Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Дослідження методів захисту інформації в безпроводових системах з технологією massive MIMO
(тема)

Виконав:
студентка 2 курсу, групи АМСЗІм-22-2
Поповська Є.О.
(прізвище, ініціали)
Спеціальність: 125 Кібербезпека
(код і повна назва спеціальності)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)
Керівник: професор кафедри ІКІ ім. В.В. Поповського Марчук В.С.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо – професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентці Поповській Єлизаветі Олегівні
(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження методів захисту інформації в безпроводових системах з технологією massive MIMO
затверджена наказом по університету від «_3_» _листопада_ 2023 р. №_1291_Ст.__
2. Термін подання студентом роботи до екзаменаційної комісії ___15.01.2024 р.___
3. Вихідні дані до роботи: Протоколи, що забезпечують функціонування безпроводових систем з технологіями MIMO і massive MIMO
4. Перелік питань, що потрібно опрацювати в роботі:
1) Огляд сучасного стану технології 5G.
2) Методи захисту мережі 5G
3) Дослідження методів забезпечення інформаційної безпеки безпроводових систем з технологією massive MIMO.

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: Демонстраційний матеріал у вигляді ppt-презентації; діаграми спрямованості антенної решітки з кількістю елементів від 5 до 50 системи з технологією MIMO і адаптивної антенної решітки для подавлення сигналів зловмисника в системі massive MIMO згідно з результатами моделювання

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	професор Марчук Володимир Степанович		15.01.24

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	03.11.23	Виконано
2	Збір матеріалів для дослідження	30.11.23	Виконано
3	Розробка 1 розділу	07.12.23	Виконано
4	Розробка 2 розділу	14.12.23	Виконано
5	Розробка 3 розділу	11.01.24	Виконано
6	Оформлення атестаційної роботи	15.01.24	Виконано

Дата видачі завдання 3 листопада 2023 року

Студент _____ Поповська Є.О.
(підпис) (прізвище, ініціали)

Керівник роботи _____ професор Марчук В.С.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 69 с., 37 рис., 4 табл., 20 джерел.

БЕЗПРОВОДОВІ МЕРЕЖІ, АРХІТЕКТУРА БЕЗПЕКИ СИСТЕМ 5G, ТЕХНОЛОГІЯ MASSIVE MIMO, МІЛІМЕТРОВИЙ ДІАПАЗОН, БАГАТОКОРИСТУВАЛЬНИЦЬКИЙ ДОСТУП, МОДЕЛЮВАННЯ ЗАХИСТУ ВІД ГЛУШІННЯ.

Об'єкт дослідження – процеси функціонування безпроводової мережі.

Предмет дослідження – характеристиики безпроводової мережі.

Мета кваліфікаційної роботи – аналіз архітектури і параметрів безпроводової мережі 5G, а також вдосконалення методів інформаційного захисту безпроводової мережі з технологією massive MIMO.

Методи дослідження – емпіричний аналіз, порівняння, аналітичне моделювання.

На сьогоднішній день впровадження вдосконалених методів інформаційного захисту безпроводових мереж є актуальною задачею, оскільки в наш час відбувається суттеве збільшення кількості користувачів і потоків інформації в безпроводових мережах.

У кваліфікаційній роботі проведено дослідження захисту безпроводових мереж 5G, в тому числі з технологією massive MIMO. Розглянуто моделі та базові види загроз. Досліджено можливості вдосконалення захисту безпроводових мереж міліметрового діапазону з технологією massive MIMO. Проведено моделювання захисту від глушіння безпроводових систем за допомогою інтелектуальних антенних граток.

Запропоновано методи збільшення захисту безпроводових мереж massive MIMO.

ABSTRACT

Explanatory note: 69 p., 37 fig., 4 table; 20 sources.

WIRELESS NETWORKS, SECURITY ARCHITECTURE OF 5G SYSTEMS, MASSIVE MIMO TECHNOLOGY, MILLIMETER RANGE, MULTI-USER ACCESS, JAMMING PROTECTION MODELING.

The object of research is the processes of functioning of the wireless network.

The subject of research is the characteristics of a wireless network.

The purpose of the qualification work is to analyze the architecture and parameters of the 5G wireless network, as well as to improve the methods of information protection of the wireless network with massive MIMO technology.

Research methods – empirical analysis, comparison, analytical modeling.

Today, the introduction of improved methods of information protection of wireless networks is an urgent task, since nowadays there is a substantial increase in the number of users and information flows in wireless networks.

In the qualifying work, a study of the protection of 5G wireless networks, including with massive MIMO technology, was conducted. Models and basic types of threats are considered. Possibilities of improving the protection of millimeter range wireless networks with massive MIMO technology have been studied. Modeling of protection against jamming of wireless systems with the help of intelligent antenna grids was carried out.

Methods of increasing the protection of massive MIMO wireless networks are proposed.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

AAR – Adaptive Antenna Array
API – Application Programming Interface
APT – Advanced Persistent Threat
ARP – Address Resolution Protocol
BPSK – Binary Phase Shift Keying
CP – Control Plane
C-RAN – Cloud-Radio Access Network
CSI – Channel State Information
CSI-RS – Channel State Information - Reference Signal
DoS – Denial of Service attack
DDoS – Distributed Denial of Service
DGA – Domain Generation Algorithm
DM-RS – Demodulation Reference Signal
DNS – Domain Name System
eMBB – enhanced Mobile Broadband
FR2 – Frequency Range 2
FSK – Frequency Shift Keying
3GPP – 3rd Generation Partnership Project
5G – Fifth Generation
ICMP – Internet Control Message Protocol
IDS/IPS – Intrusion Detection System/ Intrusion Prevention System
IMS – Information Management System
IoT – Internet of Things
ITU-R – International Telecom Union Radiocommunication Sector
LTE – Long-Term Evolution
M2M – Machine-to-Machine
MAC – Media Access Control
MEC – Mobile Edge Computing
MIMO – Multiple Input Multiple Output
MU-MIMO – Multiple User - Multiple Input Multiple Output
MIoT – Massive Internet of Things

MITM – Man in the middle
mMTC – Massive Machine-Type Communications
NESAS – Network Equipment Security Assurance Scheme
NGFW – Next Generation Firewall
NRZ – Non Return to Zero
OAM – Operations, Administration and Management
O&M – Operation and Maintenance
POD – Ping of Death
RMI – Recoding Matrix Indicator
RAN – Radio Access Network
RIS – Reconfigurable Intelligent Surfaces
SCAS – Security Assurance Specifications
SDN – Software-Defined Networking
SIM – Subscriber Identification Module
SOC – Security Operations Center
SU-MIMO – Single User - Multiple Input Multiple Output
TVRA – Threat, Vulnerability And Risk Assessment
UE – User Equipment
UDP – User Datagram Protocol
UICC – Universal Integrated Circuit Card
UP – User Plane
URLLC – Ultra-Reliable Low Latency Communication
V2X – Vehicle-to-Everything
NFV – Network Functions Virtualization

ВСТУП

В наш час телекомунікаційні системи швидко змінюються і набувають нових якостей. Але окрім позитивних змін постають питання безпеки мереж.

З'явились мережі п'ятого покоління. Вони надають більше видів послуг і вирішують значний спектр задач. Одним з важливих переваг таких мереж в порівнянні з попередніми є високі пропускні здатності каналів і збільшення кількості абонентів, що обслуговує кожна сота. Це дозволило використовувати такі мережі для передачі інформації в системах, що працюють по технології Інтернету речей (IoT).

Що стосується безпеки в мережах нових поколінь, то, як правило, в них використовуються функції безпеки попередніх поколінь які доповнюються новими. Але не завжди ці зміни надають достатній рівень захисту.

Наприклад, мережі 5G мають вразливості, що були в попередньому поколінні і до них приєднуються нові.

Це пов'язано з високими швидкостями передачі інформації, що призводить до швидкого розповсюдження шкідливих впливів. В мережах побудованих по новим технологіям впроваджується багато програмних елементів замість апаратних. Очікується використання технологій віртуалізації мережевих функцій (Network Function Virtualization). Заміна апаратних елементів програмними дає багато позитивних переваг таким мережам, але збільшує вразливість мереж.

Класична технологія MIMO в мережах 5G зазнала суттєвих змін. В міліметровому діапазоні радіохвиль, що є другим частотним піддіапазоном FR2 для 5G має місце значне загасання радіохвиль. Для збільшення радіусу соти потрібно збільшувати концентрацію радіохвиль у напрямку апаратури користувачів. Вирішити цю задачу можливо за рахунок використання антенних решіток з великою кількістю антенних елементів. В міліметровому діапазоні це нескладно зробити, тому що антенні елементи мають малі розміри. На базових станціях встановлюються антенні системи з великою кількістю елементів. Така технологія отримала назву massive MIMO. На передавальному кінці кількість антенних елементів набагато більша ніж на приймальних пристроях.

Окрім того в напрямках на користувачів формуються індивідуальні промені. Використовується багатокористувальницька технологія Multiple User - Multiple Input Multiple Output (MU-MIMO).

Впровадження нових технологій обміну інформацією призводить до збільшення швидкостей і кількості обслуговуємих користувачів, але з іншого боку породжує нові проблеми з забезпеченням безпеки.

У кваліфікаційній роботі проведено дослідження захисту безпроводових мереж 5G, в тому числі з технологією massive MIMO. Розглянуто моделі та базові види загроз. Досліджено можливості вдосконалення захисту безпроводових мереж міліметрового діапазону з технологією massive MIMO. Проведено моделювання захисту від глушіння безпроводових систем за допомогою інтелектуальних антенних граток.

Запропоновано методи збільшення захисту безпроводових мереж massive MIMO.

Окремі результати роботи доповідались на трьох Міжнародних наукових конференціях [1 – 3].

1 ОГЛЯД СУЧАСНОГО СТАНУ ТЕХНОЛОГІЇ 5G

1.1 Загальні відомості про 5G

Нове покоління мобільних мереж розширило можливості доступу до Інтернету і надає більш надійні з'єднання з смартфонами та іншими пристроями ніж раніше. Але головне, що ємність сот суттєво збільшилась.

Найбільшою відмінністю 5G від мереж попереднього покоління є високі швидкості передачі інформації. Кількісно швидкості коливаються в межах від 10 до 20 Гбіт/с. При цьому мають місце дуже малі приблизно в 10 разів меньші затримки в передачі сигналів. Це відкриває багато можливостей для впровадження нових застосувань швидкісних мереж [4 – 6].

З’являються нові види послуг і сервісів, що були не можливі в попередніх поколіннях мобільних мереж. По перше – це можливість забезпечити широкосмуговий доступ до телебачення з надвисокою якістю картинки і якісного звуку. По друге – це можливість використовувати канали мереж 5G для передачі трафіка IoT від великої кількості датчиків.

В наш час існує тенденція заміни апаратури на віртуальні елементи. Віртуалізація надає багато позитивних якостей телекомунікаційним системам. Але з іншого боку виникають нові вразливості, що притаманні программним системам. Захист переміщається з фізичного на програмний рівень більш складний і вразливий, який потребує інших методів.

Проводяться роботи по розробці глобального стандарту, який служитиме для розгортання мереж п’ятого покоління мобільного зв’язку. Цим займається ряд міжнародних організацій, серед яких 3GPP і ITU-R.

Спочатку міжнародна організація ITU-R розробила стандарт IMT-2020, в якому містилися ключові вимоги до технології нового покоління 5G. Попередній стандарт IMT-Advanced був розроблений для покоління 4G. В новому стандарті визначено нові підвищені вимоги до параметрів систем 5G. Порівняння параметрів для систем 4G і 5G надведено в таблиці 1.1.

Таблиця 1.1 – Основні вимоги до 5G згідно з IMT-2020 в порівнянні з 4G [7]

Параметри	4G	5G
Пікова швидкість завантаження. Гбіт/с	1	20
Швидкість завантаження користувачів, Мбіт/с	10	100
Затримка, мс		
Максимальна швидкість переміщення без втрати сигналу, км/год.	10	1-2
Щільність підключення, пристроїв/кв.км	350	500
Трафік на одиницю площі, Мбіт/с/кв.м	100 тис.	1 млн.

Технологія 5G – це наступне покоління мобільних мереж, яке слідує за технологією четвертого покоління 4G (LTE). При цьому подальший розвиток LTE не припиняється і продовжується розробка нової та розширення існуючої функціональності для цієї технології. Спочатку технологія LTE розроблялася з метою надати високошвидкісну передачу даних на базі IP протоколу. Однак у ході розвитку також було додано функціональність, щоб підтримати нові сфери застосування. Наприклад, можливість масового підключення низькобюджетних пристроїв для Інтернеу речей IoT (Internet of Things), для чого висуваються специфічні вимоги до безпроводових мереж передачі даних, і ці вимоги суттєво відрізняються від встановлених вимог до мереж LTE. На відміну від LTE, технологія 5G розроблена для різних областей застосування.

Прийнято виділяти три основні сфери застосування для мереж 5G [4].

1) Enhanced Mobile BroadBand (eMBB) – надання покращеного широкосмугового мобільного доступу.
2) Massive Machine-Type Communication (mMTC) – можливість підключення дуже великої кількості пристроїв (датчики, лічильники тощо.).
3) Ultra-Reliable and Low-Latency Communication (URLLC) – надання високонадійного з'єднання з низькою затримкою передачі даних.

Розглянемо показники кожної з областей.

Область eMBB (Enhanced Mobile BroadBand) забезпечує надання покращеного мобільного широкосмугового доступу. Це характеризує поступовий

розвиток мереж мобільної передачі. З іншого боку це початкова сфера застосування технології LTE, для якої вона й розроблялася. Технологія 5G повинна забезпечити ще більший рівень обслуговування для абонентів та ще більші швидкості передачі даних. Як цільові значення для швидкості передачі даних в 5G розглядаються десятки гігабіт за секунду (до 20 Гбіт/с в низхідному каналі). Для того, щоб забезпечити такі високі швидкості передачі даних, використовуються дуже широкий канал до 1 – 2 ГГц і багатоантенні технології передачі даних. Практично весь діапазон низьких частот (частоти <6 ГГц) вже розподілений, то щоб мати можливість використовувати канали шириною в кілька сотень МГц або навіть одиниць ГГц для технології 5G передбачається використання міліметрового діапазону частот (наприклад, 28 ГГц). Саме в цьому діапазоні є необхідна кількість вільних частот. Також для технології 5G використовуються і більш низкі частоти сантиметрового діапазону (наприклад, 3,5 ГГц) та частоти нижче 1 ГГц.

Багатоантенні технології дозволяють формувати діаграму спрямованості, що збільшує спектральну ефективність системи, а також розширює зону покриття мережі. Останнє є особливо важливим при використанні частот міліметрового діапазону.

Нижче наводиться орієнтовна таблиця зі швидкостями передачі в залежності від частотного діапазону.

Таблиця 1.2 – Швидкості передачі для різних варіантів частотних діапазонів

Частотний діапазон, ГГц	Ширина канала, МГц	MIMO	Максимальна швидкість передачі даних, Гбіт/с
24 – 28	1000	2x2/ 4x4	10 / 20
3.3 – 4.9	100	4x4	2
<1	20	2x2	0.2

Область застосування mMTC (massive Machine-Type Communication) характеризується можливістю підключення дуже великої кількості дешевих (вартістю не більше 5 доларів) пристроїв. Прикладами таких пристроїв є різні датчики, наприклад, датчики пожежної сигналізації, задимлення, температури, лічильники води, газу, тепла, сенсори, тощо. Крім низької вартості, відмінною

особливістю таких пристроїв є низьке споживання енергії. Це необхідно для того, щоб забезпечити тривалий час (кілька років) роботи від автономних джерел живлення (наприклад, батарейок). Обсяги даних, передані цими пристроями, також незначні. Тому високі швидкості передачі даних у mMTC області не є критичним аспектом.

Область URLLC (Ultra-Reliable and Low-Latency Communication) відрізняється низькими затримками передачі даних (<1 мс в один бік) та високою надійністю та доступністю з'єднання. Прикладами сценаріїв або областей застосування, де висуваються такі вимоги, служать: віддалене управління різними механізмами і роботами, автоматизація виробничих ліній, різні сценарії у сфері безпілотного транспорту (Vehical to Everything V2X), тощо. Для того, щоб забезпечити вимоги, що висуваються даними застосуваннями, у специфікаціях 5G передбачений набір спеціальних механізмів. Наприклад, підтримка так званих міні слотів часу mini-slot, яка дозволяє передавати дані на радіоінтерфейс між базовою станцією (gNB) і абонентським пристроєм (UE) протягом дуже короткого інтервалу часу (долі мс). Крім цього, у технології 5G помітно вищі вимоги до часу обробки даних як на боці базової станції, так і на стороні мобільного терміналу (тобто часу на обробку даних відводиться істотно менше порівняно з тим, що було відведено в технології LTE).

1.2 Основні характеристики мереж 5G

Аналіз областей застосування технології 5G, наведених вище, свідчить про значний набір вимог, що висуваються до цієї новітньої технології. Більше того, деякі галузі застосування висувають певною мірою конфліктуючі між собою вимоги. Це робить розробку 5G специфікацій та подальшу реалізацію цих специфікацій виробниками обладнання вкрай складним та трудомістким завданням. Нижче наведено список основних вимог, яким має відповідати технологія 5G. Варто відзначити, що більшість наведених значень становлять граничні випадки і навряд чи буде можливість досягти всіх цих граничних значень одночасно (наприклад, забезпечити передачу даних зі швидкістю 20 Гбіт/с із затримкою <1 мс для всіх користувачів мережі).

Таблиця 1.3 – Основні характеристики систем 5G

Параметр	Значення	Примітка
Максимальна швидкість передачі даних	DL: 20 Гбіт/с UL: 10 Гбіт/с	Для ідеальних умов (немає помилок при передачі даних), весь радіоресурс використовується одним абонентским пристроєм
Максимальна спектральна ефективність	DL: 30 біт/Гц/с UL: 15 біт/Гц/с	Для ідеальних умов (немає помилок при передачі даних), весь радіоресурс використовується одним абонентским пристроєм
Ширина канала	від МГц до ГГц	
Затримка передачі даних	URLLC: 0,5 мс eMBB: 4 мс	Приведені значення для передачі даних в одну сторону
Надійність передачі даних	URLLC: 1-10-5 eV2X: 1-10-5	Параметр визначає ймовірність успешної передачі X байт даних з заданою затримкою. URLLC: X = 32 байта, затримка 1 мс eV2X: X = 300 байт, затримка 3 – 10 мс
Запас потужності	164 дБ	Параметр MaxCL (Maximum Coupling Loss) – максимальне загасання сигнала, при якому дані могут бути успішно прийняті. Значення MaxCL є різницею між потужністю передавача і чутливістю приймача. MaxCL задано при швидкості передачі даних що дорівнює 160 біт/с

Продовження табл.1.3

Параметр	Значення	Примітка
Час роботи абонентського термінала	>10 років, бажано 15 років	Значення тільки для mMTC. Даний параметр задає час роботи абонентського термінала без підзарядки / заміни батарейок. При цьому передбачається, що об'єм передаваємих даних у висхідному каналі не перевищує 200 байт, а в нисхідному каналі не більше 20 байт в день.
Практичні швидкості передачі даних	DL: 100 Мбіт/с UL: 50 Мбіт/с	
Щільність абонентів	1 000 000 аб/км^2	
Мобільність	500 км/год	Максимальна швидкість руху абонента, при якій дотримуються параметри якості обслуговування (QoS)

1.3 Архітекура мереж 5G

Модель три шарової архітектури мережі 5G представлена на рисунку 1.1.

Ця модель розроблена фірмою Huawei [8].

Модель системи 5G має три шари: перший рівень джерел і функціональний, другий мережевий рівень і третій рівень сервісів.

На першому рівні розташовані безпроводовий і фіксований доступ, що контактують з гранічною хмарою і далі з'єднані з широкосмуговою мережею, яка в свою чергу поєднана з ядром – центральною хмарою. Перший рівень управляється мережевою операційною системою. На другому рівні знаходяться хмари віртуальних функцій VNF і хмари IoT. Третій рівень – це рівень сервісів.

