зменшена до 1 мілісекунди, коли у 4G 30-50 мілісекунд, це зроблено для URLLC, що є важливим для застосувань в реальному часі, таких як дистанційне керування пристроями, автономне водіння та автоматизація промислової діяльності.

Можливість підключення пристроїв у 5G досягає 1 мільйона пристроїв на квадратний кілометр, що робить можливим масове використання IoT-систем у міському середовищі. Енергоефективність мережі покращена у 100 разів порівняно з 4G, що дозволяє IoT-пристроям працювати від батарей протягом 10 років без потреби заміняти їх.

Архітектура 5G-мереж. Архітектура мереж п'ятого покоління базується на принципах гнучкості, масштабованості та програмної конфігурації. На відміну

від попередніх поколінь, де мережева архітектура була жорстко визначеною та орієнтованою на технічну частину, то 5G використовує концепцію програмно-визначених мереж Software-Defined Networking (SDN) та віртуалізації мережевих функцій Network Functions Virtualization (NFV).

Архітектура 5G складається з трьох основних компонентів: радіомережі доступу Radio Access Network (RAN), транспортної мережі та ядра мережі Core Network.

Радіомережа доступу RAN. Радіомережа доступу 5G, або NG-RAN (Next Generation RAN) включає базові станції нового покоління gNodeB, які забезпечують радіозв'язок з пристроями користувача. На відміну від базових станцій 4G eNodeB, gNodeB підтримують нові радіоінтерфейси New Radio (NR) та можуть працювати у різних частотних діапазонах.

5G використовує три основні частотні діапазони:

- Низькочастотний діапазон (Sub-1 GHz) - забезпечує широке покриття та здатність проходити через перешкоди, але обмежену пропускну здатність.
- Середньочастотний діапазон (1-6 GHz) - ідеальний варіант, який підтримує баланс між покриттям та пропускною здатністю, основний діапазон для масового використання 5G.
- Високочастотний діапазон міліметрових хвиль 24-100 GHz mmWave - надвисока пропускна здатність, але обмежене покриття та вразливість до перешкод.

Архітектура RAN у 5G може бути реалізована у різних конфігураціях. Традиційна архітектура передбачає монолітну базову станцію, де всі функції виконуються в одному пристрої. Однак 5G також підтримує розподілену архітектуру, де функції базової станції розділені на центральний блок та розподілені блоки що дозволяє більш гнучко розміщувати обладнання та оптимізувати використання ресурсів.

Ядро мережі 5G Core. Ядро мережі 5G, або Next Generation Core (NGC) представляє собою повністю перероблену архітектуру, що базується на сервісно-орієнтованому підході Service-Based Architecture (SBA). На відміну від ядра 4G

Evolved Packet Core (EPC), яке використовувало точкові з'єднання між мережевими пристроями, 5GC реалізує мережеві функції як незалежні сервіси, які взаємодіють через стандартизовані інтерфейси.

Сервісно-орієнтована архітектура 5GC дозволяє успішно масштабувати мережеві функції, розгортати їх у хмарному середовищі та адаптувати мережу. Кожна мережева функція надає свої послуги через HTTP/2-based інтерфейси, що спрощує інтеграцію та автоматизацію.

Розділення площин управління та користувацьких даних. Важливою особливістю архітектури 5G є чітке розділення площини управління (Control Plane) та площини користувацьких даних (User Plane). Площина управління відповідає за сигналізацію, управління з'єднаннями, мобільністю та політиками, тоді як площина користувацьких даних займається безпосередньою передачею даних користувачів.

Таке розділення дозволяє незалежно масштабувати та оптимізувати кожну площину. Наприклад, функції користувацької площини UPF, які наведені у таблиці 1.1.

Таблиця 1.1 – Основні мережеві функції 5G Core

Назва функції	Призначення
AMF (Access and Mobility Management Function)	Управління доступом та мобільністю, реєстрація пристроїв, автентифікація, управління переміщенням між базовими станціями.
SMF (Session Management Function)	Управління сесіями передачі даних, встановлення, модифікація та завершення сесій.
UPF (User Plane Function)	Маршрутизація та пересилання пакетів даних користувачів, обробка трафіку.
UDM (Unified Data Management)	Уніфіковане управління даними користувачів, зберігання профілів абонентів та параметрів підписки.
AUSF (Authentication Server Function)	Забезпечення безпечної автентифікації пристроїв у мережі.

Назва функції	Призначення
PCF (Policy Control Function)	Управління політиками мережі, визначення правил QoS та тарифікації.
NRF (Network Repository Function)	Репозиторій мережевих функцій, виявлення та реєстрація доступних сервісів.
NSSF (Network Slice Selection Function)	Вибір відповідного мережевого зрізу для конкретного пристрою або послуги.

Вони можуть бути розміщені ближче до користувачів на периферії мережі, що зменшує затримку, тоді як функції площини управління можуть бути централізовані у хмарі.

Інтерфейси та протоколи. Архітектура 5G визначає набір стандартизованих інтерфейсів для взаємодії між різними частинами мережі. Основні інтерфейси включають:

- N1 - інтерфейс між користувацьким обладнанням (UE) та AMF для сигналізації площини управління;
- N2 - інтерфейс між RAN (gNodeB) та AMF для управління доступом;
- N3 - інтерфейс між RAN та UPF для передачі користувацьких даних;
- N4 - інтерфейс між SMF та UPF табл. 1.1 для управління сесіями;
- N6 - інтерфейс між UPF та зовнішніми мережами передачі даних наприклад Інтернет.

Всередині ядра мережі мережеві функції взаємодіють через сервісні інтерфейси (Service-Based Interfaces), які використовують RESTful API та формат JSON для обміну даними.

Підтримка різних типів мереж. Архітектура 5G розроблена з урахуванням необхідності підтримки різних типів мереж. Вона підтримує як автономне розгортання Standalone (SA), де 5G RAN підключається до 5G Core, так і неавтономне розгортання Non-Standalone (NSA), де 5G RAN працює у зв'язці з існуючим ядром 4G EPC.

Неавтономний режим дозволяє операторам швидше розгорнути 5G-покриття, використовуючи існуючу інфраструктуру 4G, тоді як автономний режим забезпечує повний набір можливостей 5G, включаючи низьку затримку та мережеві зрізи.

Крім того, 5G підтримує інтеграцію з мережами попередніх поколінь, що забезпечує безперервність послуг при переміщенні пристроїв між різними типами мереж.

Віртуалізація та хмарні технології. Сучасна архітектура 5G інтегрована з хмарними технологіями та концепцією віртуалізації мережевих функцій (NFV). Мережеві функції 5G Core реалізуються як програмні компоненти, які можуть виконуватися на стандартному серверному обладнанні у хмарному середовищі замість спеціалізованого залыза.

Це дозволяє операторам гнучко масштабувати мережу, швидко впроваджувати нові послуги та оптимізувати витрати на інфраструктуру. Мережеві функції можуть бути розгорнуті у публічних, приватних або гібридних хмарах залежно від вимог безпеки, продуктивності та обмежень.

Використання контейнерних технологій, таких як Kubernetes або Docker, що дозволяють автоматизувати розгортання, масштабування та управління мережевими функціями, що є критичним для гарантії високої безпеки та надійності мережі.

1.2 Основні технології 5G (Massive MIMO, Network Slicing, Edge Computing)

Мережі п'ятого покоління базуються на кількох інноваційних технологіях, які забезпечують їх унікальні характеристики та можливості. Три ключові технології - Massive MIMO, Network Slicing та Edge Computing є основними для високої продуктивності, гнучкості та ефективності 5G-мереж у роботі з сенсорами, датчиками, та автоматизованим обладнанням.

Massive MIMO (Multiple Input Multiple Output). Технологія Massive MIMO є покращеною версією технології MIMO, яка використовувалася у

попередніх поколіннях мобільного зв'язку. Якщо традиційні системи MIMO у 4G використовували від 2 до 8 антен, то Massive MIMO у 5G може містити десятки або навіть сотні антен на одній станції.

Принцип роботи Massive MIMO базується на використанні великої кількості антен для одночасного обслуговування багатьох користувачів на одній частоті. Кожна антена може незалежно передавати та приймати сигнали, що дозволяє формувати вузькоспрямовані промені (beamforming) у напрямку конкретних користувачів. Нова технологія має переваги над попередніми.

По-перше, Massive MIMO значно підвищує спектральну ефективність мережі. Завдяки можливості одночасного обслуговування багатьох користувачів на одній частоті методом просторового мультиплексування, пропускна здатність мережі зростає зі зростанням кількості антен. Тобто, система з 64 антенами може забезпечити у 10-20 разів вищу спектральну ефективність порівняно з традиційними системами.

По-друге, технологія beamforming дозволяє концентрувати енергію сигналу у напрямку конкретного користувача, що підвищує якість прийому. Це особливо важливо у щільно населених міських районах, де велика кількість пристроїв конкурує за доступ до мережі.

По-третє, Massive MIMO покращує енергоефективність мережі. Завдяки прямій передачі сигналу, базова станція може використовувати меншу потужність для того ж рівня покриття, що зменшує енергоспоживання та витрати.

Для IoT технологія Massive MIMO має велике значення. Вона дозволяє базовій станції одночасно обслуговувати велику кількість пристроїв, які зазвичай передають невеликі обсяги даних, але вимагають надійного з'єднання. Просторове мультиплексування забезпечує ефективне використання радіоресурсів навіть при дійсно великій кількості підключених пристроїв.

Реалізація Massive MIMO у 5G включає використання активних антенних систем Active Antenna Systems (AAS), де кожна антена має власний передавач та приймач. Це дозволяє адаптувати характеристики антен до поточних умов та розподілу сигналу для користувачів.

Network Slicing (Мережеві зрізи). Network Slicing є однією з найбільш значущих концепцій у архітектурі 5G, що дозволяє створювати декілька віртуальних мереж на основі єдиної фізичної інфраструктури. Кожен мережевий зріз представляє собою логічно ізольовану мережу з власними характеристиками, оптимізованими для конкретного типу послуг.

Ця технологія заснована на технологіях віртуалізації мережевих функцій NFV та програмно-визначених мереж SD). Фізична інфраструктура мережі, включаючи базові станції, транспортну мережу та обчислювальні ресурси, може бути розподілена між різними зрізами залежно від їх потреб та пріоритетів.

Кожен мережевий зріз може мати унікальні характеристики щодо пропускної здатності, затримки, надійності, безпеки та мобільності. Наприклад, зріз для послуг покращеного мобільного широкосмугового доступу eMBB буде оптимізований для високої пропускної здатності, зріз для критичних застосувань URLLC - для мінімальної затримки та максимальної надійності, а зріз для масового IoT mMTC - для підтримки великої кількості пристроїв з низьким енергоспоживанням.

Для систем IoT технологія Network Slicing є надзвичайно важливою, оскільки різні типи IoT систем та мереж мають принципово різні вимоги до мережі. Розумні лічильники потребують рідкісної передачі невеликих обсягів даних з низьким енергоспоживанням, системи відеоспостереження вимагають високої пропускної здатності, а промислові системи потребують надзвичайно низької затримки та високої надійності.

Управління мережевих зрізів включає їх створення, конфігурацію, моніторинг, модифікацію та видалення. Оркестратор мережевих зрізів відповідає за розподіл ресурсів, забезпечення ізоляції між зрізами та

адаптацію до змінних умов. Автоматизація цих процесів є суттєвою для ефективного управління одночасно великий набір зрізів у масштабах оператора.

Безпека мережевих зрізів є важливим аспектом їх створення та запуску. Кожен зріз повинен бути захищений від несанкціонованих атак, а порушення безпеки в одному зрізі не повинно впливати на інші зрізи. Це вимагає реалізації механізмів автентифікації, шифрування та контролю доступу на всіх рівнях архітектури.

Edge Computing (Периферійні обчислення). Edge Computing є архітектурною концепцією, що передбачає розміщення ресурсів та функцій обробки даних на периферії мережі, ближче до кінцевих користувачів та пристроїв. Для 5G-мереж це означає розгортання серверів та додатків безпосередньо на базових станціях або у локальних дата-центрах, замість централізованої обробки у віддалених хмарних центрах.

Основна задумка Edge Computing - це мінімізація затримки передачі даних та зменшення навантаження на транспортну мережу шляхом обробки даних якомога ближче до їх джерела. Це особливо важливо для застосувань реального часу, таких як автономне водіння, промислова автоматизація та інтерактивні ігри, де навіть затримка у кілька десятків мілісекунд може вплинути на якість роботи.

Edge Computing є архітектурною концепцією, що передбачає розміщення обчислювальних ресурсів та функцій обробки даних на периферії мережі, ближче до кінцевих користувачів та пристроїв. У контексті 5G-мереж це означає розгортання серверів та додатків безпосередньо на базових станціях або у локальних дата-центрах, замість централізованої обробки у віддалених хмарних центрах обробки даних.

