МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Сумський державний університет

Класичний фаховий коледж

(повна назва інституту/факультету)

(повна назва кафедри)

«До захисту допущено»

_____

_____ _____

(підпис) (Ім'я та ПРІЗВИЩЕ)

____ _____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавр

(бакалавр / магістр)

зі спеціальності 171 Електроніка ,

(код та назва)

освітньо-професійної програми Електронні інформаційні системи

(освітньо-професійної / освітньо-наукової)

(назва програми)

на тему: **Сучасна технологія високошвидкісного зв'язку MIMO**

Здобувача групи ЕІз-01к М.О. Анцибора

(шифр групи) (прізвище, ім'я, по батькові)

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

_____ _____

(підпис) (Ім'я та ПРІЗВИЩЕ здобувача)

Керівник ст. викладач. к.т.н. В.І. Васильєв

(посада, науковий ступінь, вчене звання, Ім'я та ПРІЗВИЩЕ) (підпис)

Консультант[1)] _____ _____

(посада, науковий ступінь, вчене звання Ім'я та ПРІЗВИЩЕ) (підпис)

Конотоп – 2024

Примітки:

1) Зазначається за наявності

ЗМІСТ

АНОТАЦІЯ

Об’єктом дослідження кваліфікаційної роботи є сучасна технологія високошвидкісного зв’язку MIMO.

Мета роботи полягає в дослідженнях рівня техніки за поставленою темою, способів визначення координат руху об’єктів, а саме: переміщення, швидкості, прискорення/уповільнення, ривку тощо. Досліджувались визначення основних параметрів руху наземних об’єктів, їх особливості, джерела похибок при проведенні контролю і способи запобігання від промислових і природних завад.

При виконанні роботи використовувалися методи математичного й цифрового й комп’ютерного моделювання процесів і систем.

Досліджувались методи забезпечення інформаційної безпеки безпроводових систем з технологією massive MIMO.

Робота викладена на 29 сторінках, у тому числі включає 12 рисунків, список цитованої літератури з 29 джерел.

КЛЮЧОВІ СЛОВА: БЕЗРОВІДНИЙ ЗВ’ЯЗОК, MIMO, WI-FI, BLUETOOTH, ZIGBEE,GSM, АНТЕНИ, ТЕХНОЛОГІЇ, БЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЇ .

ВСТУП

В даний час, що характеризується інформаційними проривами і активним використанням нових способів і методів передачі інформації, набули широкого поширення бездротові технології обміну даними з відповідними пристроями для реалізації точок входу, які можуть створювати віртуальні мережі. Протягом ряду років протікав процес стандартизації бездротових технології, збільшуваася швидкість передачі даних. Сьогодні вони дозволяють надавати підключення там, де неможливо кабельне з'єднання або потрібна повна мобільність.

При цьому потрібно зазначити, сумісність бездротових мереж з кабельними. Бездротові технології - це інформаційні технології, призначені для бездротової передачі інформації на відстані між двома і більше об'єктами. Інформація може передаватися з використанням інфрачервоного випромінювання, радіохвиль, оптичного або лазерного випромінювання. На сьогоднішній день розроблено вже велика кількість бездротових технологій, відомих по своїм маркетинговим назвами, наприклад, Bluetooth, WiMAX, Wi-Fi, MIMO та інші. Кожна технологія має певні характеристики, які визначають сферу її застосування.

Успіхи сучасної радіоелектроніки, розвиток мікропроцесорної техніки і нові алгоритми цифрової обробки сигналів разом з використанням перспективних телекомунікаційних технологій відкривають нові можливості по створенню безпровідних систем зв'язку з виконанням жорстких вимог, що стосуються високої пропускної здатності і перешкодозахищеності. Такі системи покликані забезпечувати розрахунок часу, ділове планування, підтримку постійного зв'язку з віддаленими станціями, зберігання документів. Принципом бездротових технологій став вираз «Ani time and ani where», тобто надання послуг зв'язку незалежно від місця і часу.

РОЗДІЛ 1
АНАЛІЗ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ ОБМІНУ ДАНИМИ

1.1 Технологія бездротової передачі даних Wi-Fi

Wi-Fi (англ. Wireless Fidelity — «безпровідна точність») — торгова марка Wi-Fi Alliance для бездротових мереж на базі стандарту IEEE 802.11.

