ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ВРАЗЛИВОСТІ БЕЗПЕКИ В 5G/6G, WIFI 6 ТА МЕРЕЖАХ СПІЛЬНОГО ВИКОРИСТАННЯ СПЕКТРУ»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Віктор ОХРЕМЕНКО
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Виконав: здобувач вищої освіти гр. _ТСДМ-62_
Віктор ОХРЕМЕНКО
Ім'я, ПРІЗВИЩЕ

Керівник: Вікторія КОРЕЦЬКА
к.п.н., доцент *Ім'я, ПРІЗВИЩЕ*

Рецензент: _____
Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Телекомунікацій

Кафедра ___Телекомунікаційних систем та мереж_____
Ступінь вищої освіти __магістр_____
Спеціальність ___172 Електронні комунікації та радіотехніка _____
Освітньо-професійна програма _____Телекомунікаційні системи та мережі_____

ЗАТВЕРДЖУЮ
Завідувач кафедри __ТСМ_____
_____ Віктор ЗАЇКА
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Охременку Віктору Анатолійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Вразливості безпеки в 5G/6G, WiFi 6 та мережах спільного використання спектру
керівник кваліфікаційної роботи Вікторія КОРЕЦЬКА, к.п.н., доцент
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» 10. 2025 р. № 467

2. Строк подання кваліфікаційної роботи «___» _____ 2025 р.

3. Вихідні дані до кваліфікаційної роботи:
1. 5G/6G, WiFi 6 та мережі спільного використання спектру.
2. Вимоги до безпеки.
3. Безпекові ризики.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Вимоги до безпеки WiFi та 6G.
2. Вразливості у 5G та WiFi 6/6E.
3. Безпекові ризики співіснування та розподілу неліцензованого спектра.
4. Пом'якшення наслідків та напрямки майбутніх досліджень.

5. Перелік ілюстративного матеріалу: ___презентація на ____слайдах_____

6. Дата видачі завдання «___» _____ 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір та аналіз науково-технічної літератури	20.10.2025	Викон.
2	Розробка першого розділу	24.10.2025	Викон.
3	Розробка другого розділу	04.11.2025	Викон.
4	Розробка третього розділу	14.11.2025	Викон.
5	Розробка четвертого розділу	24.11.2025	Викон.
6	Висновки, вступ, реферат	04.12.2025	Викон.
7	Розробка презентації	14.12.2025	Викон.

Здобувач вищої освіти _____ Віктор ОХРЕМЕНКО
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Вікторія КОРЕЦЬКА
(підпис) *(Ім'я ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій
ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Охременко В.А. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)
на тему: «Вразливості безпеки в 5G/6G, WiFi 6 та мережах спільного використання спектру»

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Охременко Віктор Анатолійович показав гарну теоретичну та інженерну підготовку, уміння володіти новими комп'ютерними технологіями, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до наукової роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Охременко Віктора Анатолійовича на оцінку «відмінно» та присвоїти йому кваліфікацію магістр з електронних комунікацій та радіотехніки.

Керівник кваліфікаційної роботи _____ Вікторія КОРЕЦЬКА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Охременко В.А. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри телекомунікаційних систем та мереж _____ Віктор ЗАЇКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня магістра

здобувача вищої освіти Охременко Віктора Анатолійовича
(прізвище, ім'я, по батькові)
на тему «Вразливості безпеки в 5G/6G, WiFi 6 та мережах спільного використання спектру»

Актуальність.
Стрімкий розвиток технологій 5G/6G і WiFi 6/6E забезпечує високі швидкості передавання даних, мінімальні затримки та підтримку мільйонів пристроїв IoT, що сприяє цифровій трансформації суспільства. Водночас збільшення відкритості та складності архітектур призводить до появи нових кіберзагроз. Недостатня ефективність традиційних механізмів захисту виявляється у вразливостях протоколів автентифікації, атаках на фізичному рівні та ризиках у мережах спільного використання спектра. Тому актуальним є дослідження сучасних і потенційних вразливостей безпеки та пошук ефективних способів підвищення стійкості безпроводових мереж нового покоління.

Позитивні сторони.
1. У роботі детально досліджено протоколи автентифікації та управління ключами, що лежать в основі сучасних систем безпеки.
2. У роботі запропоновано перспективні напрямки розвитку безпеки — інтеграція Zero Trust Architecture, постквантова криптографія, блокчейн та фізична автентифікація (PLA).

Недоліки.
1. У роботі не наведено прикладів практичного впровадження технологій захисту чи архітектурних рішень.
2. У роботі не розглянуто, які саме атаки становлять найбільшу небезпеку за ймовірністю чи впливом.

Відзначені зауваження не впливають на загальну позитивну оцінку магістерської кваліфікаційної роботи

Висновок: *кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "відмінно", а здобувач Охременко Віктор Анатолійович заслуговує присвоєння кваліфікації: магістр з електронних комунікацій та радіотехніки.*

Рецензент
науковий ступінь, вчене звання _____ (підпис) _____ *(Ім'я ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 79 стор., 15 рис., 27 джерел.

Мета роботи – провести комплексний аналіз існуючих і потенційних вразливостей безпеки в мережах 5G/6G, WiFi 6/6E та системах спільного використання спектра, визначити основні вектори атак і розробити рекомендації щодо підвищення стійкості цих мереж до сучасних і майбутніх кіберзагроз.

Об’єкт дослідження – процеси забезпечення інформаційної безпеки в сучасних і перспективних безпроводових телекомунікаційних мережах 5G/6G, WiFi 6/6E та середовищах спільного використання радіочастотного спектра.

Предмет дослідження – механізми, протоколи та технології автентифікації, шифрування, управління ключами та захисту фізичного рівня, а також їхні вразливості й методи нейтралізації в умовах гетерогенних мереж і спільного використання спектра.

Короткий зміст роботи: у роботі проведено аналіз вразливостей безпеки в сучасних і перспективних телекомунікаційних системах — 5G/6G, WiFi 6/6E та мережах спільного використання спектра. Розглянуто недоліки протоколів автентифікації (5G-AKA, EAP-AKA’, WPA3), атаки на фізичному рівні (beamforming, pilot contamination) та ризики в гетерогенних середовищах співіснування. Визначено типові загрози, як-от захоплення спектра, PUE та SSDF-атаки, що знижують QoS і QoE. Запропоновано напрями вдосконалення захисту, зокрема впровадження Zero Trust Architecture, постквантової криптографії, блокчейн-рішень і поєднання фізичної автентифікації з протоколами вищих рівнів.

КЛЮЧОВІ СЛОВА: БЕЗПЕКА МЕРЕЖ, 5G, 6G, WIFI 6, ГЕТЕРОГЕННІ МЕРЕЖІ, ПРОТОКОЛИ АВТЕНТИФІКАЦІЇ, АТАКИ НА ФІЗИЧНОМУ РІВНІ, СПЕКТРАЛЬНА БЕЗПЕКА, КІБЕРЗАГРОЗИ, ZERO TRUST ARCHITECTURE, БЛОКЧЕЙН, УПРАВЛІННЯ СПЕКТРОМ, ЗАХИСТ ІНФОРМАЦІЇ

ABSTRACT

Text part of the master's qualification work: 79 pages, 15 figures, 27 sources.

The purpose of the work is to conduct a comprehensive analysis of existing and potential security vulnerabilities in 5G/6G, WiFi 6/6E networks and spectrum sharing systems, identify the main attack vectors and develop recommendations for increasing the resilience of these networks to current and future cyber threats.

Object of the study is the processes of ensuring information security in modern and promising wireless telecommunication networks 5G/6G, WiFi 6/6E and radio frequency spectrum sharing environments.

Subject of the study is mechanisms, protocols and technologies of authentication, encryption, key management and physical layer protection, as well as their vulnerabilities and methods of neutralization in heterogeneous networks and spectrum sharing.

Summary of the work: the work analyzes security vulnerabilities in modern and promising telecommunication systems - 5G/6G, WiFi 6/6E and spectrum sharing networks. The shortcomings of authentication protocols (5G-AKA, EAP-AKA', WPA3), physical layer attacks (beamforming, pilot contamination) and risks in heterogeneous coexistence environments are considered. Typical threats such as spectrum grabbing, PUE and SSDF attacks that reduce QoS and QoE are identified. Areas of improvement for protection are proposed, in particular the implementation of Zero Trust Architecture, post-quantum cryptography, blockchain solutions and the combination of physical authentication with higher-level protocols.

KEYWORDS: NETWORK SECURITY, 5G, 6G, WIFI 6, HETEROGENEOUS NETWORKS, AUTHENTICATION PROTOCOLS, PHYSICAL ATTACKS, SPECTRAL SECURITY, CYBER THREATS, ZERO TRUST ARCHITECTURE, BLOCKCHAIN, SPECTRUM MANAGEMENT, INFORMATION PROTECTION

ЗМІСТ

ВСТУП 9
РОЗДІЛ 1 ВИМОГИ ДО БЕЗПЕКИ WIFI ТА 6G 11
1.1 WiFi маршрутизатори 11
1.2 Проблеми безпеки в 6G 14
1.3 Основні проєкти 6G 18
РОЗДІЛ 2 ВРАЗЛИВОСТІ У 5G ТА WIFI 6/6E 21
2.1 Основні проблеми 21
2.2 Безпека на фізичному рівні 24
2.3 Безпека доступу в 5G 29
2.4 Безпека доступу в WiFi 6/6E 42
РОЗДІЛ 3 БЕЗПЕКОВІ РИЗИКИ СПІВІСНУВАННЯ ТА РОЗПОДІЛУ НЕЛІЦЕНЗОВАНОГО СПЕКТРА 52
3.1 Спільне використання спектру 52
3.2 Безпека в системах спільного використання спектру 55
3.3 Захват спектру та погіршення якості обслуговування 58
3.4 Pseudo MitM та фізичний шар безпеки 62
РОЗДІЛ 4 ПОМ'ЯКШЕННЯ НАСЛІДКІВ ТА НАПРЯМКИ МАЙБУТНІХ ДОСЛІДЖЕНЬ 68
4.1 Рішення для безпеки фізичного рівня 68
4.2 Рішення в області безпеки доступу 71
4.3 Напрями досліджень у галузі безпеки співіснування 74
ВИСНОВКИ 78
ПЕРЕЛІК ПОСИЛАНЬ 80
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 83

ВСТУП

Стрімкий розвиток телекомунікаційних технологій останніх десятиліть призвів до появи нового покоління безпроводових мереж, серед яких ключовими є 5G, WiFi 6/6E та перспективні 6G. Вони забезпечують високі швидкості передачі даних, наднизькі затримки, підтримку масових підключень пристроїв Інтернету речей (IoT/IoE), інтеграцію штучного інтелекту та нові підходи до управління спектром. Ці фактори створюють основу для цифрової трансформації суспільства, розвитку «розумних міст», безпілотного транспорту, критичних сервісів охорони здоров'я, промислової автоматизації та глобальних інформаційних систем.

Однак разом із новими можливостями виникають і нові загрози. Традиційні механізми безпеки, які достатньо ефективно функціонували в мережах попередніх поколінь, виявляються недостатніми у відкритих, динамічних і багаторівневих середовищах співіснування. Серед ключових викликів можна відзначити уразливості протоколів автентифікації (5G-AKA, EAP-AKA', WPA2/WPA3), атаки на ключові механізми (переустановка ключів, пониження версії), розкриття ідентифікаторів абонентів (IMSI, SUPI, SUCI), компрометацію конфіденційності місцеположення та появу нових векторів атак на фізичному рівні (beamforming, MIMO, атаки пілотного забруднення).

Окремим викликом стали мережі спільного використання спектра, у яких різні системи (5G і WiFi 6/6E) конкурують за доступ до одних і тих же частотних ресурсів. У таких умовах виникають проблеми прихованих вузлів, атаки на захоплення спектра, маніпуляції протоколами LBT, а також складність розмежування легітимної та зловмисної активності. Це не лише знижує якість обслуговування (QoS) і досвід користувачів (QoE), але й становить загрозу для критичних інфраструктур.

Дослідження проблем безпеки в цих мережах має подвійне значення. З одного боку, воно дозволяє систематизувати відомі уразливості та класифікувати сучасні атаки. З іншого – створює передумови для розробки нових підходів до захисту, які

враховують специфіку середовищ співіснування, використання відкритих архітектур і перспективу квантових обчислень.

Таким чином, актуальність теми дипломної роботи зумовлена необхідністю глибокого аналізу існуючих та потенційних вразливостей безпеки в мережах 5G/6G, WiFi 6 і системах спільного використання спектра, а також визначення шляхів підвищення їхньої стійкості до сучасних і майбутніх загроз.

1 ВИМОГИ ДО БЕЗПЕКИ WIFI ТА 6G

1.1 WiFi маршрутизатори

Протягом останніх років методи геопозиціонування мобільних пристроїв істотно еволюціонували, і сьогодні смартфони на базі Android та iOS активно застосовують інформацію про навколишні беспроводові мережі Wi-Fi для визначення свого місцеположення. Сучасний мобільний телефон періодично здійснює сканування простору у пошуках доступних точок доступу, фіксуючи їхні унікальні ідентифікатори (BSSID) та паралельно визначаючи власні координати за допомогою GPS-модуля. Усі ці дані передаються виробнику операційної системи, де формуються великі централізовані бази геоприв’язки Wi-Fi-мереж.

Отримана інформація не зберігається лише для внутрішніх потреб. І Google, і Apple відкривають доступ до своїх геолокаційних даних за допомогою спеціалізованих API, які можуть використовувати сторонні розробники. Проте дослідження науковців з Університету Меріленду (США) продемонструвало, що реалізація цих API містить приховані ризики: за допомогою доступних інтерфейсів можна фактично відстежувати переміщення Wi-Fi-маршрутизаторів по всьому світу, а отже, побічно контролювати й пересування людей, що ними користуються.

Архітектура WPS від Google та Apple

Обидві компанії розробили власні системи позиціонування на основі Wi-Fi — так звані **WiFi-based Positioning Systems (WPS)**. Їхня робота полягає у зборі специфічних апаратних ідентифікаторів від усіх точок доступу, що опиняються у полі дії смартфонів. Ідентифікатор Media Access Control (MAC) реєструється як **Basic Service Set Identifier (BSSID)** та використовується як прив’язка до певних географічних координат.

У випадку системи Google пристрій формує список доступних BSSID та рівнів сигналу, надсилає його через API у хмарну систему WPS, яка виконує обчислення координат та повертає результат. Для визначення приблизного місцеположення достатньо щонайменше двох BSSID.

Система Apple функціонує дещо інакше. Замість повернення кінцевих координат пристрою, API надає геолокаційні дані до 400 найближчих точок доступу. Сам смартфон, використовуючи приблизно вісім таких BSSID як орієнтири, обчислює своє місцеположення самостійно. Таким чином, Google централізовано визначає географічні координати пристрою, тоді як Apple передає великий обсяг «сирих» даних, що дозволяють смартфону виконувати обчислення локально.

Потенційні загрози безпеці

Як показало дослідження американських вчених, саме ця особливість реалізації системи Apple створює нові ризики. Надмірно детальна інформація про навколишні BSSID може бути використана для відстеження переміщення не лише точок доступу, але й кінцевих користувачів. Дослідники експериментально довели, що отримані дані дають змогу будувати карти пересування пристроїв у будь-якому регіоні світу. Особливо тривожним є те, що такі можливості можна застосувати навіть у зонах бойових дій, відслідковуючи, звідки саме прибувають користувачі. Це безпосередньо створює ризик витоку чутливої інформації та може становити загрозу життю людей.

Протягом місяця автори експерименту здійснили понад мільярд запитів до API, використовуючи випадково згенеровані BSSID. Хоча з них лише близько 3 мільйонів відповідали реальним пристроям, система Apple надала координати ще 488 мільйонів точок доступу, що вже зберігалися в її базі даних. Це демонструє масштабність зібраної інформації та підтверджує, що обсяг даних у WPS фактично дозволяє створювати глобальні карти беспроводових мереж і переміщення їхніх користувачів.

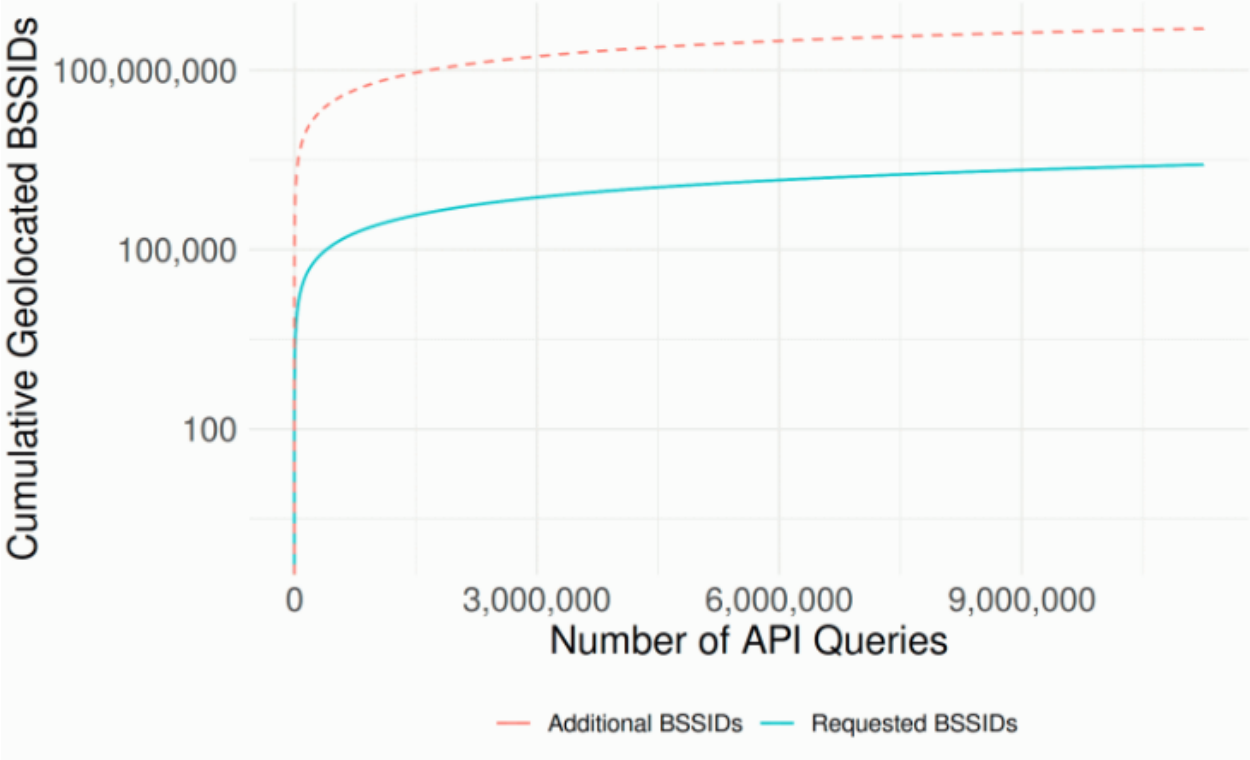


Рис. 1.1 Кількість BSSID, виявлених шляхом випадкового вгадування серед OUI, призначених IEEE, порівняно з додатковими BSSID, які повертає API для геолокації Wi-Fi від Apple

У ході проведеного дослідження науковці здійснили масштабний аналіз даних, зібраних за допомогою системи **Apple WPS** у часовому проміжку з листопада 2022 року по листопад 2023 року. Використавши отриману інформацію про координати точок доступу, вони нанесли ці дані на карту світу. Результати виявилися вражаючими: дослідники отримали фактично глобальне охоплення, яке дало змогу сформувати цілісне уявлення про розташування понад **двох мільярдів** точок доступу Wi-Fi.

Створена карта демонструє географічне положення Wi-Fi-інфраструктури у найрізноманітніших регіонах світу — від великих мегаполісів і промислових зон до невеликих населених пунктів і навіть віддалених територій. Іншими словами, база даних, яку надав Apple WPS через свій API, охоплює практично кожен куточок планети, дозволяючи простежити щільність розподілу мереж, їхні географічні особливості та навіть оцінити рівень проникнення беспроводових технологій у різних країнах.

Подібний масив даних можна розглядати не лише як технічне досягнення, а й як джерело серйозних ризиків для приватності. Адже геолокація точок доступу, розподілених по всій земній кулі, опосередковано відображає і маршрути переміщення людей, які користуються цими мережами. Наприклад, можна простежити, які точки доступу з'являються або зникають у конкретних регіонах, як змінюється інфраструктура в умовах воєнних дій чи масових міграцій, або навіть визначити мобільність окремих користувачів на основі динаміки BSSID.

Таким чином, нанесення даних WPS на карту перетворилося на своєрідну «теплову карту світу», що відображає живу динаміку розвитку цифрової інфраструктури. Це наочно показує, що Apple WPS фактично володіє майже глобальною системою спостереження за беспроводовими мережами, і використання цих даних може як принести користь у сфері телекомунікаційних досліджень та розвитку технологій, так і стати потенційною загрозою інформаційній безпеці та приватності мільйонів користувачів у всьому світі.

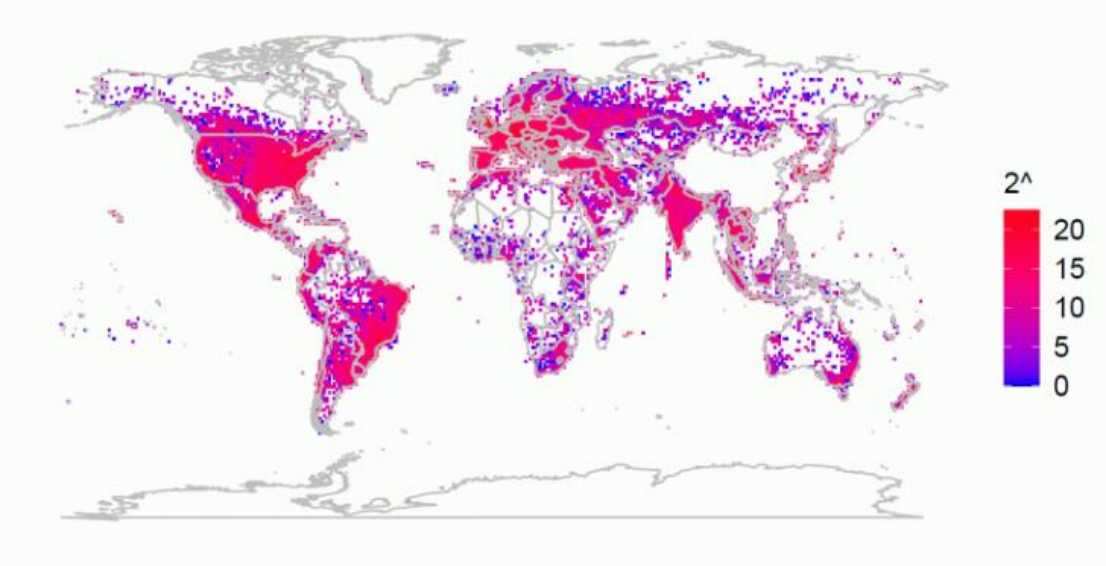


Рис. 1.2 Теплова карта BSSID, виявлених шляхом випадкового вгадування серед OUI, призначених IEEE

1.2 Проблеми безпеки в 6G

У процесі розвитку телекомунікаційних технологій від покоління 5G до 6G постає низка нових викликів у сфері кіберзахисту. Хоча такі інноваційні підходи, як

Multi-access Edge Computing (MEC), Software-defined Networking (SDN), Network Functions Virtualization (NFV) та мережеве розділення (network slicing), забезпечують значне зростання гнучкості та масштабованості, вони одночасно формують і нові вектори атак. За прогнозами, кількість підключених пристроїв до мереж 6G до 2030 року може перевищити 500 мільярдів одиниць, а це означає, що будь-яка вразливість потенційно створюватиме глобальний ефект.

Найнебезпечнішими залишаються атаки на SDN-контролери, які відповідають за централізоване управління маршрутизацією та потоками даних. Дослідження показують, що успішна атака на один контролер може вплинути на десятки тисяч одночасних з'єднань, фактично вивівши з ладу критичну інфраструктуру. Віртуальні машини, гіпервізори та системи управління віртуальними мережевими функціями (VNF managers) уразливі до атак, які дозволяють зловмиснику перехопити контроль над сотнями віртуалізованих сервісів одразу. MEC, що переносить обробку даних ближче до користувача, піддається як фізичним ризикам (втрата або пошкодження обладнання на периферії), так і DDoS-атакам. Наприклад, масована DDoS-атака потужністю у кілька терабіт за секунду здатна вивести з ладу цілу групу MEC-вузлів, порушивши роботу розподілених сервісів.

Додаткову небезпеку становить використання пристроїв Інтернету речей (IoT). У 2025 році їхня кількість перевищить 75 мільярдів, а в умовах IoE (Internet of Everything) вони стануть повноцінними учасниками 6G-екосистеми. Значна частина таких пристроїв має обмежені обчислювальні можливості й не підтримує складних криптографічних протоколів. Наприклад, понад 60 % сучасних фітнес-трекерів та розумних сенсорів взагалі не шифрують дані на рівні пристрою. У майбутньому ці слабкі місця можуть використовуватися як «ворота» для атак на всю мережеву інфраструктуру.

Архітектура безпеки мереж 6G

Мережі шостого покоління будуть ґрунтуватися на автоматизованій архітектурі управління та концепції Zero-touch Service Management (ZSM). Це дасть змогу значно скоротити експлуатаційні витрати (очікується зменшення витрат на

управління мережею до 40 % у порівнянні з 5G) та мінімізувати людські помилки. Проте забезпечення безпеки в умовах повної автоматизації стає значно складнішим, оскільки будь-яка уразливість у програмних компонентах може бути використана для масштабної атаки.

Особливу увагу слід приділити відкритому характеру мереж 6G. Якщо архітектура 5G ще передбачала відносно чітке розмежування внутрішніх і зовнішніх сегментів, то в 6G ці кордони будуть практично знівельовані. Це означає, що класичні методи захисту, як-от файрволи, VPN чи брандмауери, вже не гарантуватимуть належного рівня безпеки.