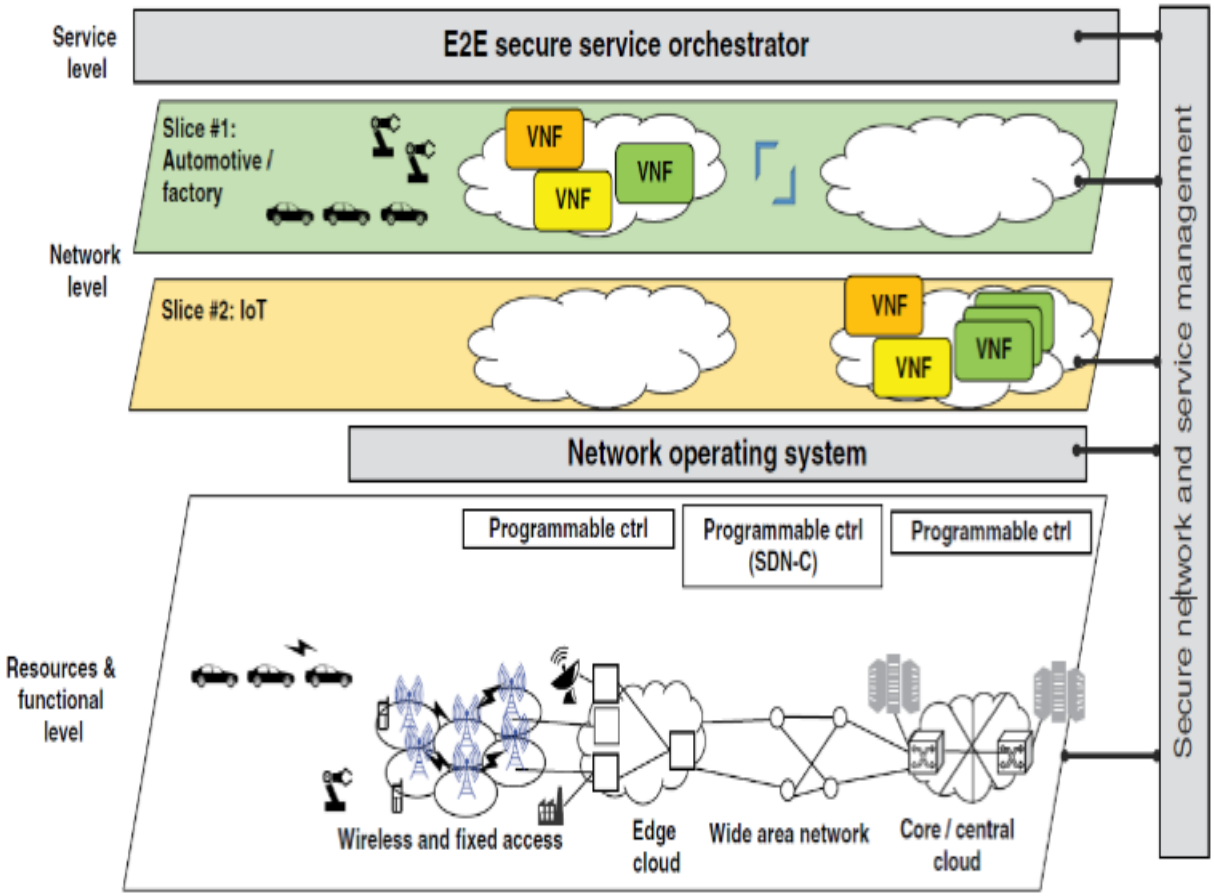

Рисунок 1.1 – Три шарова модель архітектури системи 5G [8]

Схема розгортання мережі 5G показана на рисунку 1.2. Мережа 5G інтегрована з різними мережами, що працюють по окремим технологіям. Використовується два діапазона для роботи апаратури 5G з частотами в одиниці ГГц – це FR1 з великим радіусом соти і з частотами в десятки ГГц – це діапазон FR2. В діапазоні міліметрових хвиль радуіс соти зменшується приблизно до 100 м. Базова станція має зв’язок з інтелектуальним домом Smart Building, медичною мережею Health Network, мережею обслуговування транспортних засобів на мілиметрових хвилях, індустріальними об’єктами M2M, високошвидкісними мобільними користувачами в транспорті, що пересувається з великою швидкістю і має вихід на хмарні сховища, або забезпечує доступ до інших хмарних сервісів.

В технології 5G з надвисокими частотами в міліметровому діапазоні, як правило, використовується багатокористувальницька технологія з великою кількістю антенних елементів на передавальному пристрої базової станції MU – massive MIMO.

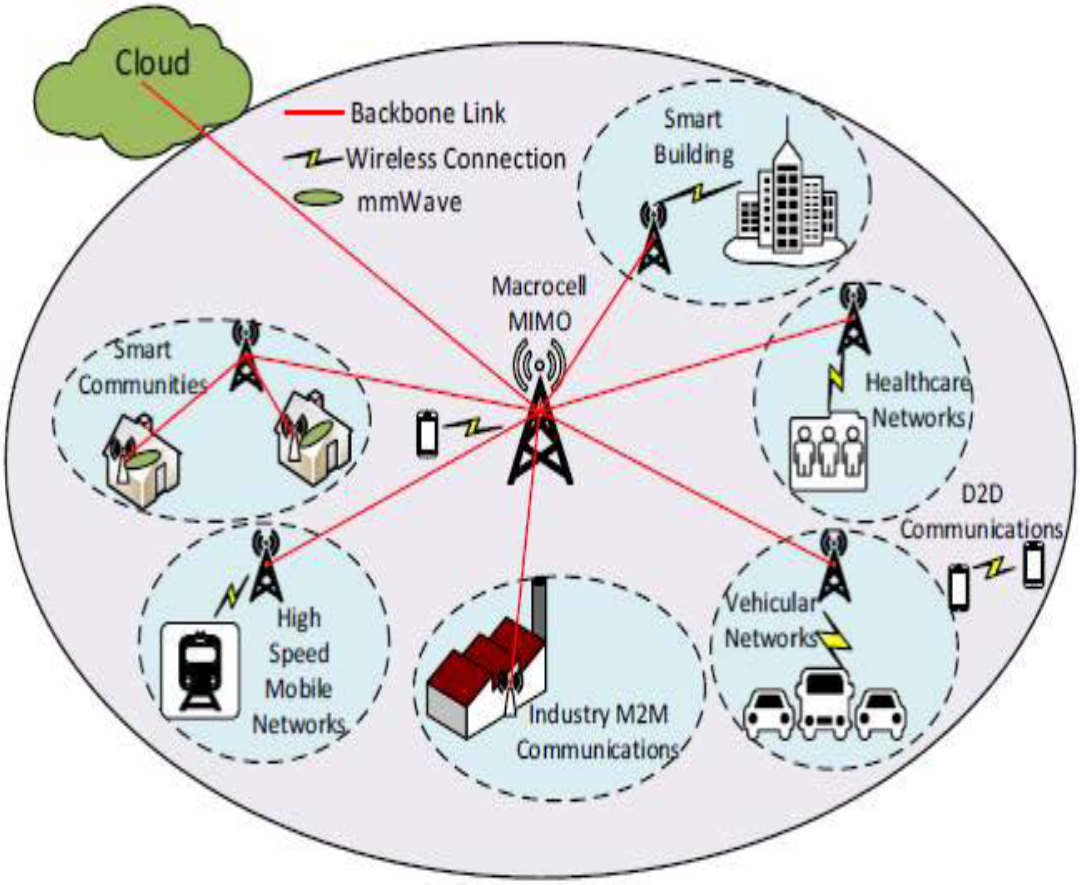

Рисунок 1.2 – Схема розгортання мережі 5G [8]

1.4 Безпека в мережах 5G

Функції безпеки логічно розділені архітектурою безпеки на окремі архітектурні компоненти, відповідно до рекомендацій Міжнародного союзу електрозв'язку ITU-T [9 – 11]. Це дозволяє систематизувати методологію наскрізної безпеки служб, а також допомагає планувати оцінку безпеки поточних мереж і використовувати нові рішення безпеки. Архітектура безпеки 5G пояснюється в останньому випуску технічної специфікації 3GPP, де показано архітектуру безпеки та містить такі ключові домени.

1) Безпека доступу до мережі.

Містить низку параметрів захисту, які дозволяють обладнанню користувача безпечно автентифікувати та отримувати доступ до мережевих ресурсів. Безпека служби вимагає моніторингу систем зв'язку 3GPP і передачі контекстів безпеки від центру до обладнання користувача.

2) Безпека мережевого домену.

Містить низку функцій безпеки, які дозволяють вузлам мережі безпечно обмінюватися сигналами та даними на рівні користувача.

3) Безпека домену користувача.

Включає заходи захисту, які дозволяють користувачам безпечно отримувати доступ до обладнання користувача.

4) Безпека домену програм.

Містить інструменти безпеки, які дозволяють програмам (домени користувачів і постачальників) безпечно обмінюватися повідомленнями.

5) Безпека домену архітектури на основі послуг.

Включає функції безпеки для реєстрації елементів мережі, виявлення та авторизації, а також безпеки інтерфейсів на основі послуг.

6) Видимість і конфігурованість безпеки

Включає сповіщення користувача про те, чи працює функція безпеки.

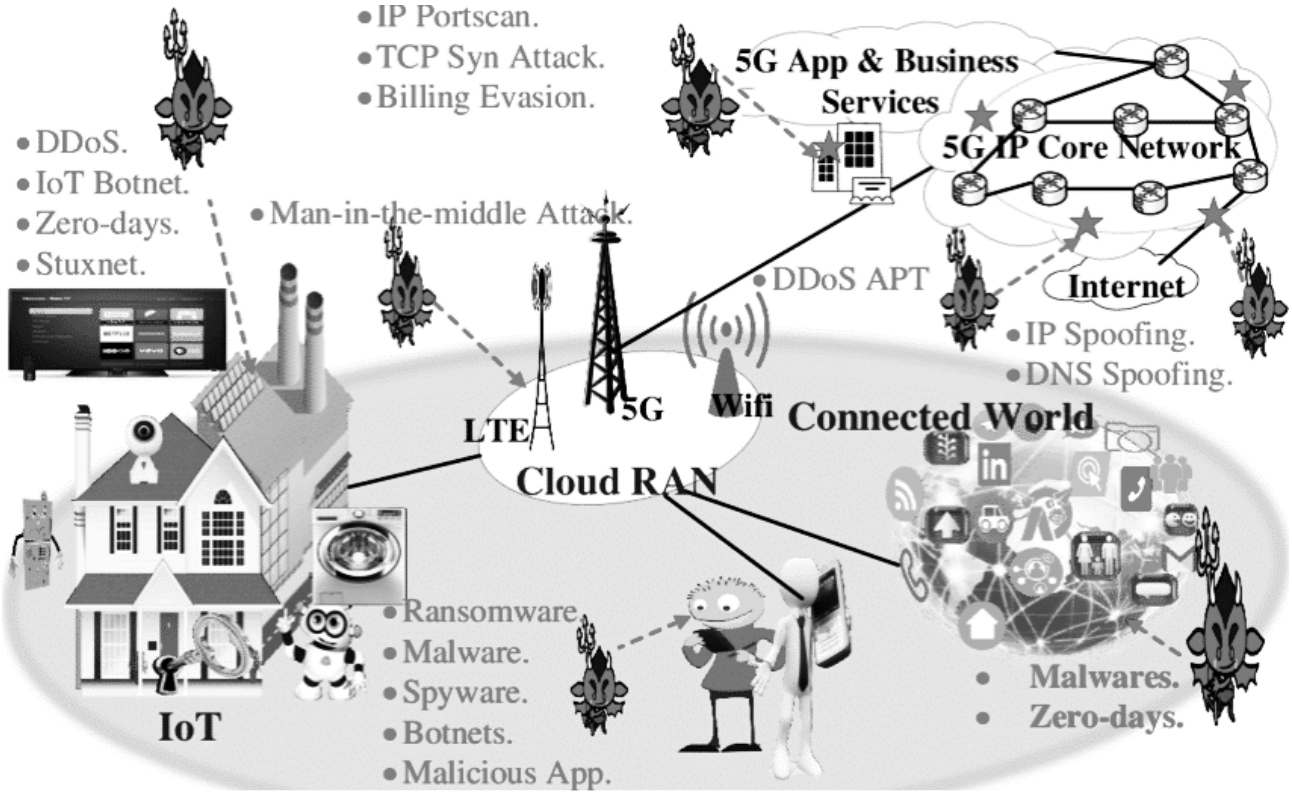

Рисунок 1.3 – Загрози безпеки в мережах 5G інтегрованих з мережами інших технологій [8]

Проблеми безпеки та конфіденційності в 5G можна легко сформулювати, якщо розпізнати ключові технології підтримки 5G. Великі антени MIMO, інтеграція з технологією програмно визначених мереж SDN, технологією

віртуальних мережевих функцій NFV, принципами хмарних мереж, таких як Multi-Access Edge Networking (MEC) є ключовими для розуміння методів захисту систем 5G.

Тому методи безпеки в системах 5G складаються з методів, що стосуються безпеки в massive MIMO, SDN, NFV і безпеки хмарних технологій.

Оскільки очікується, що до майбутньої мережі 5G, яка включає величезну кількість пристроїв Інтернету речей (IoT), буде підключено величезну кількість пристроїв. Це створить нові проблеми безпеки та виклики для мережі 5G. В даний час широко використовуються три протоколи зв'язку, які базуються на криптографічних алгоритмах, наприклад криптосистеми з еліптичною кривою ECC. Інтеграція з мережами доступу, в яких використовуються протоколи зв'язку: IEEE 802.15.4, стандарт IPv6 через малопотужні безпроводові персональні мережі (6LoWPAN) і протокол обмеженого застосування (CoAP) можуть стати суттєвими слабими. З появою квантових обчислень і великої потужності мережі ці протоколи не будуть захищені для зв’язку.

В подальшому функції безпеки, реалізовані в програмному забезпеченні, які можуть бути розгорнуті на будь-якому периметрі мережі, нададуть багато можливостей для посилення безпеки мережі, особливо для віртуалізованих мереж.

1.5 Технологія massive MIMO в 5G і її вразливості

5G FR2 сильно відрізняється від звичайних поколінь, таких як 4G тим, що використовує хвилі міліметрового діапазону mmWave. Нижче наведені переваги та недоліки mmWave у порівнянні з Sub-6 [12 – 17].

Системи 5G FR2 мають такі переваги:

- широку смугу пропускання, що забезпечує одночасно високу швидкість, велику ємність та малу затримку;
- безліч вузьких променів діаграми спрямованості, які легко формуються антенною решіткою, оскільки довжина хвилі коротка, а розмір антен малий.

До недоліків можна віднести:

- високе просторове загасання, що обмежує дальність передачі;
- передача по прямій лінії і, отже, система вимагає прямої видимості шляхів LOS;

- високі втрати при проникненні через скло та стіни, що ускладнюють проходження сигналів;
- довжина ланцюгів для розподілу та подачі сигналів повинна бути зведена до мінімуму, оскільки сигнали сильно спотворюються при проходженні через діелектричні матеріали, а це ускладнює відокремлення активних пристроїв від антенних елементів;
- необхідно замінити фільтри, що працюють на технології ПАР, на інші фільтри, що безпосередньо обробляють електромагнітні хвилі у зв’язку з тим, що робоча частота перевищує допустимий діапазон для приладів на поверхневих акустичних хвилях ПАР.

Оскільки mmWave поширюється лише на короткі відстані, а зв'язок mmWave неможливий в умовах відсутності прямої видимості, необхідно розгортати безліч невеликих стільників з малим покриттям [9].

На рис.1.4 показана антенна система базової станції 5G діапазону FR2.

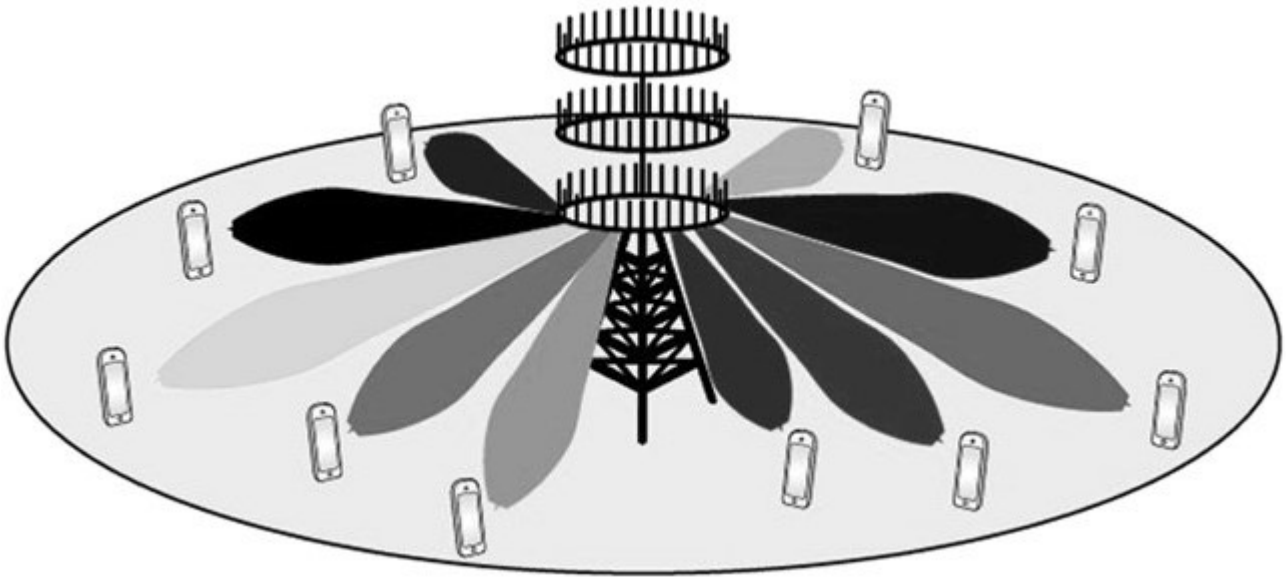

Рисунок 1.4 – Антенна система базової станції 5G діапазону FR2

В системах 5G міліметрового діапазону використовується багатоантенна технологія massiveMIMO (mMIMO). Технологія mMIMO використовує велику кількість антен для передачі та отримання сигналу, що дозволяє покращити пропускну здатність, якість зв'язку та покриття. Проте, існують фактори, які можуть спричинити глушіння сигналу mMIMO, котрими можуть скористатися зловмисники, а саме спробувати створити міжсимвольну інтерференцію.

Сигнали від інших пристроїв або мереж можуть створювати інтерференцію з сигналом mMIMO, особливо в мережах, що активно використовуються. При високих швидкостях передачі даних в 5G, символи стають дуже короткими, а вплив каналу може спричинити їх розмиття. Це може призвести до перекриття сигналів, відповідних різним символам, і створення міжсимвольної інтерференції. Тому використання технології mMIMO окрім позитивних якостей має вразливості до глушіння. Наявність багатої кількості променів дозволяє кожним променем покривати частину площі навколо базової станції і обслуговувати певну кількість користувачів або окремого користувача вузьким променем і таким чином збільшити загальну кількість користувачів.

Поділ користувачів на групи, що обслуговуються різними променями дає також можливість збільшити захист від взлому зловмисниками. Але з іншого боку така технологія вразлива до глушіння.

2 МЕТОДИ ЗАХИСТУ МЕРЕЖІ 5G

2.1 Забезпечення безпеки на основі захищеного Internet протоколу

Протокол IPsec заведено використовувати у не сервісно-орієнтованих інтерфейсах між базовою станцією gNB і ядром 5G. Прикладами таких інтерфейсів можна назвати N2, N3, Xn, E1 та F1. У цьому випадку, IPsec є необхідним компонентом безпеки в мережах 5G, де забезпечення безпеки та захисту даних є критично важливим завданням [6].

Протокол IPsec є набором протоколів та алгоритмів, призначених для забезпечення безпеки та захисту комунікації в мережах на основі Internet Protocol (IP). IPsec надає механізми для шифрування, аутентифікації та цілісності даних, що передаються мережею.