Технологія Wi-Fi [1] - є першим промисловим стандартом, який дозволив організувати бездротову локальну мережу (Wireless Local Area Networks - WLAN) на обмеженій території, тобто коли кілька користувачів мають рівний доступ до загального каналу передачі даних. Стандарт був створений в Інженерному інституті електротехніки та радіоелектроніки (Institute Electrical and Electronics Engineers - IEEE) і може зрівнятися зі стандартом 802.3 для звичайних дротяних Ethernet мереж.

Зазвичай схема Wi-Fi мережі містить не менше однієї точки доступу (так званий режим infrastructure і не менше одного клієнта. Також можливе підключення двох клієнтів в режимі точка-точка, коли точка доступу не використовується, а клієнти з’єднуються за допомогою мережевих адаптерів «безпосередньо»

Перша специфікація стандарту WI-FI була прийнята в 1997 році. Вона встановила передачу даних на швидкості 1 і 2 Мбіт / с в неліцензійному діапазоні частот 2,4 ГГц, а також механізм управління доступом до фізичної середовищі (радіоканалу), який використовує метод множинного доступу з розпізнаванням несучої і усуненням колізій (Carrier Sense Multiple Access with Collision Avoidance, CSMA-CA).

Одночасно потрібно зазначити, що Міжнародна організація Wi-Fi Alliance презентувала новий стандарт бездротового зв'язку Wi-Fi 802.11ah «На Low» [2]. Діапазон роботи нового стандарту 900 МГц, саме на цій частоті пристрої Wi-Fi Certified можуть підключатися на більшій відстані з найменшими витратами енергії. За радіусу дії Wi-Fi «HaLow» приблизно в два рази перевершує використовувані в даний час варіанти Wi-Fi. Крім того, діапазон 900 МГц надає можливості, які необхідні для таких додатків, як мобільні електронні пристрої і датчики, які користувачі носять з собою.

На відміну від уже прийнятих стандартів, які працюють на частоті в 2,4 ГГц і 5 ГГц, Wi-Fi 802.11ah подвоює радіус дії сигналу, забезпечує надійне з'єднання, в разі,

якщо радіохвилі проникають через перешкоди, наприклад, стіни (див. Рис .1.1). Окремо потрібно звернути увагу на той факт, що, у зв'язку з альтернативної частотою, новий стандарт не схильний до перешкод від мікрохвильових печей і інших побутових приладів.

Розглядаючи більш детально сфери застосування технології бездротової передачі даних Wi-Fi [10], можна відзначити, що сьогодні вона використовується в багатьох областях діяльності. Найбільший попит технологія отримала у Інтернет провайдерів, оскільки це дозволяє їм відмовитися від десятків кілометрів проводів.. Також дана технологія використовується в ігровій індустрії. Такі відомі бренди як Sony і Nintendo монтують Wi-Fi пристрої в свої ігрові консолі, для забезпечення доступу до Інтернету. Деякі комерційні організації надають доступ до мережі Інтернет з використанням даної технології. Якщо ж розглядати великі компанії і корпорації, то вони використовують Wi-Fi для створення корпоративної мережі, так як це дешевше ніж створювати дротову мережу Ethernet.

Переваги технології [12]:

• Простота використання.

• Дозволяє розгорнути мережу без прокладки кабелю, що може зменшити вартість розгортання і / або розширення мережі.

• Wi-Fi пристрої широко поширені на ринку. Гарантується сумісність обладнання завдяки обов’язковій сертифікації обладнання з логотипом Wi-Fi.

Недоліки Wi-Fi:

• Високе, в порівнянні з іншими стандартами, споживання енергії, що зменшує час життя батарей і підвищує температуру пристрою.

• Найпопулярніший стандарт шифрування WEP може бути відносно легко зламаний навіть при правильній конфігурації (через слабку стійкість алгоритму).

Незважаючи на те, що нові пристрої підтримують досконаліший протокол шифрування даних WPA і WPA2, багато старих точки доступу не підтримують його і вимагають заміни. Прийняття стандарту IEEE 802.11i (WPA2) в червні 2004 року зробило доступною безпечнішу схему, яка доступна в новому устаткуванні. Обидві схеми вимагають більш стійкий пароль, ніж ті, які зазвичай призначаються

користувачами. Багато організацій використовують додаткове шифрування (наприклад VPN) для захисту від вторгнення

• Wi-Fi мають обмежений радіус дії. Типовий домашній маршрутизатор Wi-Fi стандарту 802.11b або 802.11g має радіус дії 45 м в приміщенні і 500 м зовні. Відстань залежить також від частоти.