У цьому контексті ключовим рішенням є впровадження парадигми Zero Trust (ZT). Вона ґрунтується на припущенні, що зловмисник може знаходитися як поза мережею, так і всередині неї. Архітектура Zero Trust Architecture (ZTA) передбачає багаторівневий контроль доступу, жорсткі протоколи автентифікації, безперервний моніторинг і динамічне управління ризиками. У межах 6G саме ZTA має стати основою для комплексної системи безпеки.

Необхідність адаптації існуючих рішень

Механізми захисту, що були успішними в межах 3G та 4G, у 6G не зможуть виконувати свої функції. Вже сьогодні експерти 3GPP визнають, що архітектура безпеки 5G буде потребувати глибокої трансформації для відповідності новим умовам.

Захист у мережах шостого покоління має включати створення нових криптографічних алгоритмів, у тому числі постквантових, здатних витримати атаки квантових комп’ютерів, які, за прогнозами, до 2035 року зможуть розшифровувати ключі RSA та ECC упродовж хвилин. Протоколи автентифікації повинні забезпечувати стійкість до атак на основі машинного навчання та моделювання користувацької поведінки. Також передбачається побудова багаторівневої системи захисту, де на фізичному, транспортному, мережевому та прикладному рівнях будуть застосовуватися спеціалізовані механізми безпеки.

Особливу складність становить захист у нових середовищах — космосі та під водою. Наприклад, супутникові канали зв’язку вразливі до перехоплення сигналу

та глушіння, тоді як підводні мережі на основі акустичного зв’язку схильні до високого рівня шуму та спотворень. Це вимагає створення унікальних протоколів шифрування та автентифікації для кожного з середовищ.

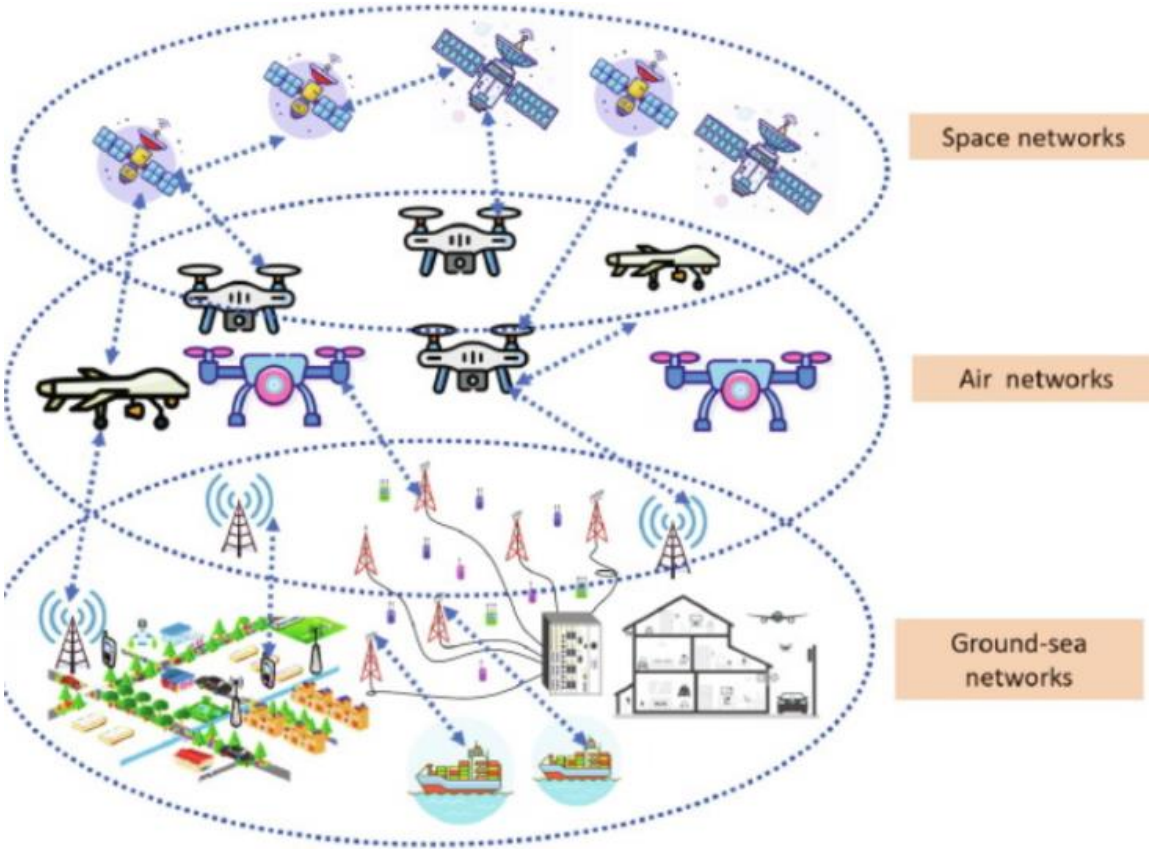


Рис. 1.3 Використання 6G в різних середовищах

Основні вимоги до безпеки в 6G

1. **Захищені системи віртуалізації.** Використання гіпервізорів (VMware ESXi, Microsoft Hyper-V, KVM) та контейнерних платформ (Docker, Kubernetes) вимагає впровадження механізмів виявлення прихованого шкідливого ПЗ, зокрема руткітів, та забезпечення жорсткої ізоляції обчислювальних ресурсів.
2. **Контроль уразливостей open-source.** За даними досліджень, понад 80 % компаній у сфері телекомунікацій застосовують відкриті бібліотеки, і більше половини виявлених уразливостей за останні роки були пов’язані саме з open-source кодом. Тому системи 6G повинні передбачати централізований моніторинг та автоматичне оновлення компонентів.
3. **Захист даних у системах ШІ.** Штучний інтелект стане ключовим елементом управління мережею, але моделі можуть бути змінені або підмінені

зловмисниками. Використання цифрових підписів та блокчейн-технологій для перевірки цілісності моделей дозволить знизити ці ризики.

4. **Конфіденційність користувачів.** У світі, де понад 60 % інтернет-трафіку належить мобільним пристроям, захист персональних даних набуває критичного значення. Інформація користувачів повинна зберігатися в довірених середовищах виконання (Trusted Execution Environment, TEE), а також проходити процедури анонімізації.
5. **Постквантова криптографія.** За прогнозами, до 2030-х років квантові обчислювальні системи матимуть можливість зламувати більшість традиційних алгоритмів шифрування. Тому впровадження постквантових алгоритмів (наприклад, CRYSTALS-Kyber чи Dilithium, рекомендованих NIST) є обов'язковою умовою для захисту 6G.

Безпека мереж 6G не може бути побудована лише на удосконаленні старих механізмів. Вона повинна ґрунтуватися на новій концепції, що враховує масштабність і відкритість архітектури, інтеграцію мільярдів пристроїв IoE, застосування штучного інтелекту для управління мережею, роботу у складних середовищах та появу квантових комп'ютерів. Тільки багаторівнева та адаптивна система безпеки здатна гарантувати надійність мереж 6G, захист інформації та конфіденційність користувачів у світі, де швидкість підключення сягатиме десятків гігабіт за секунду, а кількість пристроїв вимірюватиметься сотнями мільярдів.

1.3 Основні проєкти 6G

Hexa-X

У 2021 році компанія *Ericsson* у партнерстві з *Nokia*, *Siemens*, *Orange*, *Telefonica*, *Intel*, а також провідними університетами та дослідницькими центрами започаткувала проєкт Hexa-X. Він реалізується за підтримки програми Horizon 2020 Європейського Союзу. Бюджет першої фази перевищив 11 млн євро, до консорціуму увійшло понад 25 партнерів з 11 країн ЄС. Основна мета — розробити фундаментальні концепції для архітектури 6G, визначити ключові напрями

стандартизації та закласти підґрунтя для глобального впровадження мереж нового покоління. У фокусі Hexa-X — питання безпеки, адже до 2030 року очікується понад 500 млрд підключених пристроїв, що створює величезний простір для потенційних атак. Тому Hexa-X розробляє комплексні рішення для гарантування конфіденційності, стійкості та цілісності комунікацій.

Hexa-X-II

У 2023 році стартувала друга фаза — Hexa-X-II, яка вже фінансується програмою Horizon Europe. Її бюджет оцінюється більш ніж у 13 млн євро, а консорціум розширився до 44 партнерів із 14 країн. Якщо перший етап був зосереджений на формуванні візії та базових принципів 6G, то друга фаза спрямована на розробку конкретних технічних рішень, які у майбутньому стануть частиною стандарту 6G. Серед ключових завдань: створення архітектури з низькими затримками (нижче 0,1 мс), розробка нових методів безпеки на основі Zero Trust Architecture (ZTA), інтеграція постквантової криптографії та підтримка сервісів із надзвичайними вимогами до надійності, наприклад у медицині чи транспорті. Hexa-X-II також приділяє особливу увагу стійкості та енергоефективності: мета — знизити енергоспоживання мереж на 20–30 % порівняно з 5G.

RISE 6G

Проєкт RISE 6G (*Reconfigurable Intelligent Sustainable Environments for 6G wireless networks*) стартував у 2021 році та має бюджет близько 12 млн євро. До консорціуму входить 13 партнерів, серед яких *NEC*, *CEA-Leti*, *Orange* та кілька провідних університетів. Головна ідея — використання технології Reconfigurable Intelligent Surfaces (RIS), яка дозволяє перетворювати поверхні довкілля на активні елементи мережі. Це дає змогу керувати поширенням радіохвиль, зменшувати енергоспоживання на до 30 %, підвищувати спектральну ефективність на 25–40 % та створювати «розумні середовища». RISE 6G поєднує технічні інновації з принципами сталого розвитку та екологічної ефективності.

New-6G

Проєкт New-6G орієнтований на інтеграцію телекомунікацій з мікро- та наноелектронікою. Бюджет оцінюється у 14 млн євро, до складу консорціуму входить понад 20 партнерів з різних секторів: від виробників напівпровідників і телекомунікаційних компаній до наукових лабораторій. Головна мета — розробка нових протоколів зв'язку, інтегральних схем та цифрових компонентів, здатних працювати у терагерцовому діапазоні (100 ГГц – 1 ТГц). Очікується, що такі рішення забезпечать швидкість передачі даних до 1 Тбіт/с та у 10–20 разів перевищать можливості 5G. Крім цього, New-6G досліджує використання постквантової криптографії та наноелектронних технологій для підвищення рівня безпеки й надійності мереж.

Таким чином, три ключові проєкти — Hexa-X (разом із його продовженням Hexa-X-II), RISE 6G та New-6G — охоплюють увесь спектр завдань, пов'язаних із розвитком мереж шостого покоління. Hexa-X та Hexa-X-II формують архітектурні основи та стандартизацію, RISE 6G створює нову концепцію «розумного середовища» на базі RIS, а New-6G розробляє апаратні та наноелектронні рішення для підтримки терагерцових частот. У сукупності ці проєкти визначатимуть глобальний розвиток телекомунікаційної інфраструктури у найближчі два десятиліття та забезпечать технологічне лідерство Європи у сфері 6G.

2 ВРАЗЛИВОСТІ У 5G ТА WIFI 6/6E

2.1 Основні проблеми

Вибухове зростання обсягів інформації, що генерується величезною кількістю різнорідних пристроїв — смартфонами, мобільними комп'ютерами, елементами Інтернету речей, безпілотними транспортними засобами та компонентами «розумної» інфраструктури, — стало ключовим чинником розвитку мереж п'ятого покоління (5G). Такий підхід до комунікаційних систем, орієнтований на управління інформаційними потоками, зумовив появу архітектури, заснованої на обслуговуванні (**Service-Based Architecture, SBA**). Дана архітектура дає можливість реалізовувати мережеві функції у хмарних середовищах, що, у свою чергу, значно полегшує управління даними, а також забезпечує масштабованість і програмованість у мережах **Beyond 5G (B5G)**. Початково архітектура мереж була оптимізована з метою досягнення високого рівня **QoE (Quality of Experience)**, що у сучасній науковій літературі визначається як один із головних показників ефективності мереж 5G. Проте варто зауважити, що архітектури безпеки розвиваються не такими швидкими темпами, як нові беспроводові технології, впроваджені для підтримки вимог QoE. Це створює підґрунтя для серйозних проблем у сфері кіберзахисту, що можуть проявлятися у вигляді нових загроз безпеці або розширення площини атак на основі наявних уразливостей.

Однією з найбільш характерних рис мереж 5G є можливість забезпечення безшовного з'єднання з низькою затримкою та високою швидкістю передачі даних для величезної кількості гетерогенних пристроїв. У цьому контексті QoE відіграє ключову роль як показник, що оцінює рівень роботи мережі з точки зору задоволення потреб користувачів. На відміну від **QoS (Quality of Service)**, який описує лише технічні характеристики (наприклад, пропускну здатність каналу чи рівень затримки), QoE відображає якість досвіду кінцевого користувача й включає такі аспекти, як своєчасність та надійність доставки контенту. Незважаючи на відсутність єдиної системи метрик для вимірювання QoE, безпека та

конфіденційність інформації мають розглядатися як його невід'ємні складові. З цієї позиції завдання оптимізації мережі у дипломній роботі доцільно трактувати як максимізацію QoE, де враховуються не лише традиційні параметри QoS, але й захист даних від несанкціонованого доступу.

Важливим прикладом унікальних можливостей 5G є використання технології множинного радіодоступу (**Multi-RAT, Multiple Radio Access Technology**). Вона дозволяє забезпечити високий рівень QoE шляхом підтримки взаємодії між різними технологіями доступу. Однак однією з найгостріших проблем залишається дефіцит частотного спектра, необхідного для різних застосувань із різними вимогами до дальності поширення сигналів. Перерозподіл невикористаних діапазонів спектра є нагальною потребою, проте він часто стикається з опором чинних користувачів і може негативно позначатися на критично важливих секторах, зокрема військових та урядових. Перспективним рішенням є концепція **спільного використання спектра**, яка розглядається як один із головних чинників розвитку B5G і забезпечення високого QoE.

Ранні приклади спільного використання спектра у США включали застосування вільних телевізійних частот (**TV White Space, TVWS**), що реалізовувалося за принципом прив'язки до географічного розташування. Інший приклад — розподіл діапазону 3550–3650 МГц між військово-морськими радарами, стаціонарними супутниковими системами та комерційною службою **Citizens Broadband Service (CBS)**. Спільне використання спектра між технологіями Wi-Fi та 4G у неліцензованому діапазоні 5 ГГц було стандартизоване 3GPP у вигляді LTE-LAA та eLAA. Крім того, Федеральна комісія зі зв'язку США (FCC) та Європейська комісія надали дозвіл на використання спектра в неліцензованих діапазонах 6 ГГц. У результаті 3GPP сформулював специфікації для використання так званого «greenfield spectrum» у технології NR-U в мережах 5G поряд із Wi-Fi 6 (IEEE 802.11ax) та Wi-Fi 6E, що функціонує у діапазоні 6 ГГц.

Існуючі архітектури безпеки будувалися за принципами автономних мереж, які повністю контролюють власні ресурси — від частотного спектра до фізичної інфраструктури. Під автономною мережею у дипломній роботі розумітимемо

інфраструктуру (базові станції, абонентські пристрої) з ексклюзивним доступом до спектра та без взаємодії із зовнішніми системами. У такій моделі будь-який доступ до ресурсів чи комунікаційного трафіку проходить автентифікацію й авторизацію лише в межах внутрішніх механізмів безпеки. Проте впровадження 5G, поява програмно-конфігурованих мереж (SDN) і концепції поділу мережі (network slicing) змінили цю парадигму: тепер кілька операторів і постачальників послуг змушені спільно використовувати одну інфраструктуру, дотримуючись при цьому різних політик безпеки та конфіденційності. Це зробило сумісність між різними системами безпеки на рівні **Core Network (CN)** складним завданням.

Схожі виклики постають і при співіснуванні різних технологій (наприклад, Wi-Fi та 5G) або в разі впровадження нових моделей спільного використання спектра. Незахищене використання спектра в таких умовах може відкрити новий канал для атак, який не відслідковується традиційними системами безпеки автономних мереж. Так званий **прихований канал** створює абсолютно нову площину ризиків, оскільки він дозволяє зловмисникам запускати атаки, для протидії яким ще не розроблені спеціальні механізми. У класичних мережах системи безпеки відслідковують дії внутрішньої інфраструктури, тоді як у випадку спільного використання спектра частина активностей відбувається поза її межами. Це відкриває можливості як для появи нових типів атак, так і для посилення вже відомих загроз.

У дипломній роботі розглянуто проблеми безпеки та потенційні експлойти на фізичному рівні та рівні доступу з акцентом на перспективи співіснування різних технологій. Наскільки відомо автору, ця дипломна робота є однією з перших спроб у вітчизняній літературі зосередитися саме на питаннях безпеки в умовах мультиоператорських середовищ та спільного використання спектра. Задля кращого розуміння того, які типи атак може активізувати незахищене використання спектра, а також які з існуючих загроз воно здатне підсилювати, спершу розглядаються уразливості автономних мереж 5G та Wi-Fi. Далі аналізуються проблеми безпеки, що виникають при спільному доступі до спектра, а також

можливості використання криптографічних методів для збереження конфіденційності мережевої інфраструктури.

2.2 Безпека на фізичному рівні

Криптографічні докази та безпека комунікацій на фізичному рівні

Згідно з сучасними стандартами, криптографічні докази захищеності комунікацій забезпечуються багаторівневими протоколами безпеки, які функціонують на різних рівнях стеку комунікаційних протоколів. Таке забезпечення починається з автентифікації користувача або пристрою, підтвердження ключів шифрування та побудови захищеного каналу на канальному рівні моделі OSI. Проте питання безпеки на фізичному рівні залишаються відкритими та активно досліджуються. Стандартизовані платформи ще не мають доведених механізмів захисту саме на цьому рівні, що пояснюється низкою факторів: мінливістю й невизначеністю умов радіоканалів, варіативністю пристроїв користувачів, а також розподіленим управлінням секретними ключами для мільярдів пристроїв до проходження автентифікації.

Класичним підходом до реалізації захисту на фізичному рівні є застосування систем з розширеним спектром у часовій або частотній області. Метод прямої послідовності DSSS (*Direct Sequence Spread Spectrum*) ґрунтується на кодуванні відліків переданого сигналу спеціальними розширювальними кодами, довжина яких значно перевищує інтервал одного біта. Якщо такі коди є секретними, DSSS забезпечує не лише автентифікацію та конфіденційність на фізичному рівні, а й підвищену стійкість до завад і захист від підробки сигналу. Показовим прикладом є використання зашифрованих DSSS-сигналів у військових системах GPS (Y-код та M-код), які досі вважаються еталоном надійності для спеціалізованих додатків.

Іншим поширеним підходом є метод **Multi-Carrier Spread Spectrum (MCSS)**, що є аналогом DSSS у частотній області. Він поєднує переваги OFDM (*Orthogonal Frequency Division Multiplexing*) і CDMA (*Code Division Multiple Access*), демонструючи високу спектральну ефективність, стійкість до

багатопроменевих затухань та ефективність у боротьбі з перешкодами. На фізичному рівні система MCSS кодує піднесучі OFDM за допомогою розширювальних кодів. Подібний підхід може бути застосований і для реалізації шифрування сигналів основної смуги (baseband) у частотній області. Це робить MCSS одним із найперспективніших методів для побудови шифрованих каналів у майбутніх системах 6G.

Теоретико-інформаційна безпека

Канальне кодування вже стало невід'ємною складовою фізичного рівня, оскільки воно підвищує надійність і стійкість лінії зв'язку. У специфікаціях 3GPP для мереж 5G eMBB застосовуються LDPC-коди (*Low-Density Parity Check*) для передачі даних та полярні коди для каналів управління. Доведено, що обидві схеми забезпечують теоретико-інформаційну безпеку в моделі «каналу прослуховування».

На відміну від класичних криптографічних алгоритмів (симетричних і з відкритим ключем), які базуються на обчислювальній складності для зловмисника, теоретико-інформаційна безпека спирається на різницю між характеристиками каналу законного отримувача та перехоплювача. Якщо канал користувача має більшу пропускну здатність, ніж канал зловмисника, передавана інформація залишиться для нього недосяжною, незалежно від рівня його обчислювальних можливостей.

У цьому контексті виділяють **сильну** та **слабку** секретність. Сильна секретність досягається, якщо взаємна інформація між переданим кодовим словом і сигналом, прийнятим перехоплювачем, прямує до нуля. Слабка секретність означає, що середнє значення взаємної інформації на один біт також прямує до нуля. Було доведено, що LDPC-коди здатні гарантувати слабку секретність, а при сприятливих умовах каналу — і сильну. Подібні результати показали і полярні коди, зокрема при використанні багатоблокових схем кодування. Це дозволяє не лише досягти сильної секретності, а й зберегти високу надійність передачі.

Дослідження також продемонстрували можливість досягнення області пропускної здатності широкомовних каналів із конфіденційними повідомленнями за допомогою полярних кодів. Поєднання схем кодування (наприклад, полярних і

LDPC-кодів) дозволяє зменшити втрати пропускної здатності та підвищити рівень секретності.

Виклики забезпечення секретності

Важливим обмеженням теоретико-інформаційної безпеки є її залежність від умов каналу, які можуть бути штучно змінені зловмисником. Навіть пасивний перехоплювач може досягти переваг, використовуючи високочутливі антени, вдосконалені схеми обробки сигналів чи складні алгоритми. Це означає, що абсолютна секретність не є повністю незалежною від якості реалізації приймального обладнання.

Ще більш загрозливим є сценарій із **активними перехоплювачами**, які можуть погіршувати якість каналу законного користувача. Одним із методів є створення додаткових завад, спрямованих на легального отримувача, що фактично знижує швидкість передачі з урахуванням секретності (*secrecy rate*) майже до нуля. У середовищах співіснування мереж, де допустимий рівень зовнішніх завад вищий, такі атаки стають ще простішими.

Окремим видом атак є втручання у процес оцінки **Channel State Information (CSI)**. Більшість схем канального кодування покладаються на точне знання CSI для гарантування обіцяного рівня секретності. Якщо перехоплювач здійснює атаку «забруднення пілотних сигналів» (*pilot contamination*), це призводить до спотворення оцінки стану каналу, внаслідок чого рівень секретності стрімко падає. У мережах із тимчасовим дуплексним поділом (TDD) було зафіксовано, що подібні атаки здатні практично повністю знищити захищеність каналу.

Технологія формування спрямованого променя (Beamforming)

Формування спрямованого променя (**beamforming**) є однією з базових та водночас найважливіших характеристик фізичного рівня сучасних мереж **5G-NR (5G New Radio)**. Сутність цієї технології полягає у можливості динамічного керування діаграмою спрямованості антенної решітки з метою максимально точного фокусування енергії сигналу в напрямку легального користувача. Це дозволяє значно підвищити ефективність використання спектра, а також

забезпечити стабільне з’єднання навіть у середовищах із високим рівнем багатопроменевого розповсюдження сигналу.

Основним завданням beamforming є збільшення співвідношення сигнал/шум та завади (**SINR, Signal-to-Interference-plus-Noise Ratio**), що безпосередньо впливає на надійність і пропускну здатність каналу. Завдяки формуванню каналу прямої видимості (LOS — *Line of Sight*), beamforming здатний зменшувати вплив багатопроменевих затухань, компенсувати інтерференцію та покращувати якість передавання даних. Крім того, технологія створює можливість реалізації просторового поділу каналів (**Space Division Duplexing**), що дає змогу одночасно обслуговувати кілька користувачів без істотного зниження швидкості.

Дослідження показують, що beamforming не лише підвищує швидкість та надійність з’єднання, а й може сприяти поліпшенню безпеки на фізичному рівні. Завдяки високій спрямованості передавання значно погіршується якість каналу для потенційного перехоплювача, який розташований поза головним променем. Таким чином, створюється ситуація, коли легальний користувач отримує стабільний та надійний канал, тоді як зловмисник у сторонньому напрямку спостерігає значні втрати сигналу, що ускладнює перехоплення даних. У симуляційних дослідженнях на міліметрових хвилях було продемонстровано, що при використанні beamforming можливо досягати рівня секретності у кілька гігабіт на секунду, що є показником, недосяжним для класичних всеспрямованих антенних систем.

Потенційні атаки та уразливості beamforming

Попри переваги, beamforming може використовуватися і зловмисниками для реалізації атак. Одним із прикладів є атака типу **«людина посередині» (Man-in-the-Middle, MitM)**. У цьому випадку зловмисник, використовуючи власні антени з підтримкою beamforming, створює приховані канали між передавачем і приймачем. При цьому він може перехоплювати, модифікувати або повторно передавати дані без відома легальних користувачів. У традиційних системах із всеспрямованою передачею подібні дії легше виявити за допомогою аналізу закономірностей сигналу, проте при застосуванні спрямованих променів атака MitM стає набагато менш помітною.

Найбільш серйозною загрозою для beamforming є атака **«забруднення пілота» (pilot contamination attack)**, що здійснюється на етапі оцінки стану каналу (**CSI, Channel State Information**). У нормальних умовах базова станція використовує пілотні сигнали для визначення оптимального напряму формування променя. Якщо ж у цей момент активний перехоплювач (Eve) передає завадові або підроблені пілотні сигнали, базова станція може помилково сформувати промінь у напрямку зловмисника замість легального користувача. У результаті перевага умов каналу для легального отримувача зникає, а рівень секретності стрімко падає. Дослідження демонструють, що така атака здатна знизити показник **secrecy rate** майже до нуля, навіть у системах із багатопроменевою компенсацією.