IPsec складається з двох основних протоколів: протоколу аутентифікації заголовка AH і протоколу шифрування пакетів ESP. AH використовується для забезпечення цілісності, аутентифікації та захисту від перебірки пакетів. ESP забезпечує шифрування та конфіденційність даних, а також можливість перевірки цілісності.

У мережах 5G IPsec використовується для забезпечення безпеки та конфіденційності комунікації. Основними функціями IPsec в 5G можна назвати наступні:

- шифрування даних;
- аутентифікація;
- цілісність даних;
- захист від повторного використання;
- керування ключами.

Ціллю шифрування даних протоколом IPsec є забезпечення конфіденційності даних, що передаються мережею 5G. Саме це забезпечує захист від несанкціонованого доступу до інформації. Аутентифікація впроваджується для перевірки ідентичності комунікуючих сторін, що дозволяє впевнитися, що комунікація відбувається між вірними сторонами та запобігає атакам підробки. Цілісність даних під час передачі досягається використанням хеш-функції. Це дозволяє виявляти будь-які зміни або модифікації даних, що могли б статися під час передачі. Захист від повторного використання перешкоджає атакам, які

базуються на повторній передачі пакетів для здійснення несанкціонованих дій. Функція керування ключами дозволяє виконувати безпечний обмін ключами між комунікуючими сторонами. В результаті, це забезпечує конфіденційність та цілісність ключів, використовуваних для шифрування та розшифрування даних.

Виходячи з положень стандарту 3GPP TS 33.210, шлюзи безпеки є невіддільною частиною архітектури NDS/IP, тому має підтримуватися тунельний режим. Для міждоменного зв'язку NDS/IP слід використовувати шлюзи безпеки. У цьому випадку застосовується лише тунельний режим. Також необхідно дотримуватися вимог щодо відповідності реалізації для операцій з шифрування ESP, включаючи шифрування з аутентифікацією згідно RFC 8221. У той же час для аутентифікації має підтримуватися AES-GMAC з AES-128.

З IPsec також впроваджено Internet Key Exchange version 2 (IKEv2), що є протоколом, який використовується для безпечного обміну ключами та налаштування безпеки в IPsec. Він є покращеною версією попереднього протоколу IKE і забезпечує швидку та надійну установку захищеного з'єднання між комунікуючими сторонами.

Роль IKEv2 в мережах 5G полягає в налагодженні безпечних тунелів IPsec та керуванні ключами між сутностями мережі. В основі мереж 5G лежить концепція віртуалізованих мережевих функцій Virtual Network Function (VNF), що дозволяє гнучко налаштовувати та керувати мережевими ресурсами. У такому випадку IKEv2 відіграє важливу роль і завдяки підтримці різних методів ідентифікації, таких як ідентифікація на основі сертифікатів, ідентифікація на основі приватних ключів та ідентифікація з використанням імені користувача та пароля, дають можливість використовувати різні механізми залежно від потреби та конфігурації мережі. IKEv2 ще забезпечує підтримку мобільності та роумінгу, що досягається дозволом зберігати безпекові асоціації та ключі під час переміщення між різними мережевими вузлами, в результаті чого зберігається безперебійна комунікація.

В 3GPP TS 33.210 для різних функціонуючих профілів IKEv2 вводяться різні алгоритми. Наприклад, для IKE_SA_INIT exchange підтримуються наступні алгоритми:

- AES-GCM з 16 октетом ICV і довжиною ключа 128 біт, що забезпечує конфіденційність;
- PRF_HMAC_SHA2_256 для формування псевдовипадкової функції:;
- AUTH_HMAC_SHA256_128, що забезпечує цілісність;
- група Діффі-Геллмана 19, що формує 256-бітну випадкову групу ECP.

Задля покращень параметрів безпеки, слід підтримувати наступні алгоритми за стандартом:

- AES-GCM з 16 октетом ICV і довжиною ключа 256 біт;
- PRF_HMAC_SHA2_384;
- група Діффі-Геллмана 20, шо формує 384-бітну випадкову групу ECP.

З міркувань безпеки використання груп MODP Діффі-Геллмана менше ніж в 2048 біт не підтримується.

Для алгоритмів автентифікації IKE_AUTH exchange потрібно виконувати наступні вимоги:

- має підтримуватися код цілісності спільного ключа, що є другим методом аутентифікації;
- для ідентифікації повинні підтримуватися IP-адреси та повні доменні імена FQDN;
- згідно з рекомендаціями RFC 7296 має підтримуватися перекодування IPsec SA та IKE SA;
- зміна ключа не повинна призводити до помітного погіршення якості обслуговування.

2.2 Забезпечення безпеки на рівні транспортного протоколу

Серед сервісно-орієнтованої архітектури усі інтерфейси на основі послуг мають бути захищені за допомогою Transport Layer Security (TLS).

TLS є протоколом безпеки, який забезпечує захищеність комунікацій між клієнтом і сервером через канал. Він забезпечує конфіденційність, цілісність та аутентифікацію даних, що передаються між комунікуючими сторонами. У мережах 5G TLS виконує важливу роль у забезпеченні безпеки комунікації на рівні транспортного протоколу.

Шифрування даних TLS відбувається не асиметрично на етапі аутентифікації, а симетрично заради захисту конфіденційності даних, що передаються між клієнтом і сервером.

TLS включає механізми аутентифікації, що дозволяють перевірити ідентичність сервера та клієнта. Це забезпечує довіру між сторонами та запобігає атакам підробки. Перевірка цілісності даних під час передачі відбувається в TLS завдяки хеш-функції, так само подібним образом це відбувається в протоколі

IPsec. Для операцій саме з довіреними сторонами використовуються сертифікати, котрі введені для підтвердження довіри до ідентичності сервера та клієнта.

Ще одним пунктом у функціях можна назвати підтримку прозорості та проксі-серверів. TLS може працювати з проксі-серверами, що дозволяє розширювати мережеві можливості та забезпечувати безпеку комунікації через проміжні вузли.

У профілях TLS, дозволених для 5G, авторизовані набори шифрів представляють усі функції аутентифікованого шифрування з асоційованими даними (AEAD). Між мережевими функціями використання TLS без шифрування не дозволяється. Рекомендованими криптографічними алгоритмами для симетричного шифрування є AES-128 або AES 256. Реалізації ECDH мають мінімальну довжину ключа 255 біт, а реалізації DHE мають мінімальну довжину ключа 2048 біт і повинна підтримуватися довжина ключа 4096 біт.

В 3GPP TS 33.210 реалізовані вимоги до TLS 1.3 та TLS 1.2. Доцільно розглядати підтримку обмежень та розширень для TLS 1.3, котра є найновішою версією цього протоколу [9].

Для виконання рекомендацій з безпеки потрібно:

- необхідно забезпечити підтримку обміну ключами з secp384r1, а для наборів шифрів TLS і групи Діффі-Геллмана слід дотримуватися вимог стандарту TLS 1.3 RFC 8446.;
- в схемах підпису TLS має підтримуватися функція ecd-sa_secp384r1_sha384;
- для розширення TLS слід дотримуватися вимог стандарту TLS 1.3 RFC 8446;
- розширення запиту статусу сертифіката OCSP слід підтримувати у протоколі згідно з рекомендаціями RFC 6066 і RFC 8466.

2.3 Проксі-сервер для забезпечення безпеки в роумінгу

5G використовує власний проксі-сервер, який має назву SEPP. SEPP відповідає за фільтрацію та передачу повідомлень між сервісно-орієнтованою та домашньою мережами, а також дозволяє операторам досягти наскрізної конфіденційності та цілісності для визначених елементів повідомлень. SEPP визначається як обов'язкова функція для з’єднання 5G мереж типу Standalone (SA), що зазначається в міжнародних стандартах 5G [10].

SEPP приховує топологію своєї внутрішньої мережі від інших мереж і може аутентифікувати інший SEPP з яким увійшло в контакт. Такий підхід забезпечує конфіденційність сервера при з’єднанні з ненадійною мережею і таким самим ненадійним SEPP, котра може бути під контролем осіб з корисливими намірами.

SEPP забезпечує функціональність сигнального ядра 5G завдяки двом окремим інтерфейсам – інтерфейсу узгодження безпеки N32c і наскрізно зашифрованому інтерфейсу програми N32f, між котрими безпека виконується завдяки протоколу TLS. Опціонально може виконуватися інкапсуляція сигнальних повідомлень ядра HTTP/2 з використанням захисту JOSE для передачі N32-f Protocol for N32 Interconnect Security (PRINS) [8]. SEPP також забезпечує надійність проміжних вузлів IP exchange (IPX), що є моделлю взаємозв'язку для обміну трафіком на основі IP у процесі роумінгу, для читання та зміни конкретних інформаційних елементів в повідомленні HTTP, при цьому повністю захищаючи конфіденційну інформацію при застосуванні PRINS.

Ще одним елементом SEPP є фреймворк авторизації з використанням OAuth2 протоколом, що призначений для організації доступу клієнтських програм до ресурсів, або даних облікових записів користувача на іншому сервісі.

2.4 Багатокористувальницька технологія масивного MIMO і особливості її безпеки

В системах 5G класична система MIMO зазнала суттєвих змін. На рисунку 2.1 представлена узагальнена схема класичного MIMO.

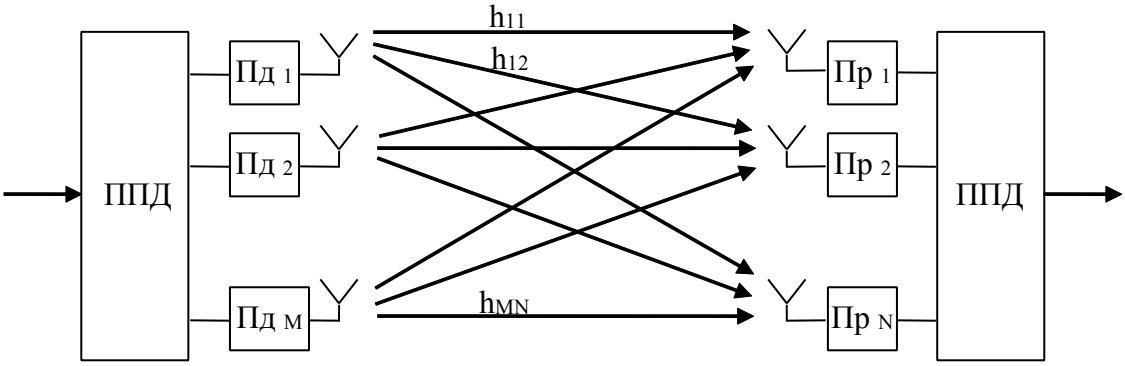

Рисунок 2.1 – Узагальнена схема класичного MIMO

Вхідний потік цифрової інформації розбивається на декілька паралельних потоків, кожен з яких подається на окремий передавач і далі на окрему антену або на багатопроменеву антенну гратку, що формує декілька просторових каналів.

Прийняті сигнали з окремих просторових каналів приймаються приймачами і далі об’днуються в блоці перетворення паралельних потоків в один послідовний.

За рахунок формування просторових каналів зростає пропускна здатність системи зв’язку.

Матрицю стовпець U_T сигналів передавального пристрою з N канальних передавачів і матрицю стовпець U_R приймального пристрою з N канальних приймачів можна записати у вигляді:

$$U_T = \begin{bmatrix} U_{T1} \\ U_{T2} \\ ? \\ U_{TN} \end{bmatrix}, \tag{2.1}$$

$$U_R = \begin{bmatrix} U_{R1} \\ U_{R2} \\ ? \\ U_{RN} \end{bmatrix}. \tag{2.2}$$

Передаточна функція багатопроменевого каналу описується матрицею H.

$$H = \begin{bmatrix} h_{11} & h_{12} & ? & h_{1N} \\ h_{21} & h_{22} & ? & h_{2N} \\ ? & ? & ? & ? \\ h_{M1} & h_{M2} & ? & h_{MN} \end{bmatrix}, \tag{2.3}$$

де $h_{i\,j}$ – передаточна функція між і-ю передавальною та j-ою приймальною антеною.

Сигнали прийняті антенами на приймальному кінці лінії зв'язку пов'язані з сигналами на передавальному кінці матричним співвідношенням:

$$U_R = H \cdot U_T . \tag{2.4}$$

Визначити, які сигнали були передані можна за допомогою пристрою, встановленого на стороні приймача системи зв'язку який вирішує систему з N лінійних рівнянь з N невідомими. У матричній формі рішення має вигляд:

$$U_T = H^{-1} \cdot U_R . \tag{2.5}$$

Для вирішення задачі необхідно знати матрицю передачі H. Значення елементів матриці H можна визначити, наприклад, посилаючи відомий тестовий (пілотний) сигнал по черзі через кожну з передавальних антен при вимкнених інших і заміряючи рівні сигналу на всіх приймальних антенах в кожному випадку.

Система рівнянь існує, якщо ранг матриці дорівнює 2 чи більше. При ранзі рівному 1 система вироджується в одноканальну. Ранг матриці системи MIMO не може перевищувати min{M,N}, де M – число передавальних, а N – число приймальних антен. Число антен на передачі та на прийомі не обов'язково рівне.

Існує така класифікація.

1) MIMO (Multi Input Multi Output) для M>1, N>1; M=N; M>N; M<N.
2) MISO (Multi Input Single Output) для M>1, N=1.
3) SIMO (Single Input Multi Output) для M=1, N>1
4) SISO (Single Input Single Output) для M=1, N=1 (випадок виродження MIMO в одноканальну систему).

Ранг матриці залежить не тільки від числа передавальних та приймальних антен. Збільшення ступеня кореляції елементів у матриці каналу MIMO призводить до зменшення рангу матриці, а кореляція у свою чергу залежить як від параметрів антен та їх просторового рознесення, так і від розподілу угруповання об'єктів у просторі між антенними структурами на передавальній та приймальній стороні системи. В даному випадку розглядаються тільки ті об'єкти, які можуть викликати явища відбиття, розсіювання, заломлення та дифракції хвиль. В

результаті сумарної дії цих об'єктів або їх угруповання у просторі вони впливають на ступінь кореляції елементів матриці.

Існує два основних типи MIMO: однокористувальницький Single User (SU) і багатокористувальницький Multi User (MU). У системах SU-MIMO потоки даних можуть одночасно взаємодіяти лише з одним пристроєм у мережі. Таким чином, системи MU-MIMO перевершують SU-MIMO, що можна спостерігати на рис. 2.2.

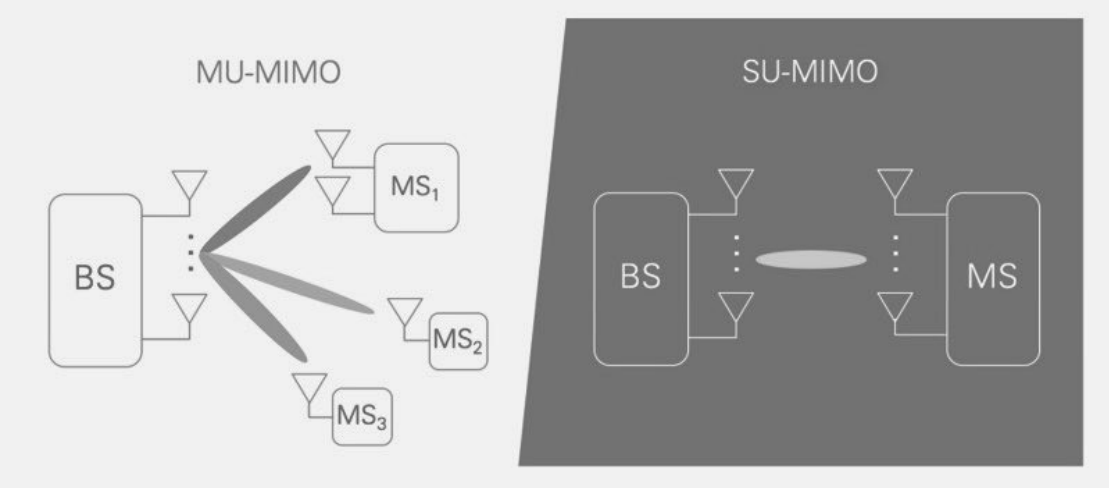

Рисунок 2.2 – Узагальнена схема MU-MIMO і SU-MIMO [15]

Математична модель систем SU-MIMO і MU-MIMO представлена на рисунку 2.3.

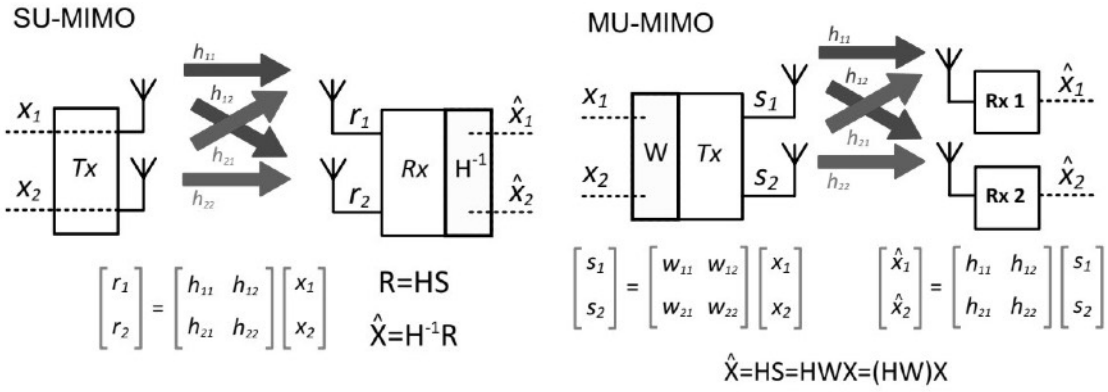

Рисунок 2.3 – Математична модель систем SU-MIMO і MU-MIMO [15]

На слідуючому етапі розвитку технології MIMO кількість антенних елементів на передавальному кінці системи зв’язку була суттєво збільшена. Це дозволило формувати надвузькі діаграми спрямованості від передавального

пристрою базової станції. Висока концентрація енергії в головному пелюстку діаграми спрямованості збільшувала радіус соти, що особливо важливо для діапазону міліметрових хвиль. Системи з великою кількістю антенних елементів на передачу назвали технологією massive MIMO. Трансформацію технології MIMO можна побачити на рис. 2.4.

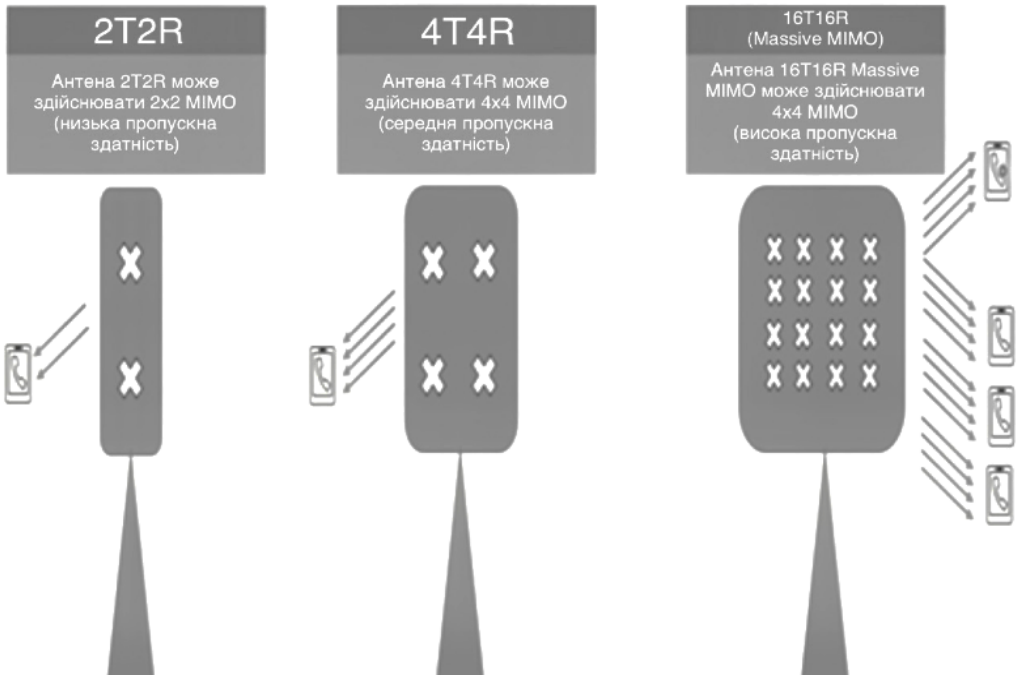

Рисунок 2.4 – Трансформація технології MIMO

Одночасно з впровадженням технології massive MIMO було інтегровано її з багатокористувальницькою технологією. Така технологія получила назву MU-MIMO, схему якої можна побачити на рис. 2.5.