• Накладення сигналів закритої точки доступу або точки, яка використовує шифрування доступу, і відкритої точки доступу, що працюють на одному або сусідніх каналах може перешкодити доступу до відкритої точки.

• Неповна сумісність між пристроями різних виробників або неповна відповідність стандарту може привести до обмеження можливостей з'єднання або зменшення швидкості.

• Зменшення продуктивності мережі під час дощу.

• Для зменшення втрати за умов поганої погоди прийнято при розрахунку Wi-Fi мережі ставити обладнання з запасом в третину потужності передавача.

• Перевантаження обладнання при передачі невеликих пакетів даних через приєднання великої кількості службової інформації.

1.2. Технологія бездротової передачі даних Bluetooth

Технологія Bluetooth (стандарт IEEE 802.15) [3-4] є першою технологією, яка дозволила організувати бездротову персональну мережу передачі даних (WPAN - Wireless Personal Network). Вона дає можливість проводити передачу голосу і даних з використанням радіоканалу на короткі відстані (10-100 м) в неліцензійному діапазоні частот 2,4 ГГц, а також з'єднувати мобільні телефони, ПК та інші пристрої в умовах відсутності прямої видимості. Стандарт Bluetooth має більше 10 профілів, тобто наборів функції пристроїв Bluetooth. Основними профілями, затвердженими групою розробників SIG є: - Advanced Audio Distribution Profile (A2DP) цей профіль призначений для забезпечення передачі музики в бездротові навушники; - Audio / Video Remote Control Profile (AVRCP) профіль, який дозволяє керувати функціями телевізора; - File Transfer Profile (FTP_profile) профіль, що забезпечує обмін даними між пристроями; - Hands-FreeProfile (HFP) профіль призначений для з'єднання бездротових навушників і мобільних пристроїв, оснащений також функцією розмови

по телефону; - LAN Access Profile (LAP) профіль, який забезпечує доступ до мереж LAN, WAN або Internet з використанням засобів іншого Bluetooth пристрою; - SIM Access Profile (SAP, SIM) профіль, що дозволяє отримати доступ до SIM-картки мобільного пристрою і використовувати одну SIM-карту на декількох пристроях; - Wireless Application Protocol Bearer (WAPB) профіль який зрівнює протокол для організації (Point-to-Point) з'єднання через Bluetooth, а також інші профілі.

Підсумовуючи можна сказати, що перевагами технології Bluetooth є: мобільність і малі розміри; простота використання готових модулів; значна швидкість передачі даних; безпеку передачі даних; доступність; необхідність авторизації пристрою; низький поріг чутливості до перешкод (залежить від товщини і матеріалу перешкоди); високий рівень стандартизації.

Однак, слід зазначити, що дана технологія не позбавлена і недоліків. Якщо, наприклад, два користувача хочуть обмінятися даними, то в процесі пошуку пристроїв один одного будуть знайдені всі пристрої, які включені в радіусі 10-15 метрів, що знижує швидкість ініціалізації пристроїв. Крім того, слід зазначити неможливість побудови мереж складної топології і великі (у порівнянні з мережами ZigBee) обсяги енергоспоживання.

Найчастіше технологія Bluetooth застосовується для забезпечення радіозв'язку між різними видами електронних пристроїв шляхом заміни ведучого послідовного з'єднання між двома пристроями на бездротове.

1.3 Технологія бездротової передачі даних ZigBee

ZigBee [5] — стандарт безпровідного зв’язку, призначений для систем управління і збору даних. Він дозволяє створювати самостійно організовуються і відновлюються бездротові мережі з підтримкою автоматичної ретрансляції повідомлень, а також мобільних і батарейних вузлів

Необхідність розробки технології ZigBee пов'язана, перш за все, з тим, що для певних операцій, наприклад, таких як дистанційне керування освітленням або воротами, зчитування інформації з датчиків, ключовими критеріями при виборі ефективної технології бездротової передачі є низька вартість і низьке енергоспоживання апаратної частини .

Мережі ZigBee називають мережами, які самоорганізуються і самовідновлюються[7]. Це пов'язано з тим, що ZigBee-пристрої, завдяки вбудованому програмному забезпеченню, при включенні харчування можуть самостійно знаходити один одного і створювати мережу, а в разі поломки будь-якого вузла наділені повноваженнями встановлювати нові маршрути для передачі повідомлень . Таким чином, технологію ZigBee можна використовувати як для забезпечення простих з'єднань «точка-точка» і «Зірка», так і для обслуговування складних мереж.