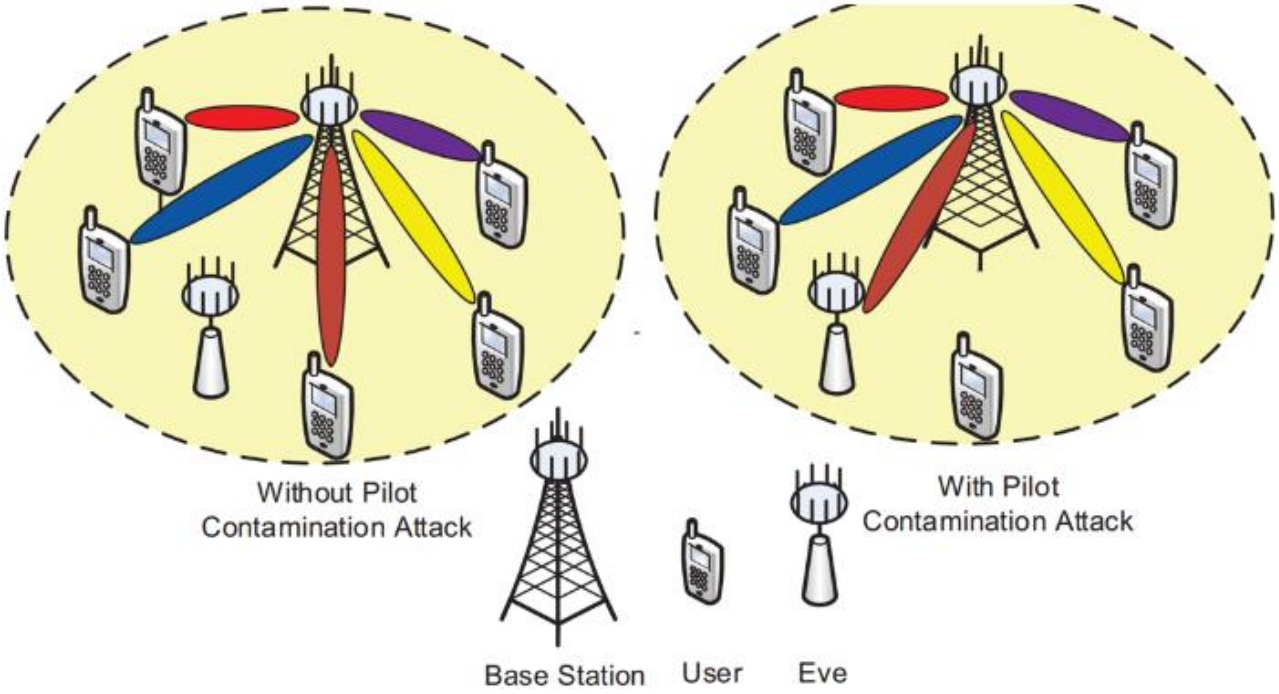


Рис. 2.1 Атака «Пілотне забруднення», коли активний перехоплювач перенаправляє промінь базової станції, призначений користувачеві (User), убік зловмисника (Eve) (зліва – без атаки «Забруднення пілота», справа – з нею)

Ризики від пасивних перехоплювачів

Окрім активних атак, небезпеку становлять і **пасивні перехоплювачі**, які не втручаються у процес передавання, а використовують фізичні властивості середовища для компрометації даних. Зокрема, показано, що відбиття міліметрових хвиль від невеликих об’єктів або поверхонь (наприклад, корпусів смартфонів чи ноутбуків) можуть створювати достатньо сильні сигнали, які підслуховуючий

пристрій здатний використати для зниження рівня секретності. Експериментальні результати на базі програмно-визначуваного радіо (**SDR, Software-Defined Radio**) свідчать, що подібні відбиття здатні зменшити секретність системи до **32%**, а за наявності додаткових блокаторів сигналу в напрямку легального користувача рівень секретності може впасти практично до нуля.

Таким чином, beamforming є потужною технологією, що дозволяє реалізувати високошвидкісні, надійні та масштабовані з'єднання у мережах 5G і майбутніх 6G. Вона створює умови для підвищення якості обслуговування та рівня секретності даних. Водночас існують серйозні виклики, пов'язані з можливістю використання beamforming зловмисниками, зокрема через атаки типу MitM, «забруднення пілота» чи використання відбиттів сигналів. Це свідчить про необхідність інтеграції додаткових механізмів безпеки, спрямованих на виявлення та протидію подібним загрозам. У майбутніх мережах 6G саме поєднання beamforming із новими методами захисту (наприклад, постквантовою криптографією, адаптивними протоколами автентифікації та алгоритмами виявлення атак на фізичному рівні) стане критично важливим для забезпечення стійкості систем до складних кіберзагроз.

2.3 Безпека доступу в 5G

Одним із фундаментальних завдань у системах мобільного та безпроводового зв'язку є захист доступу користувача до мережі. Це завдання реалізується за допомогою протоколів AKA (Authentication and Key Agreement — автентифікація та узгодження ключів), які забезпечують надійний обмін ключами між користувацьким обладнанням (UE, User Equipment) та мережею, а також формують базовий рівень захисту на канальному рівні моделі OSI. Протоколи AKA створюють основу для подальших рівнів безпеки, забезпечуючи перевірку автентичності користувачів і захист від підробки або несанкціонованого доступу.

У стандартах 3GPP передбачено розширюваний протокол автентифікації EAP (Extensible Authentication Protocol), що отримав специфікацію EAP-AKA'. Його

ключовим призначенням є інтеграція різних мереж доступу, які не належать до 3GPP, із мобільними мережами четвертого покоління (4G). Одним із найпоширеніших прикладів такої інтеграції є WLAN (безпроводові локальні мережі), які реалізують платформу EAP у межах WPA2 (WiFi Protected Access 2). Таким чином, протокол EAP виступає універсальним інструментом для автентифікації як у Wi-Fi, так і в мобільних мережах.

З розвитком мобільних систем нового покоління протокол EAP-AKA’ продовжив своє застосування і в мережах 5G, де він використовується як один із альтернативних механізмів автентифікації поряд із спеціалізованим протоколом 5G-AKA. Останній багато в чому повторює логіку EAP-AKA’, проте має низку відмінностей, які підвищують рівень безпеки. Головна з них полягає в інтеграції функції SEAF (Security Anchor Function — якорна функція безпеки). На відміну від EAP-AKA’, де підтвердження відповідей UE відбувається лише у домашній мережі, у 5G-AKA первинна перевірка здійснюється безпосередньо в обслуговуючій мережі. Це дозволяє знизити затримки, пов’язані з автентифікацією, підвищує стійкість до атак повтору (replay attacks) та зменшує ймовірність компрометації ключів.

У загальному вигляді процес EAP-AKA’ включає кілька етапів: ініціація автентифікації з боку користувача, передавання запиту до автентифікаційного сервера, генерування ключів і підтвердження з боку UE та, нарешті, встановлення захищеного сеансового ключа, що надалі використовується для шифрування даних. Цей процес дозволяє захистити мережу від більшості базових атак, таких як несанкціонований доступ, підробка користувацького обладнання чи підміна сигналів.

Однак, навіть у випадку використання сучасних протоколів, мережі доступу залишаються потенційно вразливими. Так, дослідження показують, що протоколи EAP-AKA’ та 5G-AKA можуть бути піддані атакам типу «людина посередині» (MitM, Man-in-the-Middle), коли зловмисник перехоплює або модифікує обмін автентифікаційними повідомленнями. Крім того, можливі атаки на канальному

рівні, спрямовані на відновлення або компрометацію ключів за допомогою аналізу трафіку.

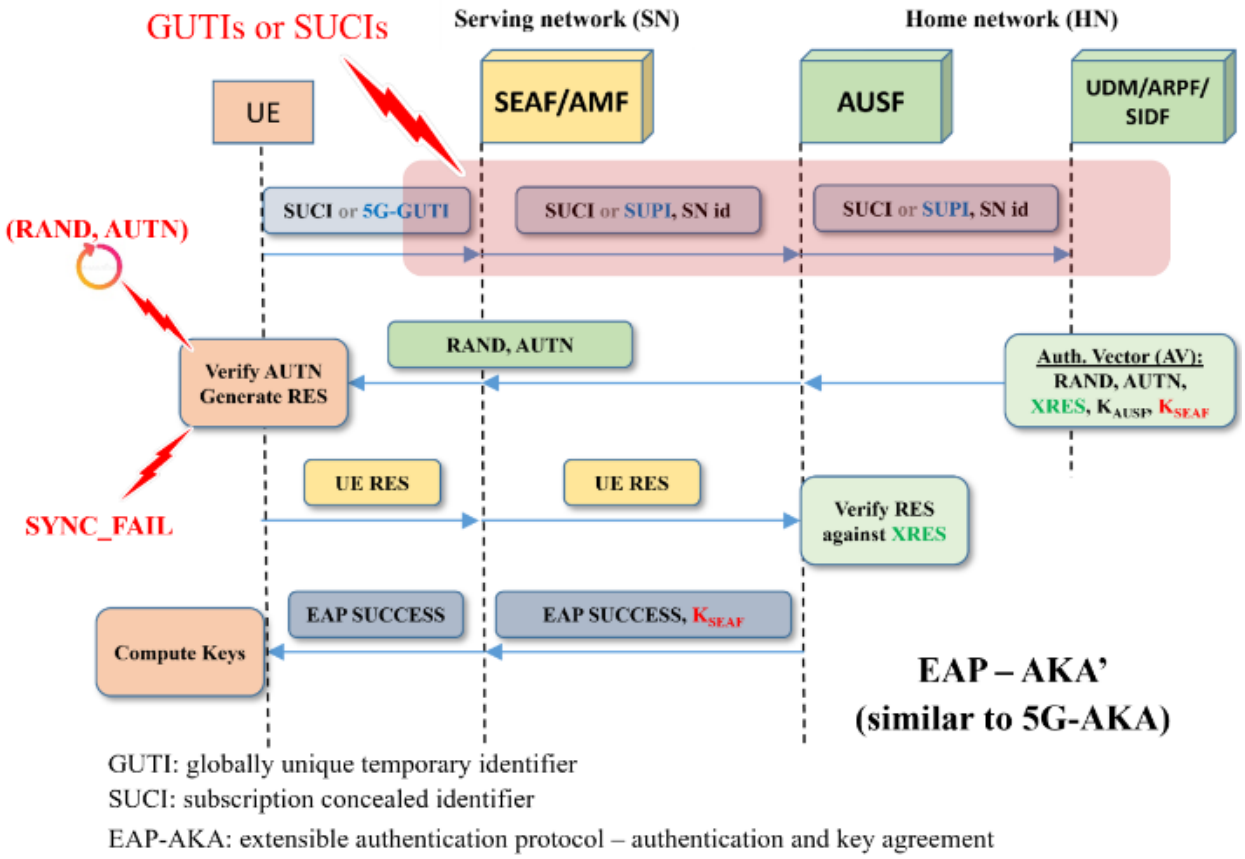


Рис. 2.2 Безпека доступу на основі EAP в мережах 5G та різні точки атаки на протокол

Таким чином, протоколи EAP-AKA' і 5G-AKA формують основу для побудови безпечної інфраструктури безпроводових мереж доступу, але водночас вимагають додаткових механізмів захисту від сучасних атак. У дипломній роботі доцільно розглядати їх не як кінцеве рішення, а як складову комплексної системи безпеки, яка у перспективі має бути підсилена механізмами багатофакторної автентифікації, постквантової криптографії та алгоритмами динамічного управління ключами.

Конфіденційність персональних даних

Забезпечення приватності абонентів завжди було одним із ключових завдань мобільних мереж. Із появою кожного нового покоління стільникового зв'язку розробники приділяли значну увагу механізмам захисту ідентифікаторів користувачів. У класичних мережах основним засобом ідентифікації виступав IMSI

(International Mobile Subscriber Identity — міжнародний ідентифікатор мобільного абонента), який є унікальним номером SIM-картки. У системах п’ятого покоління його функції виконує SUPI (Subscriber Permanent Identifier — постійний ідентифікатор абонента). Важливо, що SUPI є більш універсальним: він не обмежується лише стільниковими сервісами, а може використовуватися і в інших середовищах, зокрема в мережах Інтернету речей (IoT), де кількість пристроїв уже обчислюється мільярдами.

Для запобігання витоку приватних даних у 5G реалізовано механізм SUCI (Subscription Concealed Identifier — прихований ідентифікатор абонента). Це зашифрована версія SUPI, що генерується у домашній мережі користувача за допомогою відкритих ключів. Під час першого з’єднання пристрій (UE, User Equipment) передає SUCI у мережу, після чого ініціюється шифрування радіоканалу. Для подальшої взаємодії абоненту призначається GUTI (Globally Unique Temporary Identifier — глобальний унікальний тимчасовий ідентифікатор), що використовується для уникнення частих передач SUCI та зменшення ризику його компрометації.

Втім, навіть у такій схемі залишаються вразливості. GUTI має відносно довгий час життя, і у випадку його розкриття (наприклад, через прослуховування радіоканалу зловмисником) може відкрити так звану «м’яку ідентичність» користувача. У поєднанні з атаками, спрямованими на компрометацію геолокаційних даних, це створює реальну загрозу. Отримавши GUTI, зловмисник може відстежувати пересування абонента, прив’язувати тимчасові ідентифікатори до конкретної особи, а згодом отримати доступ до історії дзвінків, SMS або навіть певної мережевої активності. Навіть оновлення GUTI не завжди захищає користувача, оскільки методи кореляційного аналізу дозволяють зіставляти старі та нові ідентифікатори. У цьому сенсі атаки на GUTI мають подібний ефект до класичних атак IMSI-catching, які активно застосовувалися проти мереж попередніх поколінь.

Ще однією слабкою ланкою залишаються екстрені виклики. Вони повинні бути доступними навіть для пристроїв, які не пройшли автентифікацію, що

відкриває можливість передавання SUPI (або IMSI) у незашифрованому вигляді. У критичних сценаріях, коли UE з певних причин не може автентифікуватися, безпека персонального ідентифікатора не гарантується. Це створює вікно можливостей для атакувальників, які можуть використовувати цю вразливість для перехоплення SUPI.

Особливу небезпеку становлять атаки у середовищах коексистенції мереж, де одночасно працюють кілька систем різних стандартів. У таких випадках зловмисник може отримати доступ до спектра і цілеспрямовано створювати збої у процесі автентифікації, залишаючись непоміченим. Викликавши штучний «екстрений сценарій», наприклад шляхом внесення помилок у сигнал, атакувальник може змусити UE передавати SUPI/IMSI у відкритому вигляді. При наявності обладнання для прослуховування каналу це дозволяє легко отримати ідентифікатор.

Не менш небезпечним є й інший підхід — використання нелегальних базових станцій, що маскуються під легітимні вузли мережі gNB (gNodeB). Такі станції можуть імітувати запити від імені екстрених служб, змушуючи пристрій користувача передати IMSI безпосередньо атакувальнику. Враховуючи відносну дешевизну обладнання для побудови фальшивих базових станцій, подібні атаки стають дедалі поширенішими і становлять серйозну загрозу для приватності користувачів у 5G.

У перспективі 6G проблема конфіденційності набуде ще більшого значення через масштабне впровадження IoE (Internet of Everything), де кожен сенсор чи пристрій потенційно може бути об’єктом атак. Це вимагає не лише вдосконалення системи SUCI та GUTI, але й розробки нових методів — наприклад, використання динамічних одноразових ідентифікаторів, технологій анонімізації даних, а також інтеграції криптографічних рішень, стійких до атак квантових комп’ютерів.

Злам IMSI та атака ToRPEDO

Хоча у мережах п’ятого покоління реалізовано більш захищені механізми ідентифікації користувачів, пов’язані з використанням SUCI (Subscription Concealed Identifier — прихований ідентифікатор абонента), повністю усунути ризик витоку

IMSI (International Mobile Subscriber Identity — міжнародний ідентифікатор мобільного абонента) не вдалося. IMSI є 49-бітним ідентифікатором, у якому 18 бітів займає код країни, що є загальнодоступним і заздалегідь відомим потенційному зловмиснику. Таким чином, реальний обсяг даних, які потрібно відновити атакуючому, значно скорочується.

Одним із найнебезпечніших методів відновлення IMSI є атака ToRPEDO (TRacking via Paging mEssage DistributiOn), що належить до класу атак на сторонніх каналах. Принцип її роботи полягає у використанні пейджингових повідомлень, які мобільний пристрій отримує у режимі очікування або енергозбереження. Пейджингові події мають чітку періодичність, що частково зафіксована у бітовій структурі IMSI. Це дозволяє атакуючому за допомогою серії коротких викликів (зазвичай менше ніж 10) відновити 7 бітів IMSI, навіть якщо TMSI (Temporary Mobile Subscriber Identity) змінюється після кожного виклику.

Таким чином, ToRPEDO дає можливість підтвердити, чи перебуває цільовий пристрій у певній географічній зоні. Це означає, що навіть без повного відновлення IMSI зловмисник отримує можливість відстежувати місцезнаходження користувача з відносно високою точністю. Для спецслужб або атакуючих груп це відкриває шлях до масового моніторингу пересувань абонентів, особливо у багатолюдних районах чи стратегічно важливих локаціях.

Залишкові 24 біти IMSI можуть бути відновлені за допомогою атаки перебором (brute-force attack), яка базується на уразливостях у механізмах автентифікації 5G. Якщо зловмисник має у своєму розпорядженні відкритий ключ домашньої мережі абонента, він може здійснити наступний сценарій:

1. Згенерувати підроблений SUCI, використовуючи передбачуване значення IMSI.
2. Надіслати SUCI до основної мережі (CN, Core Network) для перевірки.
3. Отримати відповідь від мережі у вигляді AUTH_REQUEST (ідентифікатор дійсний) або REGISTRATION_REJECT (ідентифікатор відхилено).

4. У разі позитивного результату переслати AUTH_REQUEST на пристрій користувача для перевірки. Відповідь UE може бути або AUTH_RESPONSE (ідентифікатор підтверджений), або AUTH_FAIL (ідентифікатор відхилений).

Ця процедура дозволяє послідовно перебирати можливі значення IMSI, поки не буде знайдено правильний ідентифікатор. Експериментальні результати доводять, що поєднання атаки ToRPEDO та перебору дає можливість повністю відновити IMSI за відносно короткий час — у середньому 74 години.

Небезпека цього підходу полягає у його масштабованості. Якщо атакуючий володіє достатньо потужними обчислювальними ресурсами та кількома пристроями для перехоплення, він здатний одночасно проводити атаки на сотні або навіть тисячі абонентів. Таким чином, навіть одинична уразливість у процедурі автентифікації 5G може призвести до масового витоку приватних даних.

Ще одним аспектом є те, що IMSI, будучи основним ідентифікатором абонента, може бути використаний для:

- встановлення номера телефону користувача;
- збирання інформації про активність у мережі (дзвінки, SMS, інтернет-сесії);
- ідентифікації географічного положення навіть після зміни тимчасових ідентифікаторів;
- кореляції даних із базами мобільних операторів чи державних систем моніторингу.

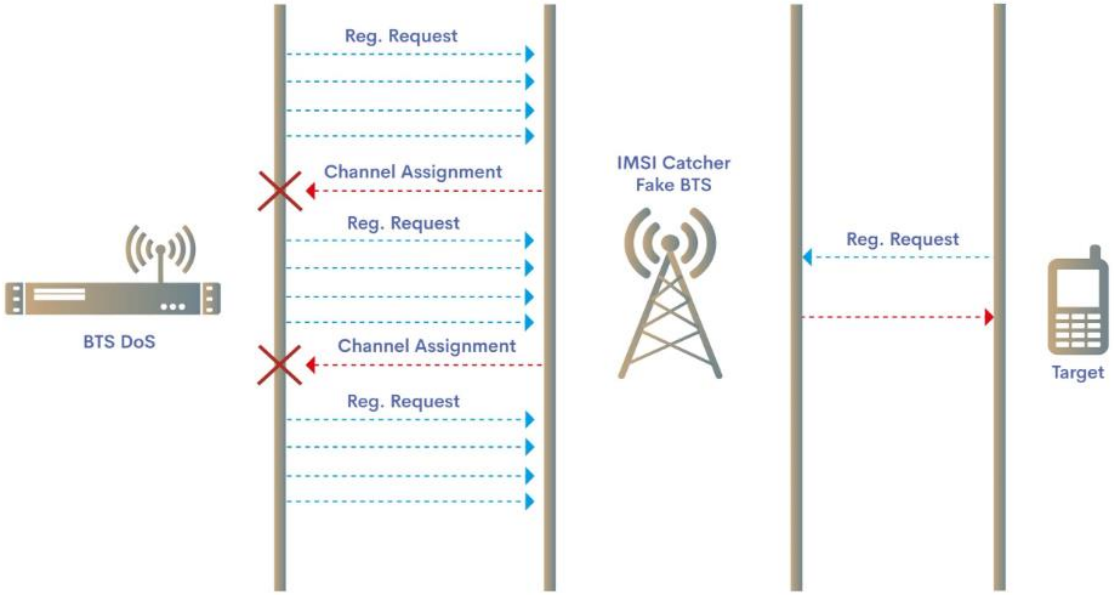


Рис. 2.3 Робота IMSI-catcher: підроблена базова станція змушує пристрій передати IMSI

Таким чином, атака ToRPEDO у поєднанні з перебором створює пряму загрозу приватності користувачів 5G, фактично відновлюючи ризики, характерні для мереж попередніх поколінь, зокрема атак на основі IMSI-catcher.

Конфіденційність місцеположення

Одним із ключових аспектів захисту даних у мережах п’ятого покоління є забезпечення конфіденційності місцеположення користувача. Проте навіть із впровадженням нових механізмів ідентифікації уразливості все ще залишаються. Як було розглянуто раніше, атака ToRPEDO (TRacking via Paging mEssage DistributiOn) дозволяє зловмиснику отримати приблизну інформацію про місцезнаходження абонента завдяки аналізу пейджингових повідомлень, які періодично надсилаються пристрою в режимі очікування. Визначаючи закономірності у частоті пейджингових подій, атакуючий здатен встановити факт присутності цільового пристрою у певній зоні, навіть не маючи доступу до повної інформації про його ідентифікатор.

Для отримання більш точної геолокації зловмисники можуть поєднувати ToRPEDO з іншими методами аналізу радіосигналів. Зокрема, застосовується

визначення кута приходу сигналу (AoA, Angle of Arrival), що дозволяє виявити напрямок на абонента, а також вимірювання рівня прийнятого сигналу (RSS, Receive Signal Strength), яке надає дані про відстань до джерела сигналу. Комбінація цих технік забезпечує можливість створення детальної карти переміщення користувача.

Особливу небезпеку становить атака на відстежуваність (traceability attack), яка використовує слабкі місця у процедурі автентифікації мереж 5G. На етапі первинної автентифікації мобільний пристрій отримує від мережі викликові повідомлення (RAND, AUTN), що є унікальними для конкретного сеансу. Зловмисник, перехопивши ці повідомлення, може пізніше повторно надсилати їх пристрою. Якщо UE відповідає повідомленням SYNC_FAIL, це підтверджує його присутність у зоні досяжності. Таким чином, навіть без взаємодії з головною мережею атакуючий отримує можливість визначати фактичне місцеположення абонента та відстежувати його пересування у реальному часі. Це відкриває нові горизонти для шпигунства, цільових атак або навіть масового моніторингу.

Відмова в обслуговуванні (DoS)

Мережі п’ятого покоління орієнтовані на обслуговування надзвичайно великої кількості підключених пристроїв — від смартфонів до мільярдів сенсорів та IoT-рішень. У таких умовах атаки типу Denial of Service (DoS) та Distributed Denial of Service (DDoS) набувають особливої небезпеки. Вони можуть порушувати роботу як окремих користувачів, так і всієї інфраструктури, оскільки мережа змушена обробляти надмірну кількість хибних запитів.

Ці атаки належать до категорії так званих малопомітних високоточних кіберзасобів (UPCW, Unintrusive Precision Cyber Weapons). Вони небезпечні тим, що потребують мінімальних витрат ресурсів для запуску, але здатні завдавати непропорційно великої шкоди. У випадку 5G атаки DoS часто спрямовані на механізми автентифікації, які є критично важливими для стабільності мережі.

Зловмисник, використовуючи підроблену базову станцію, може надсилати численні запити автентифікації до пристроїв, змушуючи їх витрачати обчислювальні ресурси на формування відповідей. Якщо таких запитів багато,

пристрій швидко виснажує акумулятор і стає недієздатним. Особливо уразливими є IoT-пристрої, які працюють від невеликих батарей і розраховані на довготривалу автономну роботу. У цьому випадку говорять про DoSL-атаки (Denial of Sleep), коли пристрій примусово утримується у «активному режимі» і не може перейти у стан енергозбереження.

З іншого боку, якщо атака спрямована на головну мережу (Core Network), величезна кількість автентифікаційних запитів призводить до перевантаження серверів обслуговуючої (SEAF) та домашньої мережі. У результаті ресурси, необхідні для обробки легітимних запитів користувачів, виснажуються, що може викликати масштабні збої у роботі всієї системи. Більш витончений сценарій полягає у зборі зловмисником великої кількості тимчасових ідентифікаторів (GUTI) або навіть зашифрованих ідентифікаторів (SUCI) та навмисному «затопленні» домашньої мережі підробленими повідомленнями. У такій ситуації мережа змушена витрачати ресурси на розшифрування та перевірку кожного запиту, що також веде до перевантаження.

Таким чином, атаки DoS і DDoS у мережах 5G є особливо небезпечними через свою здатність ефективно виснажувати як ресурси користувацьких пристроїв, так і інфраструктурні потужності мережі. У середовищі, де одночасно працюють мільярди IoT-пристроїв, навіть локалізована атака може призвести до каскадних збоїв глобального масштабу. Це підкреслює необхідність розробки адаптивних механізмів захисту, що в реальному часі виявлятимуть аномальну активність і блокуватимуть шкідливі запити, перш ніж вони зможуть завдати шкоди інфраструктурі.

Безпека хендоверу

Процес хендоверу (handover) — це ключовий механізм у мобільних мережах, який забезпечує безперервність зв’язку під час переміщення користувача між базовими станціями. У мережах п’ятого покоління (5G) хендовер набуває ще більшої ваги, оскільки він відбувається набагато частіше, ніж у 4G, з огляду на використання високочастотних діапазонів, де радіус дії соти є меншим. У перспективі мереж 6G, де використовуватимуться міліметрові та терагерцові хвилі

з надзвичайно малою зоною покриття, процес хендоверу стане ще більш критичним — пристрої можуть перемикатися між сотами десятки разів за хвилину.

Саме тому безпека хендоверу є одним із фундаментальних аспектів архітектури майбутніх мобільних систем. Вона повинна враховувати як низьку затримку для забезпечення безперервності сервісу, так і високий рівень захисту від атак у період найбільшої вразливості з'єднання.