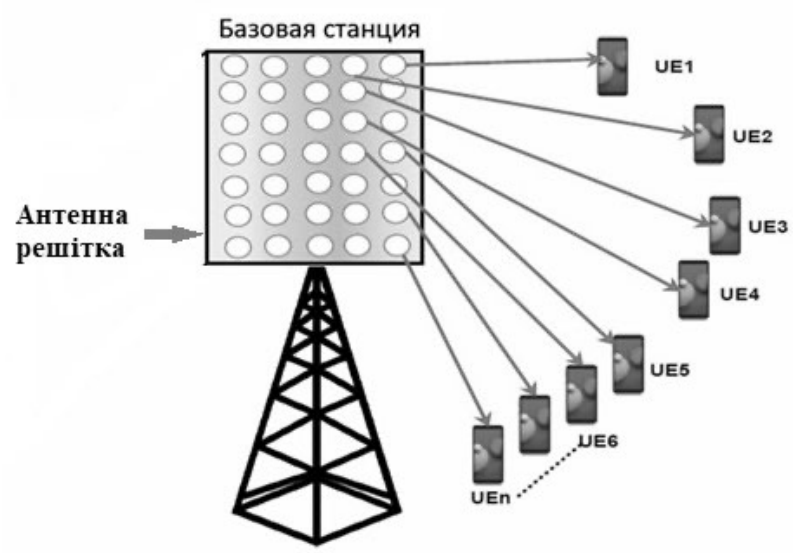

Рисунок 2.5 – Схема системи MU-MIMO

Суттєве збільшення кількості антенних елементів в антенній решітці забезпечило збільшення радіусу дії системи зв’язку, що має суттєве значення для міліметрового діапазону радіохвиль з великим загасанням хвиль в цьому діапазоні.

Особливо важливим в технології MU-massive MIMO є формування окремих променів на апаратуру користувача, що представлено на рис. 2.6.

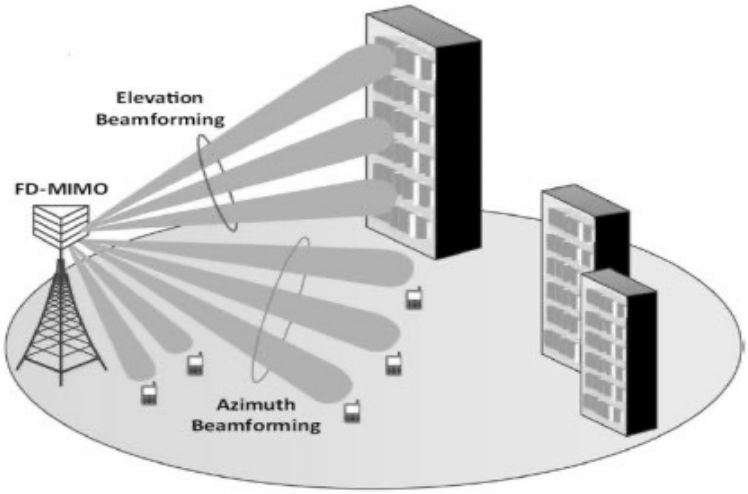

Рисунок 2.6 – Формування окремих променів на апаратуру користувача в технології MU-massive MIMO

Для виконання поставлених задач по формуванню променів на кожного користувача треба мати зворотній зв’язок. На рис. 2.7 представлена система зворотнього зв’язку.

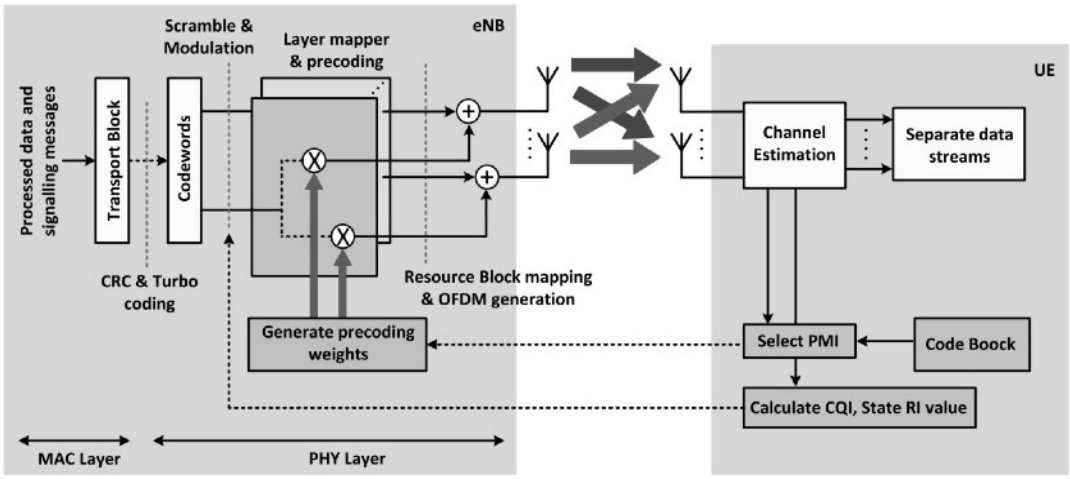

Рисунок 2.7 – Система зворотнього зв’язку [15]

Наявність зворотнього каналу для передачі службової інформації, що забезпечує позиціонування променів і передачу багатьох кількісних параметрів, відкриває шлях для атак для зловмисників, якого не було у попередніх поколінь технологій зв’язку.

2.5 Особливості DoS і DDoS атак на системи 5G

Нове покоління стільнікових систем 5G надає користувачам можливості передачі інформації з значно більшими швидкостями в порівнянні з попереднім поколінням. Це збільшує можливості зловмисників для здійснення DoS і DdoS атак тому, що розсилки спаму суттєво прскорюються. Особливо слід звернути увагу на використання зловмисниками ботнетів типу Mirai. Такі ботнети, запущені з одного джерела, призводять до лавино подібного завантаження спаму за рахунок поступового зараження вузлів, які, в свою чергу, стають джерелами атак.

Тому розгляд особливостей DoS і DDoS атак на системи 5G є актуальними.

2.5.1 Атаки на об’єкти інфраструктури.

Типові атаки на рівні інфраструктури є DDoS-атаки, атаки з відбиттям протоколу користувацьких дейтаграм UDP та SYN-флуд. Зловмисник може використовувати будь-який з цих методів, щоб генерувати великі обсяги трафіку, які можуть переповнити пропускну здатність мережі або зв'язати ресурси таких систем, як сервери, брандмауери, системи запобігання вторгненням IPS або

балансувальники навантаження. Хоча ці атаки легко ідентифікувати, для їх ефективної протидії необхідно мати мережу або системи, які можуть нарощувати пропускну здатність швидше, ніж вхідний потік трафіку. Ця додаткова пропускна здатність необхідна для фільтрації або поглинання атакуючого трафіку, звільняючи систему і додатки для реагування на легальний трафік клієнтів.

2.5.2 Атака UDP reflection.

Атаки UDP reflection використовують той факт, що UDP є протоколом без стану. Тобто, UDP не гарантує доставку повідомлень, та відправник не запам'ятовує стан вже відісланих повідомлень. Зловмисники створюють дійсний пакет запиту UDP, вказуючи як адресу відправника IP-адресу цілі атаки. Зловмисник підробляє IP-адресу джерела пакету запиту UDP. UDP-пакет містить підроблену IP-адресу джерела і надсилається зловмисником на проміжний сервер. Таким чином, відповіді сервера у вигляді UDP пакетів змушують надіслати на цільову IP-адресу жертви, а не назад на IP адресу зловмисника. Проміжний сервер використовується тому, що він генерує відповідь, яка в кілька разів перевищує розмір пакету запиту, ефективно посилюючи обсяг атакуючого трафіку, що надсилається на цільову IP адресу. Коефіцієнт посилення – це відношення розміру відповіді до розміру запиту, і він змінюється залежно від того, який протокол використовує зловмисник: DNS, Network Time Protocol (NTP), Simple Service Discovery Protocol (SSDP), Connectionless Lightweight Directory Access Protocol (CLDAP), Memcached, Character Generator Protocol (CharGen) або Quote of the Day (QOTD). Наприклад, коефіцієнт підсилення для DNS може в 28-54 разів перевищувати початкову кількість байт. Таким чином, якщо зловмисник надсилає на DNS-сервер запит з корисним навантаженням 64 байти, він може згенерувати понад 3400 байт небажаного трафіку на ціль атаки. Атаки з відбиттям UDP трафіку генерують більші обсяги трафіку порівняно з іншими атаками. Рисунок 2.8 ілюструє тактику відбиття та ефект посилення.

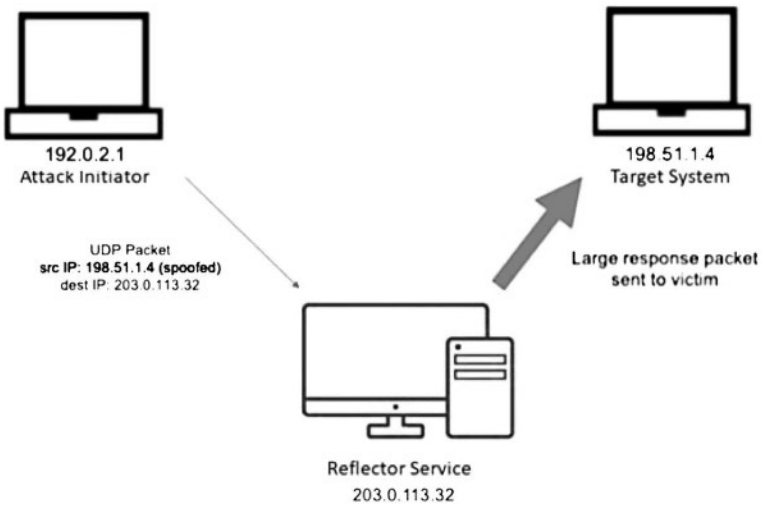

Рисунок 2.8 – Діаграма, що відображає атаку з відображенням UDP

2.5.3 Атака SYN-FLOOD.

SYN-флуд є специфічною формою мережевої атаки, яка відноситься до категорії DDoS. Вона включає надсилання великої кількості запитів SYN, що є частиною процедури встановлення з'єднання в TCP, протягом короткого періоду часу, щоб перевантажити цільову систему.

Коли користувач підключається до служби протоколу управління передачею TCP, наприклад, до веб-сервера, його клієнт надсилає SYN-пакет. Сервер повертає пакет підтвердження синхронізації SYN-ACK, і, нарешті, клієнт відповідає пакетом підтвердження ACK, що завершує очікуване тристороннє рукостискання. На рис. 2.9 ілюструється типове рукостискання.

Під час SYN-флуд атаки зловмисний клієнт надсилає велику кількість SYN пакетів, але ніколи не надсилає фінальні ACK пакети для завершення рукостискання. Сервер залишається в очікуванні відповіді на напіввідкриті TCP з'єднання і зрештою вичерпує свою пропускну здатність для прийняття нових TCP з'єднань. Це може призвести до того, що нові користувачі не зможуть підключитися до сервера. Атака намагається зв'язати доступні серверні з'єднання так, щоб ресурси були недоступні для легальних з'єднань. Хоча SYN-флуд може досягати сотень мільярдів біт в секунду (Гбіт/с), основною метою атаки не є збільшення обсягу SYN трафіку.

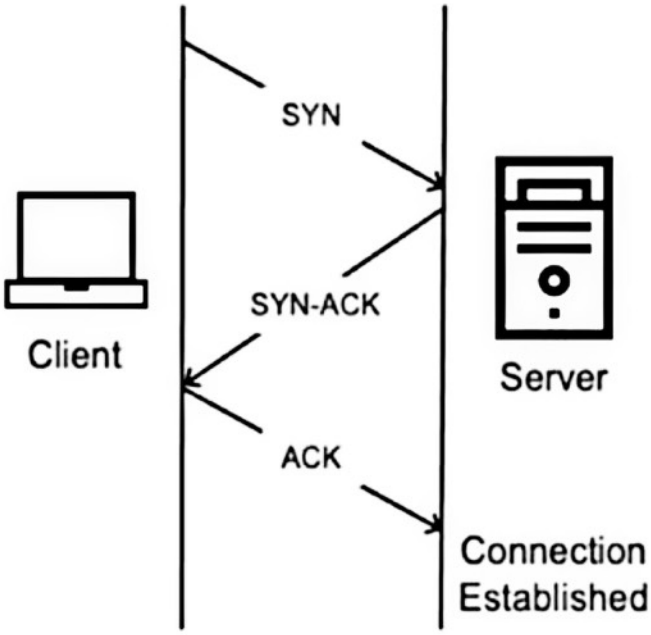

Рисунок 2.9 – Схема, що зображує тристороннє рукостискання SYN

2.5.4 Атака Ping flood.

Атака Ping-флуд – типовий приклад атаки через протокол ICMP, поряд із ping flood та атакою Smurf. Швидкість роботи комп'ютерів, які потрапляють під такі атаки, значно знижується, що впливає на всі додатки, які використовують Інтернет, а також призводить до проблем з підключенням до Інтернету.

Подібно до UDP атаки, Ping-флуд атака переповнює цільовий ресурс так званими пакетами ICMP (Echo Request ping), зазвичай надсилаючи пакети якомога швидше, не чекаючи відповідей. Цей тип атаки може споживати як вхідну, так і вихідну смугу пропускання, оскільки сервери жертви часто намагаються відповісти пакетами ICMP Echo Reply, що призводить до значного уповільнення роботи системи.

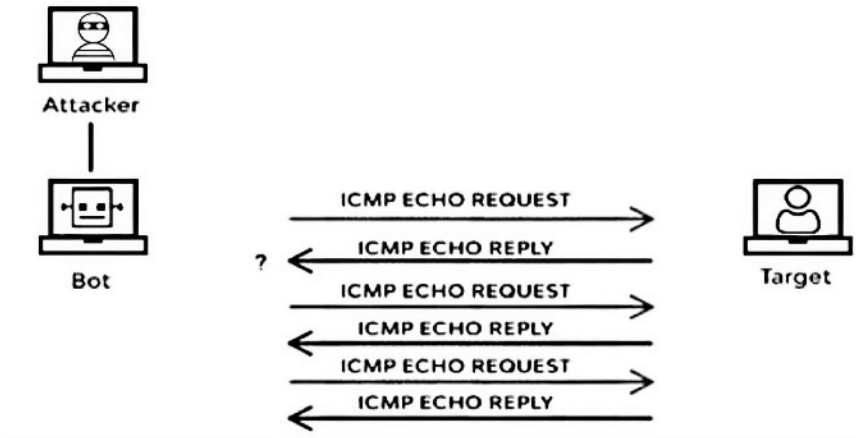

Рисунок 2.10 – Потік пакетів ICMP Ping

2.5.5 Атака Ping of death.

Атака Ping смерті (POD – Ping of Death) – тип атаки відмови у обслуговуванні (DoS). Вона полягає в тому, що зловмисник надсилає на комп'ютер кілька зловмисних або неправильно сформованих пінгів. Максимальна довжина IP пакету (включаючи заголовок) становить 65535 байт. Однак на канальному рівні часто встановлюються обмеження на максимальний розмір кадру - наприклад, 1500 байт у мережі Ethernet. У цьому випадку великий IP пакет розбивається на різні частини IP пакетів (фрагменти), а хост-одержувач знову збирає IP фрагменти в повний пакет.

У сценарії "пінг смерті" після зловмисного маніпулювання вмістом фрагментів одержувач отримує IP пакет, розмір якого перевищує 65535 байт при повторному складанні. Це може перевищити буфери пам'яті, призначені для пакета, що спричиняє відмову в обслуговуванні легітимних пакетів.

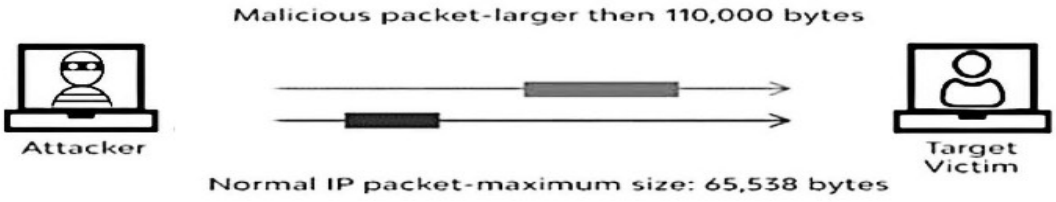

Рисунок 2.11 – Атака Ping of death

2.5.6 Атаки прикладного рівня.

Атаки прикладного рівня можуть бути або DoS, або DDoS-загрози. Зловмисник може націлитися на сам додаток, використовуючи атаку на сьомому (прикладному) рівні. Прикладний рівенб є найіищим та відповідає за відправлення та отримання даних між програмою та мережею. У цих атаках, подібно до атак на інфраструктуру SYN-flood, зловмисник намагається перевантажити певні функції програми, щоб зробити її недоступною або такою, що не реагує на запити легальних користувачів. Іноді цього можна досягти за допомогою дуже малих обсягів запитів, які генерують лише невеликий обсяг мережевого трафіку. Це може ускладнити виявлення та усунення наслідків атаки. Прикладами атак на прикладному рівні є HTTP флуди, атаки на кеш-пам'ять та XML-RPC флуди типу WordPress.

Під час атаки HTTP флуду зловмисник надсилає HTTP запити, які виглядають як такі, що надходять від дійсного користувача веб додатку. Деякі HTTP атаки націлені на певний ресурс, тоді як більш складні HTTP атаки намагаються імітувати взаємодію людини з додатком. Це може ускладнити використання поширених методів захисту, таких як обмеження швидкості запитів.

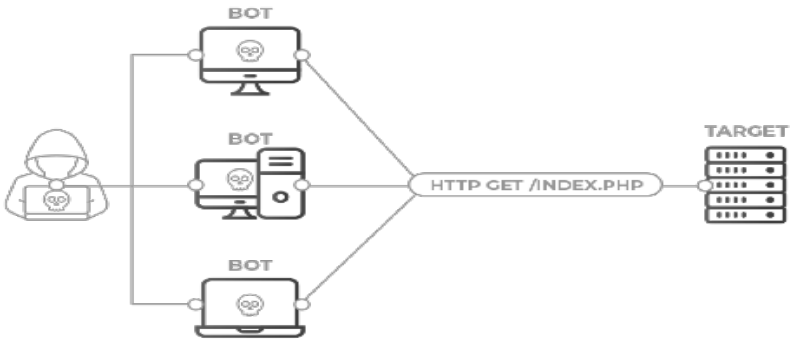

Рисунок 2.12 – Атака HTTP-флудом

Атаки на переповнення кешу – це різновид HTTP флуду, який використовує варіації в рядку запиту, щоб обійти кешування мережі доставки контенту CDN. Замість того, щоб повертати кешовані результати, CDN повинна зв'язуватися з сервером джерелом для кожного запиту сторінки, і ці запити спричиняють додаткове навантаження на веб сервер додатку.

Так звана атака Slowloris вирізняється з-поміж інших тим, що вимагає дуже низької пропускної здатності і може бути здійснена за допомогою лише одного комп'ютера. Вона працює шляхом ініціювання декількох паралельних з'єднань з

веб сервером і утримання їх відкритими протягом тривалого періоду часу. Зловмисник надсилає часткові запити і час від часу доповнює їх HTTP-заголовками, щоб переконатися, що вони не дійшли до стадії завершення. В результаті сервер виснажується, і він більше не може обробляти з'єднання від легітимних клієнтів.