Стандарт передбачає роботу в частотних діапазонах 868 МГц, 915 МГц і 2,4 ГГц. Досягти максимальної швидкості і завадостійкості можливо використовуючи діапазон 2,4 ГГц. З цієї причини багато виробників мікросхем виробляють приймачі саме під цей діапазон. Він передбачає 16 частотних каналів з кроком 5 МГц. Технічна швидкість передачі даних, враховуючи службову інформацію, досягає 250 кбіт/с. Для передачі корисних даних, в залежності від кількості ретрансляцій і завантаженості мережі, середня пропускна спроможність вузла варіюється від 5 до 40 кбіт/с

ZigBee застосовується у випадку, коли в межах прямої видимості дальність радіозв’язку є недостатньо великою, і виникає потреба в її нарощуванні зі збереженням енергоспоживання на низькому рівні[13-14]. При веденні роботи всередині приміщення, відстані між вузлами мережі можуть становити десятки метрів, на відкритому просторі — сотні метрів. Зону покриття мережі можна значно збільшити за рахунок застосування репітерів.

Переваги технології:

• підтримка високого рівня захисту даних, що передаються;

• гнучкість в налаштуванні вузлів мережі;

• отримання швидкості обміну інформації по радіоканалу до 250 кбіт/с;

• підтримка в одній мережі до декількох тисяч вузлів;

• створення складних мережевих рішень, застосовуючи автоматичну маршрутизацію, ретрансляцію пакетів даних, а також відновлення роботи мережі при виході з ладу її окремих ділянок.

1.4 ТЕХНОЛОГІЯ GSM

Стандарт GSM (від назви групи Groupe Special Mobile, пізніше перейменований в Global System for Mobile Communications) [6] — глобальний цифровий стандарт для мобільного стільникового зв'язку другого покоління, з поділом каналу за принципом TDMA та високим ступенем безпеки завдяки шифруванню з відкритим ключем. Розроблено під егідою Європейського інституту стандартизації електрозв'язку (ETSI) наприкінці 80-х років.

Стандарт GSM є цифровим і забезпечує високу якість і конфіденційність зв'язку і надає абонентам великий набір послуг: автоматичний роумінг, прийом-передача даних, SMS-сервіс, голосова та факсимільна пошта. Основні недоліки стандарту: спотворення голосу при цифровій обробці і передачі його по радіоканалу, невеликий радіус дії базової станції, GSM телефон не може працювати при відстані від базової станції в 35 км.

GSM на сьогоднішній день є найбільш поширеним стандартом зв’язку[11]. За даними асоціації GSMA на даний стандарт доводиться 82% світового ринку мобільного зв’язку, 29% населення земної кулі використовує глобальні технології GSM. У GSMA в даний час входять оператори більш ніж 210 країн і територій.

Особливість GSM-1800 полягає в тому, що зона охоплення для кожної базової станції значно менше, ніж в стандартах GSM-900, AMPS / DAMPS, NMT-450. Необхідно більше число базових станцій. Чим вище частота випромінювання, тим менше проникаюча здатність (характеризується так званою глибиною скін-шару) радіохвиль і тим менше здатність відбиватися і огинати перешкоди.

Налаштувати зв’язок контролера та сервера за допомогою технології GSM можна використавши GSM модуль. Ціна такого модуля починається від 161 грн.

РОЗДІЛ 2
СУЧАСНА ТЕХНОЛОГІЯ ВИСОКОШВИДКІСНОГО ЗВ'ЯЗКУ MIMO

2.1 Принцип роботи технології MIMO

MIMO (англ. *Multiple Input Multiple Output*) — системи зв'язку з рознесеними передавальними і приймальними антенами [8]. Їхнє використання дозволяє проводити просторову і часову обробку сигналів, ефективніше використовувати випромінювану передавачем потужність і знижувати негативний вплив завад. Внаслідок цього пропускна спроможність MIMO-систем теоретично може бути збільшена пропорційно числу антенних елементів у порівнянні зі звичайними системами зв'язку, що використовують одноелементні антени (без збільшення повної випромінюваної потужності і смуги частот). Дана технологія є антиподом SISO, коли один вхід і один вихід.