Виклики безпеки під час хендоверу

Основні загрози виникають через те, що у момент хендоверу пристрій:

- має ослаблений або нестабільний канал зв'язку,
- активно обмінюється критично важливими службовими повідомленнями (ключами, ідентифікаторами),
- змінює точку підключення, покладаючись на довіру до нової gNB.

У результаті зловмисник може використати цей період для реалізації таких атак:

1. **Атаки повторення (Replay Attack)** — перехоплені повідомлення між базовими станціями повторюються для зриву синхронізації.
2. **Атаки глушіння (Jamming Attack)** — створення перешкод, які блокують обмін службовими даними й примушують пристрій витрачати ресурси на повторні спроби підключення.
3. **Атаки десинхронізації (De-synchronization Attack)** — підміна значення **NCC (Next Hop Chaining Counter)**, що призводить до невідповідності ключів між UE та цільовою gNB.
4. **Атаки шахрайських базових станцій (Rogue gNB)** — створення підроблених базових станцій, які видають себе за легітимні та змушують пристрої передавати конфіденційні дані.
5. **DoS/DDoS під час хендоверу** — масовані атаки, спрямовані на одночасне перевантаження великої кількості пристроїв у процесі перемикання.

Протоколи безпечного хендоверу в 5G

У 5G для мінімізації затримок використовується механізм прямої безпеки (forward security). Коли відбувається рішення про хендовер, вихідна gNB генерує

новий сесійний ключ K*gNB на основі наявного KgNB. Для цього використовується KDF (Key Derivation Function) разом із параметрами PCI (ідентифікатор соти) та ARFCN (частотний номер каналу). Цей новий ключ разом із NCC передається у цільову gNB.

Такий підхід гарантує, що компрометація поточного ключа не дозволить зловмиснику відновити попередні ключі. Однак тут є серйозне обмеження: зворотна безпека (backward security) не реалізована. Якщо зловмисник отримає доступ до ключів на вихідній gNB, він автоматично зможе передбачати майбутні ключі, а отже, скомпрометує всі подальші хендовери.

Для часткового вирішення цієї проблеми в 5G застосовується додаткова процедура автентифікації вже після того, як пристрій підключився до нової gNB. Проте цей процес залишається досить складним з точки зору обчислювальних витрат і може викликати додаткові затримки.

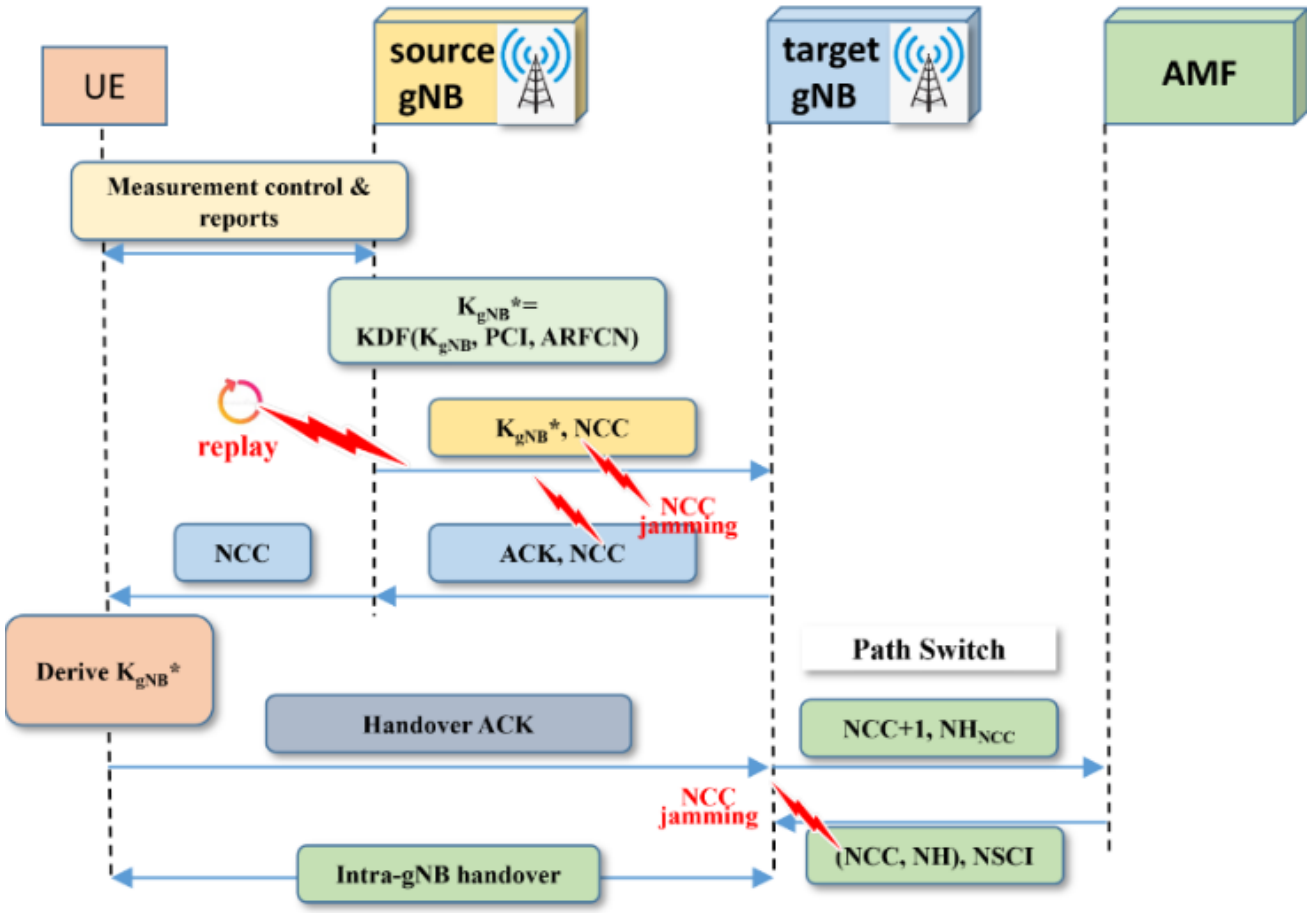


Рис. 2.4 Протокол безпеки хендовера в мережах 5G з різними вразливими точками для атак із повторенням та глушенням

Вразливості та практичні приклади атак

- **Атаки повторення.** Якщо шахрайська gNB перехоплює повідомлення з ключами (K*gNB, NCC), вона може багаторазово відправляти їх цільовій gNB. Через відсутність механізму автентифікації для цих повідомлень цільова станція приймає їх як дійсні, що призводить до збоїв хендоверу.
- **Атаки глушіння.** У дослідженнях показано, що навіть незначне збільшення рівня шуму в каналі під час хендоверу різко підвищує ймовірність зриву перемикання, оскільки UE не встигає завершити обмін службовими повідомленнями.
- **Атаки десинхронізації.** Підміна значення NCC змушує UE та gNB використовувати різні значення ключів. У результаті автентифікація не завершується, і хендовер скасовується.
- **Rogue gNB.** Подібні станції використовуються зловмисниками для отримання **IMSI/SUPI** або для навмисного перенаправлення пристроїв у небезпечні канали.

Порівняння з Wi-Fi

У корпоративних Wi-Fi мережах аналогічні проблеми виникають при перемиканні між точками доступу. Наприклад, у стандарті WPA2-Enterprise пристрій мусить проходити повторну автентифікацію на кожній точці доступу, що створює значні затримки. У WPA3 запроваджено механізми швидшого обміну ключами, проте проблема залишається актуальною. У 5G ця ситуація ще складніша, оскільки кількість перемикань набагато більша через менший розмір сот.

Перспективи для 6G

У майбутніх мережах **6G** очікується:

- **Інтеграція Zero Trust Architecture (ZTA)** — постійна перевірка довіри на кожному етапі, навіть у процесі хендоверу.
- **Адаптивне оновлення ключів** — використання короткоживучих ключів, які змінюються після кожного перемикання.

- **Застосування штучного інтелекту** — алгоритми машинного навчання для виявлення аномалій у процесі хендоверу та ідентифікації шахрайських базових станцій у режимі реального часу.
- **Забезпечення forward та backward security одночасно** — використання квантово-стійких методів криптографії, які унеможливлюють відновлення майбутніх ключів навіть у разі компрометації поточних.

Безпека хендоверу є одним із найбільш критичних аспектів розвитку мобільних мереж. Вона визначає не лише якість користувацького досвіду, а й стійкість усієї системи до атак. Затримка, викликана складними протоколами автентифікації, неприйнятна для застосувань, чутливих до часу, але спрощення процедур без захисту відкриває нові вразливості. Баланс між продуктивністю та безпекою має бути досягнутий шляхом впровадження нових підходів у 6G — від нульової довіри до постквантових алгоритмів та інтелектуальних систем моніторингу.

2.4 Безпека доступу в WiFi 6/6E

Зловмисні точки доступу

Однією з найпоширеніших і водночас найбільш небезпечних атак на безпеку доступу у Wi-Fi мережах є використання шахрайських точок доступу, відомих як «злий близнюк» (evil twin). Суть атаки полягає в тому, що зловмисник створює фальшиву точку доступу, яка імітує справжню, змушуючи користувачів підключатися саме до неї. Основна вразливість полягає в тому, що маячкові пакети (beacon packets), які поширюють інформацію про мережу, не шифруються. Це дозволяє легко перехопити базові параметри мережі, такі як SSID (ідентифікатор мережі) та BSSID (MAC-адреса точки доступу). Отримавши ці дані, зловмисник може налаштувати власний пристрій так, щоб він виглядав як легітимна точка доступу (LAP, legitimate access point) та почати «переманювати» клієнтів.

Зазвичай для того, щоб користувацькі пристрої підключалися до злого близнюка, шахрайська точка доступу передає сигнал вищої потужності. Якщо ж

пристрій уже з’єднаний із легітимним Wi-Fi AP, зловмисник може скористатися атакою деаутентифікації (de-authentication attack). Така атака змушує пристрій втратити підключення до справжньої мережі, після чого користувач автоматично підключається до фальшивої точки доступу, не підозрюючи про підміну.

Уразливості та методи виявлення

Найбільша загроза від атаки «evil twin» полягає в можливості реалізації сценарію «людина посередині» (MitM, man-in-the-middle). Зловмисник не лише контролює канал передачі даних, а й може маніпулювати трафіком — змінювати, блокувати або підміняти інформацію. Це відкриває шлях до крадіжки облікових даних, перехоплення сесій чи навіть впровадження шкідливого ПЗ у пристрої користувачів.

Водночас сучасні системи безпеки намагаються протидіяти таким загрозам. Існують механізми перевірки дублюючих з’єднань клієнта з кількома точками доступу, коли легітимна та шахрайська точки намагаються взаємодіяти з одним клієнтом на одному каналі. У такому разі політики безпеки можуть заборонити підключення до тієї точки доступу, яка не підтримує взаємну автентифікацію. Проте варто наголосити, що такі механізми залежать від конкретної реалізації мережевого обладнання і не гарантують повного захисту на криптографічному рівні.

Атака блокування сервісу

Окрім MitM, атака «злий близнюк» може бути використана для блокування сервісу (service blocking attack), яке фактично є варіантом DoS-атаки. У цьому випадку шахрайська точка доступу не прагне створити канал для подальшого контролю трафіку. Натомість вона втручається у процес автентифікації протоколу WPA2, порушуючи процедуру встановлення з’єднання та унеможливлюючи підключення клієнта до легітимної мережі.

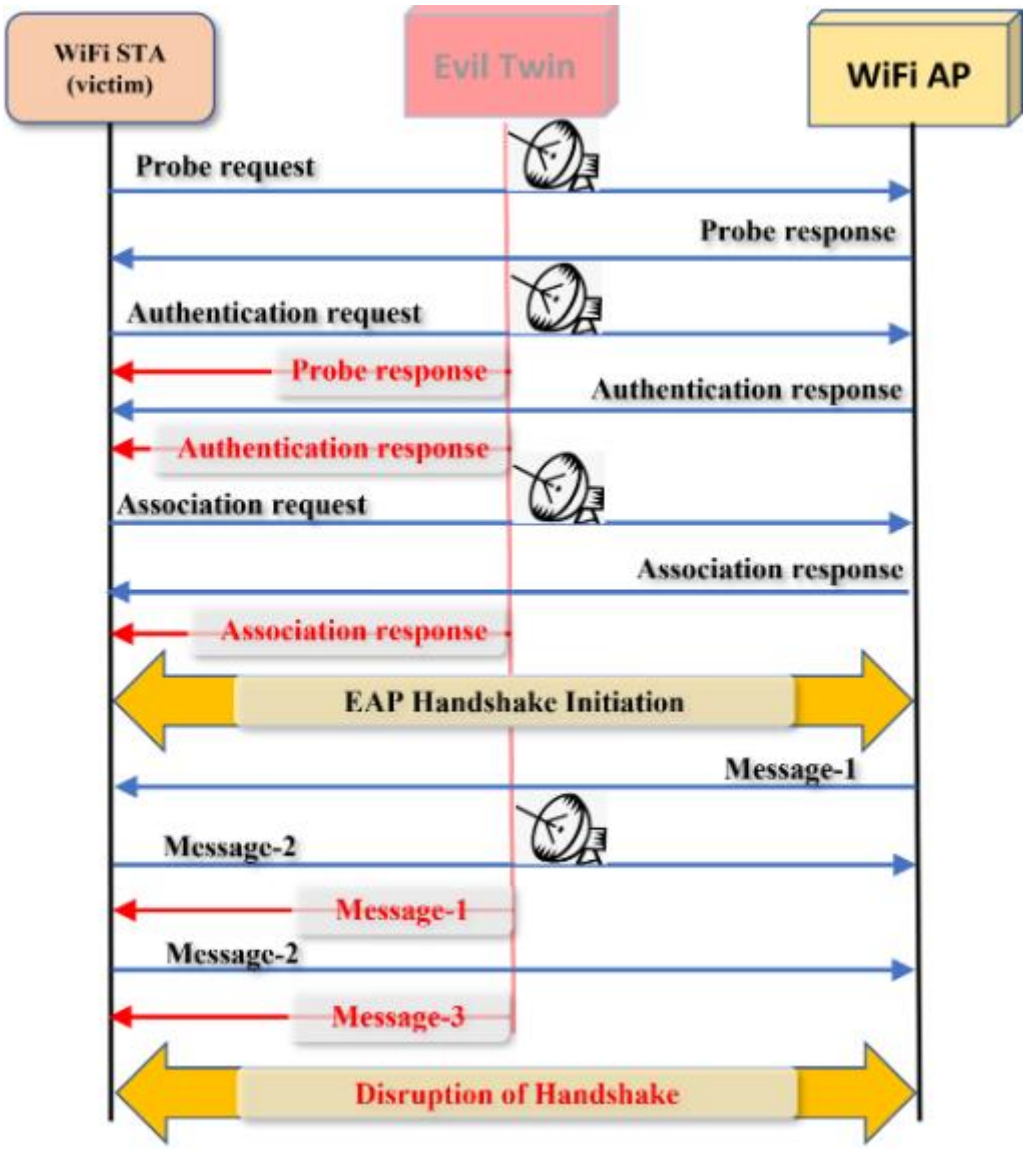


Рис. 2.5 Схема атаки «Блокування сервісу» за допомогою злого близнюка під час автентифікаційного рукостискання EAP у WPA2 Wi-Fi

Як показано на рисунку, пристрій користувача (Wi-Fi STA) надсилає probe-запити та запити автентифікації до легітимної точки доступу (AP) для ініціалізації підключення. Легальна точка доступу відповідає на кожен запит. Проте в цей процес втручається «злий близнюк», який так само надсилає відповіді на ті ж запити. У результаті клієнт одночасно отримує відповіді і від легітимної точки доступу, і від шахрайської. Коли починається процедура 4-стороннього рукостискання EAP, клієнт відправляє повідомлення-2 у відповідь на перше отримане повідомлення-1. Але як тільки приходить повторне повідомлення-1 з іншої точки доступу, протокол завершується помилкою. У підсумку легітимне

підключення не встановлюється, і користувач фактично позбавляється доступу до мережі.

Порівняння з мобільними мережами

Цікаво відзначити, що атака «evil twin» у Wi-Fi має багато спільного з атаками у стільникових мережах, де використовуються шахрайські базові станції (rogue gNB у 5G). У обох випадках противник створює фальшивий вузол мережі, який видає себе за легітимний, примушуючи клієнтські пристрої підключатися до нього. У Wi-Fi атака зручна через нешифрованість службових пакетів (SSID, BSSID), а у 5G — через можливість експлуатувати вразливості в процедурах автентифікації під час хендоверу. В обох сценаріях результат однаковий: користувачі втрачають контроль над своїми даними, а зловмисники отримують можливість перехоплювати чи змінювати трафік.

Перспективи захисту

Для протидії таким загрозам у Wi-Fi 6 і Wi-Fi 7 впроваджуються нові механізми безпеки, серед яких:

- **більш стійкі процедури автентифікації (SAE, Simultaneous Authentication of Equals)**,
- **захист службових пакетів** для унеможливлення збору SSID/BSSID,
- **системи моніторингу спектра**, які дозволяють швидко виявляти аномальні точки доступу.

У корпоративних мережах все частіше застосовуються спеціалізовані рішення з виявлення «evil twin», які аналізують усі точки доступу у зоні дії та визначають їхню легітимність.

Атаки на перевстановлення ключа (Key Reinstallation Attacks, KRACK)

У сучасних системах безпеки Wi-Fi, зокрема у WPA та WPA2, механізм взаємної автентифікації між клієнтським пристроєм (STA) та точкою доступу (AP) базується на використанні попередньо згенерованого попарного майстер-ключа (PMK, Pairwise Master Key). На основі цього ключа формуються тимчасові попарні ключі (PTK, Pairwise Transient Key), які використовуються безпосередньо для шифрування сесійних даних. Процес формування PTK здійснюється із залученням

випадкових чисел SNonce (з боку точки доступу) та ANonce (з боку клієнта). Саме цей механізм реалізується у добре відомому 4-сторонньому рукостисканні EAP.

Атака на перевстановлення ключа (Key Reinstallation Attack, KRACK) ґрунтується на слабкостях цього процесу. Її суть полягає у повторному відтворенні третього повідомлення рукостискання, що призводить до скидання внутрішніх лічильників повторів і таймерів. Як наслідок, вже встановлений PTK може бути перевстановлений для наступних сеансів комунікації. У результаті зловмисник отримує можливість реалізувати атаки на відтворення (replay attacks), розшифровувати трафік та навіть здійснювати підміну повідомлень.

Для успішної реалізації атаки KRACK зловмисник мусить зайняти позицію «людина посередині» (Man-in-the-Middle, MitM). Це дозволяє блокувати або затримувати четверте повідомлення рукостискання, яке завершує процес автентифікації, та примушувати точку доступу повторно надсилати повідомлення-3. У той момент, коли жертва отримує повторне повідомлення, її пристрій знову перевстановлює вже використаний PTK, що є критичною помилкою в архітектурі WPA2.

Вразливості та приклади експлуатації

Попри те, що різні постачальники програмного забезпечення реалізували власні засоби для виявлення та запобігання повторному надсиланню повідомлення-3, багато апаратних платформ залишаються вразливими. Причина полягає у складній взаємодії між програмними компонентами (ЦП), які реалізують протокол рукостискання, та апаратними модулями (NIC, контролер мережевого інтерфейсу), які відповідають за конфіденційність даних. У таких системах виникає стан гонки (race condition), коли різні компоненти обробляють повідомлення асинхронно, що створює вікно для атаки.

Прикладом є операційні системи OpenBSD, OS X та macOS, де для додаткового захисту передбачено шифрування повідомлення-3. Однак навіть у таких випадках вразливості залишаються: під час оновлення ключа зловмисник може перехопити та одночасно передати клієнту кілька варіантів повідомлення-3, використовуючи старий PTK. У результаті одноразове значення (nonce), що має

збільшуватись для унікальності кожної сесії, перезапускається з 1. Це відкриває можливості для атак відтворення та повторного використання ключів.

Наслідки атак KRACK

Дослідження, проведені у 2017 році, показали, що атаки на перевстановлення ключа торкнулися практично всіх пристроїв з підтримкою WPA2 — від смартфонів і ноутбуків до IoT-сенсорів та маршрутизаторів. Зловмисники змогли не лише відновлювати частину переданого трафіку у відкритому вигляді, а й інжектувати шкідливий код у незахищені HTTP-з'єднання. Таким чином, атака KRACK є універсальною: вона дозволяє перехоплювати паролі, повідомлення у месенджерах, дані про місцезнаходження та іншу конфіденційну інформацію.

Особливо небезпечними такі атаки є для IoT-пристроїв, які часто працюють із мінімальними механізмами захисту та рідко отримують оновлення прошивки. Це робить їх «слабкою ланкою» в інфраструктурі безпеки безпроводових мереж.

Заходи протидії

Основними методами захисту від атак на перевстановлення ключа є:

- **оновлення прошивки та ОС**, що включає патчі для коректної обробки повідомлень рукостискання;
- використання більш сучасних протоколів безпеки, таких як **WPA3**, де реалізовано **Simultaneous Authentication of Equals (SAE)**, що виключає можливість повторного використання ключа;
- **моніторинг аномалій у мережевому трафіку**, здатний виявляти повтори службових повідомлень;
- застосування додаткового рівня захисту даних (наприклад, VPN або TLS), що дозволяє мінімізувати наслідки навіть у випадку компрометації WPA2.

Перспективи досліджень

Попри розроблені заходи, атаки на перевстановлення ключа залишаються актуальними, адже значна кількість старих пристроїв і далі експлуатує WPA2 без оновлень. У контексті розвитку 6G та Wi-Fi 7 дослідники наголошують на необхідності розробки криптографічних гарантій на рівні фізичного та канального

рівнів, щоб виключити повторне використання ключів навіть у випадку помилок реалізації.

Таким чином, атаки KRACK продемонстрували, що навіть добре перевірені стандарти безпеки можуть містити критичні вразливості, які стають очевидними лише після багаторічного використання. Вони показали важливість комплексного підходу до безпеки, де оновлення програмного забезпечення, модернізація протоколів та багаторівневий захист мають однакове значення.

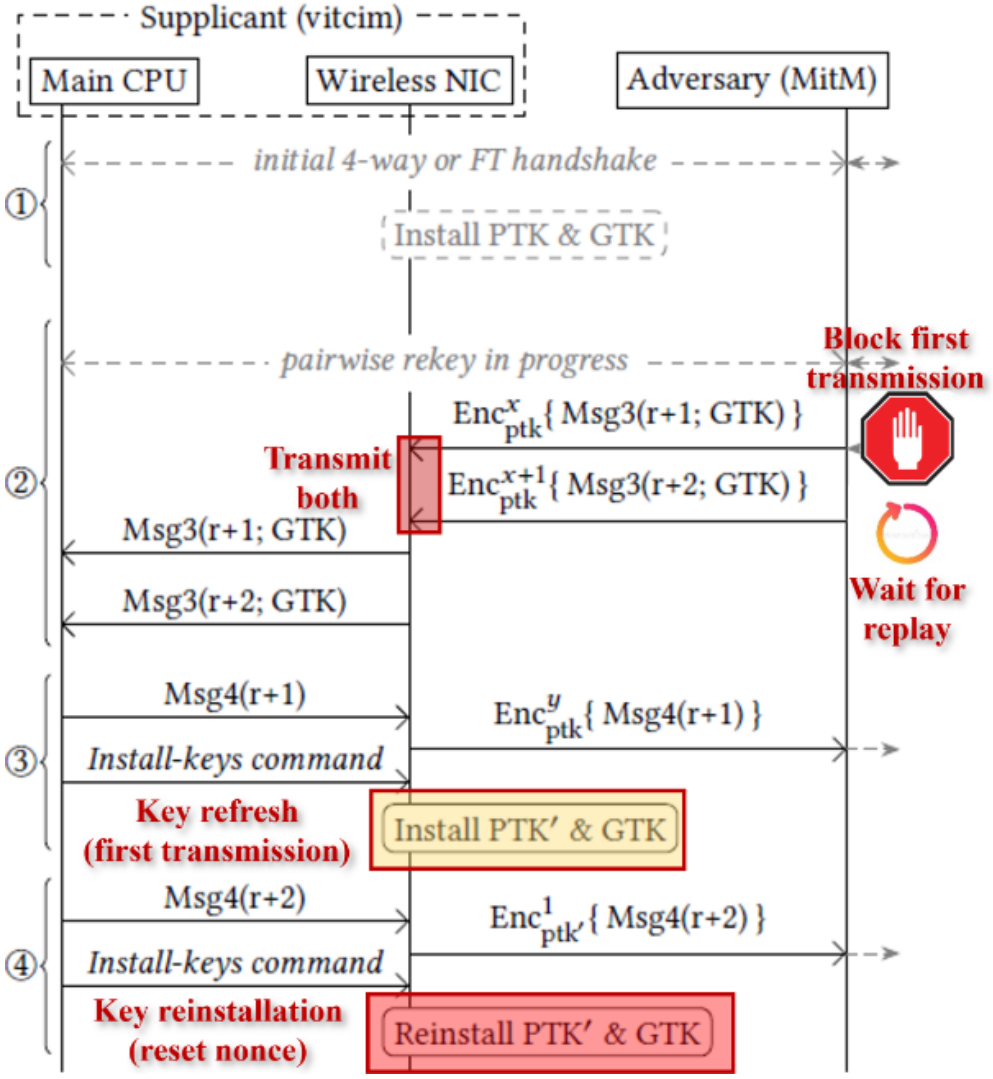


Рис. 2.6 Атака на перевстановлення ключа з використанням MitM на автентифікаційному рукостисканні, заснованому на EAP, у WPA2 WiFi

Атаки DoS у контексті WPA3

Поява стандарту WPA3 стала відповіддю альянсу Wi-Fi на серйозні уразливості, виявлені у WPA2, зокрема на атаки на перевстановлення ключів (KRACK). Основою WPA3 є протокол рукостискання Dragonfly, який працює на

базі алгоритму SAE (Simultaneous Authentication of Equals). Його перевага полягає у тому, що він забезпечує стійкість до атак перебором та гарантує значно вищий рівень конфіденційності під час автентифікації. Однак, як показує практика, навіть нові механізми безпеки створюють умови для появи нових векторів атак.