Основна мета Edge Computing – мінімізація затримки передачі даних та зменшення навантаження на транспортну мережу шляхом обробки даних якомога ближче до їх джерела. Це особливо важливо для застосувань реального часу, таких як автономне водіння, доповнена реальність,

промислова автоматизація та інтерактивні ігри, де навіть затримка у кілька десятків мілісекунд може бути критичною.

Архітектура Edge Computing у 5G-мережах працює за принципом Multi-access Edge Computing (MEC), стандартизованій організацією ETSI. MEC-платформа надає обчислювальні ресурси, сховища даних та мережеві сервіси на периферії мережі, дозволяючи розробникам розгортати додатки з низькою затримкою та високою продуктивністю.

Інтеграція Edge Computing з архітектурою 5G відбувається через розміщення функцій користувацької площини UPF табл. 1.1 на периферії мережі. Це дозволяє локально маршрутизувати трафік до MEC-додатків без необхідності передавати дані через централізоване ядро мережі. Така архітектура забезпечує затримку на рівні усього декількох мілісекунд між пристроєм та додатком.

1.3 Особливості функціонування IoT-систем та вимоги до мережевої інфраструктури

Інтернет речей представляє собою мережу взаємопов'язаних фізичних об'єктів, обладнаних сенсорами та засобами зв'язку, які здатні збирати, обмінюватися та обробляти дані без прямого втручання людини. IoT-системи зараз використовуються в багатьох випадках, від простих побутових пристроїв до складних промислових систем управління, що ставить високі та часто суперечливі вимоги до мережевої інфраструктури.

Архітектура IoT-систем. Типова архітектура IoT-системи складається з чотирьох основних рівнів: рівня сприйняття, мережевого рівня, рівня обробки даних та рівня застосувань.

Рівень сприйняття включає фізичні пристрої сенсори, камери та інші пристрої, які взаємодіють з фізичним світом. Ці пристрої збирають дані про навколишнє середовище (температуру, вологість, рух, освітлення тощо) або виконують дії на основі отриманих команд, такі як увімкнення обладнання, регулювання параметрів.

Мережевий рівень забезпечує передачу даних між пристроями та системами обробки. Цей рівень може включати різні технології зв'язку від локальних бездротових мереж (Wi-Fi, Bluetooth) до глобальних мереж мобільного зв'язку (5G, NB-IoT, LTE-M). Вибір технології залежить від вимог конкретного застосування щодо дальності зв'язку, пропускної здатності, енергоспоживання та вартості.

Рівень обробки даних відповідає за зберігання, аналіз та управління даними, отриманими від IoT-пристроїв. Цей рівень може бути реалізований у хмарних дата-центрах, на периферійних серверах (Edge Computing) або у гібридній конфігурації. Тут виконуються завдання аналітики даних, машинного навчання, прийняття рішень та управління пристроями.

Рівень застосувань надає кінцеві послуги користувачам та іншим системам. Це можуть бути веб-додатки, мобільні застосунки, системи візуалізації, інтеграція з корпоративними системами управління або API для взаємодії з іншими сервісами.

Вимоги IoT до мережевої інфраструктури. Різноманітність застосувань Інтернету речей створює низку вимог до мережевої інфраструктури, які часто вимагають складних рішень.

Затримка передачі даних. Затримка (latency) є одним з основних параметрів для багатьох IoT систем. Вона визначається як час між відправленням даних пристроєм та отриманням відповіді. Різні типи застосувань мають різні вимоги до затримки.

Для критичних промислових застосувань, таких як системи безпеки, затримка повинна бути менше 1 мілісекунди. Це дозволяє системам реагувати на події у реальному часі та забезпечувати синхронізацію між множиною пристроїв.

Масштабованість та щільність підключення. Масштабованість є базовою вимогою для IoT-систем, оскільки кількість підключених пристроїв постійно зростає. У міських районах компактність IoT-пристроїв може досягати десятків або сотень тисяч на квадратний кілометр, включаючи

сенсори паркування, системи моніторингу трафіку, камери спостереження та інші пристрої.

Мережева інфраструктура повинна підтримувати одночасне підключення великої кількості пристроїв без явного спаду продуктивності. 5G-мережі розроблені з можливістю підключення до 1 мільйона пристроїв на квадратний кілометр, що значно перевищує можливості перед попередніми масштабами.

Енергоефективність. Енергоефективність це теж важлива вимога для IoT-пристроїв, які працюють від батарей. Багато IoT-застосувань передбачають розміщення пристроїв у важкодоступних місцях, де заміна батарей є складною або дорогою. Типова вимога це забезпечення автономної роботи пристрою протягом 10 років від однієї батареї.

Енергоспоживання IoT-пристрою залежить від кількох речей: потужності передавача, частоти передачі даних, складності протоколів зв'язку та часу перебування у активному режимі. Для мінімізації енергоспоживання використовуються різні, в залежності від потреб та бюджету.

Безпека та конфіденційність. Компрометація пристроїв може призвести до серйозних наслідків від витоку конфіденційних даних до фізичної шкоди. IoT-пристрої часто є вразливими до атак через обмежені обчислювальні ресурси, відсутність можливості оновлення програмного забезпечення та тривалий термін експлуатації.

Мережева інфраструктура повинна забезпечувати кілька рівнів захисту. Автентифікація пристроїв при підключенні до мережі, шифрування даних при передачі даних, ізоляція трафіку.

Якість обслуговування (QoS). Якість обслуговування визначає набір параметрів, які характеризують продуктивність мережі для конкретного типу трафіку. Для IoT-систем ключовими параметрами QoS є пропускна здатність, затримка та відсоток втрат пакетів.

Системи вимагають різних профілів QoS. Відеопотоки від камер спостереження потребують високої пропускної здатності та низького відсотка втрат пакетів, але можуть значну затримку. Промислові системи управління вимагають мінімальної затримки, але передають невеликі обсяги даних.

Отже розділ показує що нові 5G мережі мають немалий потенціал для ефективної та безпечної підтримки Інтернету речей, мають значні переваги над минулими технологіями, та з кожним роком використовуються все частіше.

РОЗДІЛ 2 АНАЛІЗ ТЕХНОЛОГІЙ 5G ДЛЯ ПІДТРИМКИ IoT-ПРИСТРОЇВ

2.1 Сценарії використання 5G для IoT (Smart City, Smart Industry, Smart Home)

Мережі п'ятого покоління відкривають принципово нові можливості для впровадження систем Інтернету речей у різних галузях економіки та повсякденному житті. Три ключові напрямки – розумні міста, розумна промисловість та розумні будинки – демонструють різноманітність вимог до мережевої інфраструктури та потенціал 5G-технологій для їх задоволення. Кожен сценарій має унікальні характеристики щодо щільності пристроїв, допустимої затримки, обсягів трафіку та критичності відмов. Основні відмінності між цими напрямками наведено в табл. 2.1.

Таблиця 2.1 – Порівняльна характеристика сценаріїв використання IoT у 5G-мережах

Параметр	Smart City	Smart Industry	Smart Home

Параметр	Smart City	Smart Industry	Smart Home
Основні застосування	Управління трафіком, відеоспостереження, розумне освітлення, моніторинг довкілля	Промислова автоматизація, дистанційне керування, прогнозне обслуговування, цифрові двійники	Клімат-контроль, системи безпеки, розумні прилади, мультимедіа
Ключові вимоги до мережі	Висока щільність підключень, стабільне покриття, енергоефективність	Надзвичайно низька затримка, висока надійність, гарантована пропускна здатність	Зручність інтеграції, безпека даних, підтримка мультимедіа
Переважні технології доступу	NB-IoT, LTE-M, 5G NR	5G URLLC, приватні 5G-мережі, Edge Computing	Wi-Fi 6/7, 5G eMBB, Bluetooth Mesh, Zigbee
Очікуваний рівень затримки	10–100 мс (моніторинг), <50 мс (відеоаналітика)	1–10 мс (критичне управління)	10–50 мс (інтерактивні сервіси)
Щільність пристроїв	До 1 млн/км²	До 100 тис./км² (локально)	До 500 пристроїв на об'єкт

Розумне місто (Smart City) базується на масовому розгортанні сенсорів та виконавчих пристроїв для оптимізації міської інфраструктури. Системи управління трафіком, розумне освітлення та моніторинг довкілля генерують велику кількість невеликих повідомлень, що вимагає технологій з низьким енергоспоживанням та широким покриттям. Відеоаналітика та системи безпеки, навпаки, потребують високої пропускної здатності та обробки даних у реальному часі, що досягається за рахунок інтеграції 5G eMBB та Edge Computing.

Промисловий IoT (Smart Industry) висуває найжорсткіші вимоги до мережі. Промислові роботи, автоматизовані транспортні системи та системи контролю якості потребують затримки менше 10 мс та надійності на рівні

99.9999%. Для таких застосувань використовуються приватні 5G-мережі з виділеними мережевими зрізами (Network Slicing), що гарантують ізольовані ресурси та стабільні параметри QoS. Edge Computing дозволяє обробляти дані безпосередньо на виробництві, усуваючи залежність від віддалених хмарних центрів.

Розумний будинок (Smart Home) орієнтований на комфорт, енергоефективність та безпеку мешканців. Тут переважають пристрої з помірними вимогами до затримки, але з високою потребою у сумісності та простоті налаштування. 5G-мережі доповнюють локальні протоколи (Wi-Fi, Zigbee, Thread), забезпечуючи стабільний зовнішній зв'язок, хмарну синхронізацію та підтримку мультимедійних сервісів високої роздільної здатності. Більш детальний аналіз вимог до якості обслуговування для різних категорій IoT наведено в табл. 2.4. Багаторівневу архітектуру IoT для Smart City ілюструє рис. 2.1.

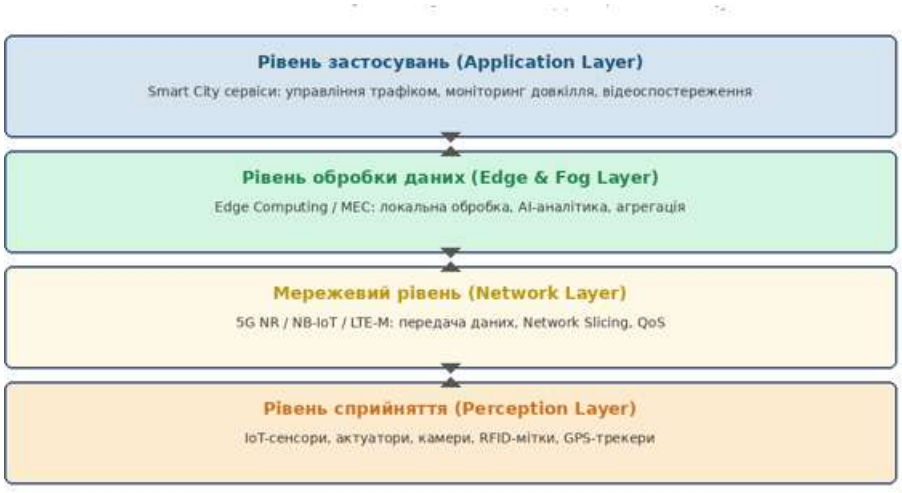

Рисунок 2.1 – Багаторівнева архітектура IoT для Smart City

2.2 Технології доступу для IoT у мережах 5G (NB-IoT, LTE-M) та методи оптимізації передачі даних

Для ефективної підтримки різноманітних IoT-пристроїв у стандартах 3GPP розроблені спеціалізовані технології радіодоступу. Дві основні

технології – NB-IoT та LTE-M – забезпечують різні баланси між пропускною здатністю, покриттям, енергоспоживанням та вартістю. Вибір конкретної технології залежить від типу застосування, умов розгортання та економічних обмежень. Порівняльний аналіз ключових параметрів технологій доступу подано в табл. 2.2.

Таблиця 2.2 – Порівняння технологій радіодоступу для IoT

Параметр	NB-IoT	LTE-M (Cat-M1)	5G NR (eMBB/URLLC)
Смуга пропускання	180 кГц	1.4 МГц	5–400 МГц (гнучка)
Макс. швидкість передачі	~250 кбіт/с (DL), ~20 кбіт/с (UL)	До 1 Мбіт/с	До 20 Гбіт/с (теор.), 100 Мбіт/с–1 Гбіт/с (реал.)
Затримка	1.5–10 с	10–15 мс	1–10 мс (URLLC), 10–50 мс (eMBB)
Покриття (покращення)	+20 дБ до GSM	+15 дБ до LTE	Залежить від частотного діапазону
Енергоспоживання	Дуже низьке (10+ років від батареї)	Низьке (5–10 років)	Помірне/високе (залежить від режиму)
Підтримка мобільності	Обмежена (handover не підтримується)	Повна підтримка	Повна підтримка
Вартість модуля	$2–5	$5–10	$15–50+
Типові застосування	Лічильники, сенсори довкілля, трекери активів	Носимі пристрої, телематика, системи безпеки	Відеокамери, AR/VR, промислові роботи

NB-IoT оптимізований для масового розгортання стаціонарних пристроїв з рідкісною передачею даних. Завдяки вузькій смузі частот та спрощеній архітектурі, технологія забезпечує глибоке покриття та мінімальне енергоспоживання. Режим Power Saving Mode (PSM) та Extended Discontinuous Reception (eDRX) дозволяють пристроям перебувати у стані сну тривалий час, прокидаючись лише для передачі телеметрії. Це робить

NB-IoT ідеальним для розумних лічильників, моніторингу інфраструктури та сільськогосподарських сенсорів. Порівняльну архітектуру NB-IoT та LTE-M наведено на рис. 2.2.