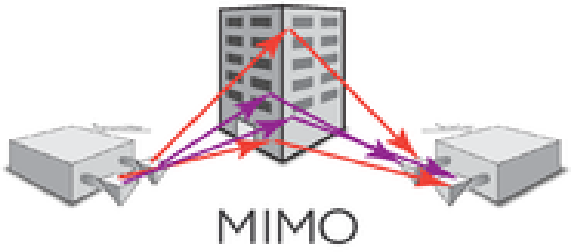

Рис. 2.1 Система MIMO

Технологія MIMO дозволяє на одному каналі організувати передачу відразу двох потоків інформації, які дублюють один одного. Зрозуміло, не можна змусити обладнання приймати і передавати два потоки просто так на програмному рівні без фізичної складової: технологію повинна підтримувати як базова станція, так і клієнтське обладнання.

Найпопулярніша і в той же час початкова конфігурація MIMO - 2x2. Також є 4x4, 8x8 і т. Д. Збільшення швидкості відбувається в два, чотири і вісім разів відповідно. Важливо відзначити, що це теоретичні дані, які на практиці можуть істотно відрізнятися.

Кожен потік приймається окремої антеною. Отже, для MIMO 2x2 потрібно 2 антени на прийом і 2 на віддачу. Усередині однієї базової станції знаходиться вісім антен, тобто чисто технічно оператори можуть передавати дані в чотири потоки (MIMO 4x4).