У перехідний період було запроваджено режим сумісності WPA3/WPA2, який дозволяє користувацьким пристроям взаємодіяти з точками доступу, що ще не підтримують новий стандарт. Цей компроміс, необхідний для плавної міграції, одночасно відкрив простір для нових атак.

Головна проблема протоколу Dragonfly — його високі обчислювальні витрати, що пов’язано з особливостями математичних операцій над еліптичними кривими (ECC) або групами скінченних полів (FFC). Протокол використовує метод try-and-increment, який перетворює хеш пароля на допустиму точку еліптичної кривої. Цей процес, хоча й підвищує захист від атак по часових характеристиках (timing attacks), вимагає виконання значно більшої кількості ітерацій.

Зловмисник може скористатися цим, організувавши DoS-атаку (Denial of Service). У цьому випадку метою є не злам шифрування, а навмисне перевантаження ресурсів точки доступу, яка змушена витрачати обчислювальну потужність на обробку великої кількості фіктивних запитів.

Для протидії було впроваджено так званий anti-clogging mechanism — механізм протидії перевантаженню, який має обмежувати кількість одночасних запитів. Проте дослідження показали, що він не забезпечує повного захисту. Експеримент з використанням Raspberry Pi B+ (процесор 700 МГц) у ролі атакуючого продемонстрував, що навіть малопотужний пристрій може ефективно перевантажити професійну точку доступу з процесором 1200 МГц. Усього 8 запитів на секунду за протоколом Dragonfly призвели до 100% завантаження процесора точки доступу, фактично вивівши її з робочого стану. Це свідчить, що WPA3 у стані COTS (commercial off-the-shelf) ще не досяг повної стійкості до практичних DoS-атак.

Атаки на пониження версії (Downgrade Attacks)

Ще одним серйозним викликом є атаки на пониження версії, які виникли саме через перехідний режим WPA3/WPA2. Обидва стандарти можуть використовувати однаковий пароль, що дозволяє зловмиснику змусити клієнт підключитися через менш захищений протокол.

Найтиповіший сценарій: противник підробляє маячкові повідомлення (beacon messages) та змушує станцію Wi-Fi ідентифікувати мережу як WPA2, навіть якщо вона підтримує WPA3. У такому випадку відкривається можливість використати уразливості WPA2 для відновлення пароля через offline dictionary attack.

Для запобігання подібним атакам у WPA2 передбачено RSNE (Robust Security Network Element), у якому зберігається список усіх підтримуваних протоколів. Це дозволяє клієнту перевіряти легітимність повідомлень і виявляти підроблені маяки. Однак у практичних умовах цей захист часто обходиться. Наприклад, якщо в мережі одночасно працюють точки доступу лише з WPA2, то пристрій користувача все одно обиратиме менш захищене з'єднання.

Окрім цього, існує поглиблений тип downgrade-атак, пов'язаний із вибором груп еліптичних кривих або мультиплікативних груп у протоколі SAE. Пріоритетність груп задається користувачем або адміністратором, і під час узгодження клієнт і точка доступу повинні домовитися про вибір однієї з них. Зловмисник, перебуваючи у позиції MitM, може блокувати частину повідомлень і примушувати обирати найслабшу групу, яка є вразливою до атак по сторонніх каналах — таких, як timing-атаки або кеш-атаки.

Цей тип атак особливо небезпечний, оскільки навіть при використанні WPA3 користувач може несвідомо опинитися в ситуації, коли його з'єднання шифрується за допомогою криптографії з низькою стійкістю.

Паралелі з мобільними мережами

Цікаво, що атаки DoS і downgrade мають свої аналоги у мобільних мережах 4G/5G:

- у 5G існують **атаки на механізми автентифікації під час хендоверу**, коли противник навмисно створює затримки або підробляє службові повідомлення, змушуючи UE використовувати менш захищений алгоритм;
- можливі атаки на **примусове переключення UE на LTE (downgrade з 5G на 4G)**, що відкриває доступ до вразливих алгоритмів шифрування LTE;
- аналог DoS у 5G — це атаки на перевантаження елементів **SEAF** чи **AMF**, коли зловмисник створює тисячі хибних автентифікаційних запитів, блокуючи обслуговування легітимних користувачів.

Таким чином, проблема атак DoS і downgrade є універсальною для всіх типів безпроводових технологій. Вона демонструє, що баланс між продуктивністю та безпекою є головним викликом у розробці сучасних протоколів.

3 БЕЗПЕКОВІ РИЗИКИ СПІВІСНУВАННЯ ТА РОЗПОДІЛУ НЕЛІЦЕНЗОВАНОГО СПЕКТРА

3.1 Спільне використання спектру

Зростання кількості безпроводових пристроїв, розвиток 5G/6G, інтернету речей (IoT/IoE), систем розумних міст та безпілотного транспорту призводить до стрімкого зростання потреб у спектральних ресурсах. Ліцензовані діапазони радіочастотних спектрів стають дедалі більш перевантаженими, тому активно розвивається підхід спільного використання спектра (spectrum sharing) у середовищах співіснування мереж (coexistence environments). Цей підхід передбачає, що декілька незалежних систем можуть паралельно функціонувати в одному й тому ж діапазоні частот, розподіляючи ресурси між собою.

Попри очевидну ефективність і гнучкість такого підходу, він відкриває принципово нові виклики у сфері безпеки. На відміну від автономних мереж, де захист забезпечується внутрішніми автентифікаційними та авторизаційними механізмами, у середовищі спільного використання спектра ці механізми активуються лише після отримання доступу до спектра. Це означає, що етап первинного доступу лишається фактично незахищеним і створює передумови для широкого спектра атак.

Уразливості традиційних моделей

В автономних мережах вважається, що кожен користувач або пристрій, який отримує доступ до спектра, уже є легітимним і перевіреним. У середовищі співіснування це припущення втрачає актуальність, оскільки у процес доступу одночасно включаються кілька незалежних систем, які можуть мати власні політики безпеки або взагалі їх не мати. Таким чином, зловмисник може брати участь у конкуренції за спектр нарівні з легітимними користувачами, не будучи виявленим.

Ця концептуальна вразливість схематично зображена на рисунку.

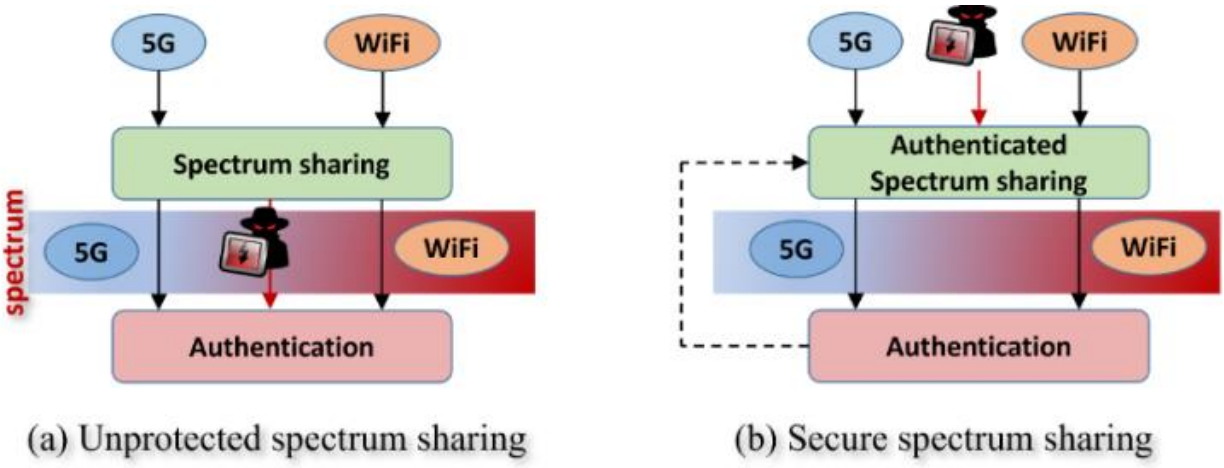


Рис. 3.1 Порівняння (a) незахищеного та (b) захищеного спільного використання спектра з точки зору дозволу зловмиснику отримувати доступ до спектру (захоплювати спектр)

Потенційні вектори атак у середовищах співіснування

1. **Jamming-атаки (глушіння сигналу).**

   Зловмисник може навмисно генерувати перешкоди, створюючи завади у виділеному діапазоні, що змушує легітимних користувачів залишати канал. У багатокористувацьких середовищах це може призвести до зупинки сервісів, критичних для інфраструктури (наприклад, систем «розумного міста» чи транспорту).

2. **Атаки типу spoofing (підміна).**

   Використовуючи слабкість систем ідентифікації, зловмисник може підміняти ідентифікаційні дані пристрою або базової станції, маскуючись під легітимного користувача. Це дозволяє йому отримувати доступ до ресурсу та перехоплювати або модифікувати передані дані.

3. **DDoS-атаки на рівні спектра.**

   Контрольована ботнетом група IoT-пристроїв може одночасно надсилати велику кількість запитів на доступ до спектра, перевантажуючи механізми координації. Це призводить до деградації QoE або навіть до повної відмови у доступі для легітимних абонентів.

4. **Атаки на справедливість розподілу.**

У системах з механізмами доступу типу **listen-before-talk** зловмисник може маніпулювати таймінгами, щоб отримати більшу частку спектра, витісняючи інших користувачів. У результаті це призводить до нерівномірного розподілу ресурсу та порушення принципів чесного доступу.

5. **Атаки на QoE.**

   Оскільки більшість поточних систем спільного використання спектра зосереджені на показниках якості досвіду користувача, зловмисники можуть спрямовано атакувати саме ці метрики, створюючи ситуації, коли користувач відчуває затримки, втрати пакетів чи зниження швидкості, навіть якщо основна мережа формально функціонує.

Обмеженість існуючих рішень

Нині більшість рішень у сфері спільного використання спектра орієнтовані на оптимізацію продуктивності та QoE, залишаючи питання безпеки на рівні вищих протоколів. Такий підхід є проблемним, адже зловмисник може атакувати саме рівень доступу, залишаючись невидимим для системи безпеки, що активується вже після виділення ресурсу.

Наприклад, у сценарії з незахищеним доступом до спектра (рисунок 6а) зловмисник може легально конкурувати за частину ресурсу поряд із легітимними користувачами. Це створює нову площину атак, яка відсутня в автономних мережах, де контроль за автентифікацією виконується одразу.

Напрямки удосконалення систем безпеки

Для того щоб мінімізувати ризики, пов’язані з використанням спільного спектра, необхідно розробити нові механізми захисту, інтегровані безпосередньо на рівні доступу. Серед перспективних напрямків:

- впровадження **систем виявлення вторгнень на рівні спектра (spectrum-level IDS)**;
- використання **криптографічних протоколів первинної ідентифікації**, які дозволяють підтвердити легітимність сутності ще до отримання доступу;
- застосування **колективних механізмів автентифікації** у багатокористувацьких середовищах;

- використання **штучного інтелекту та машинного навчання** для аналізу шаблонів використання спектра, виявлення аномалій та прогнозування потенційних атак;
- розробка **багаторівневої моделі безпеки**, де захист реалізується одночасно на фізичному, канальному, мережевому та прикладному рівнях.

Паралелі з мобільними мережами

Аналогічні проблеми виникають у мобільних мережах п’ятого та майбутнього шостого покоління. Тут також існує потреба у механізмах спільного використання спектра між операторами, супутниковими системами та локальними мережами. Досвід уже показує, що без додаткових засобів захисту такі середовища стають уразливими до атак на автентифікацію, цілісність даних і навіть на фізичний рівень сигналу.

3.2 Безпека в системах спільного використання спектру

Стрімкий розвиток мобільних технологій і вибухове зростання кількості безпроводових пристроїв призводять до того, що проблема дефіциту спектра стає однією з найгостріших для систем зв’язку нового покоління. Одним із можливих шляхів її вирішення є співіснування мереж різних стандартів у неліцензованих діапазонах спектра, зокрема систем 5G та WiFi. Такий підхід дозволяє підвищити ефективність використання обмежених частотних ресурсів, збільшити загальну пропускну здатність та забезпечити гнучкіший розподіл навантаження між різними типами мереж.

Проте попри очевидні переваги, питання безпеки у середовищах співіснування залишається недостатньо дослідженим. Якщо продуктивність, пропускна здатність і якість користувацького досвіду (QoE) активно вивчаються у контексті сумісної роботи 5G і WiFi, то безпекові ризики здебільшого розглядаються як другорядні. Це створює потенційні загрози, адже механізми спільного доступу до спектра суттєво відрізняються від класичних моделей і відкривають нові площини для атак.

Асиметричний і симетричний доступ: принципові відмінності

У традиційних системах спільного використання спектра (spectrum sharing, SS) реалізується асиметричний доступ, відомий як двоступеневий механізм. У ньому виділяються два класи користувачів:

- **первинні користувачі (PU, primary users)** – ті, хто має пріоритетний доступ до спектра,
- **вторинні користувачі (SU, secondary users)** – отримують можливість працювати лише у разі відсутності активності первинних користувачів.

Такий підхід дозволяє повторно використовувати спектр у часових слотах або географічних зонах без активності PU. Водночас він не створює справжнього механізму одночасного симетричного доступу між кількома незалежними мережами.

На відміну від цього, мережі співіснування (coexistence networks) реалізують симетричний доступ. Це означає, що різні системи (наприклад, 5G і WiFi) мають рівні права на використання ресурсу у спільному середовищі, де діють механізми справедливого розподілу у часовій та частотній областях. Такий підхід знижує ймовірність перебоїв у роботі й дозволяє підвищити середню пропускну здатність системи.

Однак проблема полягає в тому, що механізми безпеки у середовищах співіснування майже повністю копіюють традиційні рішення SS. Відповідно, всі відомі вразливості SS-систем автоматично стають актуальними і для мереж співіснування.

Відомі атаки у традиційних SS-системах

Однією з найбільш вивчених є атака емуляції первинного користувача (PUE, primary user emulation). У цьому випадку зловмисник імітує сигнали PU, змушуючи SU утримуватися від доступу до спектра. Для первинної мережі існують механізми розпізнавання таких атак, але SU зазвичай не мають засобів перевірки автентичності сигналів. Це робить PUE ефективним інструментом для DoS-атак на динамічний доступ до спектра (DSA).

Ускладнений варіант такої атаки — Spectral Honeypot, коли зловмисник навмисно блокує більшість каналів і залишає SU можливість підключатися лише до конкретного «цільового» каналу. Це створює умови для MitM-атаки або контрольованого створення завад, що знижують продуктивність мережі.

Інша проблема полягає у створенні SU небажаних перешкод для PU. Якщо SU не здатний виявити сигналів PU (наприклад, через багатопроменеві затухання), він починає передачу, що може серйозно зашкодити роботі первинної системи. Одним із можливих рішень є використання централізованих систем доступу до спектра (Spectrum Access System, SAS). У цьому випадку всі SU передають дані своїх спектральних сенсорів у SAS, яка вирішує, чи дозволяти доступ. Проте така модель є вразливою до атак на фальсифікацію даних сенсорів (SSDF, spectrum sensing data falsification), коли зловмисник видає себе за SU і надсилає у SAS неправдиві результати.

Ризики конфіденційності та прослуховування

Неминучим наслідком спільного використання спектра є підвищений ризик перехоплення трафіка та втрати конфіденційності. Сигнали мереж повинні бути доступними для виявлення, що дозволяє стороннім учасникам аналізувати їхню активність. Це становить небезпеку витоку даних про місцезнаходження користувачів і навіть їхню мережеву поведінку.

Дослідження в цій сфері пропонують застосування методів теорії ігор для захисту інформації про місцезнаходження PU та SU. Додатково використовуються рішення на основі MIMO та beamforming, які дозволяють створювати канали з підвищеною секретністю. Ще один перспективний напрямок — використання штучного шуму, який передається у невикористані ділянки каналу для ускладнення роботи перехоплювачів. Однак усі ці методи вимагають точного знання інформації про стан каналу (CSI), яка сама може стати об’єктом атак.

3.3 Захват спектру та погіршення якості обслуговування

Однією з найбільш небезпечних уразливостей у середовищах співіснування є атака на захоплення спектра, яка виникає через те, що процес спільного доступу до частотних ресурсів починається ще до активації механізмів безпеки, притаманних автономним мережам. Це створює можливість для зловмисника замаскуватися під легітимну мережеву сутність (наприклад, базову станцію або користувацький пристрій), використовуючи спектр у відкритому режимі та залишаючись невиявленим. На відміну від автономних мереж із жорсткою централізованою автентифікацією, у спільному середовищі подібні атаки неможливо відразу заблокувати.

Вплив на якість обслуговування та громадську безпеку

Подібні атаки мають подвійний негативний ефект. По-перше, вони суттєво знижують QoE (якість користувацького досвіду). Це особливо критично, адже ключовою перевагою мереж співіснування вважається саме здатність підтримувати високий рівень QoE навіть за умов підвищеної конкуренції за спектральні ресурси. Втрата стабільності з’єднання, підвищені затримки чи деградація пропускної здатності фактично нівелюють переваги архітектури співіснування.

По-друге, атаки на захоплення спектра створюють пряму загрозу громадській безпеці та критично важливим комунікаціям. Мережі 5G і WiFi 6/6E розглядаються як базова інфраструктура для:

- безпілотного транспорту (автомобілів, дронів, вантажних систем),
- систем «розумного міста» та критичної інфраструктури (енергомереж, водопостачання, транспортних вузлів),
- служб екстреного реагування (швидка допомога, пожежна служба, поліція),
- систем відеоспостереження та аналітики безпеки.

У більшості цих застосувань затримка навіть у кілька секунд може мати катастрофічні наслідки. Наприклад, у випадку безпілотного автомобіля, що рухається на високій швидкості, затримка сигналу від сенсорів чи втручання у канал управління може призвести до аварії. У системах відеоспостереження це

може спричинити втрату критичних кадрів у режимі реального часу, а у службах екстреної допомоги — затримку у передачі координат чи медичних даних. Таким чином, навіть примітивна атака на захоплення спектра може стати причиною масштабних перебоїв, що матимуть як економічні, так і соціальні наслідки.

Причини вразливості та складність захисту

Додатковою проблемою є те, що в умовах співіснування мережі мають незалежні механізми безпеки, що розроблені для роботи в автономному режимі. У той час як кожна мережа окремо забезпечує автентифікацію та шифрування, у спільному середовищі вони не обмінюються інформацією про легітимність користувачів. Це означає, що зловмисник може поводитися як «законний» учасник процесу розподілу спектра і при цьому не бути виявленим.

Окремим бар'єром виступають вимоги до конфіденційності в автономних мережах. Для захисту приватності користувачів сучасні стандарти передбачають приховування ідентифікаторів та мінімізацію обміну особистими даними між мережами. Хоча це важливо з точки зору користувацької приватності, воно одночасно ускладнює реалізацію колективних міжмережевих механізмів захисту, необхідних у середовищах співіснування.

Можливі підходи до захисту

Одним із запропонованих рішень є використання довіреної третьої сторони, яка надає сервіс автентифікації для різних мереж (наприклад, 5G та WiFi 6/6E). У такій схемі кожна мережа може отримувати токени доступу від незалежного безпечного провайдера та використовувати їх для підтвердження легітимності учасників. Це забезпечує базовий рівень міжмережевої довіри.

Однак практична реалізація подібної моделі має низку суттєвих труднощів:

- необхідність кардинальної перебудови архітектури безпеки,
- підвищене навантаження на інфраструктуру та додаткові затримки,
- потенційний конфлікт з існуючими політиками захисту приватності, які обмежують обмін ідентифікаційними даними між мережами.

Через це сьогодні атаки на захоплення спектра залишаються одним із найсерйозніших викликів для середовищ співіснування, а їхнє вивчення і створення

спеціалізованих засобів захисту є одним із ключових напрямів розвитку кібербезпеки для 5G/6G.

Використання вразливості прихованого вузла в мережах співіснування

Одним із серйозних викликів у середовищах співіснування є можливість зловмисника використати незахищеність механізмів спільного доступу до спектра для навмисного погіршення роботи мереж. У таких випадках атака може проявлятися у вигляді штучного створення перешкод, що призводять до значного погіршення якості обслуговування (QoS). Наслідки таких атак зазвичай виражаються у збільшенні часу затримки, зменшенні пропускної здатності каналів, зростанні ймовірності колізій пакетів, а також у підвищенні рівня енергоспоживання пристроїв через повторні передачі.

Щоб зрозуміти механізм подібних атак, необхідно розглянути базовий принцип функціонування спільного використання спектра (SS) у середовищах співіснування мереж 5G і WiFi 6/6E. Як показано на рисунку 7, усі безпроводові пристрої застосовують протоколи на основі LBT (Listen Before Talk), які передбачають «прослуховування» каналу перед передаванням даних. Це дозволяє системам WiFi та LTE спільно використовувати неліцензовані частотні діапазони, зберігаючи при цьому коректну роботу кожної системи.

У технології WiFi 6 реалізовані два режими доступу до спектра:

- **однокористувацький (SU)** – кожна станція WiFi (STA) індивідуально змагається за доступ до вільного каналу;
- **багатокористувацький (MU)** – роль координатора бере на себе точка доступу WiFi або базова станція gNB у мережі 5G. Після отримання спектра вони розподіляють ресурси між абонентами у вигляді блоків **OFDMA**. MU-режим є близьким за принципом до висхідної лінії зв’язку (uplink) у мережах 5G.

Проблема прихованого вузла

Однією з найбільш небезпечних вразливостей у таких системах є проблема прихованого вузла. Вона виникає тоді, коли одна базова станція або точка доступу не може виявити сигнали іншої через обмеження дальності або багатопроменеві

ефекти. У такому випадку обидві мережі можуть призначити своїх користувачів на один і той самий ресурс OFDMA, що призведе до накладання сигналів і колізій.

У класичних автономних мережах цю проблему вдається мінімізувати за допомогою MAC-протоколів, однак у середовищах співіснування це завдання стає набагато складнішим. Причина полягає в тому, що кожна мережа використовує власний протокол MAC, і відсутній механізм обміну службовою інформацією між різними системами. У результаті приховані вузли з'являються значно частіше, створюючи додатковий простір для атак.

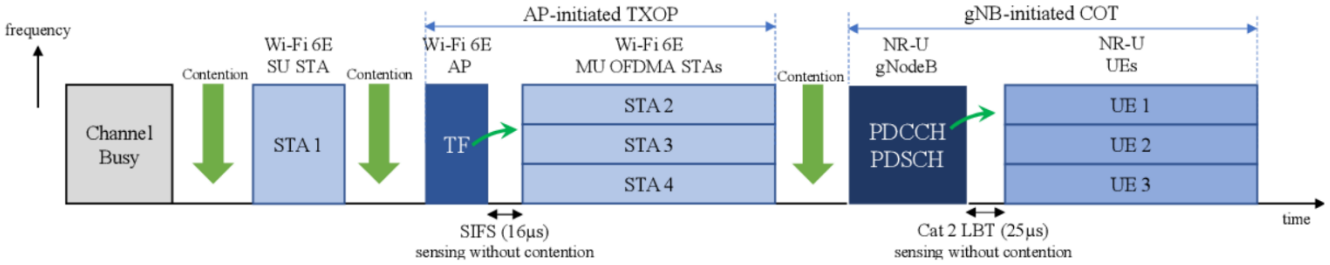


Рис. 3.2 Доступ до спектру, що базується на LBT-протоколах для співіснування 5G та WiFi 6/6E

Атаки на основі прихованих вузлів

Зловмисники можуть свідомо експлуатувати проблему прихованого вузла для погіршення QoS у мережах співіснування. Навіть у тих випадках, коли реальних прихованих вузлів немає, атакувальник може підробляти пакети керуючих каналів (наприклад, від імені точки доступу або gNB). Це змушує легітимні мережі призначати своїх користувачів на однакові канали OFDMA.

У результаті виникають такі наслідки:

1. **Зростання затримки** – абоненти обох мереж змушені чекати, поки канал звільниться, що суттєво погіршує продуктивність.
2. **Колізії пакетів** – ймовірність одночасних передач від різних систем збільшується, що призводить до втрати даних і необхідності повторних передач.
3. **Підвищене енергоспоживання пристроїв** – через часті повтори передавання ресурс акумулятора у мобільних і IoT-пристроїв витрачається значно швидше.

4. **Розширення зони впливу атаки** – у великих середовищах, де затримка поширення сигналів вища, проблема прихованого вузла проявляється гостріше, що дозволяє атакувальнику впливати на більшу кількість користувачів.

Наслідки для критичних систем

Такі атаки можуть мати особливо негативний ефект у сценаріях, що потребують низької затримки та стабільного з’єднання:

- у системах керування безпілотним транспортом;
- у телеметрії «розумних міст»;
- у промислових безпроводових мережах (IIoT);
- у службах екстреного реагування.

Затримка навіть на кілька сотень мілісекунд може призвести до зриву виконання критично важливих операцій, а втрата пакетів – до повної відмови системи у режимі реального часу.

3.4 Pseudo MitM та фізичний шар безпеки

Більшість сучасних атак на системи безпеки доступу в безпроводових мережах, як уже зазначалося у попередніх розділах, або безпосередньо реалізуються, або значно спрощуються за рахунок використання атаки типу «Людина посередині» (Man-in-the-Middle, MitM). До найбільш характерних прикладів належать атаки на переустановку ключа та пониження версії в протоколах WPA2/WPA3 для WiFi.