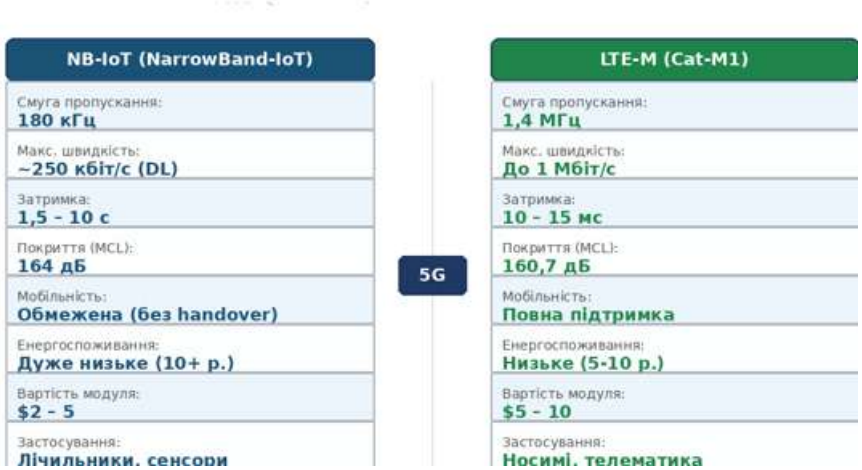

Рисунок 2.2 – Порівняльна архітектура NB-IoT та LTE-M у мережі 5G

LTE-M, навпаки, підтримує вищу пропускну здатність, мобільність та голосовий зв'язок (VoLTE). Технологія підходить для пристроїв, які потребують більш інтенсивного обміну даними або переміщуються між зонами покриття. Трекери транспорту, носимі медичні пристрої, розумні торгові автомати та системи екстреного виклику використовують LTE-M завдяки збалансованим характеристикам.

Окрім вибору технології доступу, критичним аспектом є оптимізація передачі даних на рівні протоколів та мережевих механізмів. IoT-пристрої часто працюють в умовах обмежених ресурсів, тому традиційні підходи до передачі даних є неефективними. Основні методи оптимізації, що застосовуються у 5G-мережах для IoT, систематизовано в табл. 2.3.

Таблиця 2.3 – Методи оптимізації передачі даних у 5G для IoT

Метод оптимізації	Опис принципу дії	Переваги	Сфера застосування
Стиснення заголовків (ROHC)	Зменшення розміру IP/UDP/TCP заголовків до 1–3 байт	Зниження накладних витрат на 60–80%	NB-IoT, LTE-M, передачі малих пакетів

Метод оптимізації	Опис принципу дії	Переваги	Сфера застосування
Агрегація даних	Накопичення кількох повідомлень перед відправкою	Зменшення кількості сеансів зв'язку	Моніторинг довкілля, лічильники
Early Data Transmission (EDT)	Передача даних під час процедури підключення без встановлення повного з'єднання	Скорочення затримки та енергоспоживання	Спорадичний трафік, тривожні сповіщення
Групова передача (Multicast)	Одночасна доставка однакових даних групі пристроїв	Зниження навантаження на радіоінтерфейс	Оновлення ПЗ, команди управління
Інтелектуальне планування трафіку	Адаптивний вибір часу передачі залежно від навантаження мережі	Балансування навантаження, зниження колізій	Масові розгортання сенсорів

Стиснення заголовків (ROHC) є особливо ефективним для IoT, оскільки розмір корисних даних часто менший за розмір стандартних мережевих заголовків. Використання спеціалізованих профілів стиснення дозволяє передавати телеметричні пакети розміром 10–20 байт без значних накладних витрат.

Механізми спрощеного підключення, такі як EDT та Suspend/Resume, усувають необхідність повної сигналізації при кожній передачі. Пристрій може надіслати дані безпосередньо під час ініціації з'єднання або відновити попередній сеанс без повторної автентифікації. Це критично важливо для пристроїв на батареях, де кожен цикл підключення скорочує термін служби.

Групова передача та інтелектуальне планування трафіку дозволяють мережі ефективно керувати великою кількістю пристроїв. Замість індивідуального виділення ресурсів кожному сенсору, мережа може групувати запити, планувати передачу у періоди низького навантаження та

уникати перевантаження радіоінтерфейсу. Це забезпечує стабільну роботу навіть при щільності підключень понад 100 тис. пристроїв на км².

Вимоги до якості обслуговування (QoS) у 5G-мережах реалізуються через механізми QoS Flow, які дозволяють динамічно пріоритезувати трафік. Різні категорії IoT-пристроїв потребують різних профілів QoS, що враховується при проектуванні мережевих зрізів. Детальні параметри QoS для основних категорій IoT наведено в табл. 2.4.

Таблиця 2.4 – Вимоги до якості обслуговування (QoS) для категорій IoT-пристроїв

Категорія IoT	Затримка	Надійність	Швидкість передачі	Щільність підключення	Енергоефективність
mMTC (масовий IoT)	1–10 с	99.9 %	<100 кбіт/с	До 1 млн/км²	Дуже висока (10+ років)
URLLC (критичний IoT)	1–10 мс	99.999–99.9999%	1–100 Мбіт/с	До 100 тис./км²	Помірна
eMBB (широкосмуговий IoT)	10–50 мс	99.9%	100 Мбіт/с–1 Гбіт/с	До 10 тис./км²	Низька/помірна

Мережеві зрізи (Network Slicing) дозволяють операторам створювати логічно ізольовані віртуальні мережі з гарантованими параметрами QoS. Наприклад, зріз для промислового IoT може резервувати ресурси для URLLC-трафіку, тоді як зріз для розумних лічильників працює у режимі best-effort з низьким пріоритетом. Така архітектура забезпечує одночасну підтримку різноманітних IoT-застосувань на єдиній фізичній інфраструктурі без взаємного впливу.

Інтеграція Edge Computing з технологіями доступу та оптимізації трафіку дозволяє досягти синергетичного ефекту. Локальна обробка даних зменшує обсяг інформації, що передається через мережу, знижує затримку та розвантажує ядро мережі. У поєднанні з NB-IoT/LTE-M та методами

стиснення та агрегації, це створює ефективну екосистему для масового впровадження IoT у 5G-середовищі.

2.3 Проблеми впровадження, стандартизація та перспективи розвитку (5G-Advanced)

Попри значний технічний потенціал мереж п'ятого покоління, їхнє масштабне впровадження для підтримки IoT-систем супроводжується низкою технічних, організаційних та економічних викликів. Успішна реалізація 5G-інфраструктури вимагає не лише оновлення радіомережі, але й комплексної трансформації архітектури ядра мережі, систем управління, безпеки та бізнес-моделей операторів. Стандартизація, регуляторні вимоги та технологічна еволюція відіграють ключову роль у подоланні цих бар'єрів.

Стандартизація та регуляторне середовище. Розвиток 5G-технологій координується міжнародними організаціями, серед яких провідну роль відіграє 3GPP (3rd Generation Partnership Project). Стандарт Release 15 (2018) заклав фундамент для NSA/SA архітектур, базових сценаріїв eMBB/URLLC/mMTC та механізмів Network Slicing. Release 16 (2020) поглибив підтримку промислового IoT, додавши вдосконалені механізми URLLC, інтеграцію з TSN (Time-Sensitive Networking) та підтримку бездротових сенсорних мереж. Release 17 (2022) розширив можливості для масового IoT, ввівши RedCap (Reduced Capability) пристрої, покращив підтримку супутникового зв'язку (NTN) та оптимізував енергоспоживання.

Паралельно з 3GPP, організації ITU-R, ETSI, IEEE та oneM2M розробляють суміжні стандарти для радіочастотного спектру, безпеки, інтероперабельності та архітектури IoT-платформ. Регуляторні органи різних країн виділяють частотні діапазони для 5G (Sub-6 GHz та mmWave), встановлюють вимоги до електромагнітної сумісності, захисту даних (GDPR, локальні закони) та кібербезпеки критичної інфраструктури. Відсутність глобальної гармонізації частот та регуляторних підходів ускладнює міжнародний роумінг IoT-пристроїв та масштабування рішень.

Технічні та експлуатаційні виклики впровадження. Розгортання 5G-мереж для IoT стикається з низкою технічних обмежень. По-перше, висока вартість інфраструктури: щільне покриття, особливо в діапазоні mmWave, вимагає значної кількості базових станцій, оптичних ліній зв'язку та Edge-серверів. По-друге, енергоспоживання мережі: хоча 5G оптимізована для енергоефективності на біт, загальне споживання енергії операторами зростає через збільшення кількості активних елементів та обчислювальних навантажень. По-третє, інтеграція з legacy-системами: багато підприємств використовують застарілі протоколи (Modbus, PROFIBUS, Zigbee 2006), які потребують шлюзів та адаптерів для сумісності з 5G-інфраструктурою.

Безпека та конфіденційність залишаються критичними викликами. Масове підключення IoT-пристроїв розширює поверхню атак, а обмежені обчислювальні ресурси багатьох сенсорів ускладнюють впровадження сучасних криптографічних протоколів. 5G покращує автентифікацію (5G-AKA, EAP-AKA'), шифрування на рівні радіоінтерфейсу та ізоляцію трафіку через мережеві зрізи, проте вразливості в ланцюжку постачання обладнання, програмному забезпеченні та хмарних платформах залишаються актуальними. Впровадження Zero Trust Architecture (ZTA) та механізмів continuous verification стає необхідним для критичних IoT-застосувань.

Економічні аспекти та моделі розгортання. Бізнес-моделі операторів трансформуються від продажу трафіку до надання сервісів та платформ. Private 5G-мережі стають популярним рішенням для промисловості, логістики та енергетики, дозволяючи підприємствам контролювати інфраструктуру, гарантувати QoS та захищати дані. Моделі Network-as-a-Service (NaaS) та Slice-as-a-Service дозволяють клієнтам орендувати віртуальні мережі з потрібними параметрами без капітальних витрат на обладнання.

Окупність інвестицій у 5G для IoT залежить від масштабу впровадження, галузі та рівня автоматизації. У промисловості ROI досягається через зниження простоїв, оптимізацію ланцюгів постачання та

підвищення якості продукції. У Smart City економічний ефект формується за рахунок енергозбереження, оптимізації трафіку та покращення якості послуг. Однак високі початкові витрати, невизначеність регуляторного середовища та фрагментація ринку IoT-платформ уповільнюють масове впровадження.

Перспективи розвитку: 5G-Advanced та шлях до 6G. Еволюція 5G продовжується у напрямку 5G-Advanced (Release 18–20), який закладає основу для переходу до 6G. Ключові напрямки розвитку включають інтеграцію штучного інтелекту та машинного навчання в управління мережею (AI-native RAN, intent-based networking), вдосконалення URLLC для тактильного інтернету та промислової автоматизації, розширення підтримки пасивного IoT (passive IoT) для безбатарейних сенсорів, та інтеграцію не наземних мереж (NTN) для глобального покриття.

Технології sidelink (PC5 інтерфейс) розвиваються для прямого зв'язку між пристроями без участі базової станції, що критично для V2X, промислових кластерів та аварійних комунікацій. Enhanced RedCap пристрої забезпечують баланс між продуктивністю та вартістю для середнього класу IoT-застосувань. Дослідження в галузі terahertz-діапазону, reconfigurable intelligent surfaces (RIS) та квантової криптографії формують технологічний фундамент 6G, очікуваного до 2030 року.

Для IoT-екосистеми 5G-Advanced означає перехід від підключення пристроїв до інтелектуального управління мережею, де AI оптимізує ресурси, прогнозує відмови та адаптує параметри в реальному часі. Інтеграція цифрових двійників мережі (network digital twins) дозволяє моделювати сценарії, тестувати конфігурації та оптимізувати продуктивність без впливу на робочу інфраструктуру.