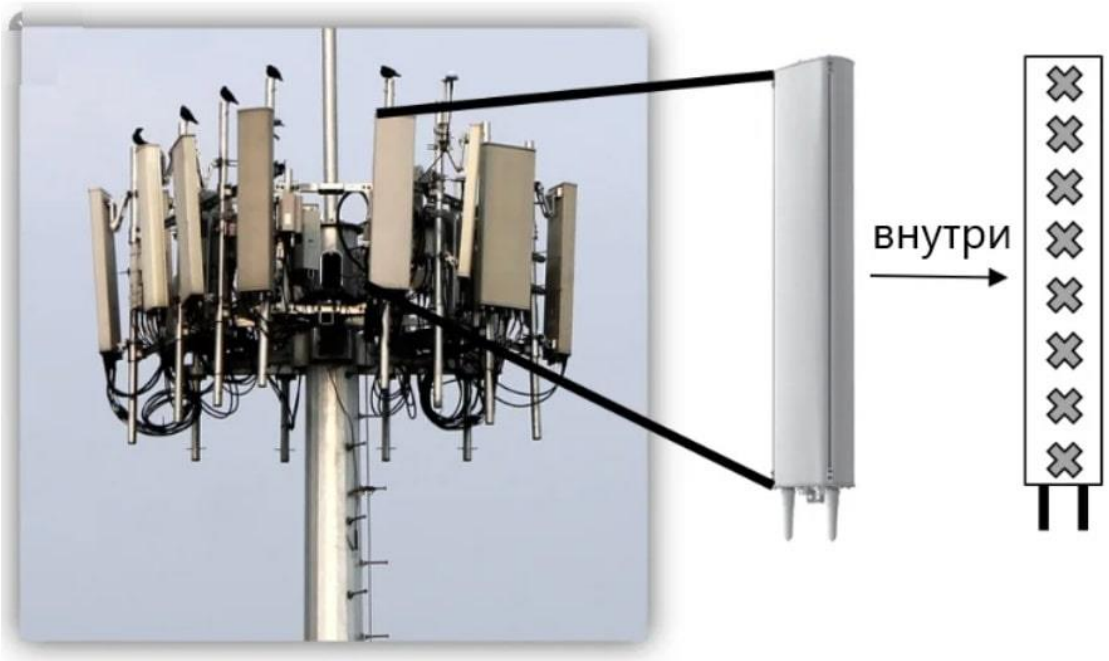

Рис. 2.2 Модель антени MIMO зсередини

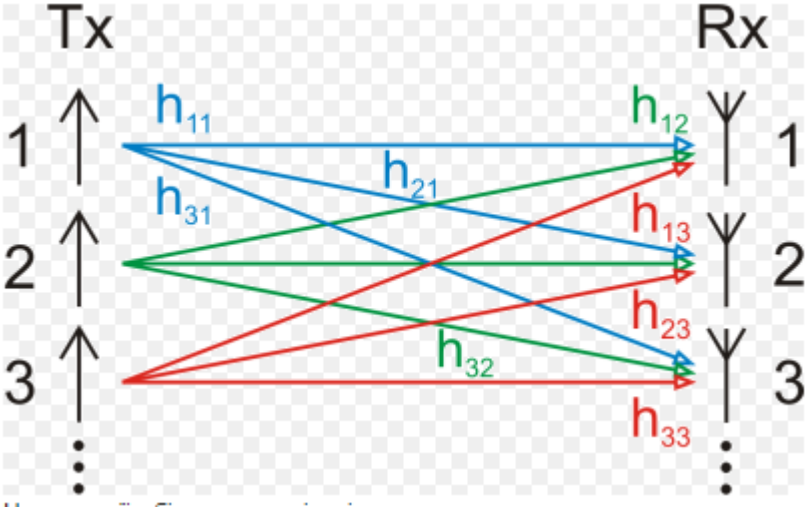

Рис. 2.3 Модель каналу MIMO

Високошвидкісний потік даних розбивається на M незалежних послідовностей з 1/M швидкості, які потім передаються одночасно з декількох антен, відповідно використовуючи тільки 1/M їх первинної смуги частот.

Перетворювач потоку даних на передавальному кінці лінії зв'язку перетворює послідовний потік у паралельний, а на приймальному — виконує зворотне перетворення.

З обладнанням користувачів все складніше: в смартфонах і модемах складно розмістити більше чотирьох антен (MIMO 2x2) через малі габарити корпусу. Що стосується модемів і роутерів, то у деяких ви можете помітити не один, а два роз'єми для зовнішньої антени. Це означає, що обладнання підтримує технологію MIMO 2x2.

Технологія MIMO використовується в базових станціях стільникового зв'язку стандарту 4G. Стандартом передбачено до 8 портів введення та 8 виведення на одну станцію. Стандарт 5G, як очікується, збільшить цю кількість вже до сотень[2]. Відповідні системи отримали назву **Massive MIMO** [20].

Massive MIMO - це система, в якій кількість терміналів користувачів набагато менше, чим кількість антен базової станції. Особливістю Massive MIMO є використання багатоелементних цифрових антенних решіток з кількістю антенних елементів 128, 256 і більше.

Відомі проекти систем стільникового зв'язку, що використовували систему Massive MIMO структури 100x100, розглядається можливість їхнього масштабування на випадок 1000-елементних цифрових антенних решіток. Зниженню вартості систем Massive MIMO у перерахунку на один канал сприятиме використання комбінованих методів децимації відліків АЦП, що сполучують зниження темпу надходження даних з їх попередньою (anti aliasing) фільтрацією, зсувом частоти і квадратурною демодуляцією сигналів. Крім того, спрощення обробки сигналів може досягатися адаптивною зміною кількості каналів у системі Massive MIMO в залежності від поточної завадової ситуації в ефірі, що забезпечується на основі кластерізації окремих груп антенних елементів цифрової антенної решітки у підрешітки.

Схемотехнічна база систем Massive MIMO спирається на використання модулів обробки сигналів стандартів CompactPCI, PCI Express, OpenVPX та інші. Технологія Massive MIMO є одною з ключових для реалізації систем стільникового зв'язку 5G і в подальшому — 6G.

2.2 Класифікація та особливості антен MIMO

Класифікація систем MIMO[9]. MIMO-системи можна класифікувати за наявністю або відсутністю зворотного зв’язку:

1) MIMO з „відкритою петлею” (open-loop). В даному випадку оцінку каналу на приймальному кінці використовується для корекції спотворень, що вносяться каналом.

2) MIMO з „замкнутою петлею” (closed-loop). Тут, крім оцінки каналу, на прийомі і компенсацією завад проводиться передача цих оцінок на передавальну сторону по т.з. зворотному (feedback) каналу.

За кількістю антен на передавальному та приймальному кінцях радіолінії розрізняють наступні системи:

MIMO – декілька передавальних та декілька приймальних антен;

MISO – декілька передавальних та одна приймальна антена;

SIMO – одна передавальна та декілька приймальних антен.

Відповідно до прийнятої класифікації звичайна радіолінія має назву SISO – одна передавальна та одна приймальна антена.

Системи радіозв’язку (СРЗ) з використанням технології MIMO забезпечують наступні преваги:

– розширення зони покриття радіосигналами та згладжування в ній „мертвих зон”;

– використання декількох незалежних шляхів розповсюдження сигналу, що підвищує ймовірність успішної роботи при впливі селективних завмирань;

– підвищення пропускної спроможності ліній зв’язку за рахунок формування фізично різних каналів (рис. 2);

– підвищення завадостійкості СРЗ.