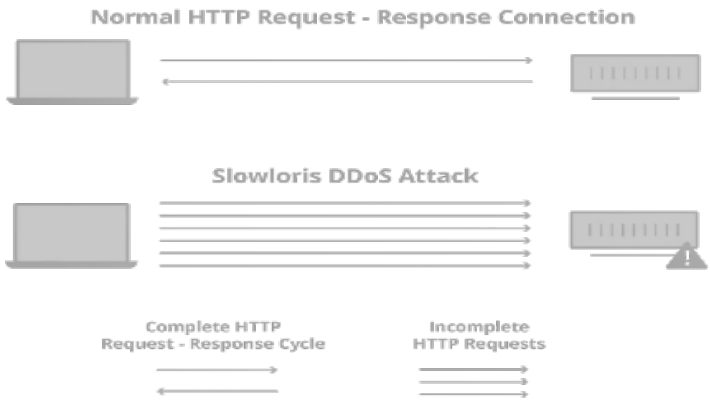

Рисунок 2.13 – Атака Slowloris

2.5.7 Атаки на систему доменних імен.

Серед відомих атак на DNS виділяють атаки переповнення і ампліфікації.

Атака переповнення DNS або DNS-флуд – це тип розподіленої атаки на відмову в обслуговуванні DDoS, коли зловмисник переповнює DNS-сервери певного домену, намагаючись порушити дозвіл DNS для цього домену, як представлено на рис. 2.14. Роздільна здатність DNS (DNS resolution) – це процес, в ході якого імена доменів перетворюються в IP-адреси, які використовуються для маршрутизації інтернет-трафіку. Порушуючи роздільну здатність DNS, атака переповнення DNS ставить під загрозу здатність інтернет-ресурсів, API або веб додатку відповідати на легальний трафік. Атаки DNS-флуду буває важко відрізнити від звичайного великого трафіку, оскільки такий обсяг трафіку часто надходить з безлічі унікальних місць, запитуючи реальні записи в домені, імітуючи легальний трафік.

DDoS атака ампліфікації DNS – об'ємна розподілена DDoS-атака на основі відображення, в якій зловмисник використовує функціональність відкритих DNS розпізнавачів, щоб перевантажити цільовий сервер або мережу збільшеним обсягом трафіку, роблячи сервер і його навколишню інфраструктуру недоступними.

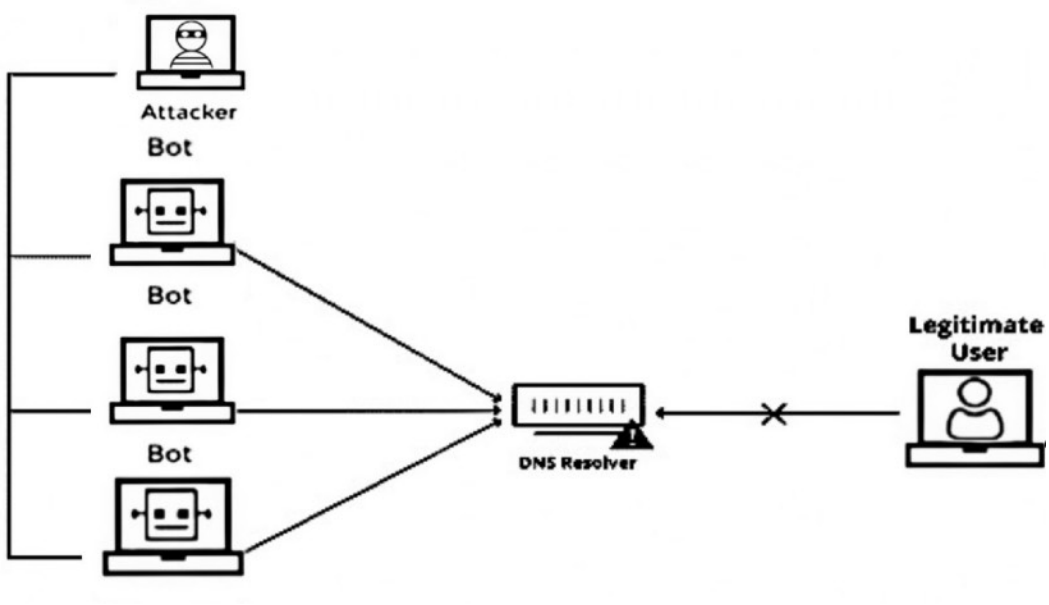

Рисунок 2.14 – Атака переповнення DNS

Усі атаки з ампліфікацією використовують невідповідність у споживанні пропускної здатності між зловмисником та інтрнет-ресурсом, на який спрямована атака. Надсилаючи невеликі запити, які призводять до великих відповідей, зловмисник може отримати більше при менших витратах. Посилюючи це збільшення за рахунок того, що кожен бот у бот мережі надсилає схожі запити, зловмисник одночасно приховує свої дії від виявлення та отримує вигоду від значного збільшення трафіку атак. Атака ампліфікаією представлена на рис. 2.15.

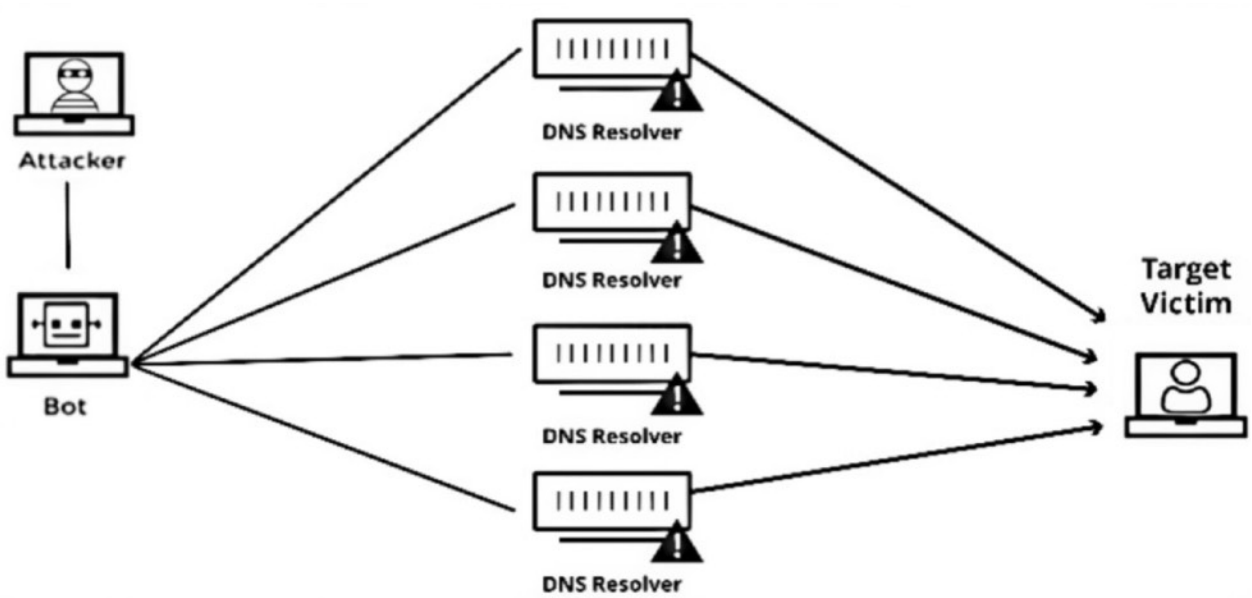

Рисунок 2.15 – Атака ампліфікації DNS

3 ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИБЕЗПРОВОДОВИХ СИСТЕМ З ТЕХНОЛОГІЄЮ MASSIVE MIMO

3.1 Захист на рівні стандарту 5G

На рівні стандарту 5G передбачено низку рішень для забезпечення захисту інформації.

1) Поділ шарів протоколу передачі на три площини: User Plane, Control Plane, Management Plane. Ізоляція, шифрування та контроль цілісності цих площин. Шифрування абонентського та сигнального трафіку.
2) Збільшення довжини ключа шифрування трафіку зі 128 біт до 256 біт.
3) Єдиний механізм автентифікації абонентів різних типів безпроводового зв'язку.
4) Підтримка гнучких політик безпеки сегментів мережі.

Трансформація систем захисту під час переходу від технології 4G до технології 5G представлена у таблиці 3.1.

Таблиця 3.1 – Трансформація захисту технології 4G в 5G

4G					
128 – бітне шифрування	Без захисту цілісності для User Plane	Передача IMSI у відкритому виді	Політика безпеки на рівні мережі	Різні методи автентифікації для різних способів доступу	Передача даних абонентів в роумінгу у відкритому виді
5G					
256 – бітне шифрування	Захист цілісності площини користувача	Захист конфідеційності користувачів (SUCI)	Політика безпеки на рівні абонентів	Єдина автентифікація для LTE, 5G, Wi-Fi	Безпека у роумінгу
Більш надійне	Підвищена безпека безпроводового інтерфейсу	Більш надійний захист конфіденційності користувача	Гнучка політика забезпечення безпеки	Уніфіковані методи автентифікації користувачів	Підвищена безпека у роумінгу

3.2 Захист на рівні обладнання та інфраструктури мережі 5G

Захист мережі 5G на рівні обладнання та інфраструктури є комплексом заходів.

1) Багаторівнева ізоляція та захист цілісності компонентів технології SDN та VNF – гіпервізора, віртуальних машин, операційних систем.
2) Забезпечення високої доступності віртуальних машин швидкого відновлення після атак.
3) Аутентифікація програм MEC (Mobile Edge Computing) та авторизація запитів API (Application Programming Interface).

Концепція «граничних обчислень» Mobile Edge Computing передбачає розміщення хмарних IT-ресурсів для віртуалізації мережі ближче до кінцевих користувачів на периферії (edge) операторської мережі.

4) Додатковий фактор автентифікації при доступі до корпоративної мережі, «білий список» пристроїв та служб. "Білий список" – блокує доступ для всіх користувачів, які не входять до списка.
5) Захищені канали зв'язку між базовою станцією, MEC та корпоративною мережею.
6) Довірене апаратне середовище – безпечне завантаження пристроїв.
7) Виявлення атак у реальному часі на мережевих вузлах та елементах віртуальної інфраструктури з використанням алгоритмів штучного інтелекту.

3.3 Захист на рівні управління мережею

Захист ефективний, якщо він забезпечується на всіх рівнях, у тому числі на рівні управління мережею. Для її реалізації використовується низка заходів.

1) Багатофакторна автентифікація та розмежування доступу до сегментів з боку O&M (Operation and Maintenance). O&M – це експлуатація та технічне обслуговування.
2) Засоби виявлення підроблених базових станцій з урахуванням моніторингу подій обслуговування.
3) Безпечне управління життєвим циклом даних користувача, а також аналітичних і службових даних оператора – це шифрування, анонімізація, безпечне зберігання та видалення.

4) Централізоване управління вразливістю, політиками інформаційної безпеки, аналіз великих даних виявлення аномалій і раннього реагування на атаки SOC (Security Operations Center).

Важливо відзначити, що безпека мереж 5G не обмежується технічними заходами захисту, а складається із спільних зусиль сторін, що довіряють один одному: розробників стандарту, регуляторів, вендорів, операторів та постачальників послуг.

Нині реалізується нова схема мобільної кібербезпеки разом із різними регуляторами кібербезпеки – NESAS/SCAS (Network Equipment Security Assurance Scheme/Security Assurance Specifications).

NESAS/SCAS дає можливість:

- забезпечити захист для найбільш специфічних для промисловості точок доступу та пов'язаних з ними загроз безпеки, таких як радіоінтерфейс, NAS (Network Attached Storage – мережеве сховище), веб-безпека тощо;
- надає уніфіковані специфікації, які можна виміряти, побачити, зіставити, зрозуміти та застосувати;
- знижує фрагментацію вимог до безпеки та скорочує непотрібні витрати операторів.

Операторам використання цих рішень дозволить скоротити час та витрати на оцінку постачальників, визначить суворі та уніфіковані стандарти безпеки та забезпечить високі рівні безпеки.

3.4 Обмін службовою інформацією між абонентською і базовою станцією в системах з технологиією massive MIMO і методи захисту

Окрім переваг системи massive MIMO відрізняються складністю технічної реалізації. У таких системах величезну роль відіграє наявність зворотних каналів між абонентськими станціями та базовою станцією. Витрати канального ресурсу на інформацію про стан каналу CSI (Channel State Information) досить великі.

Кількість антен у massive MIMO значно зростає в порівнянні з системами з технологією класичного MIMO, тому збільшується і кількість каналів, що передають інформацію. Отже, щоб забезпечити необхідну якість передачі та побудувати коректну матрицю прекодування (попереднього кодування) для каналів massive MIMO, потрібно збільшити і число індикаторів PMI (precoding matrix indicator), переданих абонентським терміналом по каналу зворотного

зв'язку вгору. Також потрібно більше ресурсу лінії вниз для передачі сигналів CSI-RS (channel state information – reference signal), бо необхідні операції прекодування на базової станції. Крім цього, для коректної роботи планувальника базової станції при використанні режимів multi-user будуть потрібні і більші витрати радіоресурсу для передачі сигналів DM-RS (demodulation reference signal), які відправляються абонентським терміналом вгору у напрямку базової станції. Таким чином, значна частина радіоресурсів піде на службову інформацію. Наприклад, при використанні 64 антенних портів більше половини елементів одного ресурсного блоку піде лише на передачу CSI-RS сигналів.

Організація передачі у системах з адаптивним формуванням вузьких променів діаграми спрямованості з високою концентрацією потужності на апаратуру користувача – це перевага таких систем. Збільшується зона дії базової станції, але з іншого боку при цьому витрачається великий обсяг канальних ресурсів на передачу службової інформації в обидві сторони: вгору та вниз.

З погляду безпеки наявність зворотних каналів надає для атакуючих системи велику кількість можливостей глушіння чи спотворення службової інформації, отже, і руйнації нормального функціонування системи зв'язку.

Для зниження можливостей спотворення сторонніми особами службової інформації можна запропонувати введення її шифрування. Однак це призведе до збільшення обсягу службової інформації, що передається. та відповідно до зниження загальної швидкості передачі інформації.

Для боротьби з глушінням службової інформації, яка передається по одному каналу з корисною інформацією, а значить і для захисту всього каналу передачі можна запропонувати метод зміни несучої частоти. Зміна частоти відбувається автоматично за фіксації інциденту порушення зв'язку. Такий метод ефективний для систем глушіння, що працюють на фіксованій частоті.

У разі більш складних систем глушіння з можливостю перебудови частоти, що переносить інформацію, можна запропонувати метод псевдовипадкових перескоків несучої частоти. Псевдовипадковий закон синхронно працює на базовій та абонентській станції. Зловмиснику такий закон не відомий і йому потрібен час для його розкриття. У системі можна періодично змінювати цей закон і таким чином ускладнювати завдання розкриття.

На рисунку 3.1 представлено узагальнену схему передавача з псевдовипадковими перескоками частоти. Потік цифрової інформації, наприклад, у коді NRZ, надходить на модулятор FSK або BPSK. Після модулятора інформація

перемножується із псевдовипадковими частотами. Для їх формування використовується блок, що складається з генератора псевдовипадкової послідовності чисел, який з'єднаний з програмною таблицею частот. Вибрані частоти формуються у синтезаторі частот. Результат перемноження псевдовипадкових несучих частот із цифровим потоком від модулятора надходить у смуговий фільтр, який пропускає суму частот.

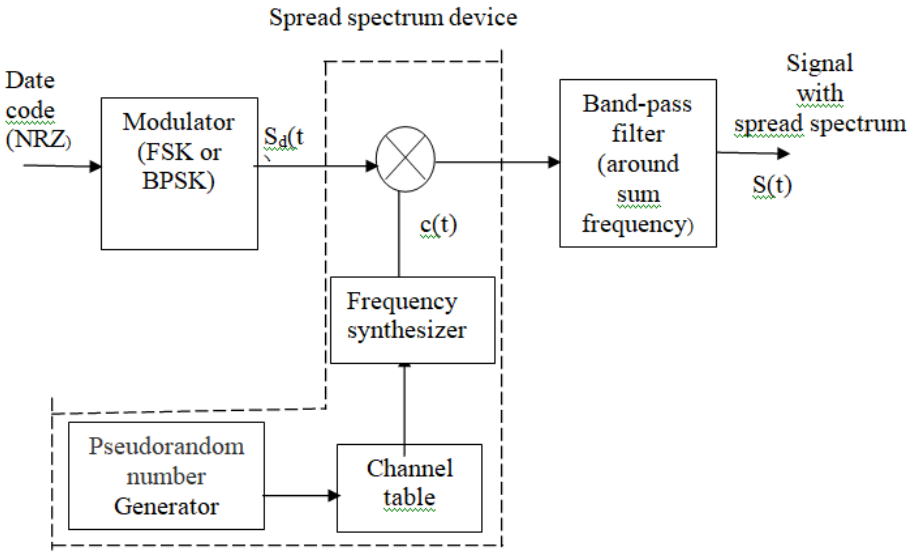

Рисунок 3.1 – Узагальнена схема передавача з псевдовипадковими перескоками частоти

Відповідно будується приймальний пристрій, як показано на рис. 3.2. Прийнятий сигнал із псевдовипадковими перескоками несучої частоти надходить у перемножувач. У цьому блоці прийнятий сигнал перемножується з потоком псевдовипадкових несучих частот, що збігається з аналогічним потоком передавача і синхронізується з ним.

Після перемноження сигналів результат подається на смуговий фільтр навколо різниці частот. Далі виконується зворотна операція демодуляції прийнятого сигналу.

У такій системі закони формування псевдовипадкової послідовності частот мають бути однаковими в передавачу та приймачу і синхронізовані за часом. Для синхронізації використовують пілотні сигнали.

Існують два способи побудови таких систем – з швидкою та повільною перебудовою частоти. Крім того, такі системи можуть мати різні значення максимального розкиду частот, що переносять інформацію.

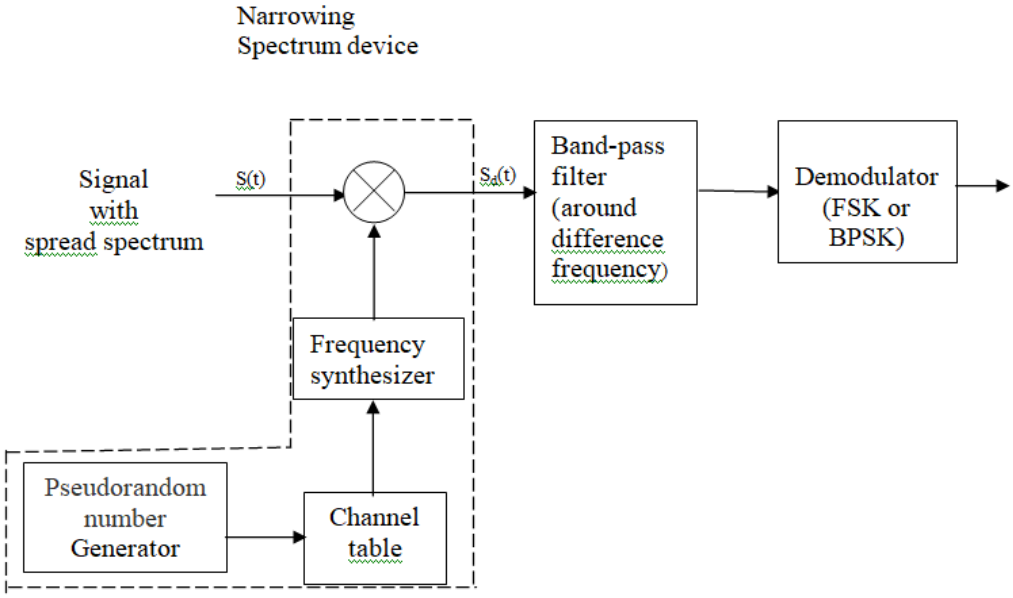

Рисунок 3.2 – Узагальнена схема приймача з псевдовипадковими перескоками частоти

Чим більший діапазон перескоків несучих частот, тим більший рівень захисту від зовнішніх впливів. Для підвищення рівня захисту необхідно періодично змінювати закон пересковів частот. У випадку, якщо зловмисник використовує передавач з вузькою діаграмою спрямованості для збільшення потужності сигналу глушіння можна запропонувати метод, що базується на можливостях технології MU-massive MIMO.