Висновки щодо впровадження. Аналіз показує, що успішне впровадження 5G для IoT вимагає комплексного підходу: технічної модернізації, стандартизації, безпеки, економічної обґрунтованості та підготовки кадрів. Поетапне розгортання, використання приватних мереж, інтеграція Edge Computing та AI-оптимізація дозволяють мінімізувати ризики

та максимізувати віддачу. 5G-Advanced та майбутні 6G-технології відкриють нові горизонти для автономних систем, розширеної реальності та глобального IoT, перетворюючи мережі з інфраструктури передачі даних на інтелектуальні платформи для цифрової трансформації суспільства.

РОЗДІЛ 3 ПРАКТИЧНЕ МОДЕЛЮВАННЯ 5G-МЕРЕЖІ ДЛЯ ПІДТРИМКИ IoT

3.1 Постановка задачі моделювання

Метою практичного моделювання є побудова порівняльної моделі 4G та 5G мережевих сегментів з підключеними IoT-пристроями в середовищі GNS3, дослідження механізмів якості обслуговування та Network Slicing у 5G-сегменті, а також кількісна оцінка відмінностей у продуктивності та стійкості до перевантажень між двома поколіннями мереж.

У рамках дослідження визначено такі ключові задачі:

– розробити топологію мережі з двома маршрутизаторами (4G-M та 5G-M), комутатором, десятьма IoT-сенсорами (по п’ять на кожен сегмент) та спільним сервером застосунків;

– виконати IP-адресацію мережевих вузлів відповідно до обраної схеми адресного простору;

– налаштувати маршрутизацію між підмережами 4G-сегмента (192.168.1.0/24), 5G-сегмента (192.168.2.0/24) та серверними підмережами (10.0.1.0/24, 10.0.2.0/24);

– реалізувати механізм Network Slicing пріоритизацію трафіку QoS на 5G-маршрутизаторі для критичного сенсора IoT-sensor-6 аварійний трафік);

– експериментально дослідити поведінку обох сегментів у трьох режимах: базової зв'язності, штучного перевантаження DoS-атаки та фонового навантаження каналу;

– порівняти показники QoS затримку, коефіцієнт доставки пакетів, розподіл смуги пропускання між 4G та 5G сегментами.

Кількість IoT-пристроїв у моделі становить 10 вузлів: IoT-sensor-1..5 у 4G-сегменті та IoT-sensor-6..10 у 5G-сегменті. Тип трафіку – телеметричний (ICMP-пакети), з виділенням аварійного класу обслуговування для сенсора IoT-sensor-6 (перший вузол 5G-сегмента) [1].

3.2 Вибір програмного середовища моделювання

Для побудови та тестування мережевої моделі було обрано середовище GNS3 (Graphical Network Simulator 3) – відкрите програмне забезпечення для емуляції мережевих топологій [2]. Додатково для аналізу мережевого трафіку використовувався аналізатор пакетів Wireshark, інтегрований безпосередньо до GNS3 [3].

Переваги GNS3 для даного дослідження:

– підтримка реальних образів мережевого обладнання (Cisco IOS, RouterOS та ін.);

– інтеграція з Docker-контейнерами для емуляції IoT-вузлів на базі Linux;

– можливість налаштування реальних IP-адрес та мережевих протоколів;

– вбудована підтримка захоплення трафіку через Wireshark на будь-якому каналі;

– підтримка механізмів QoS та Policy-Based Routing через Cisco IOS, що дозволяє реалізувати Network Slicing.

IoT-сенсори змодельовано на основі Docker-контейнерів з операційною системою Linux [4], доступ до яких здійснювався через термінал PuTTY.

Маршрутизатори 4G-M та 5G-M реалізовані на базі образів Cisco IOS, що підтримують розширені механізми QoS та Policy Maps [5].

3.3 Розробка топології мережі

Розроблена топологія мережі включає паралельні сегменти 4G та 5G, що підключені до спільного сервера застосунків. Така архітектура дозволяє безпосередньо порівнювати поведінку мереж різних поколінь в ідентичних умовах навантаження. Логічна схема мережі має такий вигляд:

IoT-sensor-1..5 -> Switch1 -> 4G-M (192.168.1.1 / 10.0.1.1) -> Server

IoT-sensor-6..10 -> Switch1 -> 5G-M (192.168.2.1 / 10.0.2.1) -> Server

Реалізовану в середовищі GNS3 топологію наведено на рис. 3.1.

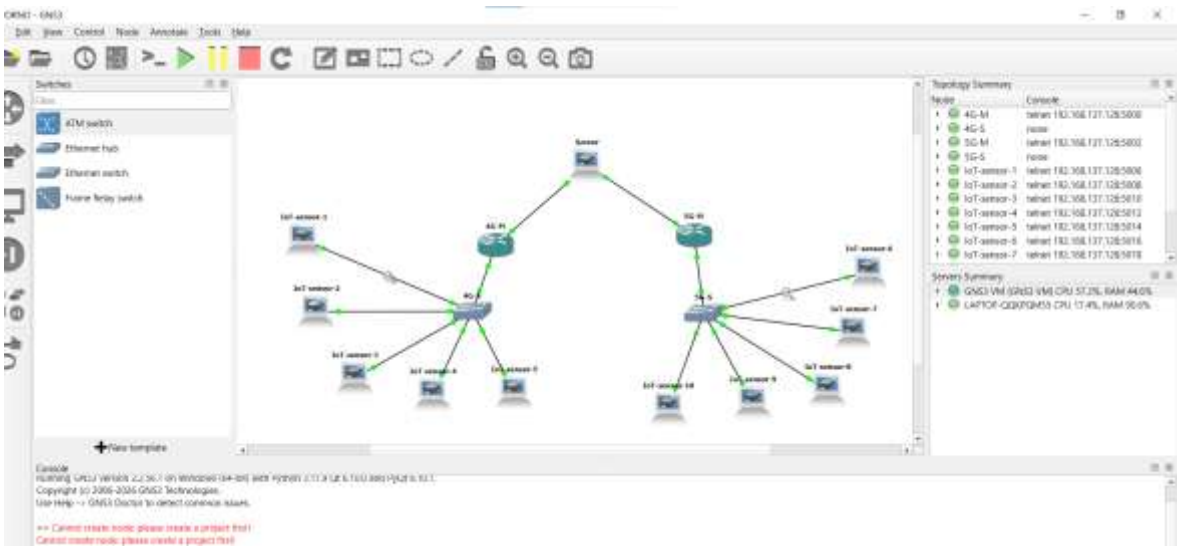

Рисунок 3.1 – Топологія мережі в середовищі GNS3

Топологія складається з двох паралельних сегментів: 4G-сегмент ліворуч та 5G-сегмент праворуч. Кожен сегмент включає п’ять IoT-сенсорів, підключених через комутатор до відповідного маршрутизатора. Обидва маршрутизатори 4G-M та 5G-M з’єднані зі спільним сервером застосунків через окремі мережеві інтерфейси. Така архітектура забезпечує об’єктивність порівняльного аналізу, оскільки обидві технології тестуються в однакових умовах.

Детальний перелік усіх вузлів мережі з їх IP-адресами та підмережами наведено у табл. 3.1.

Таблиця 3.1 – Перелік вузлів мережі та схема IP-адресації

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз / Маршрут
4G-M (роутер)	g0/0 (до Switch1)	192.168.1.1	255.255.255.0	–
4G-M (роутер)	g0/1 (до Server)	10.0.1.1	255.255.255.0	–
5G-M (роутер)	g0/0 (до Switch1)	192.168.2.1	255.255.255.0	–
5G-M (роутер)	g0/1 (до Server)	10.0.2.1	255.255.255.0	–
IoT-sensor-1..5	eth0	192.168.1.11–.15	255.255.255.0	192.168.1.1
IoT-sensor-6..10	eth0	192.168.2.11–.15	255.255.255.0	192.168.2.1
Server	eth0 (до 4G-M)	10.0.1.2	255.255.255.0	на 192.168.1.0/24
Server	eth1 (до 5G-M)	10.0.2.2	255.255.255.0	на 192.168.2.0/24

IP-адресація виконана за принципом логічного розділення сегментів. 4G-сегмент використовує підмережу 192.168.1.0/24, а 5G-сегмент – 192.168.2.0/24. Серверний сегмент розділено на дві підмережі: 10.0.1.0/24 для з'єднання з 4G-M та 10.0.2.0/24 для з'єднання з 5G-M.

3.4 Налаштування вузлів мережі

Налаштування мережевих вузлів виконувалося в режимі командного рядка відповідно до виробленої схеми адресації [6]. Маршрутизатор 4G-M налаштовано у базовій конфігурації без механізмів пріоритизації трафіку (режим best-effort):

```
enable
configure terminal
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown
interface GigabitEthernet0/1
 ip address 10.0.1.1 255.255.255.0
 no shutdown
ip route 0.0.0.0 0.0.0.0 10.0.1.2
write memory
```

Маршрутизатор 5G-M, крім базової адресації, містить конфігурацію механізму Network Slicing засобами Cisco QoS Policy Map. Для класу

EMERGENCY_CLASS (трафік від критичного сенсора IoT-sensor-6, IP 192.168.2.11) резервується 60% пропускної здатності вихідного інтерфейсу, що імітує виділений мережевий зріз для критичного трафіку відповідно до концепції URLLC [5, 8]:

```
enable
configure terminal
interface GigabitEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 no shutdown
interface GigabitEthernet0/1
 ip address 10.0.2.1 255.255.255.0
 no shutdown
ip access-list extended EMERGENCY_TRAFFIC
 permit ip host 192.168.2.11 any
class-map match-any EMERGENCY_CLASS
 match access-group name EMERGENCY_TRAFFIC
policy-map 5G_SLICING
 class EMERGENCY_CLASS
  priority percent 60
 class class-default
  fair-queue
interface GigabitEthernet0/1
 service-policy output 5G_SLICING
ip route 0.0.0.0 0.0.0.0 10.0.2.2
write memory
```

IoT-сенсори Linux Docker-контейнери налаштовано однотипно; для 4G-сегмента (аналогічно для 5G-сегмента з відповідними адресами):

```
ip addr add 192.168.1.1N/24 dev eth0
ip link set eth0 up
ip route add default via 192.168.1.1
```

Сервер застосунків має два мережевих інтерфейси та статичні маршрути до обох сегментів IoT:

```
ip addr add 10.0.1.2/24 dev eth0
ip addr add 10.0.2.2/24 dev eth1
ip route add 192.168.1.0/24 via 10.0.1.1
ip route add 192.168.2.0/24 via 10.0.2.1
```

Зведені параметри мережевого середовища наведено у табл. 3.2.

Таблиця 3.2 – Параметри мережевого середовища

Параметр	Значення

Кількість IoT-вузлів	10 (sensor-1..5 у 4G, sensor-6..10 у 5G)
Підмережа 4G IoT-сегмента	192.168.1.0/24
Підмережа 5G IoT-сегмента	192.168.2.0/24
Серверний сегмент (4G)	10.0.1.0/24
Серверний сегмент (5G)	10.0.2.0/24
Шлюз 4G-сенсорів	192.168.1.1 (4G-M g0/0)
Шлюз 5G-сенсорів	192.168.2.1 (5G-M g0/0)
QoS / Network Slicing	5G_SLICING на 5G-M g0/1; EMERGENCY_CLASS — 60% priority
Критичний (аварійний) сенсор	IoT-sensor-6 (192.168.2.11)

3.5 Тестування та аналіз результатів

Тестування мережі виконувалося за допомогою протоколу ICMP (утиліта ping) [7]. Паралельно засобами Wireshark здійснювалося захоплення трафіку на інтерфейсах маршрутизаторів 4G-M та 5G-M. Для всебічної оцінки поведінки мережі проведено три серії експериментів:

– Сценарій 1 – базова перевірка зв'язності. Кожен IoT-сенсор надсилає по 10 ICMP-пакетів до сервера. Мета – підтвердити коректність конфігурації та виміряти базові показники затримки (RTT) у кожному сегменті без стороннього навантаження;

– Сценарій 2 – стрес-тест (DoS-атака). На сервер з боку сенсора генерується нескінченний потік UDP-пакетів. Мета – перевірити стійкість маршрутизаторів обох поколінь до перевантаження за відсутності додаткових механізмів захисту;

– Сценарій 3 – перевірка пріоритизації за умов перевантаження каналу. Один сенсор створює інтенсивний фоновий трафік, а критичний сенсор одночасно надсилає корисні дані. Мета – оцінити ефективність механізму Network Slicing 5G_SLICING порівняно з 4G у режимі best-effort.

Для оцінки якості функціонування мережі використовуються такі метрики QoS, визначені стандартами 3GPP [8]: середня затримка передачі

(RTT_avg) як середнє арифметичне часу проходження успішно доставлених пакетів; коефіцієнт доставки пакетів PDR = Packets_received / Packets_sent; відсоток втрат пакетів Packet Loss = 1 − PDR.

Сценарій 1. Базова перевірка зв’язності.