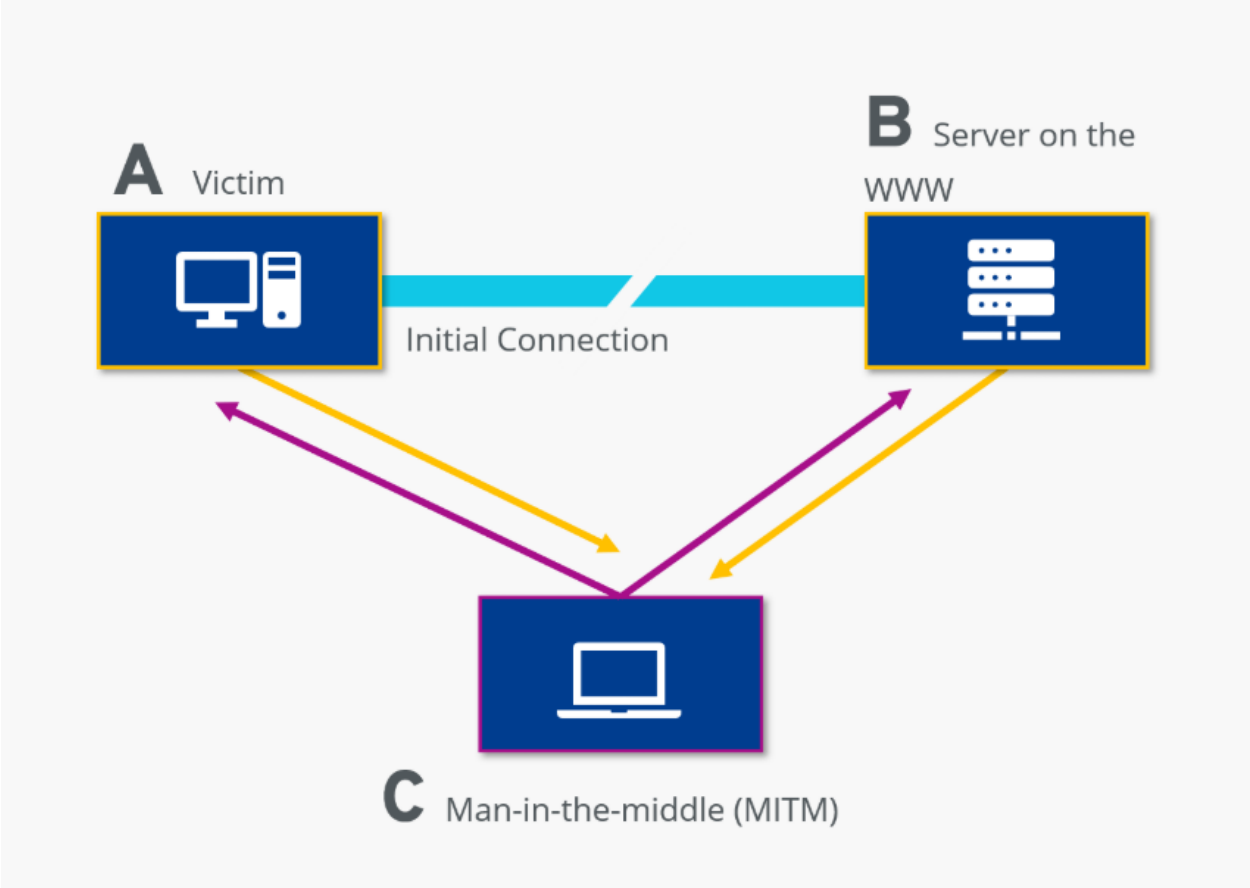


Рис. 3.3 «Людина посередині» (MitM): зловмисник перехоплює комунікацію між користувачем та сервером

У подібних сценаріях зловмисник вибірково блокує, затримує або відтворює повідомлення під час виконання автентифікаційного «рукостискання». Наприклад, при переході з WPA3 у режим WPA2 (атака на пониження версії) MitM-позиція дає можливість зменшити ризик виявлення, адже атакувальник має змогу маніпулювати пакетами таким чином, щоб клієнт автоматично перейшов на менш захищений протокол. Атаки на блокування сервісу (DoS) із використанням **«злого близнюка» (Evil Twin)** також стають значно результативнішими, якщо зловмисник контролює канали як посередник. Хоча саме підключення до злого близнюка може сигналізувати про аномалію у мережі, у випадку, коли цей вузол функціонує у режимі MitM, його виявлення стає набагато складнішим.

MitM-атаки у мережах 5G

У мережах п’ятого покоління загроза MitM зберігає свою актуальність. Приклади включають масові атаки повторення автентифікаційних повідомлень, що перевантажують ресурси головної мережі, а також DoS-атаки, спрямовані як на

кінцеві пристрої (UE), так і на елементи основної інфраструктури. Хоча реалізація подібних атак можлива і без повноцінної MitM-позиції, саме вона дає змогу атакувальнику залишатися менш помітним у спектральному аналізі, що проводиться базовою станцією. Таким чином, навіть попри удосконалені механізми безпеки в 5G, шахрайські базові станції та зловмисники, що застосовують MitM, залишаються критичними загрозами для стійкості системи.

Псевдо-MitM у середовищах співіснування

У випадках, коли йдеться про мережі співіснування (наприклад, 5G та WiFi 6/6E), зловмисник може сформувати так звану псевдо-MitM-позицію, використовуючи вразливості, пов’язані з проблемою прихованого вузла. У такій ситуації атакувальник здатен створювати перешкоди для базової станції під час висхідних (uplink) передач і водночас перехоплювати повідомлення користувачів. Аналогічно можна здійснювати атаки на окремі пристрої під час завантаження даних: зловмисник може блокувати певні пакети й вибірково повторювати їх до базової станції або клієнтського обладнання. Це відрізняється від класичного MitM, де зловмисник контролює весь трафік, але за своїми наслідками може бути не менш небезпечним.

Ще одним небезпечним варіантом є використання псевдо-MitM як інструменту для впровадження несанкціонованої базової станції. Зловмисник навмисно блокує канали зв’язку легітимної станції, створюючи перешкоди у комунікаціях, і водночас пропонує підключення до власної фальшивої gNB. Користувачі, втративши стабільний канал, автоматично приєднуються до підробленої базової станції, вважаючи її легальною. У таких випадках легітимна gNB фактично позбавлена можливості відрізнити «шум» від законної активності у середовищі співіснування і цілеспрямовані зловмисні дії.

Наслідки MitM-атак

Наслідки подібних атак можуть бути масштабними:

- **компрометація автентифікаційних даних** (паролів, ключів шифрування, токенів доступу);

- **підвищення затримки та втрата пакетів**, що у критичних застосуваннях (наприклад, у системах керування безпілотним транспортом чи телемедицини) може мати катастрофічні наслідки;
- **повна втрата конфіденційності користувачів**, адже зловмисник у MitM-позиції здатен отримувати персональні дані, інформацію про місцеположення та історію комунікацій;
- **створення умов для складніших комбінованих атак**, зокрема вторгнень у мережеву інфраструктуру через підробку контрольних повідомлень чи зміну параметрів сесії.

У підсумку можна зазначити, що атаки типу MitM і псевдо-MitM у середовищах співіснування є одним із ключових викликів безпеці в епоху 5G і майбутніх мереж 6G. Їхня небезпека полягає не лише у складності виявлення, а й у здатності комбінувати прості механізми (наприклад, блокування чи відтворення пакетів) із серйозними наслідками для продуктивності та конфіденційності користувачів.

Фізичний рівень безпеки

Сучасні специфікації стандартів мобільного зв’язку поки що не містять уніфікованих протоколів, що безпосередньо орієнтовані на забезпечення безпеки на фізичному рівні. Попри це, у наукових колах і серед розробників інфраструктури телекомунікацій спостерігається підвищений інтерес до створення таких механізмів. Йдеться насамперед про протоколи автентифікації, які могли б використовувати унікальні характеристики радіочастотного середовища як основу для захисту від несанкціонованого доступу. До таких характеристик відносяться параметри поширення хвиль, індивідуальні особливості передавачів і приймачів, а також відбиткові ознаки сигналів.

Найбільш відомими прикладами досліджень у цій сфері є рішення, реалізовані у фізичному рівні технологій 5G New Radio (NR) та WiFi 6. Тут застосовуються методи радіочастотного «відбитка» пристрою (RF fingerprinting), який дозволяє ідентифікувати термінали на основі їхнього унікального спектрального «почерку», а також технологія формування вузьконаправлених

променів (beamforming), що може слугувати додатковим інструментом перевірки легітимності користувачів. Такі рішення відкривають нові горизонти в підвищенні рівня безпеки, але залишаються й серйозні виклики, серед яких — мінливість каналів поширення радіосигналів, залежність від місця розташування й часу, різниця в апаратних реалізаціях пристроїв та необхідність уніфікації механізмів управління ключами для мільярдів терміналів.

Механізми безпеки фізичного рівня наразі переважно орієнтовані на автономні мережі або ж на сценарії мережевого співіснування, і їхня ефективність тестується саме в таких умовах. Наприклад, використання RF-fingerprinting може надавати додаткові ідентифікаційні ознаки для підтвердження автентичності пристрою всередині контрольованої мережі. Проте у середовищах співіснування постає проблема: зовнішні пристрої, які не належать до даного домену, можуть сприйматися як легітимні, оскільки протоколи не передбачають достатніх механізмів для їхньої перевірки. Це зменшує ефективність захисту та відкриває нові вектори для атак.



Рис. 3.4 Використання beamforming у середовищах співіснування для формування ефективної MitM-позиції

Парадоксально, але саме ті технології фізичного рівня, що пропонуються як інструменти підвищення безпеки, можуть бути використані для організації більш витончених атак. Зокрема, у поєднаних сценаріях, де застосовуються особливості 5G NR, WiFi 6/6E та середовища співіснування, протидія зловмисним діям суттєво ускладнюється. Так, на рисунку 8 наведено приклад атаки, коли зловмисник використовує beamforming для створення локалізованих перешкод на каналі легітимної базової станції, залишаючи при цьому без змін трафік користувачів. Одночасно він спрямовує інший вузьконаправлений промінь на пристрій-жертву, непомітно перехоплюючи його комунікації. У такій ситуації базова станція не здатна відрізнити, чи є перешкоди результатом природного багатокористувацького середовища співіснування, чи вони навмисне створені атакувальником. Сам користувач, своєю чергою, не має жодних індикаторів присутності зловмисника.

Щоб зробити атаку ще небезпечнішою, зловмисники можуть поєднувати beamforming із радіочастотним fingerprinting. Це дає змогу точно ідентифікувати конкретний термінал за його унікальними апаратними характеристиками, навіть без знання таких ідентифікаторів, як 5G-GUTI. У результаті зловмисник здатний відстежувати активність обраної жертви, аналізувати її поведінку та здійснювати таргетований перехоплення даних.

Таким чином, навіть такі передові механізми, як beamforming, OFDM-модуляції чи RF-fingerprinting, у середовищах співіснування можуть перетворитися на інструмент атак, а не захисту. Це вкотре доводить: розробка спеціалізованих механізмів безпеки саме для систем спільного використання спектра є критично важливим завданням на шляху до впровадження мереж шостого покоління.

4 ПОМ'ЯКШЕННЯ НАСЛІДКІВ ТА НАПРЯМКИ МАЙБУТНІХ ДОСЛІДЖЕНЬ

4.1 Рішення для безпеки фізичного рівня

Фізичний рівень є фундаментом усієї архітектури телекомунікаційних систем, адже саме тут відбувається перетворення інформації у вигляді електромагнітних хвиль, їхнє поширення та прийом. Традиційно цей рівень розглядався як основа для забезпечення пропускної здатності, зменшення втрат і підвищення ефективності використання спектра. Проте з розвитком мобільних систем нового покоління (5G і особливо 6G) його роль значно розширилася: тепер фізичний рівень сприймається також як ключовий інструмент забезпечення безпеки, здатний протидіяти атакам ще до того, як включаються механізми класичної криптографії вищих рівнів OSI.

Криптографічний захист на фізичному рівні

Одним із перспективних напрямів є створення зашифрованого фізичного рівня, де сама передача сигналу відбувається так, що навіть за наявності перехоплення інформація втрачає будь-яку цінність. Секретність тут забезпечується не лише ключами, а й особливостями середовища поширення сигналів. Наприклад, якщо легітимний отримувач має кращі умови каналу (вищий SNR або кращу геометрію розташування антен), то він здатен декодувати інформацію, у той час як перехоплювач бачить лише шумоподібний сигнал.

Проте реалізація такого підходу стикається з проблемами масштабування. У майбутніх мережах кількість пристроїв IoT, сенсорів, мобільних терміналів та «розумної» інфраструктури може перевищувати 10–20 мільярдів підключень. Це означає, що механізми синхронізації, генерації та розповсюдження ключів повинні бути надзвичайно ефективними, масштабованими та безпечними.

Використання класичних протоколів обміну ключами

Для генерації ключів часто застосовується протокол Діффі–Геллмана (D-H). Він дозволяє обмінюватися ключами без передачі самого секрету. Однак для його

реалізації потрібна інфраструктура відкритих ключів (PKI) та сертифікаційні центри, що ускладнює його застосування в умовах, коли мова йде про сотні тисяч приватних 5G нано-базових станцій чи точок доступу WiFi у містах. Крім того, цей протокол вимагає значних обчислювальних потужностей, що є непосильним для малопотужних пристроїв на кшталт датчиків «розумного міста» чи носимих гаджетів.

Beamforming та узгодження ключів

У мережах 5G NR одним із рішень проблеми є використання beamforming. Ця технологія дозволяє спрямовувати енергію сигналу у конкретний напрямок, формуючи вузький промінь. На практиці це означає, що можна створити умови, коли легітимний користувач отримає сигнал із високою якістю, тоді як перехоплювач, який знаходиться в іншому напрямку, отримає слабкий або спотворений сигнал.

У низці досліджень пропонується використовувати beamforming як основу для протоколів узгодження ключів. Базова станція передає випадкові пілотні сигнали, а легітимні користувачі формують на їхній основі секретні ключі. Перехоплювач, намагаючись зіпсувати канал за допомогою атаки «пілотного забруднення», може бути виявлений за рахунок аналізу відхилень у сигналі. У таких випадках базова станція здатна змінювати довжину чи параметри ключів, зберігаючи секретність.

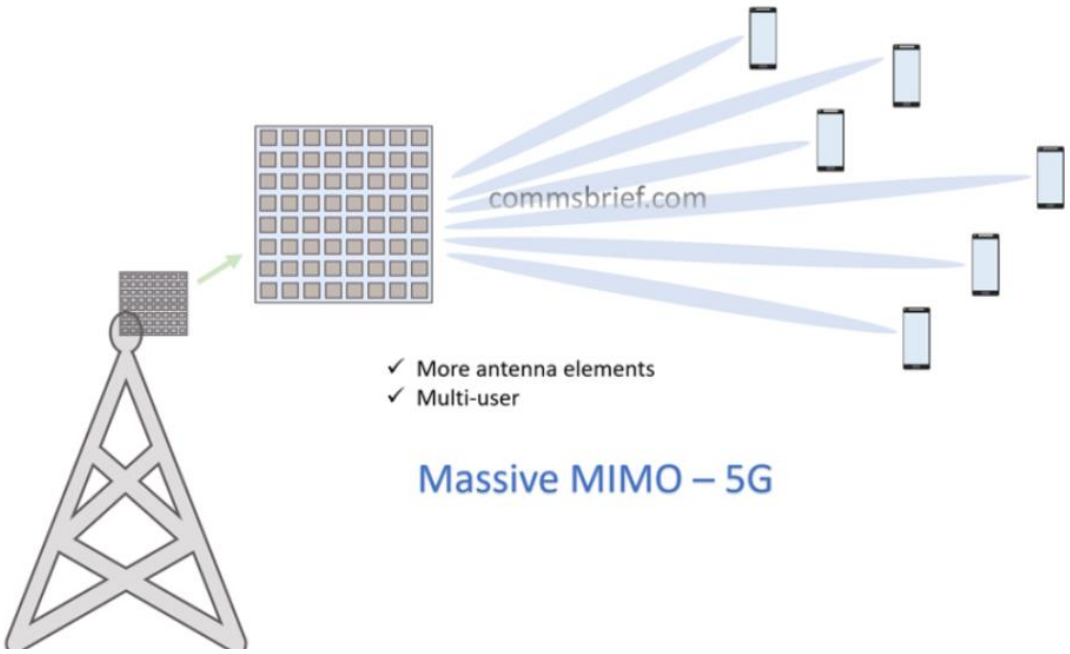


Рис. 4.1 Massive MIMO 5G multi-user beamforming — приклад з кількома користувачами, кожен отримує промені від спільної базової станції

Цікаво, що цей метод було протестовано в системах із масивними антенними решітками (Massive MIMO). Результати симуляцій показали, що навіть за наявності активного перехоплювача система здатна формувати ключі з ентропією, достатньою для криптографічного захисту.

Використання штучного шуму

Ще одним потужним механізмом є додавання штучного шуму (Artificial Noise, AN). Ідея полягає в тому, щоб передавати додатковий шум у просторових вимірах, які недоступні легітимному користувачу, але спотворюють сигнал для перехоплювача. У системах MIMO цей метод дозволяє значно знизити ефективність атак, особливо якщо поєднувати його з технікою нульового простору (null-space precoding). У результаті законний користувач отримує чистий сигнал, тоді як перехоплювач бачить лише хаотичний шум.

Автентифікація на фізичному рівні (PLA)

Окрему увагу дослідники приділяють методам Physical Layer Authentication (PLA). На відміну від класичних протоколів, PLA використовує унікальні фізичні характеристики каналів та пристроїв як додатковий «пароль». Це можуть бути:

- радіочастотні «відбитки» (RF fingerprinting);

- кут прибуття сигналу (AoA, Angle of Arrival);
- варіації у спектральних характеристиках пристрою;
- часові затримки та фазові зсуви.

Завдяки цьому PLA дозволяє розпізнати, чи дійсно сигнал надходить від легітимного користувача, чи його підробив зловмисник. У поєднанні з класичною криптографією PLA формує додатковий бар'єр безпеки, унеможливлюючи доступ сторонніх пристроїв навіть за умови компрометації ключів.

Практичні експерименти та перспективи

На практиці більшість досліджень PLA та зашифрованого фізичного рівня проводиться за допомогою SDR-платформ (Software-Defined Radio), таких як USRP. Наприклад, у лабораторних умовах було продемонстровано, що RF-fingerprinting здатен відрізнити два смартфони навіть однієї моделі з точністю понад 95%, використовуючи їхні унікальні спектральні відмінності.

У майбутніх мережах 6G ці методи планується інтегрувати у поєднанні з постквантовою криптографією, щоб забезпечити захист навіть від атак квантових комп'ютерів. Очікується, що фізичний рівень стане першою лінією оборони, а його механізми будуть доповнювати традиційні криптографічні протоколи вищих рівнів.

Фізичний рівень стає невід'ємним елементом архітектури безпеки майбутніх телекомунікаційних систем. Його унікальна властивість — використання невідтворюваних характеристик середовища поширення сигналів і обладнання — робить його надзвичайно перспективним у протидії атакам. Однак залишаються проблеми: складність масштабування, залежність від точності оцінки каналів, високі вимоги до обчислювальних ресурсів і необхідність розробки уніфікованих стандартів безпеки фізичного рівня. Саме вирішення цих завдань стане визначальним на шляху до розбудови безпечних мереж шостого покоління (6G).

4.2 Рішення в області безпеки доступу

Забезпечення прямої секретності та інтеграція новітніх механізмів автентифікації

Одним із ключових викликів у сучасних мобільних мережах є гарантування ідеальної прямої секретності (Perfect Forward Secrecy, PFS) під час процедури автентифікації. Традиційні протоколи, такі як 5G-AKA, уже містять базові механізми захисту, однак їхня ефективність у протидії пасивним перехоплювачам залишається обмеженою. Перспективним рішенням є інтеграція протоколу обміну ключами Діффі–Геллмана (D-H) безпосередньо в архітектуру 5G-AKA. Такий підхід ускладнює компрометацію сесійних ключів навіть у випадку, якщо зловмисник володіє довгостроковими секретними ключами. Завдяки використанню одноразових числових значень (nonce), цей метод унеможливлює розкриття ключів під час атаки пасивного перехоплювача.

Цей підхід має пряму аналогію з механізмами безпеки WiFi, зокрема з протоколом WPA3, який застосовує рукопотискання Dragonfly замість класичного D-H. Така інтеграція довела свою ефективність у захисті від атак на одноразові номери та у забезпеченні конфіденційності переданих даних.

Використання D-H для захисту ідентифікаторів і даних

Застосування протоколу D-H дозволяє ефективно захистити користувацькі ідентифікатори (SUPI/IMSI) від атак на приватність та від атак повтору. Сеансовий ключ, отриманий під час процедури рукопотискання, може бути використаний для шифрування чутливих даних абонента. Це гарантує, що навіть за умови перехоплення трафіку особисті ідентифікатори залишаються прихованими від зловмисників.

Крім того, обмін повідомленнями у магістральній мережі 5G супроводжується використанням MAC-кодів (Message Authentication Code), які виконують функцію перевірки цілісності переданих даних. Завдяки цьому стає можливим захист від підробки повідомлень та атак на відтворення. Використання таких механізмів також допомагає протидіяти атакам на відстеження абонентів, забезпечуючи стійкість до маніпуляцій із повідомленнями SYNC_FAIL та MAC_FAIL.

Блокчейн як інноваційний інструмент

Ще одним перспективним напрямом для посилення захисту є застосування блокчейн-технологій у комбінації з класичною інфраструктурою відкритих ключів (PKI, Public Key Infrastructure). Такий підхід дозволяє створювати легковагові та децентралізовані платформи довіри, що особливо актуально для комунікацій «пристрій–пристрій» (D2D) та для транспортних систем.

Наприклад, у сфері автомобільних однорангових мереж (VANET) блокчейн може виступати у ролі реєстру сертифікатів доступу користувачів, що гарантує прозоре керування доступом та захист приватності. Подібні підходи вже реалізовані у рішеннях на базі Ethereum, де блокчейн виступає децентралізованою базою даних для перевірки та збереження прав доступу абонентів. Це дозволяє мінімізувати ризики підробки сертифікатів і гарантує прозорість управління ідентифікаційною інформацією.

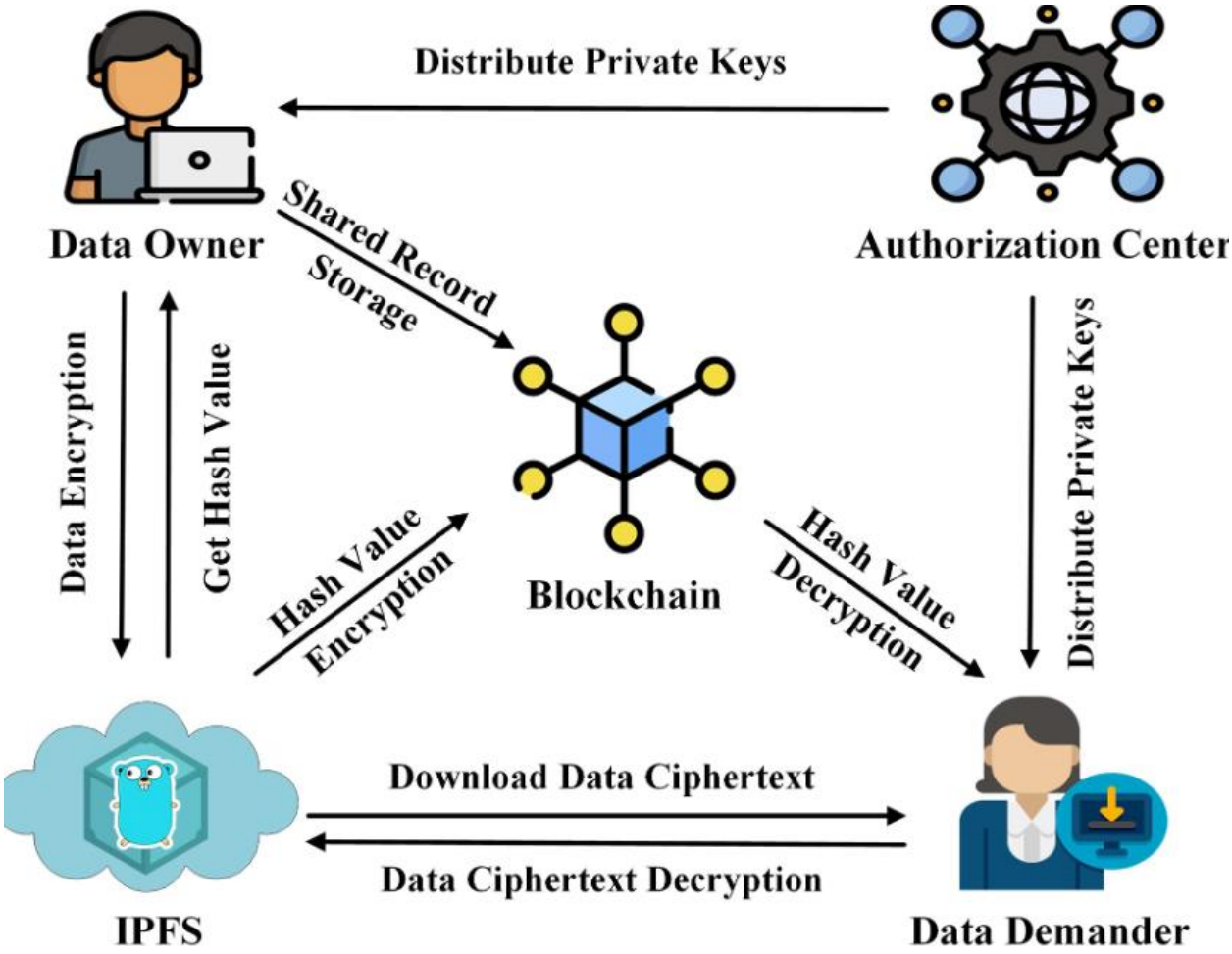


Рис. 4.2 Блок-схема з blockchain та ключовим розподілом / управлінням привілеями

Крос-рівневі механізми автентифікації

Особливу увагу останнім часом привертають крос-рівневі техніки автентифікації, що поєднують механізми фізичного рівня (PLA, Physical Layer Authentication) із класичними методами другого рівня. Така інтеграція підвищує стійкість систем безпеки, дозволяючи захистити конфіденційність місцеположення, протидіяти атакам «людина посередині» (MitM) та блокувати діяльність шахрайських базових станцій.

У більшості сучасних рішень характеристики фізичного рівня, зокрема CSI (Channel State Information) та RSS (Received Signal Strength), використовуються як унікальні відбитки пристрою (fingerprints). Ці параметри стають основою для генерації випадкових послідовностей і попередньої ідентифікації користувачів.