3.5 Захист від глушіння в системах MU - massive MIMO

В технології MU-massive MIMO використовується адаптивна фазована антенна решітка, що формує промені у напрямку апаратури користувачів. Це інтелектуальна багатопроменева антенна система, в якій встроєні фазообертачі, що управляються спеціальною програмою від мікропроцесорів.

Загальна схема однопроменевої інтелектуальної антенної решітки з управлінням напрямку головного пелюстка діаграми спрямованості за допомогою системи фазообертачів, що управляються мікропроцесором з спеціальною програмою представлена на рисунку 3.3. Програма складена таким чином, що фазовий фронт має вид прямої лінії і повертається за допомогою управляємих фазообертачів.

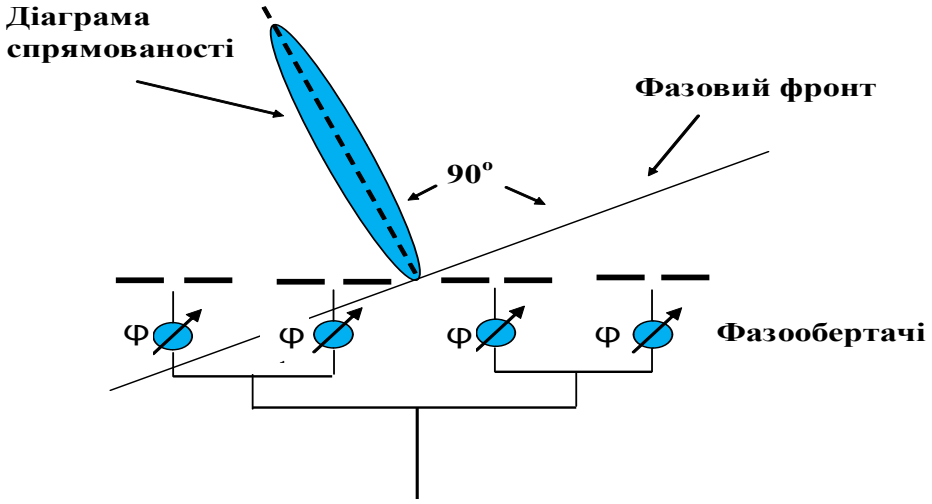

Рисунок 3.3 – Узагальнена схема однопроменової антенної гратки з електронним управлінням головного пелюстка діаграми спрямованості

Приклад двопроменевої антенної гратки з електронним управлінням напрямком головного пелюстка діаграми спрямованості наведено рисунку 3.4. Слід зауважити, що управління кожним з пелюстків діаграми не залежить один від одного.

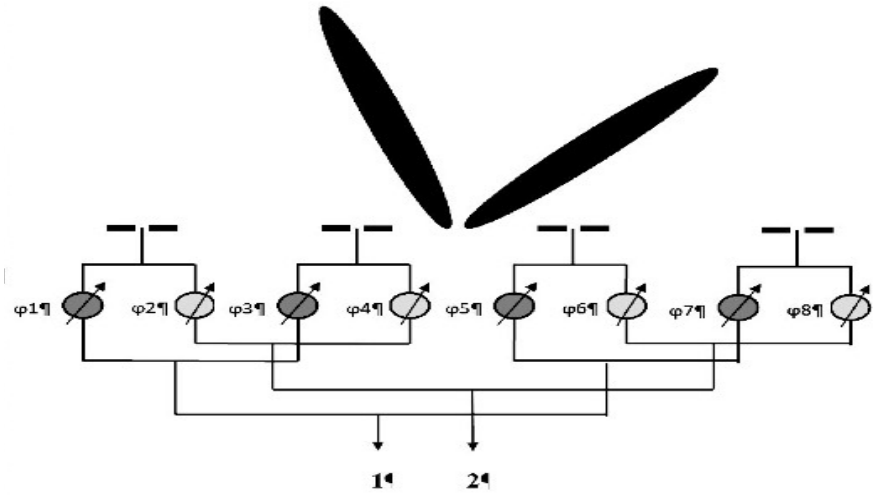

Рисунок 3.4 – Узагальнена схема двопроменової антенної гратки з електронним управлінням напрямком головного пелюстка діаграми спрямованості

У звичайному режимі в технології MU-massive MIMO антенна система формує велику кількість променів, що використовуються для зв’язку з окремими користувачами.

Поява сигналу глушіння в якомусь з напрямків на базову станцію відразу виявляється, тому що сигнал глушіння надто сильно відрізняється від сигналів службової інформації якими обмінюються абонентська і базова станція. На рис. 3.5 зображене блокування глушіння передавача з вузькою діаграмою спрямованості.

На базовій станції загружається програма виявлення сигналу відмінного від стандартних службових сигналів. Ця програма відключає формування променя в напрямку глушника за допомогою управляємих фазообертачів. Як результат базова станція не приймає сигнали глушіння. Цей метод не можна використовувати в старих технологіях без формування променів в напрмку користувачів.

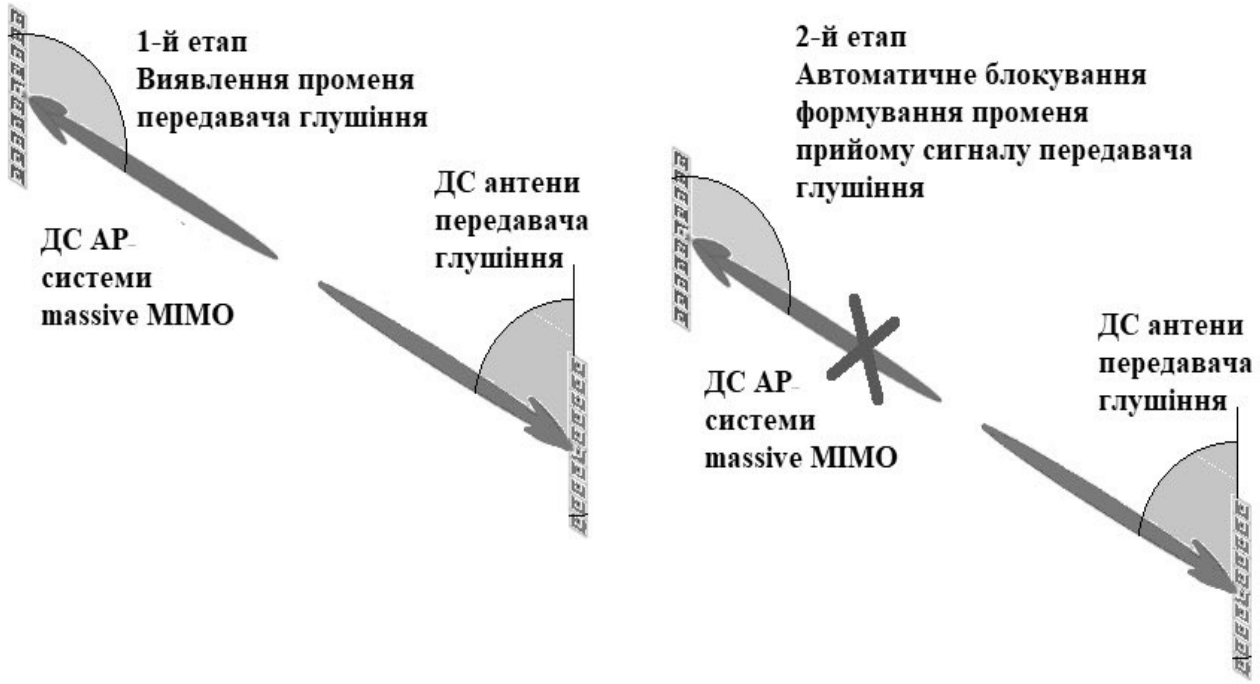

Рисунок 3.5 – Блокування глушіння передавача з вузькою діаграмою спрямованості

У випадку передавачів для глушіння з широкою діаграмою спрямованості більш ефективнім є метод зміни робочих частот, що переносять інформацію як це розглянуто в попередньому підрозділу.

Було проведено моделювання діаграм спрямованості антенних решіток з різною кількістю антенних елементів. В якості елементів антенних решіток були

взяті симетричні вібратори з розміром плеча λ/4. Відстань між центрами живлення складала λ/2.

На рисунках 3.6 – 3.9 представлени результати моделювання ненормованих діаграм з кількістю вібраторів від 10 до 50. Антенні решітки не мали відбиваючих екранів. Якщо доповнити антенні гратки екранами головний пелюсток діаграми направленості буде направлений тільки в одну сторону і потужність випромінювання в головному напрямку збільшиться.

З аналізу результатів моделювання можна зробити висновок, що використання замість класичної технології MIMO технології з великою кількістю антенних елементів на передавальному кінці на базовій станції дає суттєвий виграш в концентрації енергії в напрямку на користувача. Тому використання технології massive MIMO дає можливість збільшити радіус соти для систем 5G в мілиметровому діапазоні з великим рівнем загасання радіохвиль.

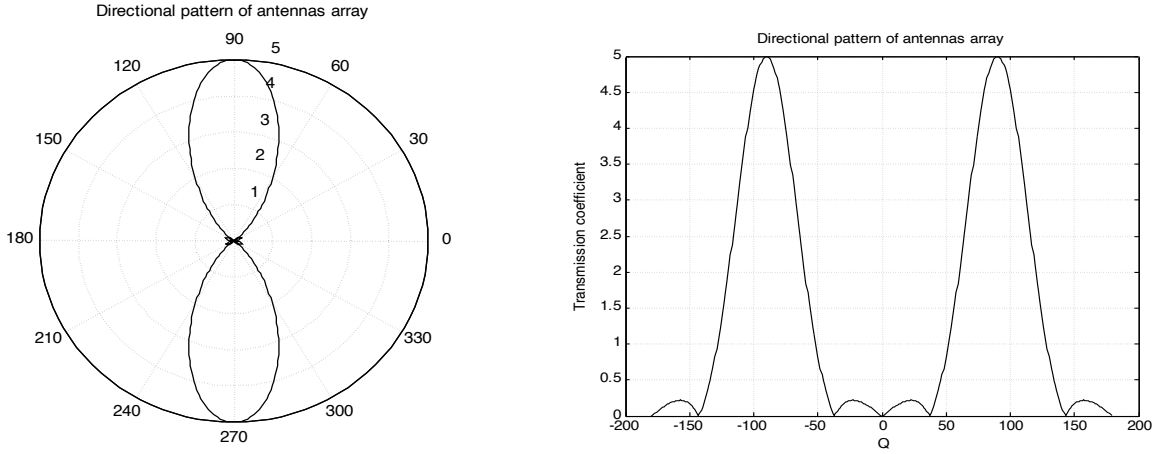

Рисунок 3.6 – Діаграма спрямованості антенної решітки з кількістю елементів N=5

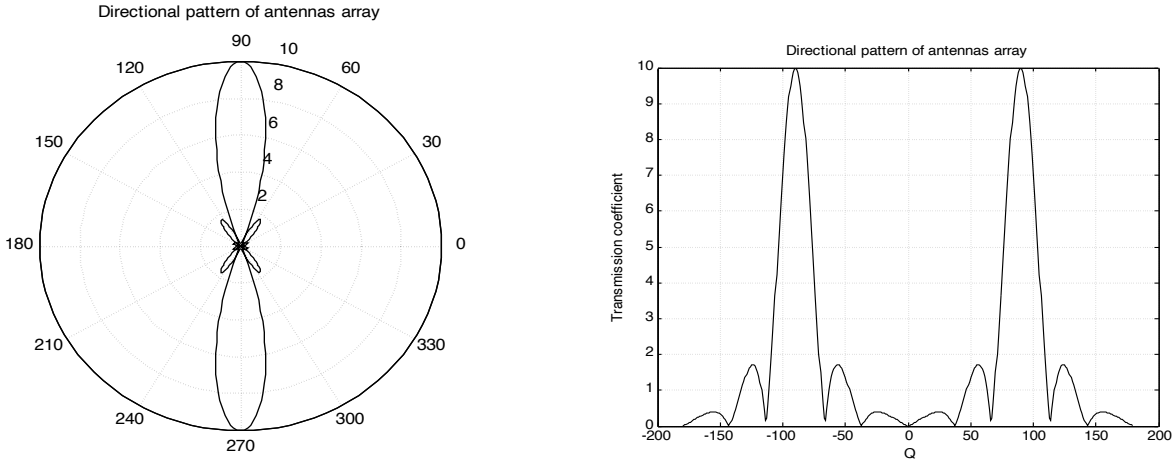

Рисунок 3.7 – Діаграма спрямованості антенної решітки з кількістю елементів N=10

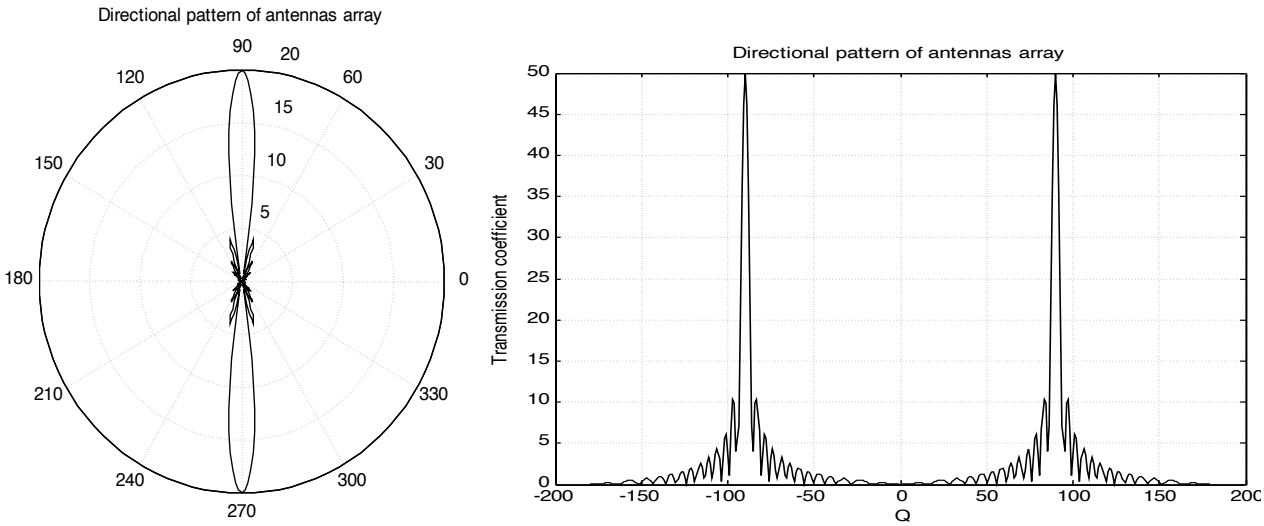

Рисунок 3.8 – Діаграма спрямованості антенної решітки з кількістю елементів N=20

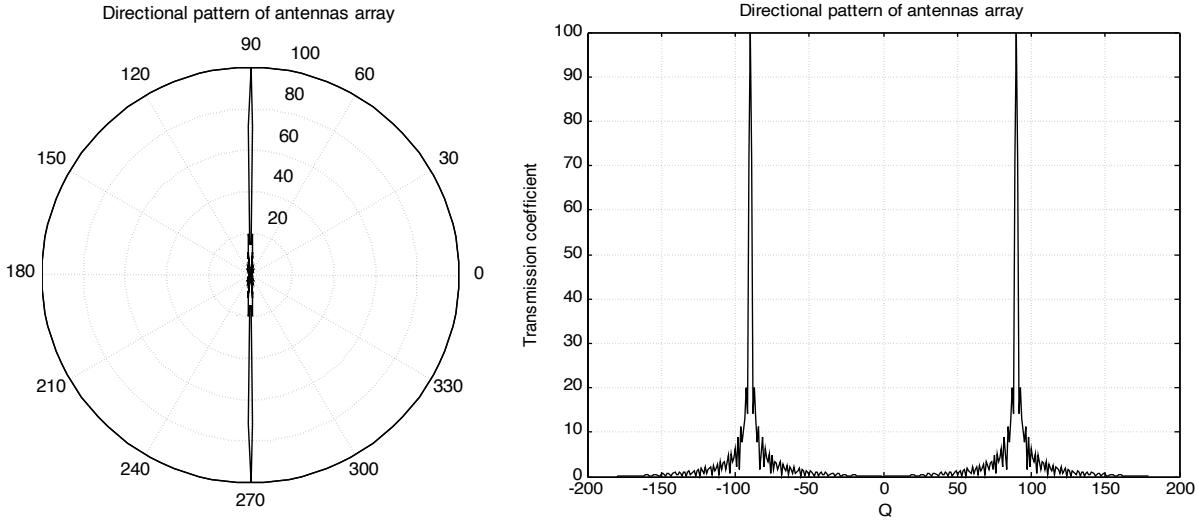

Рисунок 3.9 – Діаграма спрямованості антенної решітки з кількістю елементів N=50

Що стосується розмірів антенних граток, то в міліметровому діапазоні довжина λ радіохвилі складає одиниці міліметрів і розміри антенних граток з великою кількістю антенних елементів не є великими. Навіть при великому значенню N.

По результатам проведеного моделювання рекомендується брати кількість елементів N > 20.

3.6 Захист інформації в системах MU massive MIMO з використанням реконфігуруємих інтеллектуальних поверхонь

Діапазон радіохвиль NR2, що використовується в системах MU-massive MIMO відноситься до міліметрового діапазону. В цьому діапазоні досить високий рівень загасання сигналів у вільному просторі. Радіус зони дії базової станціїї суттєво зменшується, як можна побачити на рис. 3.10.

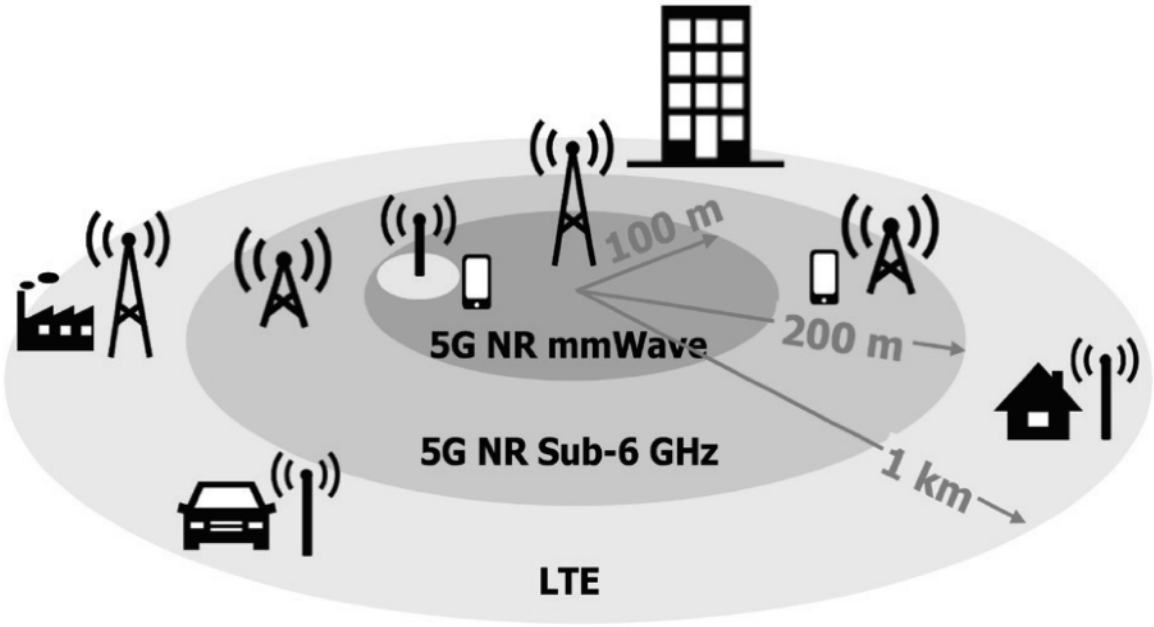

Рисунок 3.10 – Зони дії базової станції телекомунікаційних систем різних поколінь

Для вирішення цієї проблеми запропоновано використовувати реконфігуруємі інтеллектуальні поверхні Reconfigurable Intelligent Surfaces (RIS) [19]. Ці поверхні працюють як пасивні відбиваючі поверхні, але з ефектом фокусування – концентрації енергії в заданих напрямках. На рисунку 3.11 представлена схема інтеллектуальної поверхні RIS.