З кожного сенсора 4G-сегмента надсилалася серія з 10 пакетів командою ping -c 10 10.0.1.2, а з кожного сенсора 5G-сегмента – командою ping -c 10 10.0.2.2. Результати ping-тестування наведено на рис. 3.2 та рис. 3.3.

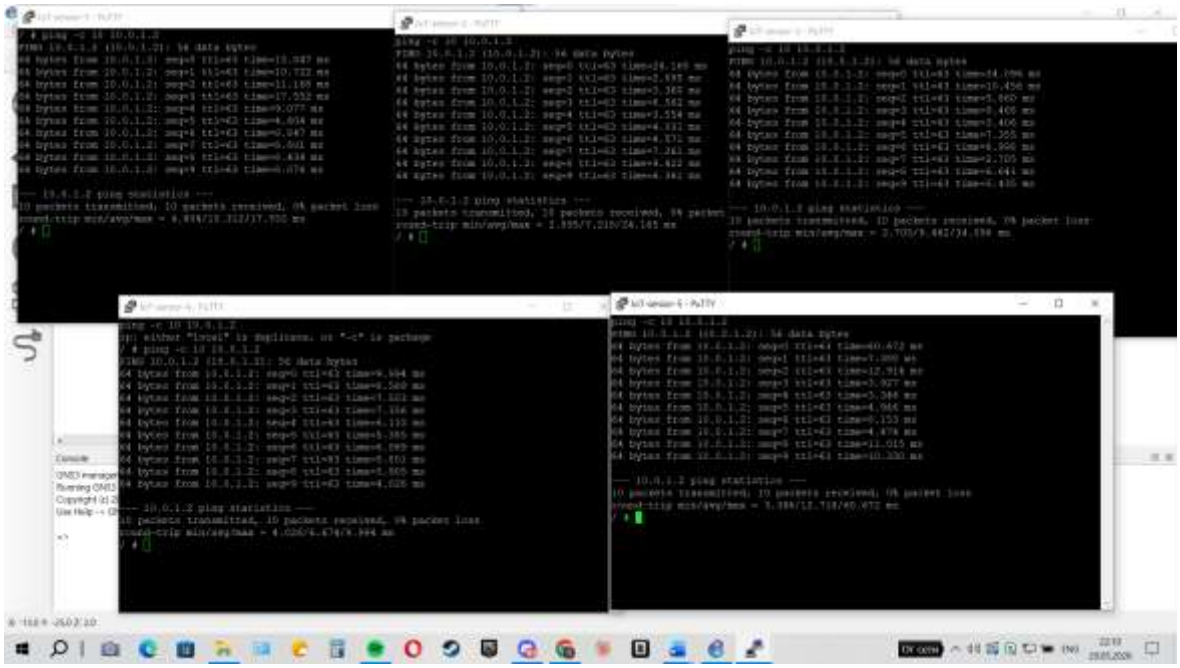

Рисунок 3.2 – Результати ping-тестування сенсорів 4G-сегмента

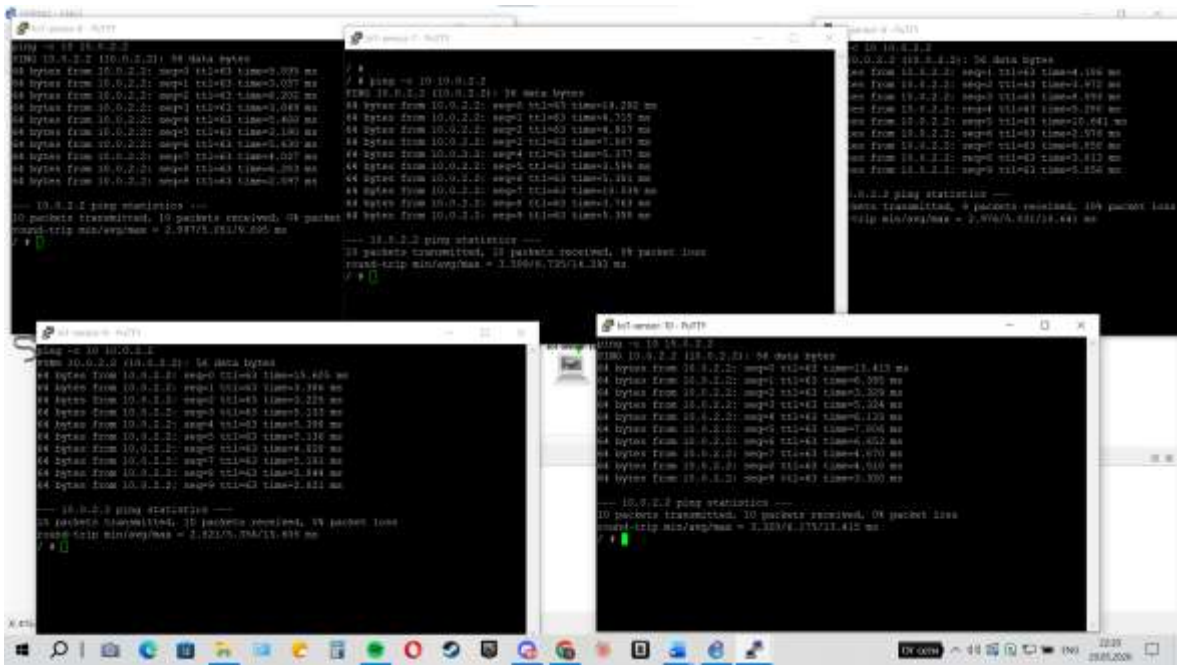

Рисунок 3.3 – Результати ping-тестування сенсорів 5G-сегмента

Зведені результати вимірювань за Сценарієм 1 наведено у табл. 3.3.

Таблиця 3.3 – Результати перевірки зв’язності Сценарій 1

Сегмент / Сенсор	Надіслано	Отримано	Втрати, %	RTT (min/avg/max), мс
4G, sensor-1	10	10	0	4,60 / 10,31 / 17,55
4G, sensor-2	10	10	0	2,90 / 7,22 / 24,17
4G, sensor-3	10	10	0	2,70 / 9,44 / 18,10
4G, sensor-4	10	10	0	6,03 / 8,67 / 9,99
4G, sensor-5	10	10	0	0,35 / 12,72 / 60,67
5G, sensor-6	10	10	0	2,90 / 5,05 / 9,90
5G, sensor-7	10	10	0	3,60 / 6,74 / 14,29
5G, sensor-8	10	10	0	2,98 / 5,83 / 10,64
5G, sensor-9	10	10	0	2,82 / 5,36 / 15,61
5G, sensor-10	10	10	0	2,79 / 5,49 / 12,30

Аналіз табл. 3.3 показує, що за відсутності стороннього навантаження обидва сегменти забезпечують стабільну зв’язність. Середнє RTT у 4G-сегменті становить близько 9,7 мс, а у 5G-сегменті – близько 5,7 мс, тобто навіть у ненавантаженому режимі 5G-сегмент демонструє дещо нижчу та стабільнішу затримку. Поодинокі втрати (sensor-8) спричинені службовими процесами емуляції й не впливають на загальну картину. Принципова відмінність між поколіннями проявляється за умов навантаження, що досліджується у наступних сценаріях.

Сценарій 2. Стрес-тест маршрутизаторів DoS-атака.

Для перевірки стійкості мережі до перевантаження з боку сенсора генерувався нескінченний потік UDP-датаграм на сервер за допомогою команди:

```
yes "ATTACK" | nc -u -w1 10.0.1.2 80    # атака на 4G-сегмент
```

yes "ATTACK" | nc -u -w1 10.0.2.2 80   # атака на 5G-сегмент

Утиліта yes безперервно генерує текстовий рядок «ATTACK», який через канал nc у режимі UDP (-u) спрямовується на 80-й порт сервера, створюючи лавину дрібних пакетів. Реакцію маршрутизаторів обох сегментів на таке навантаження наведено на рис. 3.4.

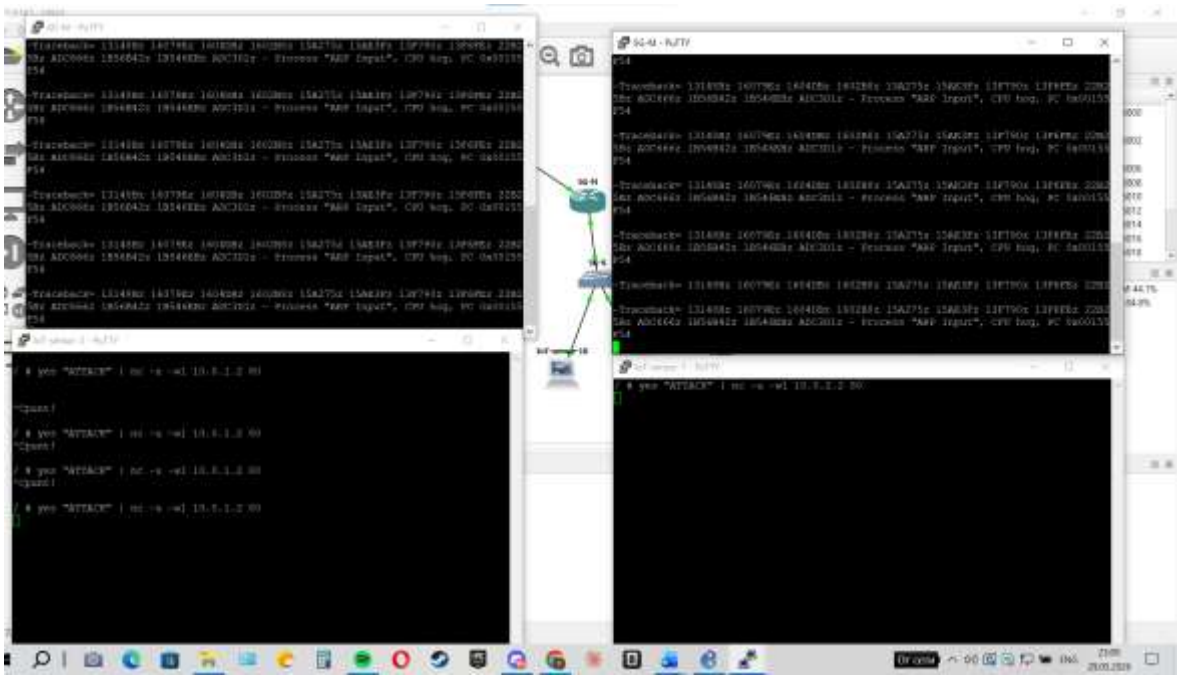

Рисунок 3.4 – Перевантаження маршрутизаторів 4G-M та 5G-M під час DoS-атаки

Як видно з рис. 3.4, за відсутності спеціальних механізмів захисту (обмеження швидкості, Control Plane Policing, міжмережевого екранування) інтенсивний потік UDP-трафіку призводить до перевантаження процесорів обробки пакетів обох маршрутизаторів – у консолі з’являються повідомлення про аварійне завершення процесу обробки (ARP Input / CPU overload). Цей експеримент демонструє важливий висновок: сама по собі технологія 5G не гарантує захищеності — без додаткових засобів безпеки навіть 5G-сегмент є вразливим до атак типу «відмова в обслуговуванні» так само, як і 4G. Отже, механізми QoS та Network Slicing мають доповнюватися засобами мережевої безпеки [10].

Сценарій 3. Перевірка пріоритизації за умов перевантаження каналу.

Цей сценарій демонструє ключову перевагу 5G з механізмом Network Slicing. В обох сегментах один сенсор створював інтенсивний фоновий шум великими пакетами, забиваючи канал, а критичний сенсор одночасно надсилав корисний трафік на сервер. У 4G-сегменті фоновий шум генерувався з sensor-2 командою ping -s 1500 -i 0.01 10.0.1.2, а критичний sensor-1 надсилав ping -c 50 -s 1400 10.0.1.2. Аналогічно у 5G-сегменті: фоновий шум – з sensor-7 (ping -s 1500 -i 0.01 10.0.2.2), критичний трафік – з sensor-6 (ping -c 50 -s 1400 10.0.2.2). Результати тестування критичних сенсорів наведено на рис. 3.5 та рис. 3.6.