Для врахування динамічного характеру мереж 5G було запропоновано парні крос-рівневі механізми, які поєднують PLA з вищими рівнями автентифікації. У такій моделі PLA застосовує кілька fingerprint-функцій фізичного рівня для підвищення стабільності, а механізми вищого рівня виконують оновлення параметрів для адаптації до умов середовища з низькою обчислювальною складністю. Це відрізняється від непарних підходів, у яких PLA застосовується лише після завершення стандартної автентифікації.

Таким чином, майбутні архітектури 5G/6G повинні поєднувати:

- класичні криптографічні протоколи (D-H, MAC, PKI);
- децентралізовані технології (блокчейн);
- адаптивні крос-рівневі механізми (PLA + L2).

Тільки така комплексна модель здатна забезпечити високий рівень конфіденційності, надійності та стійкості до атак у мобільних мережах наступних поколінь.

4.3 Напрями досліджень у галузі безпеки співіснування

Більшість сучасних наукових робіт у сфері телекомунікацій зосереджені на класичних підходах до захисту автономних мереж. Там увага приділяється

фізичному рівню та протоколам керування доступом, які діють у відносно «закритому» середовищі, де всі учасники вважаються частиною єдиної системи. Однак із розвитком мереж п’ятого покоління (5G) та подальшим переходом до мереж шостого покоління (6G) стає очевидним, що концепція співіснування (coexistence), де паралельно функціонують кілька незалежних систем (наприклад, 5G, WiFi 6/6E, IoT-мережі), є неминучою. Це дозволяє ефективніше використовувати обмежений частотний ресурс, але водночас створює новий спектр викликів у сфері кібербезпеки.

Ключова проблема полягає в тому, що у середовищі співіснування традиційні механізми безпеки активуються занадто пізно. Коли пристрій чи базова станція отримують доступ до спектра, механізми автентифікації ще не встигли перевірити, чи є джерело сигналу легітимним. Це створює можливість для атаки на захоплення спектра, яка фактично не має аналогів в автономних мережах.

Незалежність протоколів MAC і проблема «прихованого вузла»

Особливістю мереж співіснування є те, що кожна система (5G, WiFi, IoT тощо) використовує власний протокол MAC (Medium Access Control). Хоча в теорії вони схожі — усі використовують механізми розподілу доступу до середовища, — на практиці вони абсолютно не узгоджені. Це створює ситуацію, коли дії легітимних користувачів однієї мережі можуть виглядати як потенційна атака для іншої.

Яскравим прикладом є проблема прихованого вузла. У класичних автономних мережах її можна локалізувати за допомогою протоколів MAC, але у співіснуванні кількох незалежних систем подібне явище виявляється неконтрольованим. Зловмисник може свідомо використати цю ситуацію, створюючи додаткові завади, які виглядатимуть як «звичайна активність іншої мережі». У результаті суттєво зростає затримка (latency), знижується пропускна здатність (throughput) і погіршується QoE (Quality of Experience) кінцевих користувачів.

Використання блокчейну як інноваційного механізму довіри

Для вирішення проблеми ідентифікації користувачів та захисту від підроблених вузлів активно досліджується використання блокчейн-технологій. Блокчейн дає можливість реалізувати:

- Прозорість — усі транзакції доступу до спектра зберігаються у відкритій розподіленій базі даних, що ускладнює маніпуляції.
- Незмінність — записи не можна підробити, тому зловмисник не зможе «заднім числом» додати собі право на використання спектра.
- Анонімність — дозволяє легітимним користувачам отримувати доступ без розкриття чутливих персональних даних.

Ці властивості особливо корисні для M2M-комунікацій (Machine-to-Machine), а також для автомобільних однорангових мереж (VANETs), де велика кількість вузлів динамічно з’являється й зникає. Наприклад, блокчейн може зберігати сертифікати доступу транспортних засобів до певних частотних діапазонів, забезпечуючи як конфіденційність, так і прозорість.

Втім, серйозним обмеженням є залежність від мережевого підключення до бази даних. Для централізованих мереж (5G, WiFi) це менш критично, адже базова станція може виступати «вузлом довіри». Але для децентралізованих однорангових систем, де пристрої повинні швидко отримати доступ до спектра без додаткових перевірок, це може стати слабким місцем.

Нові виклики у захисті даних та протоколах автентифікації

У середовищах співіснування зростає ризик того, що зловмисники використають «шум» від інших мереж для маскування атак. Це можна порівняти з ефектом у системах NOMA (Non-Orthogonal Multiple Access), де сигнали кількох користувачів передаються на одних і тих самих частотах. У такому середовищі важко визначити, чи є інтерференція результатом легальної активності, чи вона створена штучно.

Особливо уразливими стають механізми PLA (Physical Layer Authentication), що базуються на CSI (Channel State Information) або радіочастотному fingerprinting. Якщо зловмисник зуміє змінити оцінку каналу, він може видати себе за легітимний пристрій, обійти протоколи автентифікації й навіть вплинути на процес узгодження

ключів (key agreement). Це створює передумови для масових атак типу MitM (Man-in-the-Middle), які раніше були значно складнішими для реалізації.

Beamforming, MIMO та атаки пілотного забруднення

Ще одним критичним аспектом є безпека технологій beamforming та MIMO, що є основою сучасних 5G/6G-систем. У нормальних умовах вони дозволяють підвищити ефективність використання спектра та збільшити швидкість передачі. Проте у співіснуванні виникає серйозна проблема: зловмисники можуть використати атаки на пілотні сигнали (pilot contamination attacks).

Такі атаки змушують антенні решітки відхиляти промінь від легітимного користувача у напрямку зловмисника. Це не лише знижує якість зв’язку (QoS), а й надає атакуючому можливість перехоплювати конфіденційні дані. У середовищах співіснування ситуація ускладнюється тим, що навіть сигнали від інших легальних мереж можуть виглядати як атаки, а отже, системам захисту стає важче визначати справжню природу перешкод.

ВИСНОВКИ

У ході дослідження було розглянуто вразливості безпеки в сучасних та майбутніх телекомунікаційних системах, зокрема в 5G/6G, WiFi 6 та мережах спільного використання спектра. Аналіз показав, що стрімкий розвиток безпровідних технологій, який супроводжується збільшенням пропускної здатності, зменшенням затримок і розширенням функціональних можливостей, водночас формує нові ризики та вектори атак, що вимагають перегляду існуючих підходів до безпеки.

У першу чергу було детально досліджено протоколи автентифікації та управління ключами, що лежать в основі сучасних систем безпеки. Протоколи 5G-AKA, EAP-AKA’ та WPA2/WPA3 забезпечують базові механізми захисту доступу, проте демонструють низку слабких місць. Атаки на повторне використання ключів (Key Reinstallation Attacks), атаки на пониження версії, експлуатація «злих близнюків» або фальшивих базових станцій, а також компрометація автентифікаційних процедур під час рукопотискань підтверджують, що навіть найновіші стандарти потребують удосконалення. Ці вразливості особливо небезпечні у сценаріях високої мобільності, де кожна затримка чи збої автентифікації можуть призвести до відмови в обслуговуванні.

Окрему увагу було приділено фізичному рівню безпеки. Технології MIMO та beamforming, які суттєво підвищують ефективність використання спектра, можуть водночас використовуватися зловмисниками для атак. Атаки на пілотні сигнали (pilot contamination) дозволяють перенаправити спрямований промінь до зловмисника, позбавляючи легітимного користувача якісного каналу зв’язку. Використання відбитих сигналів може знизити рівень секретності на десятки відсотків, а у деяких випадках – повністю нівелювати її. Перспективні методи фізичної автентифікації (PLA), засновані на радіочастотному fingerprinting та інформації про стан каналу (CSI), відкривають нові можливості для захисту, однак у середовищах співіснування вони також можуть бути скомпрометовані.

Найбільш складні виклики спостерігаються в мережах спільного використання спектра. Якщо автономні мережі працюють у контрольованому середовищі з чітким розподілом частотних діапазонів, то у випадках співіснування (наприклад, 5G та WiFi 6/6E) різні системи змушені конкурувати за той самий спектр. Це створює умови для атак на захоплення спектра, маніпуляцій із протоколами LBT (Listen-Before-Talk), атаки імітації первинного користувача (PUE), підробки даних сенсорів спектра (SSDF), а також формує передумови для зростання кількості прихованих вузлів. Усі ці фактори ведуть до зниження QoS та QoE користувачів, а в критичних застосуваннях – до загрози для систем громадської безпеки, транспорту чи інфраструктури «розумного міста».

Водночас аналіз показав і перспективні напрями розвитку захисту. Очевидно, що подальший поступ у сфері кібербезпеки не може обмежуватися лише вдосконаленням наявних протоколів. Важливо інтегрувати концепцію Zero Trust Architecture, яка виходить із припущення, що потенційний зловмисник може перебувати всередині системи, тому доступ має контролюватися на всіх рівнях незалежно від статусу користувача. Не менш значущим є перехід до постквантових алгоритмів шифрування, адже з розвитком квантових обчислень асиметричні криптосистеми можуть втратити стійкість. Перспективним напрямом також є застосування блокчейн-технологій для управління доступом до спектра, що дозволяє гарантувати прозорість і незмінність записів, а також поєднання PLA із протоколами вищих рівнів у рамках крос-рівневих механізмів автентифікації. Саме така інтеграція фізичного та логічного рівнів може створити багатошаровий захист, що враховує динамічність середовища та складність сучасних загроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Wi-Fi 6 Protocol and Network. Susinder Rajan Gulasekaran. Artech House, 2021. – шифрування, автентифікація, уразливості WiFi 6.
2. Wireless Network Security: A Beginner's Guide. O'Reilly, 2018. – базові атаки та захист WiFi, WPA2/WPA3.
3. From 5G to 6G: Technologies, Architecture, AI, and Security. Wiley, 2024. – архітектури 6G, питання безпеки та загрози.
4. 5G Cyber Risks and Mitigation. Soni, S. Routledge, 2023. – ризики 5G, mmWave, MIMO, атаки і стратегії захисту.
5. Security and Privacy Preserving for IoT and 5G Networks. Springer, 2022. – приватність і безпека у 5G та IoT.
6. A Comprehensive Guide to 5G Security. Wiley, 2023. – системний огляд безпеки 5G, архітектура та контрзаходи.
7. Ramezanpour, K.; Jagannath, J.; Jagannath, A. Security and Privacy Vulnerabilities of 5G/6G and WiFi 6: Survey and Research Directions from a Coexistence Perspective. 2022. – вразливості при спільному використанні спектру, MAC, приховані вузли.
8. Performance Analysis of Coexistence Mechanism between 5G/Wi-Fi 6. 2025. – оцінка методів коекзистенції (CAC vs duty cycle).
9. Securing Wi-Fi 6 Connection Establishment Against Relay, Preamble Spoofing, and Relaying Attacks. 2024/2025. – атаки на фазу встановлення з'єднання WiFi 6, захисні рішення.
10. Wi-Fi 6 Cross-Technology Interference Detection and Mitigation. 2024. – виявлення та зниження завад між різними технологіями.
11. 5G Security Features, Vulnerabilities, Threats, and Data Protection in IoT and Mobile Devices: A Systematic Review. 2024. – захист IoT і мобільних пристроїв у 5G, огляд загроз.
12. On Challenges of Sixth-Generation (6G) Wireless Networks. 2022. – виклики й слабкі місця в архітектурі 6G.

13. A Comprehensive Survey on 6G-Security: Physical, Connection, and Service Layers. 2025. – уразливості 6G на різних рівнях.
14. Security Requirements and Challenges of 6G Technologies and Architectures. 2021/2022. – довіра, автентифікація, приватність у 6G.
15. Coexistence in Wireless Networks: Challenges and Opportunities. 2023. – проблеми та ризики спільного використання спектру.
16. Evaluating Private 5G and Wi-Fi 6: Key Features and Decision. 2024. – порівняння архітектури, продуктивності й безпеки.
17. Attacks and Vulnerabilities of Wi-Fi Enterprise Networks: Credential Stealing Experiments. 2023. – викрадення облікових даних у WiFi корпоративних мережах.
18. A Technical Review of Wireless Security for the Internet of Things. 2021. – уразливості безпроводових мереж, включно з WiFi і спектральним доступом.
19. 5G Network Slicing: Security Challenges, Attack Vectors, and Mitigation Strategies. 2024/2025. – уразливості network slicing, способи протидії.
20. Mitigating Security Vulnerabilities in 6G Networks: DMRN Protocol Analysis. 2024. – вразливості автентифікаційного протоколу 6G.
21. Systematic Meets Unintended: Prior Knowledge Adaptive 5G Vulnerability Detection via Multi-Fuzzing. 2023. – фуззинг для виявлення прихованих уразливостей 5G.
22. NLP-based Cross-Layer 5G Vulnerabilities Detection via Run-Time Profiling. 2023. – виявлення уразливостей 5G із ML-підходами.
23. Adversarial Machine Learning for 5G Communications Security. 2021. – атаки на ML-системи спектрального доступу та фізичної автентифікації.
24. Adversarial Security Mitigations of mmWave Beamforming Prediction Models. 2022. – уразливості beamforming-моделей та захист через adversarial retraining.
25. Overview of 5G Security and Vulnerabilities. 2020. – базовий аналіз слабких місць у 5G-архітектурі.

26. Potential Threat Vectors to 5G Infrastructure. CISA, 2020. – можливі вектори атак на інфраструктуру 5G.
27. Machine Learning Assisted Security Analysis of 5G-Network-Connected Systems. 2021. – аналіз уразливостей 5G із використанням ML.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

КВАЛІФІКАЦІЙНА РОБОТА

ВРАЗЛИВОСТІ БЕЗПЕКИ В 5G/6G, WIFI 6 ТА МЕРЕЖАХ СПІЛЬНОГО ВИКОРИСТАННЯ СПЕКТРУ

ВИКОНАВ:
СТУДЕНТ ГРУПИ ТСДМ-62
ВІКТОР ОХРЕМЕНКО

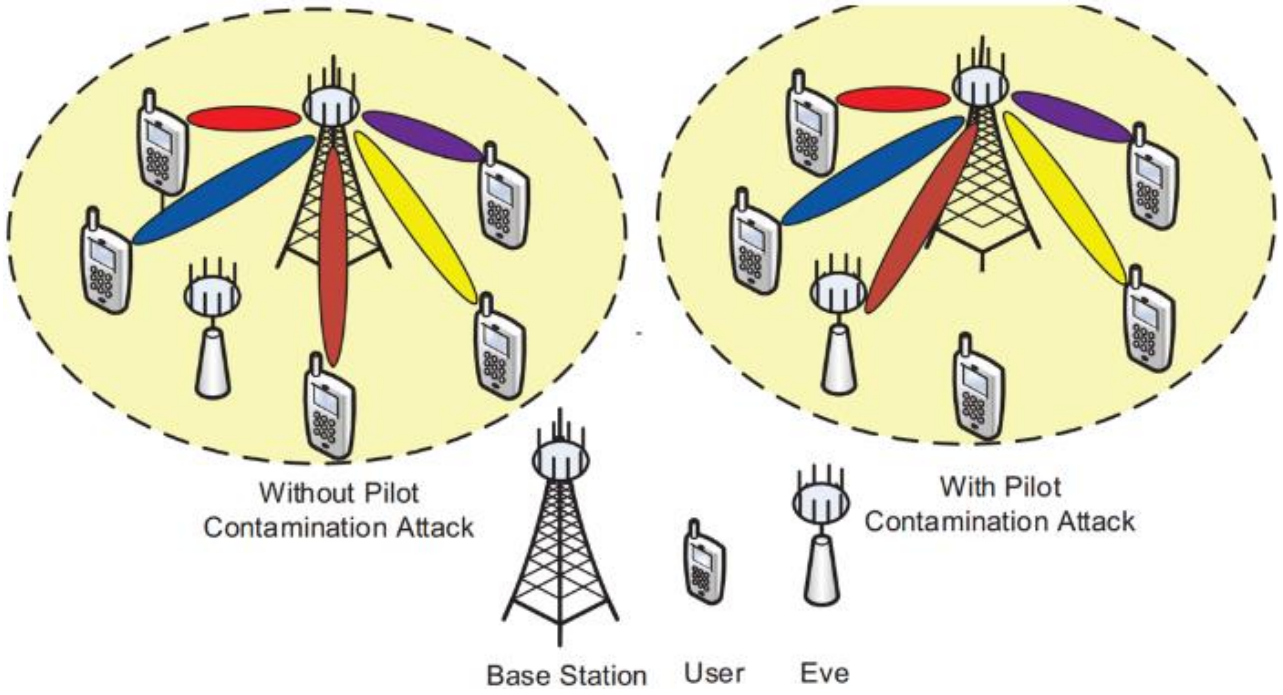
МЕТА РОБОТИ ТА АКТУАЛЬНІСТЬ

- Мета роботи – провести комплексний аналіз існуючих і потенційних вразливостей безпеки в мережах 5G/6G, WiFi 6/6E та системах спільного використання спектра, визначити основні вектори атак і розробити рекомендації щодо підвищення стійкості цих мереж до сучасних і майбутніх кіберзагроз.
- Об’єкт дослідження – процеси забезпечення інформаційної безпеки в сучасних і перспективних безпроводових телекомунікаційних мережах 5G/6G, WiFi 6/6E та середовищах спільного використання радіочастотного спектра.
- Предмет дослідження – механізми, протоколи та технології автентифікації, шифрування, управління ключами та захисту фізичного рівня, а також їхні вразливості й методи нейтралізації в умовах гетерогенних мереж і спільного використання спектра.

Актуальність.

- Стрімкий розвиток технологій 5G/6G і WiFi 6/6E забезпечує високі швидкості передавання даних, мінімальні затримки та підтримку мільйонів пристроїв IoT, що сприяє цифровій трансформації суспільства. Водночас збільшення відкритості та складності архітектур призводить до появи нових кіберзагроз. Недостатня ефективність традиційних механізмів захисту виявляється у вразливостях протоколів автентифікації, атаках на фізичному рівні та ризиках у мережах спільного використання спектра. Тому актуальним є дослідження сучасних і потенційних вразливостей безпеки та пошук ефективних способів підвищення стійкості безпроводових мереж нового покоління.

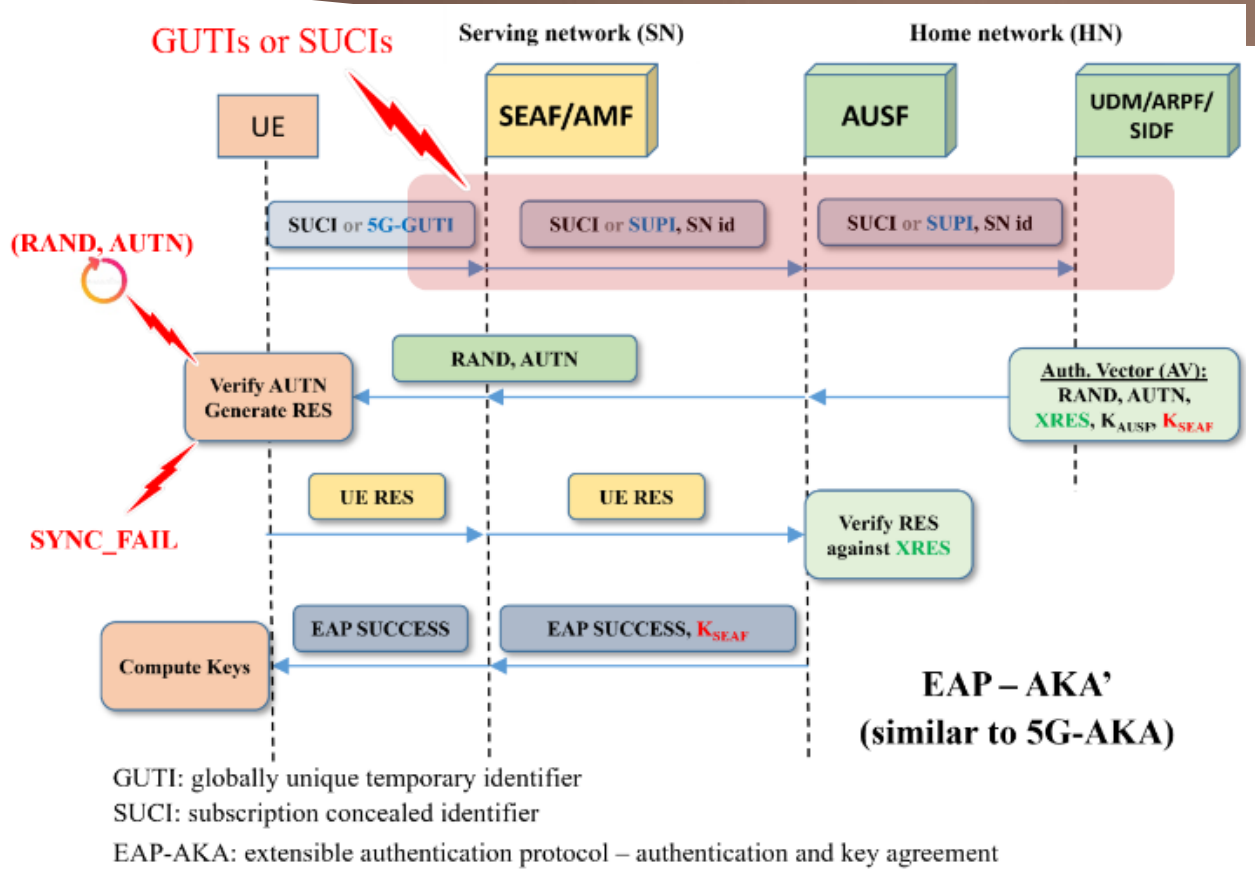
БЕЗПЕКА НА ФІЗИЧНОМУ РІВНІ



Атака «Пілотне забруднення», коли активний перехоплювач перенаправляє промінь базової станції, призначений користувачеві (User), убік зловмисника (Eve) (зліва – без атаки «Забруднення пілота», справа – з нею)

- Криптографічний захист комунікацій забезпечується багаторівневими протоколами, але безпека на фізичному рівні залишається проблемною через мінливість радіоканалів і розподілене управління ключами. Класичні методи DSSS і MCSS забезпечують автентифікацію, конфіденційність та стійкість до перешкод, а теоретико-інформаційна безпека з LDPC і полярними кодами гарантує слабку або сильну секретність. Beamforming підвищує SINR, стабільність зв’язку та секретність, фокусуючи сигнал на легальному користувачеві. Проте існують загрози від атак MitM, «забруднення пілота» та відбиттів сигналу, що вимагає інтеграції додаткових механізмів захисту для майбутніх 6G мереж.

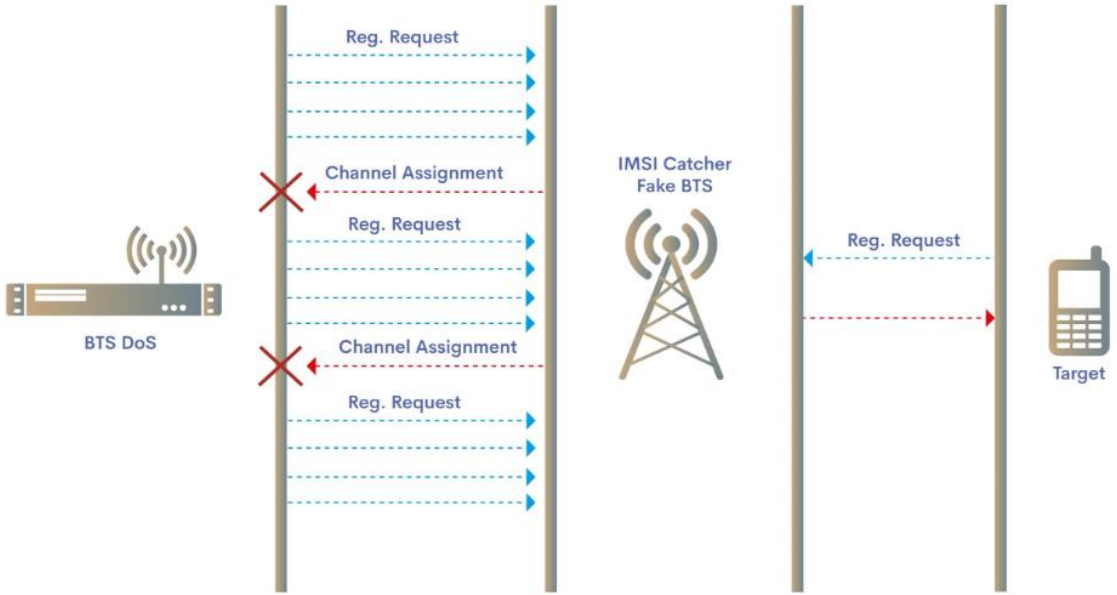
БЕЗПЕКА ДОСТУПУ В 5G



Безпека доступу на основі EAP в мережах 5G та різні точки атаки на протокол

- Захист доступу в мобільних мережах забезпечується протоколами AKA та EAP-AKA', що гарантують автентифікацію UE та обмін ключами, формуючи базовий захист на канальному рівні. У 5G додатково застосовується 5G-AKA із SEAF, що знижує затримки та підвищує стійкість до replay-атак. Для конфіденційності використовуються SUPI, SUCI та тимчасові GUTI, проте вони залишаються вразливими до MitM, IMSI/SUPI-catching, атак на екстрені виклики та нелегальні gNB. У 6G масштаби IoE потребують нових механізмів динамічних ідентифікаторів і криптографії, стійкої до квантових атак.