Одним із способів подолати обмеження максимальної відстані і зробити зв'язок можливим у сценаріях «відсутності прямої видимості» є використання вузлів-ретрансляторів між передавачем та приймачем. Ретранслятор – це активний елемент, в якому він приймає сигнал від передавача, підсилює та повторює його у бік передбачуваного кінцевого приймача. Це може компенсувати втрати на поширення та проникнення, що виникають при поширенні поза прямою видимістю. Однак ретранслятори складаються з дорогих радіочастотних ланцюгів,

що складаються з перетворювачів сигналів, фільтрів, змішувачів та підсилювачів потужності. Отже, це непривабливий варіант для широкомасштабного розгортання.

Ефект фокусування – концентрації енергії RIS в заданих напрямках забезпечується за рахунок використання управляємих фазообертачів.

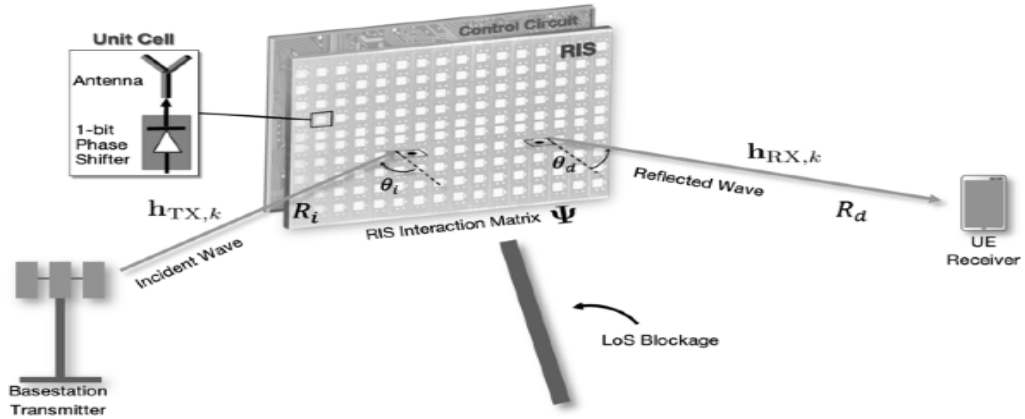

Рисунок 3.11 – Схема інтеллектуальної поверхні RIS [16]

Поверхня RIS складається з недорогих пасивних елементів, що відбивають електромагнитні хвилі. В якості елементів використовуються друковані диполі. Кожен з цих елементів може викликати програмований зсув фази падаючої електромагнітної хвилі, що забезпечує пасивне формування діаграми спрямованості для поліпшення потужності сигналу. При ефективному керуванні RIS допомагає вирівнювати сигнали на приймачі, створюючи кероване радіосередовище. Таким чином, RIS може збільшити коефіцієнт концентрації енергії в промені в системі з massive MIMO, діючи як відбивач вихідного променя від передавача та змінюючи його напрямок до приймача. Поверхня RIS, що складається з пасивних елементів, не може перевершити класичний ретранслятор. Проте нижча вартість та вища енергоефективність роблять ці інтеллектуальні поверхні привабливою альтернативою класичним ретрансляторам. Порівняння систем з ретранслятором і інтеллектуальною поверхньою RIS представлено на рис. 3.12.

Поверхня RIS, що є масивом пасивних відбиваючих елементів, вимагає інтелектуального алгоритму контролера для його ефективного використання. Розробка алгоритмів для роботи RIS досить складна задача. Основне достоінство таких систем – це простота розгортання, обслуговування і вартість.

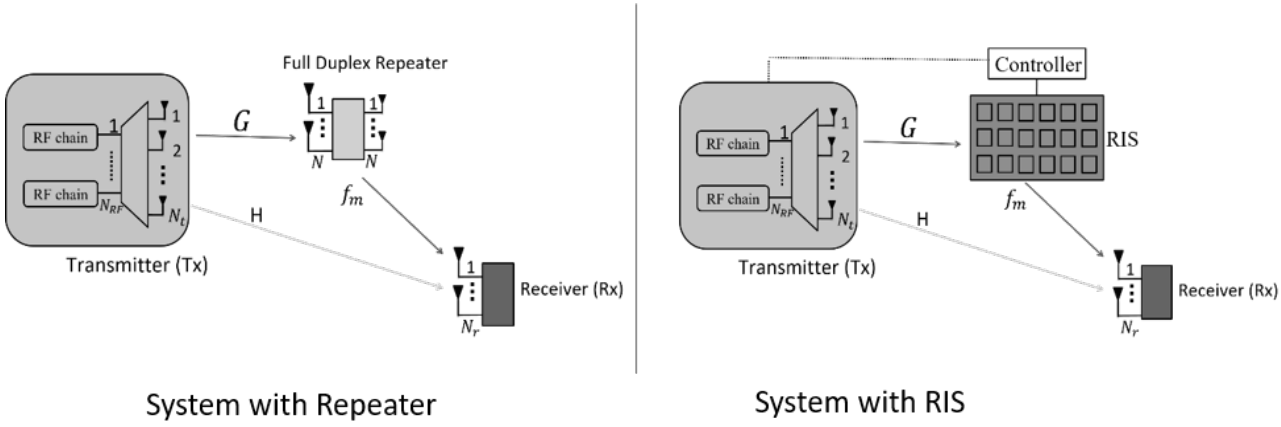

Рисунок 3.12 – Порівняння систем з ретранслятором і інтеллектуальною поверхньою RIS [20]

При використанні RIS необхідно враховувати аспекти можливості стороннього втручання. Конфігурація RIS в одному секторі стільника може відбивати сигнал небажаного користувача в непередбаченому напрямку, що призводить до серйозних перешкод. Окрім того RIS можуть відбивати сигнали за межами однієї ліцензованої смуги оператора, коли сусідні смуги частот використовуються різними операторами. У випадку RIS, керованих одним оператором, можуть відбиватися сигнали іншого сусіднього діапазону, що використовується іншим оператором. Це вимагатиме міжоператорської координації використання RIS у межах географічної зони. Крім того, така координація може також вимагати регулюючого органу для визначення використання.

Для захисту інформації можна рекомендувати ввести в програму управління контролера ключ, що відкриває доступ тільки для фреймів від однієї базової станції. В програмному забезпеченні базової станції також повинен бути такий ключ доступу. Таким чином RIS буде прив’язана до своєї базової станції.

Від якості ключа буде залежати рівень захисту інформації.

3.7 Моделювання захисту інтелектуальних поверхонь від впливу зовнішніх систем в напрямках бокового пелюстка діаграми спрямованості антенної системи

Основним елементом інтелектуальної поверхні RIS є антенна решітка, що приймає сигнали від базової станції і потім направляє їх в напрямку апаратури користувача. Чим більше елементів в цій решітці і більші її розміри тим більша

концентрація енергії в напрямку кінцевого користувача. Головний пелюсток діаграми спрямованості звужується і радіус соти збільшується.

Але у антенних решіток окрім головного пелюстка діаграми спрямованості завжди є бокові пелюстки. Тому виникає ситуація, коли зловмисник, маючи спеціальну апаратуру, може з бокових напрямків впливати на RIS, наприклад, організувати глушіння.

Одним з методів боротьби з впливами через напрямок бокових пелюстків антенної системи можна запропонувати інтелектуальну (smart) фазовану антенну решітку, що змінює напрямок бокового пелюстка. В цьому випадку сигнал глушіння може бути спрямований в «нуль» діаграми спрямованості і система не буде приймати цей сигнал. Звичайно на практиці нуль не є абсолютним, але при рівнях в мінус десятки децибел сигнал практично не діє на нашу систему.

Для моделювання була написана програма в середовищі Matlab. Результати моделювання наведені на рисунках 3.13 – 3.15.

Слід зазначити, що при зближенні кута променя зловмисника до головного напрямку корисного сигналу якість подавлення знижується.

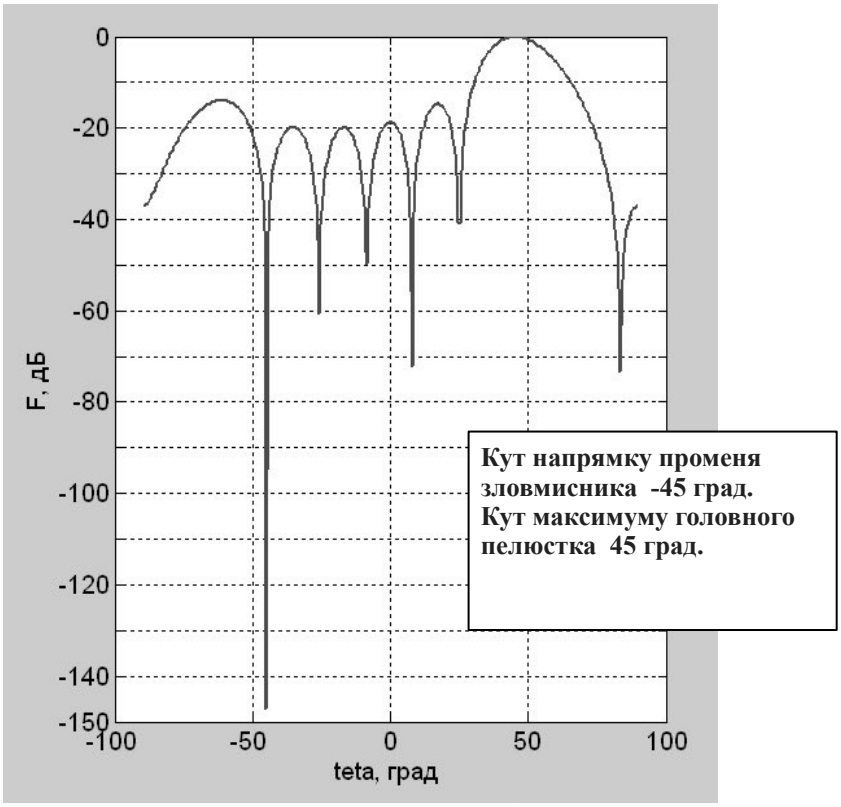

Рисунок 3.13 – Подавлення сигналу зловмисника (варіант 1)

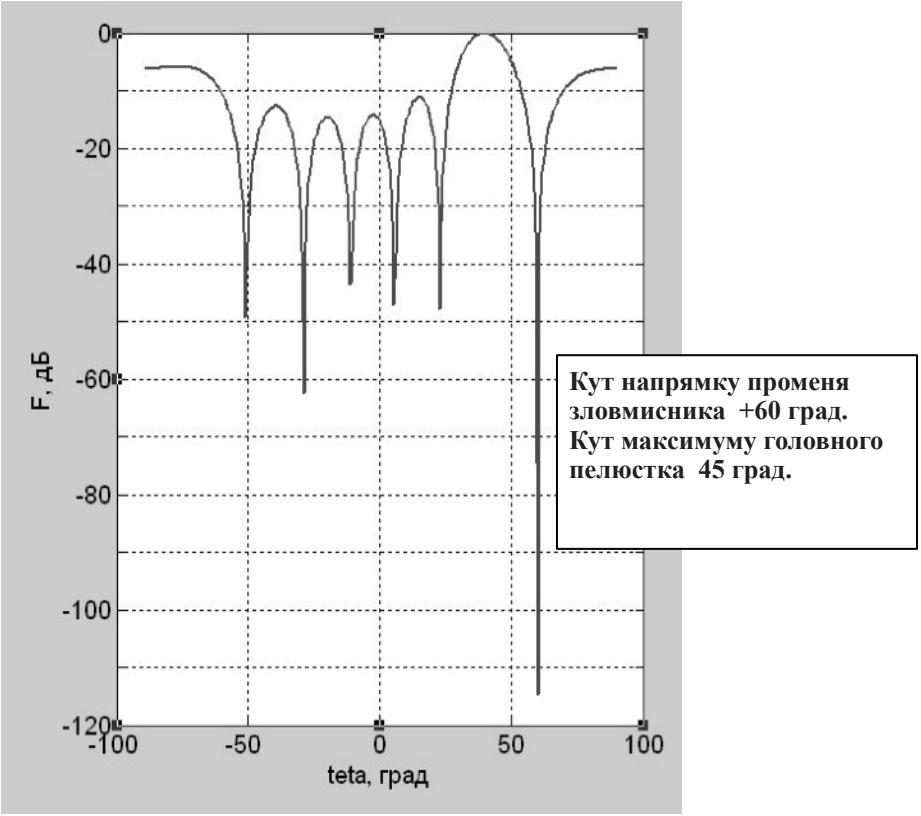

Рисунок 3.14 – Подавлення сигналу зловмисника (варіант 2)

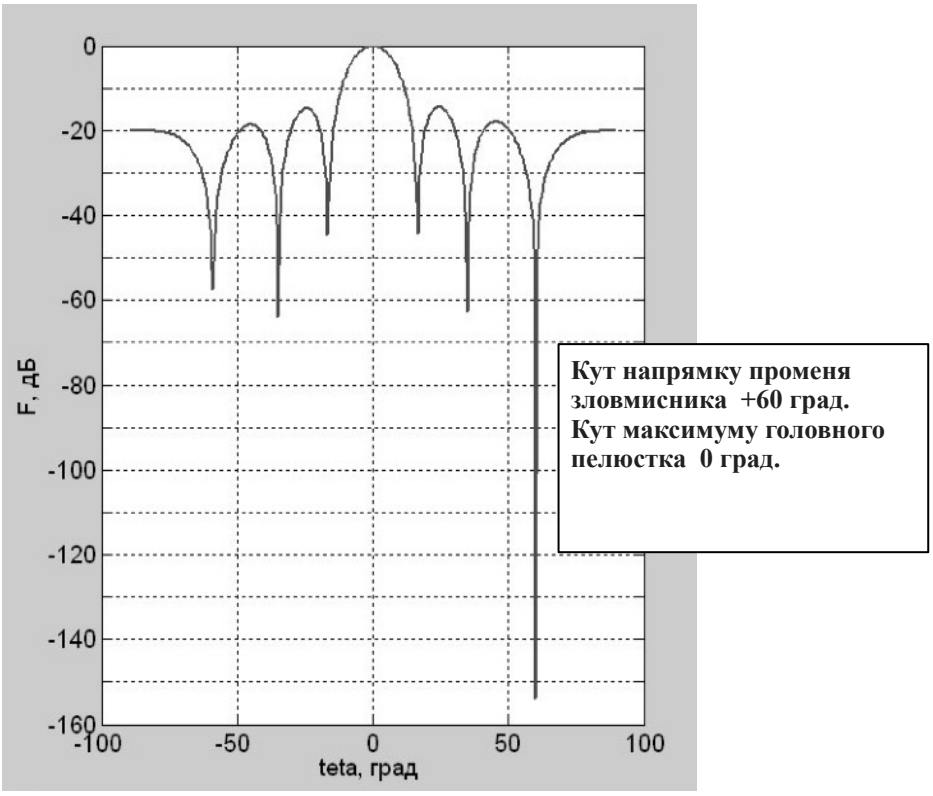

Рисунок 3.15 – Подавлення сигналу зловмисника (варіант 3)

Аналіз отриманих результатів моделювання показує, що використання системи подавлення зовнішніх впливів за рахунок адаптивного повороту бокового пелюстка працює. При цьому слід звернути увагу на те, що провали в діаграмах спрямованості досить глибокі, але по куту інтервал значного загасання зовнішнього сигналу невеликий. Цей недолік не є надто суттєвим, тому, що навколо провалу приблизно до сотні децибел є достатня область по куту значень подавлення в десятки децибел. На рівні мінус 20дБ область по куту складає приблизно 20 град. Таких значень подавлення практично достатньо для захисту RIS від сигналів, що атакують систему з бокових напрямків.

Результати досліджень доповідались на конференціях [1 – 3].

3.8 Дослідження захисту систем 5G від атак через сторонні мережі

Системи 5G мають суттєві переваги порівняльно з системами попередніх поколінь по пропускній здатності і кількості користувальницьких пристроїв. Такі системи ефективні при їх використанні в IoT технологіях.

Особливість мереж IoT в надвеликій кількості датчиків і інших елементів, що мають спрощене програмне забезпечення. Такі елементи дешеві і, як правило не мають захищених протоколів для передачі інформації. Окрім того програмне забезпечення, як правило, не обновлюється і має слабкі системи інформаційного захисту.

Тому для технології 5G виникає проблема захисту від зовнішніх слабозахищених мереж.

Для вирішення цієї задачі можна використати багатоступеневий захист з класичних елементів захисту.

Проведемо аналіз можливостей використання мережевих екранів нового покоління Next Generation Firewall (NGFW). Зазвичай NGFW називають міжмережевим екраном для глибокої фільтрації трафіку, інтегрований з IDS/IPS і має можливість контролювати і блокувати трафік на рівні додатків. Під таке, досить ємне визначення підпадає ціла низка рішень, що мають різний функціонал.

Проаналізуємо від яких загроз і яким чином NGFW захищають мережу. По-перше це мережеві загрози.

Розглянемо типовий набір атак на інфраструктуру. Тут на першому місці зазвичай стоять DDoS атаки, далі йдуть різні фішингові активності, спроби

підбору паролів. Для закріплення в атакованій мережі зловмисники зазвичай використовують різні види шкідливого програмного забезпечення. Також, отримавши доступ до мережної інфраструктури, зловмисник може намагатися здійснити перехоплення трафіку за допомогою атак "людина посередині" MitM. Ну і ще одним, вектором атак є експлуатація вразливостей у програмному забезпеченні.

Це те, що стосується типових векторів атак, проте не варто також забувати про APT-атаки. APT атака це цільова тривала атака підвищеної складності, завданням якої є виявлення на пристрої користувача секретної, конфіденційної або будь-якої цінної інформації і використання її в інтересах кіберзлочинців.

Типовими ознаками APT-атаки є її розподіл у часі, спрямованість на велику організацію та її співробітників, використання цільового фішингу та технологій соціальної інженерії, спрямованих на конкретних співробітників з метою отримання конкретних доступів та інформації. Також характерними ознаками APT є різні підозрілі активності у неробочий час, наприклад, спроби підбору паролів для облікових записів, пошук та копіювання великих обсягів інформації, а також спроби розповсюдження різних бекдорів та троянів.

Класичні засоби захисту, такі як міжмережеві екрани та антивіруси, не надто корисні у боротьбі з APT-загрозами. Так, стандартний міжмережевий екран розбирає пакет лише до транспортного рівня, не заглядаючи в "начинку" рівня додатків. У результаті зловмисники для своїх комунікацій можуть використати дозволені у списках доступу протоколи та адреси, внаслідок чого підозріла активність може залишитися непоміченою. З антивірусами історія схожа, але тут зловмисник, знаючи, який саме антивірус використовується в організації, може обфуцювати свій код таким чином, що цей антивірус нічого не запідозрить. Від мережевих загроз певною мірою нас можуть захистити засоби виявлення атак IDS/IPS.

Однак, функціонал NGFW може бути набагато ширше, ніж у IPS, що дозволяє ефективніше боротися з різними атаками, включаючи APT. Звичайно, коли ми говоримо про широкий функціонал рішень NGFW, певною мірою працює маркетинг, оскільки багато з цих функцій раніше вже входили до рішень класу Unified Threat Management (UTM) – це комплексний захист від мережевих загроз.

Що може входити до складу сучасного рішення NGFW. Насамперед це аналіз на рівні додатків – Application Control. Отримавши пакет, NGFW розбирає його, починаючи з рівня L3 і закінчуючи рівнем L7. Таким чином, можливо

виявити підозрілі активності у мережі. Наприклад, зловмисник, оселившись у мережі, використовує для з'єднання спеціальні доменні імена згенеровані за допомогою DGA (Domain Generation Algorithm). Ці імена дозволяють шкідливим користувачам підключатися до C&C серверів використовуючи різні доменні імена. Сервер керування та контролю, або C&C, – це загальна назва сервера, який використовується для керування ботнетами – мережами комп’ютерів, заражених певним шкідливим програмним забезпеченням. Ботнети покликані створювати масовані заходи, переважно шкідливого характеру. Усі DDoS атаки та ефективні спам-кампанії здійснюються за допомогою ботнетів. Особливо небезпечний ботнет Mirai. Він поступово заражає термінали, що в свою чергу становляться джерелами DDoS атак.