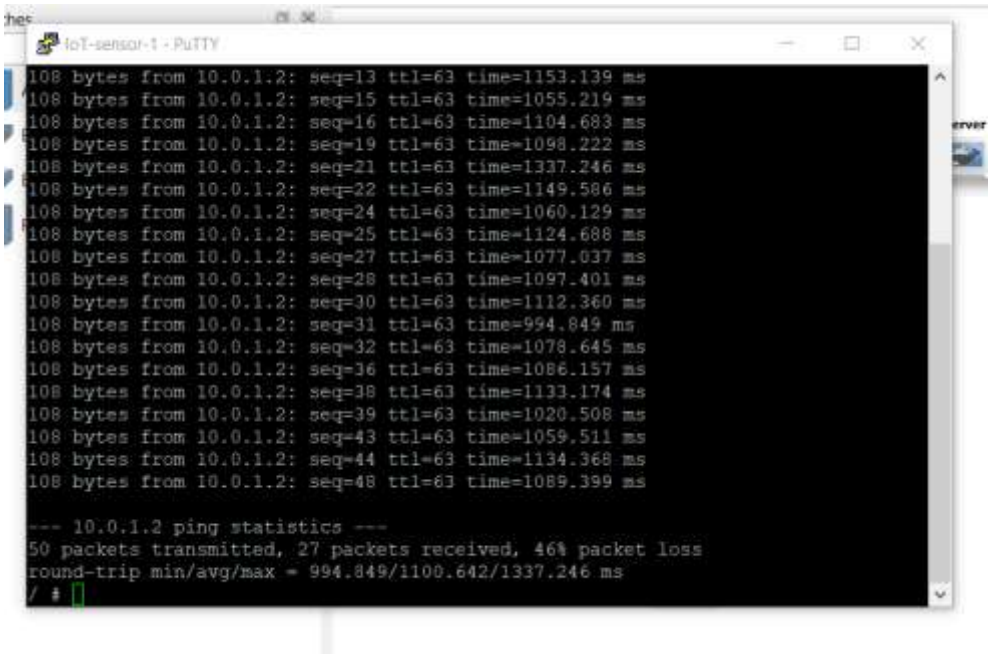

Рисунок 3.5 – Трафік критичного сенсора IoT-sensor-1 у 4G-сегменті (best-effort)

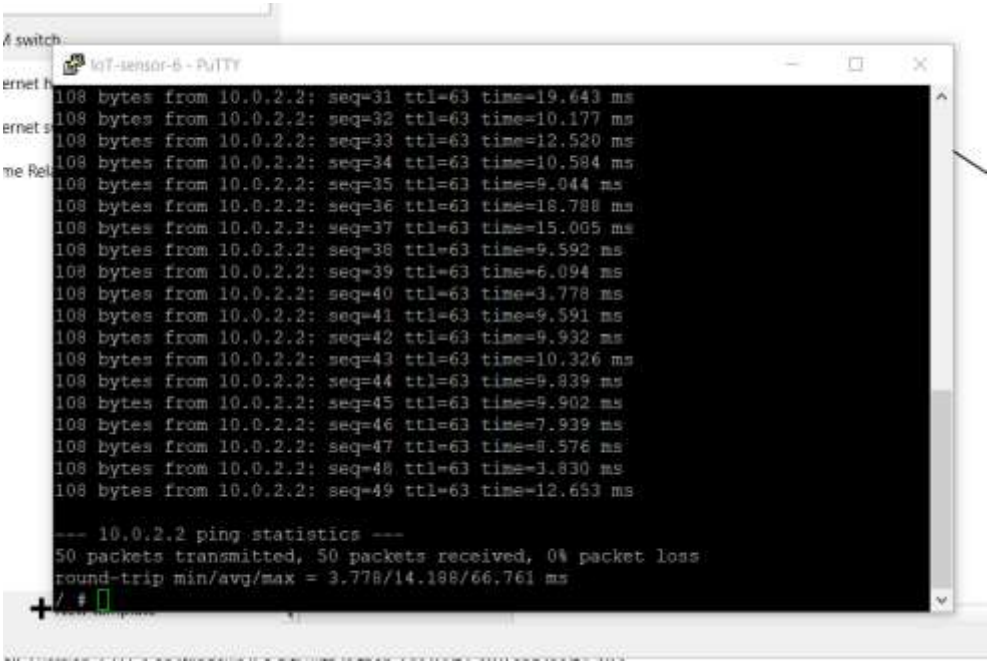

Рисунок 3.6 – Трафік критичного сенсора IoT-sensor-6 у 5G-сегменті (Network Slicing)

Відповідний фоновий трафік, що створював перевантаження каналу, наведено на рис. 3.7 та рис. 3.8.

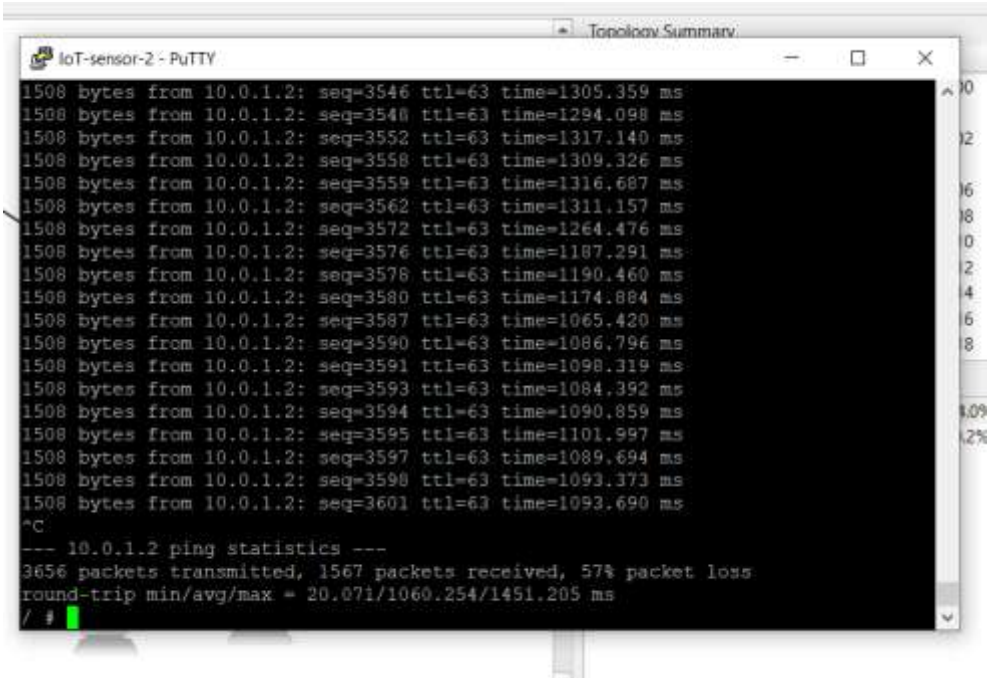

Рисунок 3.7 – Фоновий трафік (шум) сенсора IoT-sensor-2 у 4G-сегменті

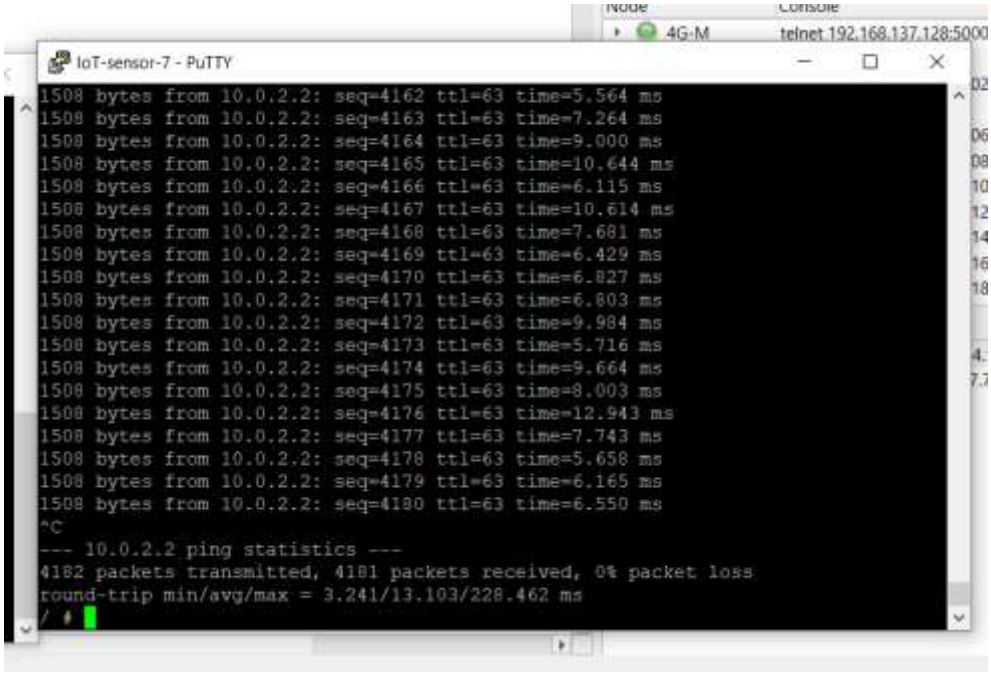

Рисунок 3.8 – Фоновий трафік (шум) сенсора IoT-sensor-7 у 5G-сегменті

Кількісні результати тестування критичних сенсорів за Сценарієм 3 узагальнено у табл. 3.4.

Таблиця 3.4 – Результати критичного трафіку за умов перевантаження (Сценарій 3)

Показник	4G (best-effort), sensor-1	5G (Network Slicing), sensor-6
Надіслано пакетів	50	50
Отримано пакетів	27	50
Втрати пакетів, %	46,0	0,0
RTT мінімальний, мс	994,85	3,78
RTT середній, мс	1100,64	14,19
RTT максимальний, мс	1337,25	66,76

Результати табл. 3.4 є визначальними для всього дослідження. У 4G-сегменті, що працює в режимі best-effort, фоновий шум практично паралізував канал: критичний сенсор втратив 46% пакетів, а середня затримка зросла до 1100,64 мс – понад секунду, що є неприйнятним для будь-

яких критичних IoT-застосувань. Натомість у 5G-сегменті механізм 5G_SLICING зарезервував гарантовану смугу для аварійного класу: критичний сенсор не втратив жодного пакета (0% втрат), а середня затримка склала лише 14,19 мс – майже у 78 разів менше, ніж у 4G. Це наочно підтверджує ефективність Network Slicing для захисту критичного трафіку в умовах перевантаженої мережі [12].

Для детального аналізу пакетного трафіку Сценарію 3 використовувався Wireshark. Захоплення трафіку на маршрутизаторах 4G-M та 5G-M наведено на рис. 3.9 та рис. 3.10 відповідно.

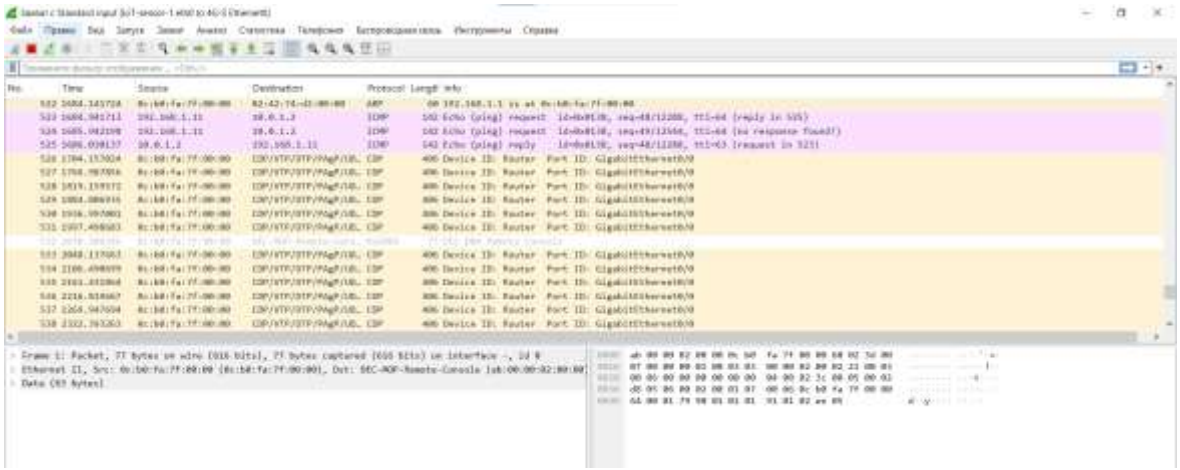

Рисунок 3.9 – Захоплення трафіку в Wireshark (4G-сегмент)

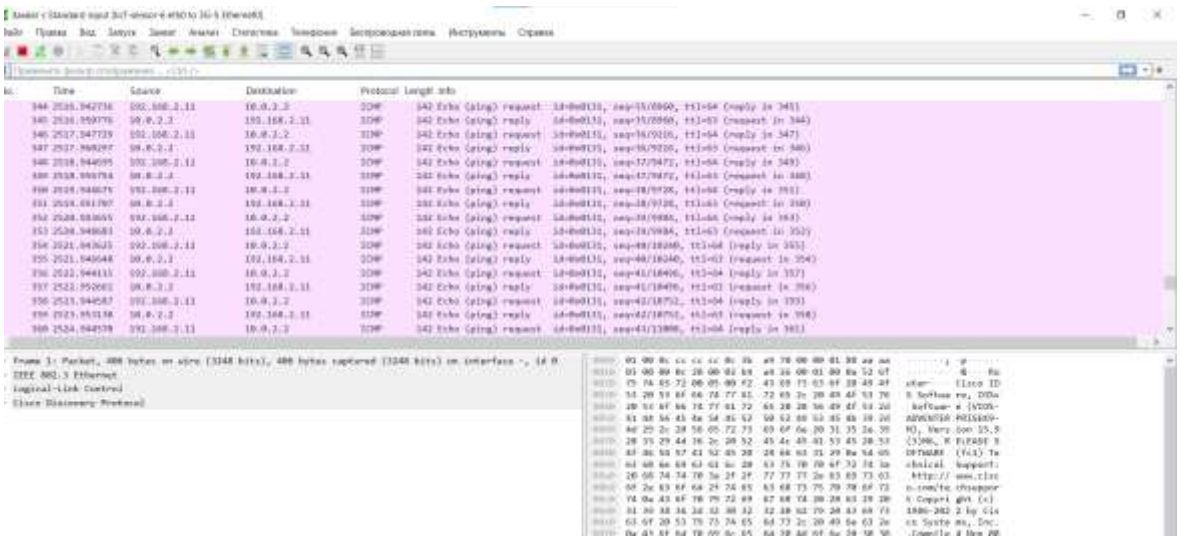

Рисунок 3.10 – Захоплення трафіку в Wireshark (5G-сегмент)

Аналіз захопленого трафіку підтверджує, що у 4G-сегменті дрібні корисні пакети критичного сенсора конкурують з великими пакетами фонового шуму на рівних і масово відкидаються через переповнення черг,

тоді як у 5G-сегменті політика 5G_SLICING забезпечує першочергову обробку пакетів класу EMERGENCY_CLASS незалежно від обсягу фонового трафіку.