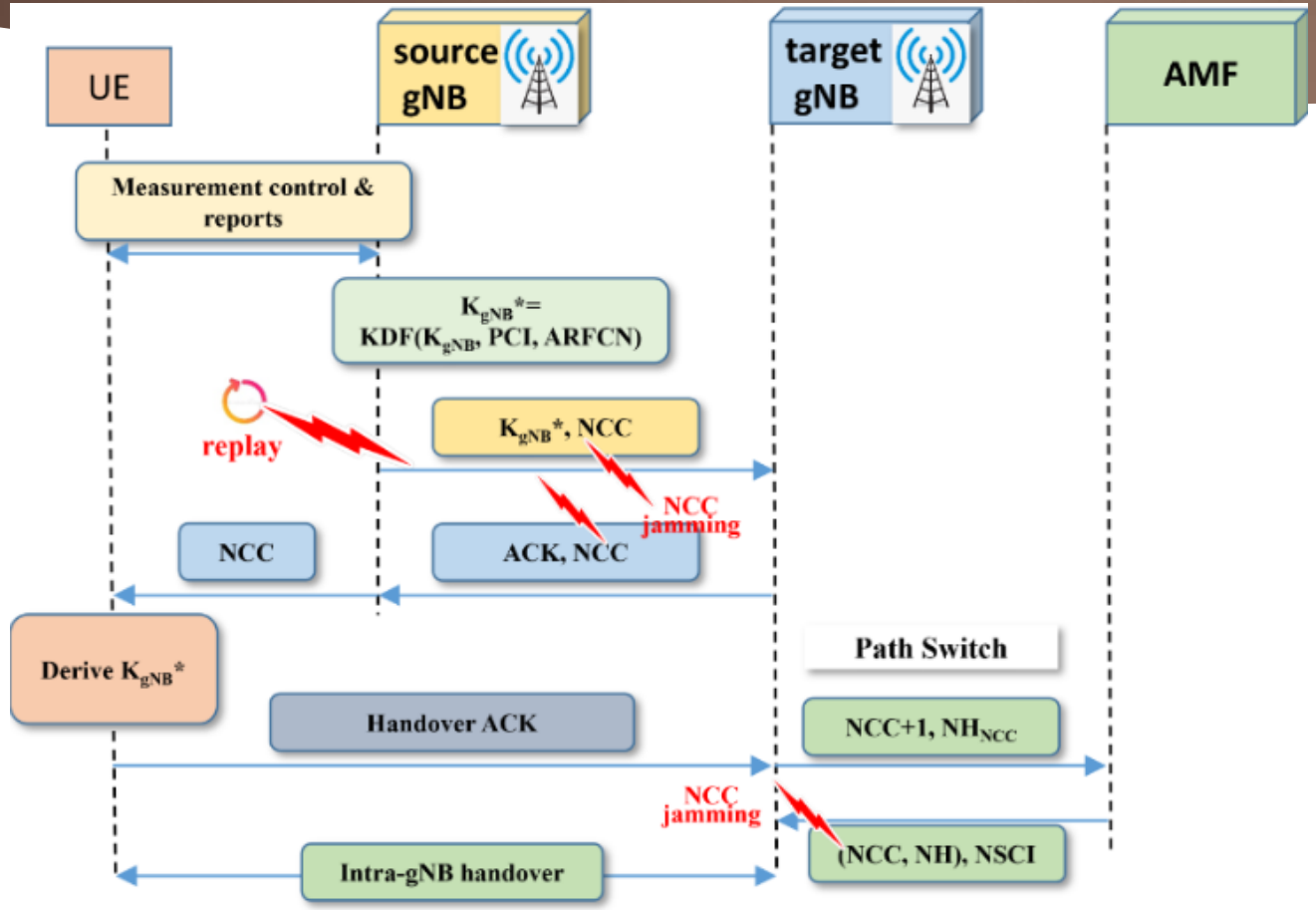
БЕЗПЕКА ДОСТУПУ В 5G



Робота IMSI-catcher: підроблена базова станція змушує пристрій передати IMSI

- У 5G навіть із SUCI залишається ризик витоку IMSI. Атака ToRPEDO використовує пейджингові повідомлення для відновлення частини IMSI та визначення присутності абонента у зоні дії. Повний IMSI можна отримати комбінацією ToRPEDO та перебору, що займає ~74 години. Це відкриває доступ до геолокації, дзвінків та мережевої активності. Додатково мережі уразливі до DoS/DDoS-атак, включно з DoSL для IoT-пристроїв, що виснажує ресурси UE та Core Network. Масштабні атаки можуть викликати глобальні збої, підкреслюючи потребу у адаптивних механізмах захисту в реальному часі.

БЕЗПЕКА ДОСТУПУ В 5G



Протокол безпеки хендовера в мережах 5G з різними вразливими точками для атак із повторенням та глушенням

- Хендовер у 5G забезпечує безперервність зв’язку під час переміщення між базовими станціями, що критично через часті перемикання на високих частотах. Під час хендоверу UE має нестабільний канал і обмінюється критичною інформацією, що робить його вразливим до атак: повторення, глушіння, десинхронізації, Rogue gNB та DoS/DDoS. 5G застосовує forward security із сесійними ключами K*gNB та NCC, але backward security обмежена. У 6G очікується інтеграція Zero Trust, адаптивне оновлення ключів, штучний інтелект для виявлення атак та квантово-стійкі алгоритми, щоб поєднати безпеку та низькі затримки під час хендоверу.

БЕЗПЕКА ДОСТУПУ В WIFI 6/6E

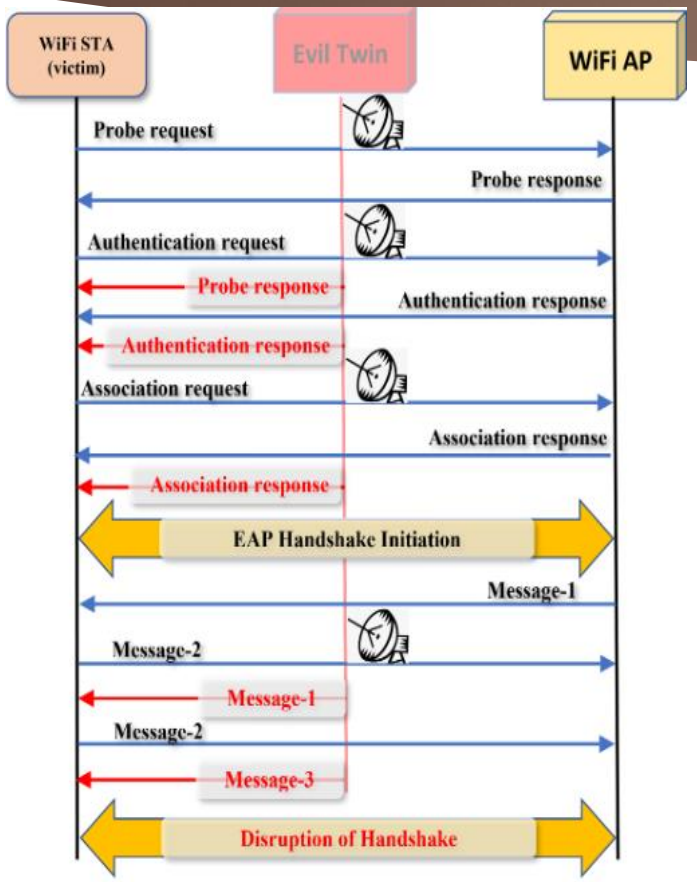
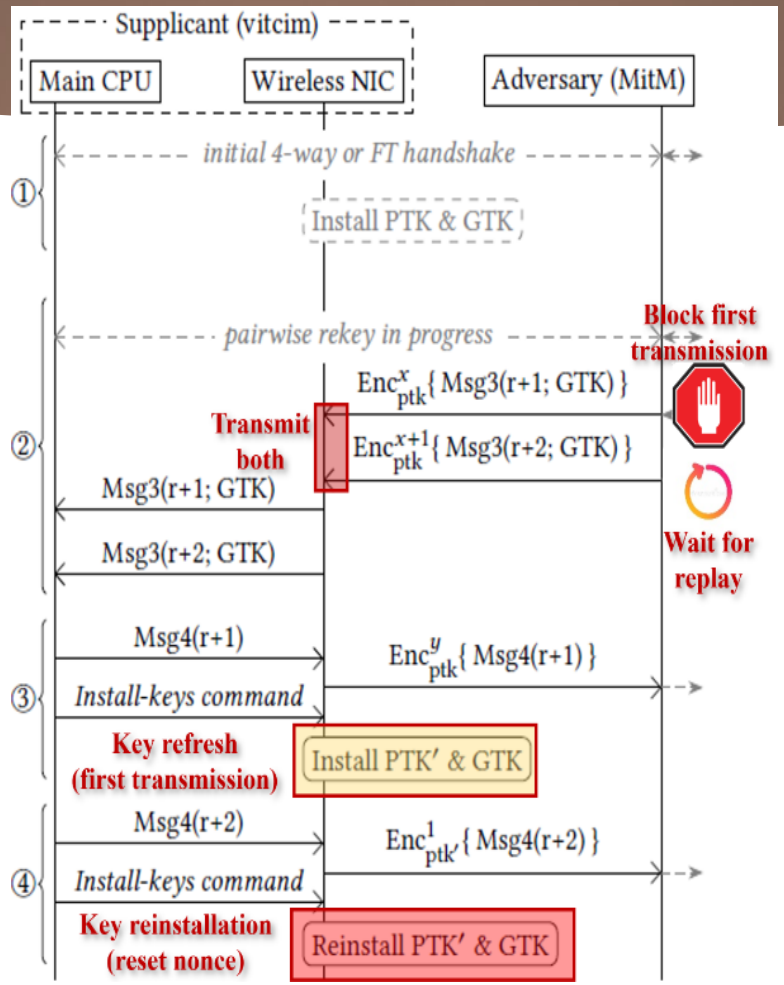


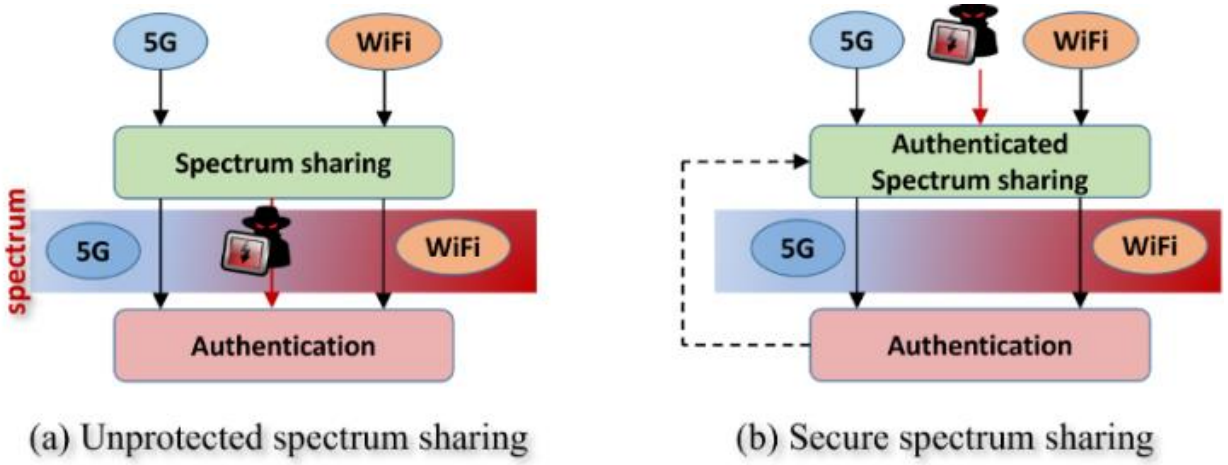
Схема атаки «Блокування сервісу» за допомогою злого близнюка під час автентифікаційного рукостискання EAP у WPA2 Wi-Fi



Атака на перевстановлення ключа з використанням MitM на автентифікаційному рукостисканні, заснованому на EAP, у WPA2 WiFi

- Атака «злий близнюк» (evil twin) у Wi-Fi полягає у створенні шахрайської точки доступу, яка імітує легітимну, змушуючи користувачів підключатися до неї. Вразливість SSID/BSSID дозволяє перехоплювати параметри мережі, а деаутентифікаційні атаки прискорюють підключення до фальшивої точки. Це відкриває MitM-атаки, викрадення даних та блокування сервісу. Атаки KRACK експлуатують повторне рукостискання WPA2, дозволяючи відтворювати трафік і змінювати повідомлення. WPA3 із протоколом Dragonfly та SAE підвищує захист, але залишає уразливість до DoS і downgrade-атак. Аналогічні проблеми спостерігаються в мобільних мережах 4G/5G.

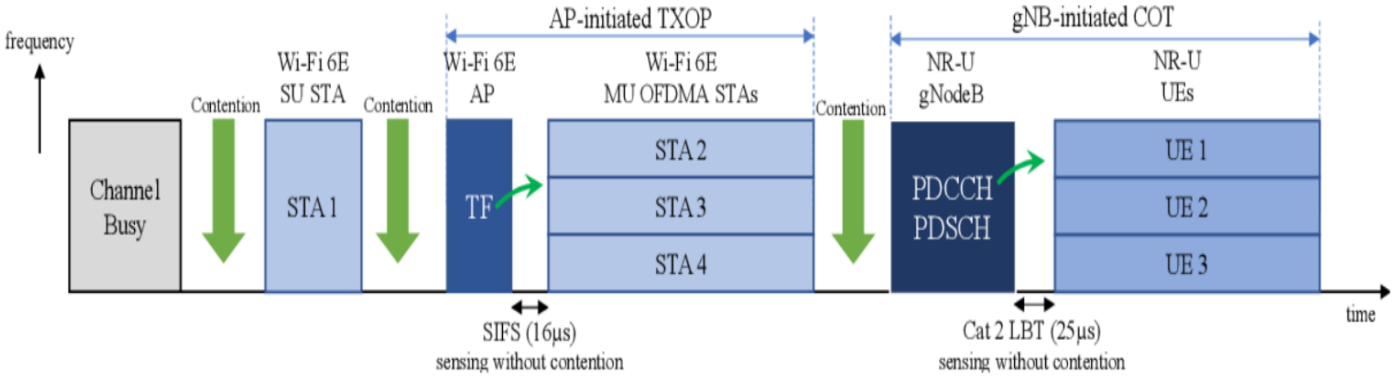
СПІЛЬНЕ ВИКОРИСТАННЯ СПЕКТРУ



Порівняння (a) незахищеного та (b) захищеного спільного використання спектра з точки зору дозволу зловмиснику отримувати доступ до спектру (захоплювати спектр)

- Зростання 5G/6G, IoT та безпілотного транспорту збільшує потребу у спектрі, що стимулює використання спільного доступу (spectrum sharing) у середовищах співіснування мереж. Це забезпечує ефективність і гнучкий розподіл ресурсів, але створює нові вектори атак: jamming, spoofing, DDoS, порушення справедливості доступу та погіршення QoE. Існуючі механізми безпеки активуються після отримання спектра, тож початковий доступ залишається вразливим. Для захисту потрібні spectrum-level IDS, криптографічна первинна автентифікація, колективні механізми довіри, AI/ML для виявлення аномалій і багаторівневі моделі безпеки на фізичному та мережевому рівнях.

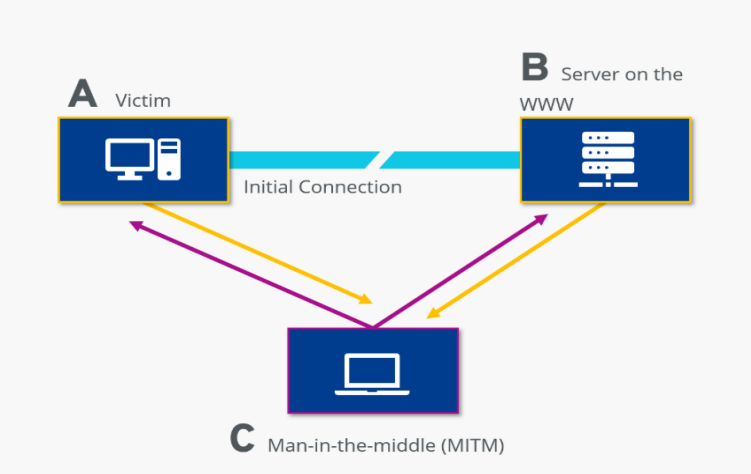
ЗАХВАТ СПЕКТРУ ТА ПОГІРШЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ



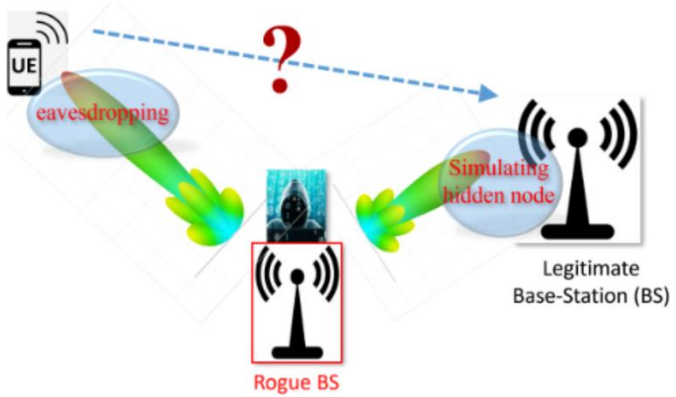
Доступ до спектру, що базується на LBT-протоколах для співіснування 5G та WiFi 6/6E

- Атаки на **захоплення спектра** у середовищах співіснування 5G і WiFi 6/6E виникають через доступ до частот до активації механізмів безпеки. Зловмисник може маскуватися під легітимну станцію, блокувати або повторювати пакети, погіршуючи **QoS** і загрожуючи громадській безпеці. Проблема **прихованого вузла** дозволяє атакувати канали OFDMA, спричиняючи колізії, затримки та підвищене енергоспоживання. Такі атаки критичні для безпілотного транспорту, «розумних міст» і служб екстреного реагування. Захист потребує міжмережевої довіри, узгодження протоколів та спеціалізованих механізмів безпеки для середовищ співіснування.

PSEUDO MITM ТА ФІЗИЧНИЙ ШАР БЕЗПЕКИ



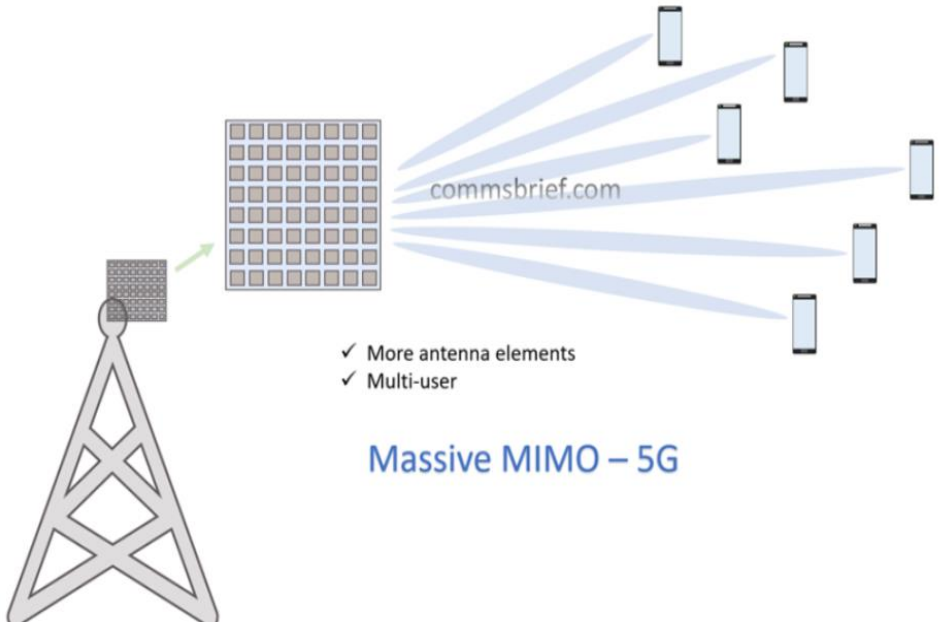
«Людина посередині» (MitM): зловмисник перехоплює комунікацію між користувачем та сервером



Використання beamforming у середовищах співіснування для формування ефективної MitM-позиції

- Атаки типу **«Людина посередині» (MitM)** є одними з найнебезпечніших у безпроводових мережах, адже дозволяють зловмиснику перехоплювати, змінювати чи відтворювати трафік між користувачем і сервером. У мережах **5G** вони можуть спричинити **компрометацію автентифікаційних даних, DoS-атаки** або **підключення до фальшивих базових станцій**. У середовищах співіснування (**5G + WiFi 6/6E**) з'являються **псевдо-MitM** сценарії, що ускладнюють виявлення атак. Навіть технології **beamforming** і **RF-fingerprinting**, призначені для захисту, можуть використовуватись зловмисниками. Тому створення нових протоколів безпеки фізичного рівня є критично важливим для **6G**.

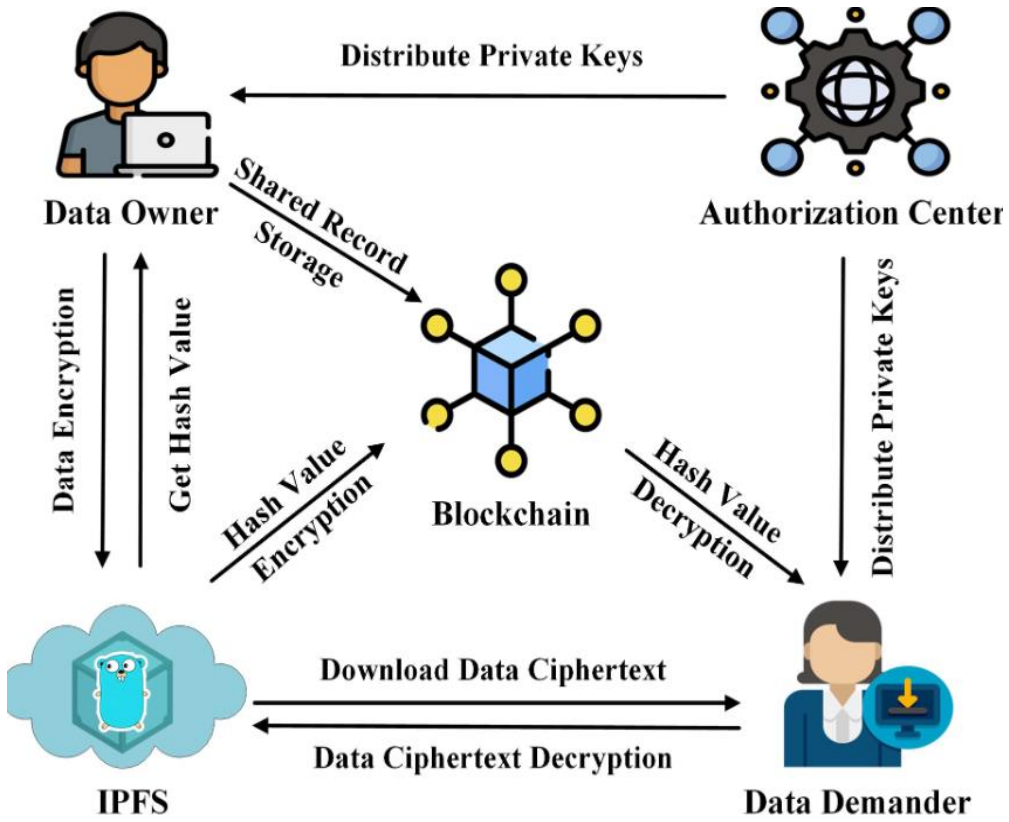
РІШЕННЯ ДЛЯ БЕЗПЕКИ ФІЗИЧНОГО РІВНЯ



Massive MIMO 5G multi-user beamforming — приклад з кількома

- Фізичний рівень телекомунікацій стає ключовим елементом безпеки в мережах 5G/6G, адже саме тут можна виявляти й блокувати атаки до активації криптографії вищих рівнів. Одним із напрямів є зашифрований фізичний рівень, де захист базується на особливостях каналу зв’язку. Технології beamforming, Massive MIMO і штучний шум (AN) забезпечують конфіденційність навіть за наявності перехоплювачів. Physical Layer Authentication (PLA) використовує унікальні характеристики сигналів як цифрові «відбитки». У поєднанні з D-H, PKI та постквантовою криптографією це формує першу лінію оборони майбутніх безпечних мереж шостого покоління.

РІШЕННЯ В ОБЛАСТІ БЕЗПЕКИ ДОСТУПУ



Блок-схема з blockchain та ключовим розподілом / управлінням привілеями

- У сучасних мобільних мережах одним із головних викликів є забезпечення прямої секретності та надійної автентифікації. Удосконалення протоколу **5G-AKA** шляхом інтеграції обміну ключами **Діффі–Геллмана (D-H)** підвищує стійкість до перехоплення, гарантуючи захист навіть при компрометації довгострокових ключів. Додаткову безпеку забезпечує застосування **MAC-кодів** для перевірки цілісності даних. Використання **блокчейн-технологій** у поєднанні з **PKI** створює децентралізовану платформу довіри для D2D-комунікацій. Поєднання **фізичного рівня автентифікації (PLA)** з класичними методами формує адаптивну модель захисту, придатну для мереж **5G/6G**, підвищуючи конфіденційність, надійність і стійкість до атак.

ВИСНОВКИ

- У роботі проведено аналіз вразливостей безпеки в сучасних і перспективних телекомунікаційних системах — 5G/6G, WiFi 6/6E та мережах спільного використання спектра.
- Розглянуто недоліки протоколів автентифікації (5G-AKA, EAP-AKA’, WPA3), атаки на фізичному рівні (beamforming, pilot contamination) та ризики в гетерогенних середовищах співіснування.
- Визначено типові загрози, як-от захоплення спектра, PUE та SSDF-атаки, що знижують QoS і QoE.
- Запропоновано напрями вдосконалення захисту, зокрема впровадження Zero Trust Architecture, постквантової криптографії, блокчейн-рішень і поєднання фізичної автентифікації з протоколами вищих рівнів.

Дякую за увагу!

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Віктор ОХРЕМЕНКО

Назва: ВРАЗЛИВОСТІ БЕЗПЕКИ В 5G/6G, WIFI 6 ТА МЕРЕЖАХ СПІЛЬНОГО ВИКОРИСТАННЯ СПЕКТРУ

Координатор: Вікторія КОРЕЦЬКА

Підрозділ: ННІТ

Коефіцієнт подібності 1:0.09

Коефіцієнт подібності 2:0

Тривога: 0

Після аналізу Звіту подібності констатую наступне:

☐ виявлені в роботі запозичення є сумлінними і не мають ознак плагіату. Тому робота визнається самостійною і допускається до захисту;

☐ виявлені в роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і самостійності її автора. Роботу направити на доопрацювання;

☐ виявлені в роботі запозичення є недобросовісними і мають ознаки плагіату або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. У зв'язку з чим, робота не допускається до захисту.

…… ……

Дата *Підпис Наукового керівника*