Мережеві екрани нового покоління Next Generation Firewall (NGFW) мають настуні основні функції:

- запобігання вторгненням;
- має програмне забезпечення та контроль, щоб бачити та блокувати програми на льоту;
- має стратегії протидії загрозам, що постійно розвиваються;
- виконує профілактику для припинення нападів до того, як вони справді відбудуться;
- фільтрує URL-адреси згідно політики фільтрації до мільйонів URL-адрес;
- має гнучкість розгортання – локально, у хмарі або як віртуальний бранмауер.

Основні переваги брандмауерів наступного покоління:

- наявність всіх стандартних можливостей брандмауерів першого покоління, таких як фільтрація пакетів, перевірка стану, NAT, VPN тощо;
- мають інтегровані системи виявлення вторгнень для підтримки керування вразливістю та пропозиції дій на основі активності IPS;
- повна видимість стека та ідентифікація додатків для застосування політики на рівні додатків або на сьомому рівні, незалежно від протоколу та порту;
- можливість створювати чорні або білі списки та відображати трафік для користувачів і груп за допомогою Active Directory;
- розшифровка SSL для ідентифікації небажаних зашифрованих програм.

На основі проведенного аналізу можна рекомендувати використання NGFW для захисту базової мережі від сторонніх мереж IoT.

3.9 Аналіз методів захисту від DDoS атак в системах 5G

Існують різні підходи до виявлення DDoS атак. Деякі з них передбачають роботу датчиків по периметру мережі та централізовану обробку даних з них, інші – встановлення додаткового програмного забезпечення на проміжних вузлах на шляху від зловмисника до жертви.

Всі широко використовувані підходи до виявлення DDoS атак відстежують трафік, спрямований із зовнішньої мережі на захищену станцію або службу, і визначають атаку як помітне відхилення від деяких спостережуваних характеристик трафіку.

3.9.1 Класифікація основних підходів до виявлення DDoS атак.

Виділяють три основні групи методів виявлення DDoS-атак.

Методи першої групи ґрунтуються на побудові профілю активності віддалених станцій по відношенню до станції (сервісу), що охороняється, під час навчання і порівнянні характеристик трафіку з характеристиками профілю в режимі виявлення. При виявленні відхилень від профілю генерується тривога. У багатьох розробках і дослідженнях основним показником є середня кількість пакетів, отриманих станцією, що захищається, або окремими мережевими сервісами. Для виявлення аномалій можуть використовуватися статистичні критерії (середньоквадратичне відхилення, хі-квадрат, відхилення від стандартного нормального розподілу, значне збільшення ентропії тощо), кластеризація тощо. Ці методи дозволяють виявляти DoS та DDoS-атаки.

До другої групи можна віднести широко використовуваний статистичний метод CUSUM, заснований на виявленні "точки зміни".

У цьому методі аналізований трафік зазвичай спочатку розділяється на основні IP-адреси порту або протоколу призначення. Далі значення певного спостережуваного параметра трафіку (кількість нових станцій, що звернулися до сервісу, різниця в кількості пакетів з прапором SYN і пакетів з прапорами SYN-ACK, різниця в кількості встановлених і закритих з'єднань тощо) перетворюються в елементи певної послідовності. Під час атаки значення поточного елемента послідовності буде суттєво відрізнятися від попередніх елементів послідовності.

Цей метод має декілька суттєвих переваг перед іншими методами. Першою перевагою методу є його висока швидкість, що дозволяє застосовувати його в реальному часі. Друга перевага полягає в тому, що метод адаптується до різних навантажень в мережі, якщо вони є постійними. Крім того, цей алгоритм вважається найкращим серед алгоритмів з визначеною частотою помилкових спрацьовувань, оскільки параметри алгоритму розраховуються на основі формули, яка пов'язує порогове значення алгоритму виявлення атаки і час виявлення.

До третьої групи методів належать спектральний аналіз та вейвлет аналіз, які базуються на аналізі спектральних характеристик трафіку для виявлення DDoS-атак. Робота методу базується на припущенні, що спектр (потужність спектральної щільності) трафіку, згенерованого кількома зловмисниками, суттєво відрізняється від спектру трафіку, згенерованого одним зловмисником. Другий підхід схожий на попередній, але його робота заснована на тому, що спектр трафіку, згенерованого зловмисником, відрізняється від спектру трафіку під час нормальної роботи мережі. Метод використовує аналіз корисного навантаження пакетів, що також уповільнює його роботу. Крім того, для вейвлет аналізу правильний вибір базисних функцій (вейвлетів) і вибір порогу виявлення атаки є досить складним завданням.

Для виявлення DDoS-атак пропонується використовувати метод, заснований на виявленні "точки зміни", завдяки його швидкості та низькому споживанню пам'яті. Для виявлення DDoS-атак пропонується відстежувати наступні характеристики трафіку:

- кількість нових станцій, які звернулися до сервісу;
- кількість різних станцій, що мають доступ до захищеного сервісу;
- різниця в кількості встановлених і закритих з'єднань.

3.9.2 Захисна система від DDoS-атак, розгорнута на кінці джерела трафіку.

Архітектура захисної системи від DDoS-атак, що розгорнута на кінці джерела показана на рисунку 3.16. Компонент заглушення використовується для обмеження швидкості вихідних з'єднань. Механізм виявлення порівнює статистику кожного вхідного та вихідного трафіку з деякими попередньо визначеними традиційними профілями.

Це найкращий захист для виявлення і зупинки DDoS-атаки на стороні джерела, що запобігає ймовірності флуду на стороні жертви, а також у всій мережі. Цей підхід має два недоліки:

- важко виявити DDoS-атаки на стороні джерела, оскільки джерела широко розподілені, а окреме джерело поводиться майже так само, як і в звичайному трафіку;
- складність розгортання системи на стороні джерела.

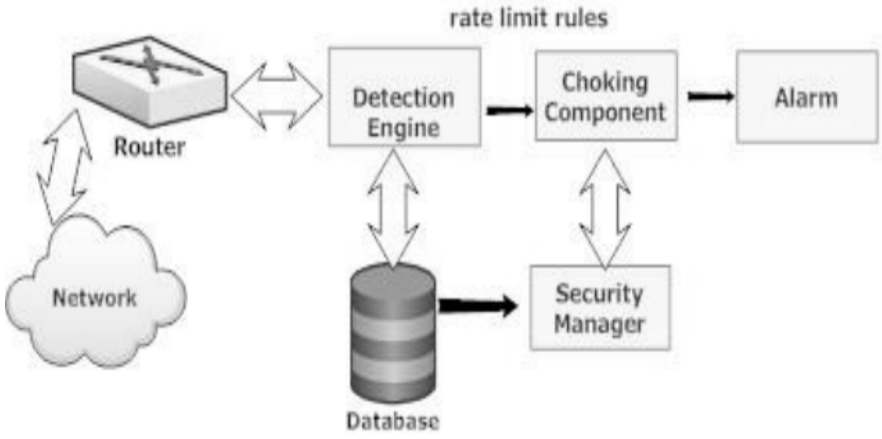

Рисунок 3.16 – Архітектура захисної системи від DDoS, що розгорнута на кінці джерела

3.9.3 Захисна система від DDoS-атак, розгорнута на кінці жертви.

Методи захисту, які використовуються цільовими системами у випадку DDoS-атак, зазвичай інтегровані у маршрутизаторах мереж жертв. Загальна архітектура таких схем показана на рисунку 3.17. Механізм виявлення використовується для виявлення атак як в мережі, так і в автономному режимі. У базі даних зберігаються дані про відомі сигнатури атак нормальної поведінки. Менеджер безпеки відповідає за оновлення сигнатур атак, коли з'являється інформація про нову поведінку, а також перевіряє наявність будь-яких важливих подій, таких як хибні тривоги.

Виявити DDoS атаки на маршрутизаторах жертвах легко завдяки високому рівню використання ресурсів. Але дуже важливо захистити мережеві ресурси, які використовуються веб серверами, що надають послуги користувачам мережі. Такий підхід має два недоліки:

- ресурси жертви зазвичай стають слабкими, і потік не може бути зупинений на віддалених маршрутизаторах жертви;
- атаки можуть бути виявлені тільки тоді, коли вони досягають жертви.

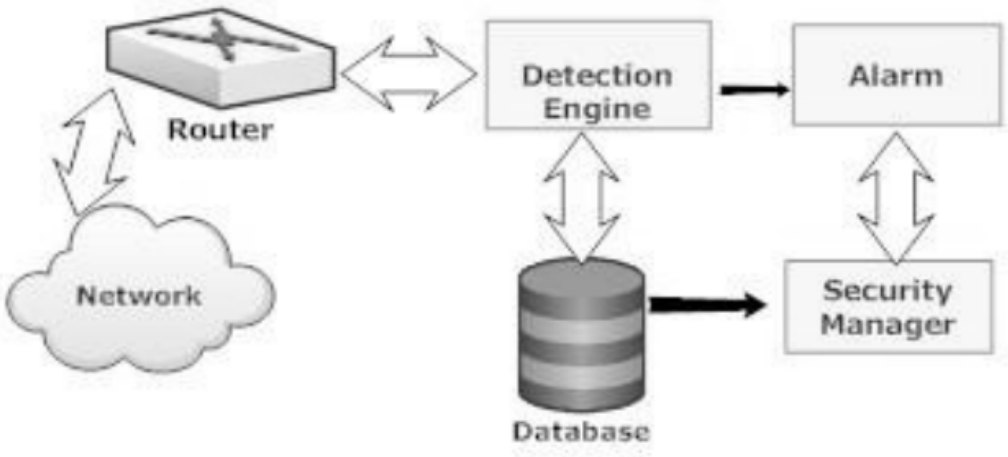

Рисунок 3.17 – Архітектура механізму захисту від DDoS, що розгорнута на стороні жертви

3.9.4 Захисна система від DDoS-атак, розгорнута на проміжній мережі.

Проміжна схема захисту мережі балансує компроміси між точністю виявлення та споживанням смуги пропускання атаки, що є основними проблемами в підходах виявлення з боку джерела та жертви. На рисунку 3.18 показано загальну архітектуру проміжної схеми захисту мережі, яка може бути використана в будь-якому мережевому маршрутизаторі. Така схема зазвичай є кооперативною за своєю природою, а також маршрутизатори діляться своїми спостереженнями з іншими маршрутизаторами. Ці схеми накладають обмеження на швидкість з'єднань, що проходять через маршрутизатор, при перевірці із затримкою на нормальних профілях.

У цьому підході виявлення та відстеження джерел атак є простим завдяки спільній роботі маршрутизаторів. Маршрутизатори можуть формувати оверлейну сітку, щоб ділитися своїми спостереженнями. Основним недоліком цього підходу є складність розгортання. Всі інші маршрутизатори в мережі повинні використовувати цю схему виявлення, щоб досягти повної точності виявлення. Очевидно, що повна практична реалізація цієї схеми є надзвичайно складною і вимагає переналаштування всіх маршрутизаторів в Інтернеті.

Останнім часом для виявлення DDoS-атак використовують ансамблі класифікаторів. Для цього використовується ансамбль класифікаторів, де в якості базового класифікатора обрано нейронну мережу зі стійким зворотним поширенням (Resilient Back Propagation, RBP).

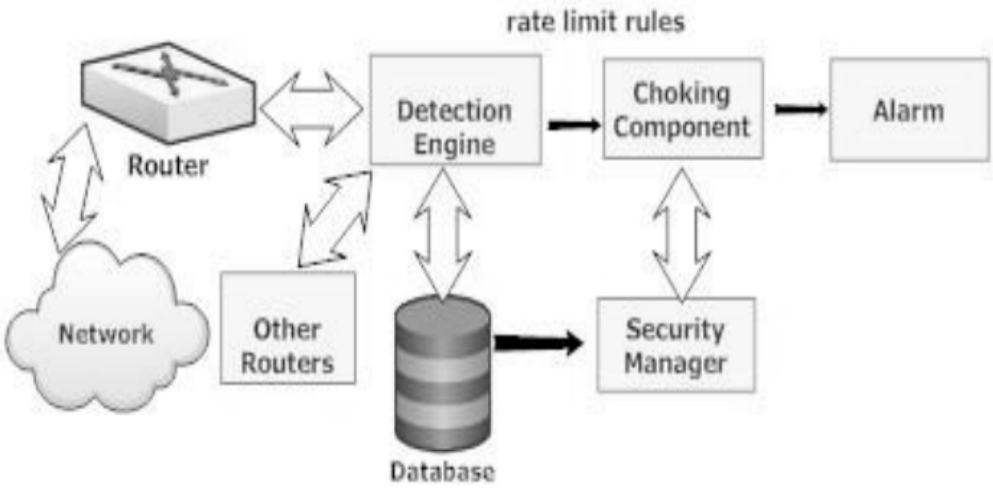

Рисунок 3.18 – Архітектура механізму захисту від DDoS, що розгорнута на проміжній мережі

ВИСНОВКИ

В роботі зроблено огляд сучасного стану технологій та протоколів, що забезпечують функціонування безпроводових систем з технологіями MIMO і massive MIMO.

Описані основні положення про мережу 5G, що базуються на принципах міжнародних стандартів, а також розглянуті основні вимоги до таких мереж.

Представлено аналіз інформації про діапазони частот і статус їх впровадження у світових операторів. Виявлено, що в наш час міліметровий діапазон використовують у мережах 5G лише в 10 % випадків і є тенденція до збільшення частки систем 5G з використанням надвисоких частот.

Виконано аналіз інформаційної безпеки, розглянуті основні протоколи та алгоритми забезпечення захисту конфіденційності та цілісності в мережах 5G.

Представлено аналіз вразливостей безпроводових телекомунікаційних систем 5G, в тому числі і з використанням багатоантенної технології massive MIMO.

Розглянуто ряд методів забезпечення інформаційної безпеки безпроводових систем покоління 5G.

Проведено моделювання захисту інтелектуальних поверхонь RIS від впливу зовнішніх систем в напрямках бокового пелюстка діаграми спрямованості антенної системи. Надані рекомендації по використанню адаптивних антенних решіток для захисту RIS.

Запропоновано використовувати відомий в інших застосуваннях метод псевдовипадкових перескоків частоти або фіксованих змін робочих частот, що переносить коливання в системах з технологією massive MIMO для захисту службової і основної інформації.

У випадку вузьких діаграм спрямованості джерел глушіння запропоновано доповнити системи MU massive MIMO програмою виявлення сигналів глушіння, що суттєво відрізняються від службової інформації, і відключати формування променя діаграми спрямованості передавача базової станції по куту приходу сигнала зловмисника для його блокування.

По результатам проведеного моделювання діаграм спрямованості антенних граток з різною кількістю антенних елементів рекомендується брати їх у кількості більше 20. Моделювання проведено для антенних елементів у вигляді

симетричних вібраторів з довжиною плеча λ/4. Рівень поля в максимумі головного пелюстка пропорційний кількості елементів в антенній гратці, а введення відбиваючого екрана збільшує поле приблизно у 2 рази. Слід зазначити, що ширина головного пелюстка діаграми спрямованості в досліджуваній площині залежить тільки від кількості антенних елементів в цій площині і не залежить від їх кількості в іншій площині. Тому слід використовувати пласкі антенні гратки з однаковою або різною кількістю елементів в кожній площині в залежності від поставлених задач.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Поповська Є.О. Дослідження методів захисту систем відеоспостереження на базі стандарту Wi-Fi // Матеріали 27-го Міжнародного молодіжного форуму «*Радіоелектроніка та молодь у XXI столітті*». – 2023. – С. 116 – 117.

2. Поповська Є.О., Куля Ю.Е. Аналіз сучасних загроз безпеці безпроводових мереж // Materials of IXth International Scientific and Technical Conference «*Information protection and information systems security*». – May 25 – 26, 2023. Lviv, Ukraine. – С. 31 – 32.

3. Поповська Є.О., Марчук В.С. Аналіз забезпечення захисту інформації в мережах 5G з технологією massive MIMO // Матеріали Міжнародної науково-технічної конференції «*Інформаційно-комунікаційні технології та кібербезпека*» (ІКТК-2023). – Грудень 7 – 8, 2023. Харків, Україна.

4. Recommendation M.2150: Detailed specifications of the 3. Report ITU-R M.2410-0: Minimum requirements related to technical performance for IMT-2020 radio interfaces. URL https://www.itu.int/pub/R-REP-M.2410-2017 (дата звернення: 05.12.2023).

5. Understanding important 5G concepts: what are eMBB, URLLC and mMTC. *Verizon: Wireless, Internet, TV and Phone Services | Official Site.* URL: https://www.verizon.com/about/news/5g-understanding-embb-urllc-mmtc. (дата звернення: 07.12.2023).

6. Report ITU-R M.2410-0: Minimum requirements related to technical performance for IMT-2020 radio interfaces. URL: https://www.itu.int/pub/R-REP-M.2410-2017 . (дата звернення: 07.12.2023).

7. Основні характеристики і області застосування 5G / New Radio. URL: http://anisimoff.org/5g/5g_overview.html (дата звернення: 08.12.2023).

8. Meer Zafarullah Noohani, Kaleem Ullah Magsi. A Review Of 5G Technology: Architecture, Security and wide Applications. URL: https://www.researchgate.net/publication/341541673 (дата звернення: 10.12.2023).

9. TS 133 501 – V15.4.0 – 5G; security architecture and procedures for 5G system (3GPP TS 33.501 version 15.4.0 Release 15). URL: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.04.00_60/ts_133501v150400p.pdf (дата звернення: 14.12.2023).

10. Security Edge Protection Proxy (SEPP). *BroadForward*. URL: https://www.broadforward.com/security-edge-protection-proxy/ (дата звернення: 17.12.2023).

11. Security and protocol exploit analysis of the 5G specifications. URL: https://arxiv.org/pdf/1809.06925.pdf (дата звернення: 18.12.2023).

12. Massive MIMO in 5G: how beamforming, codebooks, and feedback enable larger arrays. URL: https://arxiv.org/pdf/2301.13390.pdf. (дата звернення: 19.12.2023).

13. 5G spectrum bands explained – low, mid and high band. URL: https://www.nokia.com/thought-leadership/articles/spectrum-bands-5g-world/. (дата звернення: 22.12.2023).

14. 5G market 2023-2033: technology, trends, forecasts, players. *IDTechEx*. URL: https://www.idtechex.com/en/research-report/5g-market-2023-2033-technology-trends-forecasts-players/895. (дата звернення: 23.12.2023).

15. TS 123 501 – V15.2.0 – 5G; system architecture for the 5G system. URL: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/15.02.00_60/ts_123501v150200p.pdf. (дата звернення: 24.12.2023).

16. TS 138 401 – V16.3.0 – 5G; NG-RAN; architecture description. URL: https://www.etsi.org/deliver/etsi_ts/138400_138499/138401/16.03.00_60/ts_138401v160300p.pdf (дата звернення: 26.12.2023).

17. TS 133 210 – V16.4.0 – Digital cellular telecommunications system. URL: https://www.etsi.org/deliver/etsi_ts/133200_133299/133210/16.04.00_60/ts_133210v160400p.pdf (дата звернення: 27.12.2023).

18. Massive MIMO Systems for 5G Communications. URL: https://bura.brunel.ac.uk/bitstream/2438/23598/2/FullText.pdf (дата звернення: 29.12.2023).

19. Georgios C. Trichopoulos, Panagiotis Theofanopoulos. Design and Evaluation of Reconfigurable Intelligent Surfaces in Real-World Environment. URL: https://www.semanticscholar.org/reader/2a694efb0408e9ec801a819531f501b847c435c5 (дата звернення: 29.12.2023).

20. Ashok Kumar Reddy Chavva, Ratnakar Rao V. R. Reconfigurable Intelligent Surface (RIS) and Factors Influencing Its Role in Future Networks. URL:

https://research.samsung.com/blog/Reconfigurable-Intelligent-Surface-RIS-and-Factors-Influencing-it-s-Role-in-FutureNetworks#:~:text=RIS%20(Reconfigurable%20Intelligent%20Surface),transmission%20losses%20at%20high%20frequencies (дата звернення: 28.12.2023).