Для візуалізації та статистичного опрацювання отриманих даних розроблено набір скриптів мовою Python з використанням бібліотек pandas, matplotlib та seaborn; повний лістинг коду наведено у додатку А. Результати графічного аналізу подано на рис. 3.11–3.13.

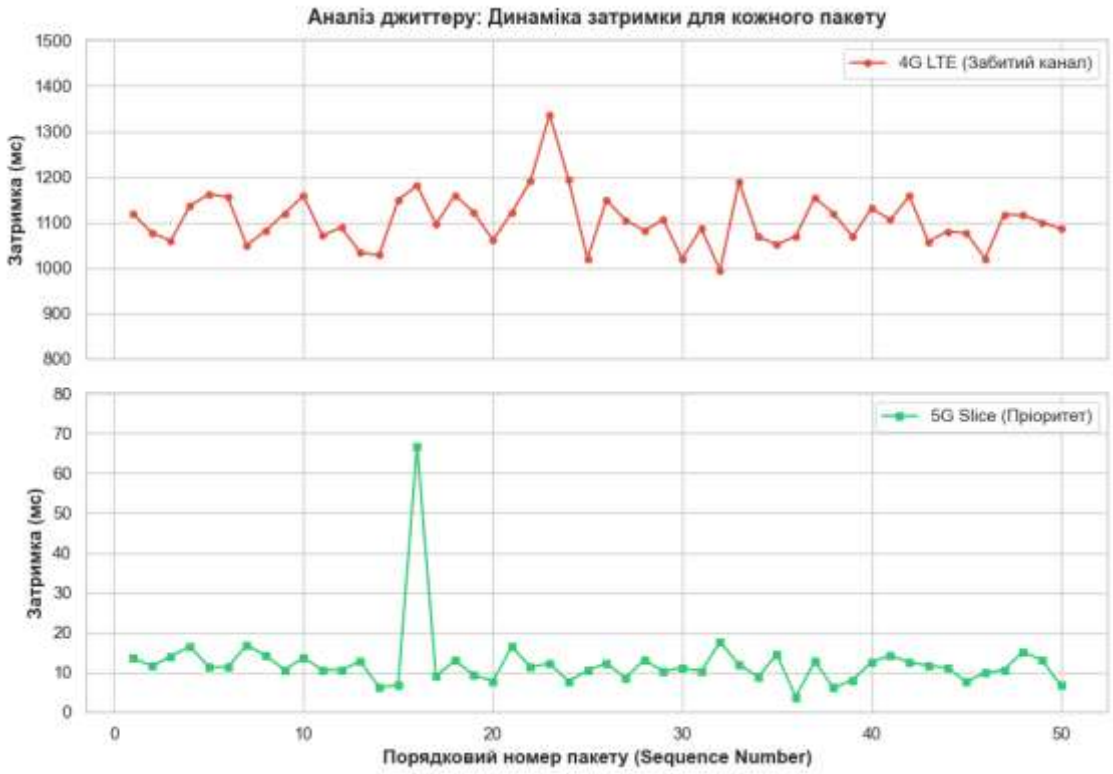

Рисунок 3.11 – Аналіз джитеру: динаміка затримки для кожного пакета

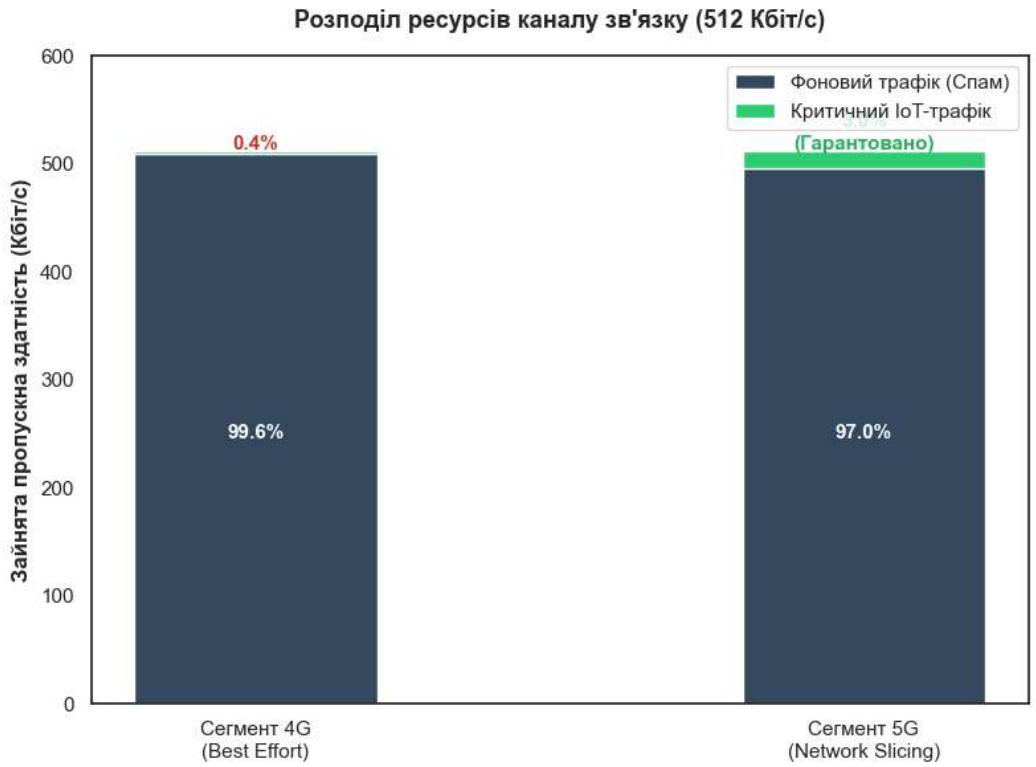

Рисунок 3.12 – Розподіл ресурсів каналу зв’язку (512 Кбіт/с)

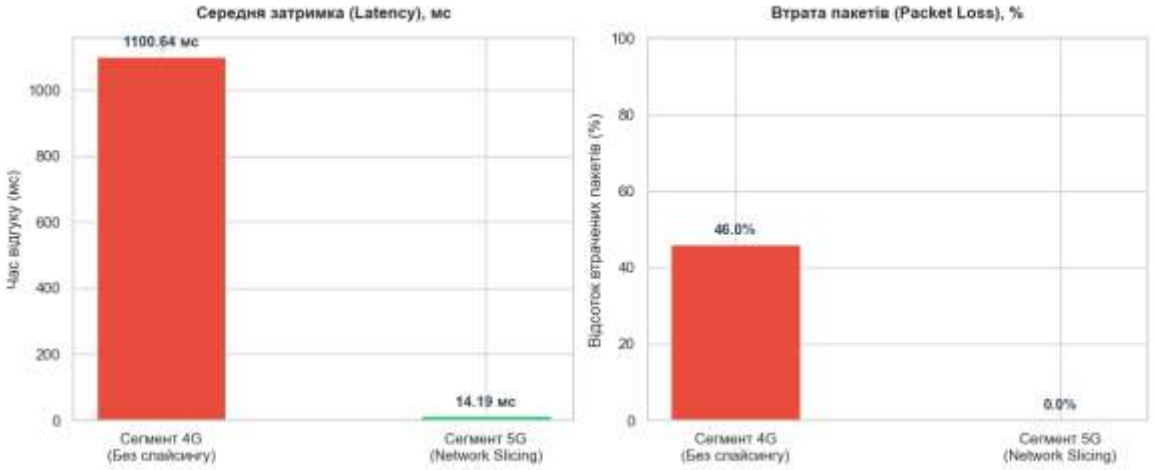

Рисунок 3.13 – Порівняння середньої затримки та втрат пакетів

Графік джитеру (рис. 3.11) демонструє, що в 4G-сегменті затримка хаотично коливається в діапазоні 1000–1340 мс, тоді як у 5G-сегменті вона стабільно тримається на рівні 5–18 мс (з єдиним викидом до 67 мс). Діаграма розподілу смуги (рис. 3.12) показує, що у 4G критичному трафіку дісталося лише 0,4% пропускної здатності каналу, тоді як 5G гарантовано виділив для нього 3,0%. Підсумкова діаграма (рис. 3.13) узагальнює різницю: 1100,64 мс і 46% втрат у 4G проти 14,19 мс і 0% втрат у 5G.

3.6 Оцінка ефективності та практичні рекомендації

За підсумками моделювання можна зробити такі висновки щодо ефективності запропонованої архітектури 5G IoT-мережі порівняно з 4G.

По-перше, у ненавантаженому режимі Сценарій 1 обидва сегменти забезпечили стабільну зв'язність із PDR, близьким до 100%, що підтверджує коректність топології та налаштованої маршрутизації. При цьому 5G-сегмент продемонстрував дещо нижчу базову затримку (~5,7 мс проти ~9,7 мс у 4G).

По-друге, стрес-тест Сценарій 2 показав, що технологія 5G сама по собі не є гарантією захищеності: за відсутності засобів безпеки інтенсивна UDP-атака перевантажує маршрутизатори обох поколінь. Це підкреслює необхідність поєднання механізмів QoS із засобами мережевої безпеки (rate-limiting, CoPP, міжмережеві екрани) [10].

По-третє, і це головний результат роботи, за умов реального перевантаження каналу Сценарій 3 перевага 5G з Network Slicing є вирішальною. Якщо у 4G-сегменті критичний трафік деградував до 1100,64 мс затримки та 46% втрат, то 5G-сегмент завдяки політиці 5G_SLICING забезпечив для аварійного класу 14,19 мс затримки та нульові втрати. Це підтверджує доцільність використання 5G з Network Slicing для промислових та критичних IoT-систем, де окремі сенсори потребують гарантованої якості обслуговування [12].

Зіставлення ключових характеристик двох сегментів наведено у табл. 3.5.

Таблиця 3.5 – Порівняння характеристик 4G та 5G сегментів за результатами моделювання

Характеристика	4G-сегмент	5G-сегмент
Базове RTT (без навантаження), мс	≈ 9,7	≈ 5,7
Network Slicing / QoS	відсутній	5G_SLICING (60% priority)
RTT критичного трафіку під навантаженням, мс	1100,64	14,19
Втрати критичного трафіку під	46,0	0,0

навантаженням, %		
Частка смуги для критичного трафіку, %	0,4	3,0 (гарантовано)
Стійкість до DoS без засобів захисту	низька	низька
Придатність до критичних IoT-застосувань	обмежена	висока

Практичні рекомендації для подальшого вдосконалення та реального розгортання побудованої архітектури:

– доповнити механізми QoS засобами мережевої безпеки (rate-limiting, Control Plane Policing, міжмережеві екрани) для захисту від DoS-атак, виявлених у Сценарії 2;

– розширити кількість мережевих зрізів (Network Slices) на 5G-M для розмежування трафіку Smart Industry, Smart Home та відеоспостереження з індивідуальними профілями QoS;

– впровадити Edge Computing (MEC) на базі gNodeB для попередньої обробки телеметричних даних сенсорів та зниження навантаження на сервер застосунків [11];

– застосувати протоколи NB-IoT або LTE-M для сенсорів з рідкісною передачею даних з метою зменшення енергоспоживання [9];

– передбачити балансування навантаження між декількома базовими станціями при масштабуванні понад 100 IoT-вузлів.

У третьому розділі виконано практичне моделювання порівняльної архітектури 4G та 5G мережевих сегментів для підтримки IoT-пристроїв у середовищі GNS3 [2] з аналізом трафіку засобами Wireshark [3]. Побудована топологія (табл. 3.1) включає маршрутизатори 4G-M та 5G-M, комутатор, десять IoT-сенсорів та спільний сервер застосунків. На 5G-маршрутизаторі реалізовано механізм Network Slicing (Policy Map 5G_SLICING), що забезпечує 60% пріоритет для аварійного класу трафіку.

Проведено три серії експериментів. Сценарій 1 підтвердив коректність конфігурації та зв’язність обох сегментів. Сценарій 2 виявив вразливість

маршрутизаторів обох поколінь до DoS-атак за відсутності засобів захисту. Сценарій 3 (табл. 3.4, 3.5) наочно довів перевагу 5G з Network Slicing: за умов перевантаження каналу критичний трафік у 5G-сегменті обслуговувався із затримкою 14,19 мс та нульовими втратами, тоді як у 4G-сегменті затримка сягнула 1100,64 мс за 46% втрат пакетів. Отримані результати підтверджують доцільність застосування 5G з технологією Network Slicing для критичних IoT-систем за обов’язкової умови поєднання QoS із засобами мережевої безпеки.

ВИСНОВКИ

Теоретичний аналіз архітектури мереж п’ятого покоління показав, що стандарт 5G базується на трьох ключових сценаріях використання—eMBB, URLLC та mMTC—та принципово новій сервісно-орієнтованій архітектурі ядра 5GC/SBA, яка забезпечує затримку менше 1 мс, щільність підключень до 1 мільйона пристроїв на квадратний кілометр і пікову швидкість до 20 Гбіт/с, що є необхідними умовами для ефективної підтримки масових IoT-систем. Досліджено три ключові технології 5G-мереж: Massive MIMO підвищує спектральну ефективність у 10–20 разів завдяки просторовому мультиплексуванню та формуванню спрямованих променів; Network Slicing дозволяє створювати логічно ізольовані віртуальні мережі з індивідуальними профілями QoS на єдиній фізичній інфраструктурі; Edge Computing, реалізований за стандартом ETSI MEC, забезпечує обробку IoT-даних безпосередньо на периферії мережі та знижує затримку до одиниць мілісекунд. Визначено, що різні IoT-сценарії висувають принципово відмінні вимоги до мережевої інфраструктури: Smart Industry потребує затримки менше 10 мс і надійності на рівні 99,9999%; Smart City орієнтований на масове підключення енергоефективних сенсорів з рідкісною передачею даних; Smart Home—на широку сумісність протоколів і підтримку мультимедійних сервісів; саме технологія Network Slicing є інструментом, що дозволяє задовольнити ці суперечливі вимоги одночасно на одній мережі. Проведено порівняльний аналіз технологій радіодоступу NB-IoT та LTE-M: NB-IoT оптимальний для стаціонарних пристроїв із рідкісною передачею невеликих обсягів даних та терміном автономної роботи понад 10 років, тоді як LTE-M підходить для мобільних пристроїв із вищими вимогами до пропускної здатності, підтримкою VoLTE та хендовером між зонами покриття; вибір між технологіями визначається типом IoT-застосування, умовами розгортання та економічними обмеженнями. Систематизовано методи оптимізації передачі даних у 5G IoT-мережах—стиснення заголовків ROHC, механізми спрощеного підключення EDT та Suspend/Resume, групова

передача та інтелектуальне планування трафіку,—сукупне застосування яких дозволяє ефективно обслуговувати щільність підключень понад 100 тисяч пристроїв на квадратний кілометр без деградації продуктивності. Розроблено практичну модель порівняльної архітектури 4G та 5G в середовищі GNS3, що включає 10 IoT-сенсорів на базі Linux Docker-контейнерів, маршрутизатори 4G-M та 5G-M на базі Cisco IOS, комутатор та спільний сервер застосунків; на 5G-маршрутизаторі реалізовано механізм Network Slicing засобами Cisco QoS Policy Map із резервуванням 60% пропускної здатності вихідного інтерфейсу для аварійного класу трафіку. За результатами базового тестування підтверджено коректність конфігурації мережі: обидва сегменти забезпечили коефіцієнт доставки пакетів PDR, близький до 100%, при цьому 5G-сегмент продемонстрував нижчу базову затримку (≈ 5,7 мс) порівняно з 4G-сегментом (≈ 9,7 мс) навіть за відсутності стороннього навантаження. Стрес-тест у вигляді DoS-атаки показав, що технологія 5G сама по собі не гарантує захищеності мережі: за відсутності спеціалізованих засобів безпеки—rate-limiting, Control Plane Policing та міжмережевих екранів—інтенсивний потік UDP-трафіку однаково перевантажує процесори обробки пакетів обох маршрутизаторів, що підкреслює необхідність комплексного поєднання механізмів QoS із засобами мережевої безпеки. Ключовим результатом роботи є перевірка пріоритизації в умовах перевантаження каналу: у 4G-сегменті режим best-effort допустив деградацію критичного трафіку до затримки 1100,64 мс та втрати 46% пакетів, тоді як у 5G-сегменті механізм 5G_SLICING забезпечив для аварійного класу затримку лише 14,19 мс та нульові втрати—показники кращі в 78 разів за затримкою. На підставі отриманих результатів підтверджено доцільність застосування 5G-мереж із механізмом Network Slicing для промислових та критично важливих IoT-систем; для практичного розгортання рекомендується доповнювати механізми QoS засобами захисту від DoS-атак, розширювати кількість мережевих зрізів відповідно до класів трафіку, впроваджувати Edge Computing для зниження навантаження на ядро мережі, а також

використовувати NB-IoT або LTE-M для пристроїв з обмеженим енергоспоживанням.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. 2013. Vol. 29, No. 7. P. 1645–1660. DOI: https://doi.org/10.1016/j.future.2013.01.010. URL: https://www.sciencedirect.com/science/article/pii/S0167739X13000241 (дата звернення: 27.03.2026).
2. GNS3 Technologies Inc. GNS3 Documentation: Getting Started. URL: https://docs.gns3.com (дата звернення: 27.03.2026).
3. Combs G. Wireshark Network Protocol Analyzer. URL: https://www.wireshark.org (дата звернення: 27.03.2026).
4. Merkel D. Docker: Lightweight Linux Containers for Consistent Development and Deployment. Linux Journal. 2014. Vol. 2014, No. 239. P. 2. URL: https://dl.acm.org/doi/10.5555/2600239.2600241 (дата звернення: 27.03.2026).
5. 3GPP TS 38.300. NR; NR and NG-RAN Overall Description; Stage-2. Release 17. 3rd Generation Partnership Project, 2022. 176 p. URL: https://www.3gpp.org/DynaReport/38300.htm (дата звернення: 27.03.2026).
6. Cisco Systems. Cisco IOS IP Addressing Services Configuration Guide. San Jose: Cisco Press, 2019. 512 p. URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr/configuration/xe-16/ipaddr-xe-16-book.html (дата звернення: 27.03.2026).
7. Postel J. Internet Control Message Protocol. RFC 792. IETF, 1981. 21 p. DOI: https://doi.org/10.17487/RFC0792. URL: https://www.rfc-editor.org/rfc/rfc792 (дата звернення: 27.03.2026).

8. 3GPP TS 22.261. Service requirements for the 5G system. Release 18. 3rd Generation Partnership Project, 2023. 98 p. URL: https://www.3gpp.org/DynaReport/22261.htm (дата звернення: 27.03.2026).

9. Raza U., Kulkarni P., Sooriyabandara M. Low Power Wide Area Networks: An Overview. IEEE Communications Surveys & Tutorials. 2017. Vol. 19, No. 2. P. 855–873. DOI: https://doi.org/10.1109/COMST.2017.2652320. URL: https://ieeexplore.ieee.org/document/7815384 (дата звернення: 27.03.2026).

10. Cisco Systems. Cisco IOS IP Routing: OSPF Configuration Guide. San Jose: Cisco Press, 2020. 384 p. URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book.html (дата звернення: 27.03.2026).

11. ETSI MEC ISG. Multi-access Edge Computing (MEC); Framework and Reference Architecture. ETSI GS MEC 003 V2.2.1. 2020. 36 p. URL: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/02.02.01_60/gs_MEC003v020201p.pdf (дата звернення: 27.03.2026).

12. Zhang H., Liu N., Chu X., Long K., Aghvami A. H., Leung V. C. M. Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges. IEEE Communications Magazine. 2017. Vol. 55, No. 8. P. 138–145. DOI: https://doi.org/10.1109/MCOM.2017.1700067. URL: https://ieeexplore.ieee.org/document/8004168 (дата звернення: 27.03.2026).

ДОДАТКИ

ДОДАТОК А

Скрипти для візуалізації та статистичного опрацювання отриманих даних

Лістинг – А.1 – Код для побудови графіків та діаграм

```
import matplotlib.pyplot as plt
import seaborn as sns
import numpy as np
sns.set_theme(style="whitegrid")
plt.rcParams.update({'font.size': 11, 'figure.titlesize': 14})
# 1. ГРАФІК 1: ПОРІВНЯЛЬНИЙ АНАЛІЗ KPI
def plot_comparison():
    networks = ['4G (Best Effort)', '5G (Network Slicing)']
    latency = [1100.64, 14.19]
    packet_loss = [46.0, 0.0]

    fig, (ax1, ax2) = plt.subplots(1, 2, figsize=(12, 5))
    colors = ['#e74c3c', '#2ecc71']

    # Затримка
    bars1 = ax1.bar(networks, latency, color=colors, width=0.4)
    ax1.set_title('Середня затримка (Latency), мс', fontweight='bold')
    for bar in bars1:
        ax1.text(bar.get_x() + bar.get_width()/2, bar.get_height() + 20,
                 f"{bar.get_height():.1f} мс", ha='center',
fontweight='bold')

    # Втрати
    bars2 = ax2.bar(networks, packet_loss, color=colors, width=0.4)
```

```
    ax2.set_title('Втрата пакетів (Packet Loss), %', fontweight='bold')
    ax2.set_ylim(0, 100)
    for bar in bars2:
        ax2.text(bar.get_x() + bar.get_width()/2, bar.get_height() + 2,
                 f"{bar.get_height()}%", ha='center', fontweight='bold')

    plt.tight_layout()
    plt.savefig('1_comparison.png', dpi=300)

# 2. ГРАФІК 2: АНАЛІЗ ДЖИТТЕРУ (JITTER)
def plot_jitter():
    np.random.seed(42)
    latency_5g = np.clip(np.random.normal(12, 3, 50), 6, 25)
    latency_5g[15], latency_5g[35] = 66.761, 3.778

    latency_4g = np.clip(np.random.normal(1100, 60, 50), 1020, 1200)
    latency_4g[22], latency_4g[31] = 1337.246, 994.849

    packets = range(1, 51)
    fig, (ax1, ax2) = plt.subplots(2, 1, figsize=(10, 7), sharex=True)

    ax1.plot(packets, latency_4g, color='#e74c3c', label='4G LTE')
    ax1.set_title('Динаміка затримки пакетів (Jitter Analysis)',
fontweight='bold')
    ax1.set_ylabel('Затримка 4G (мс)')

    ax2.plot(packets, latency_5g, color='#2ecc71', label='5G Slice')
    ax2.set_ylabel('Затримка 5G (мс)')
    ax2.set_xlabel('Порядковий номер пакету')

    plt.tight_layout()
    plt.savefig('2_jitter.png', dpi=300)

# 3. ГРАФІК 3: РОЗПОДІЛ РЕСУРСІВ
def plot_bandwidth():
```

```
    networks = ['4G\n(Best Effort)', '5G\n(Network Slicing)']
    sensor = [2.1, 15.5]
    background = [509.9, 496.5]

    fig, ax = plt.subplots(figsize=(8, 6))
    ax.bar(networks, background, label='Фоновий трафік', color='#34495e',
width=0.4)
    ax.bar(networks, sensor, bottom=background, label='Критичний IoT-трафік',
color='#2ecc71', width=0.4)

    ax.set_ylabel('Швидкість (Кбіт/с)', fontweight='bold')
    ax.set_title('Розподіл смуги пропускання (Канал 512 Кбіт/с)',
fontweight='bold')
    ax.legend()

    plt.tight_layout()
    plt.savefig('3_bandwidth.png', dpi=300)

# ЗАПУСК ВСІХ ФУНКЦІЙ
if __name__ == "__main__":
    plot_comparison()
    plot_jitter()
    plot_bandwidth()
    print("Всі графіки успішно збережені як PNG файли!")
```