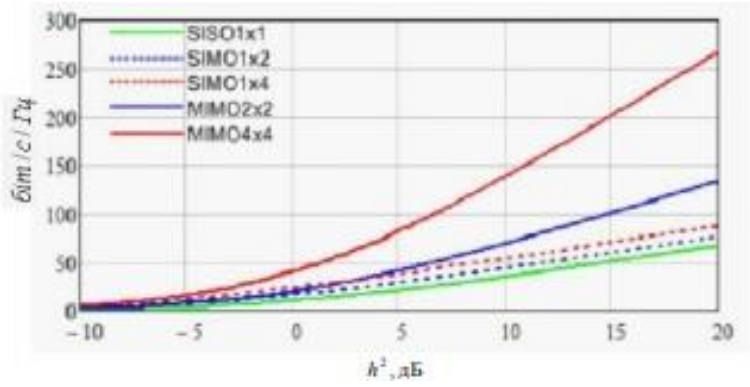

Рис. 2.4 Залежність пропускної спроможності від відношення сигнал/завада при різній кількості передавальних та приймальних антен

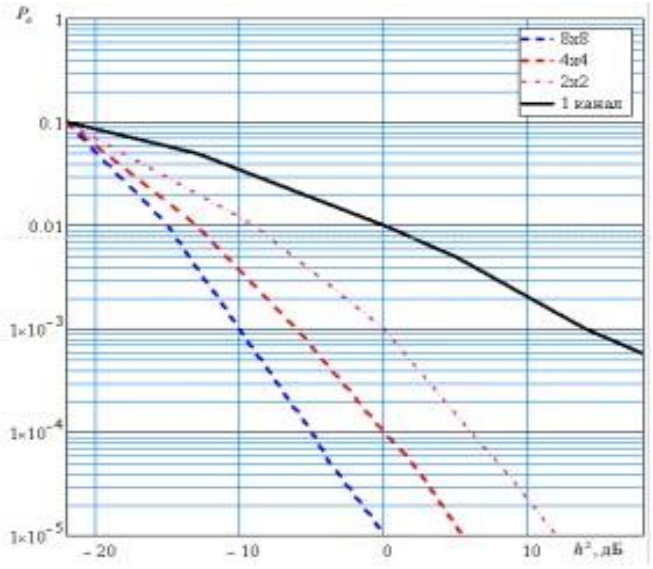

Рис. 2.5 Залежність ймовірності бітової помилки від відношення сигнал/шум для різної кількості антен

Системи MIMO з рознесеними передавальними і приймальними антенами дозволяють проводити просторову і часову обробку сигналів, ефективніше використовувати випромінювану передавачем потужність і знижувати негативний вплив завад [18]. Внаслідок цього пропускна спроможність теоретично може бути збільшена пропорційно числу антенних елементів в порівнянні зі звичайними системами зв’язку, що використовують одноелементні антени (без збільшення повної випромінюваної потужності і смуги частот).

2.3 Особливості антен MIMO

Сигнал від базової станції за технологією MIMO доноситься в горизонтальній і вертикальній поляризації (він посилається під різними кутами для кращого проходження через перешкоди)[17]. Стандартна антена здатна сприймати сигнал тільки у вертикальній поляризації, через що частина інформація просто втрачається. MIMO-антена, наприклад PicoCell AP-1700 / 2700-12 / 15 OD, - це по суті дві антени в одному корпусі. Це пояснює, чому такі вироби мають два роз'єми для підключення кабелю.

Деякі ентузіасти ставлять дві антени типу хвильовий канал, тільки одну кріплять на щоглі горизонтально, а другу - вертикально. Ефект від такого рішення мінімальний. Куди краще витратитися на якісну антену з узгодженням 50 Ом на роз'ємах.

Рис. 2.6 Порівняння антен з різною поляризацією

Раз заговорили про узгодження лінії, то відзначимо, що звичні багатьом телевізійні F-роз'єми - це рішення, які не годяться для мобільного обладнання, так як мають опір 75 Ом, тоді як гнізда у роутерів і модемів узгоджені на 50 Ом. Наш магазин пропонує тільки «правильне» обладнання з роз'ємами N-типу або SMA, які багаторазово знижують рівень шуму в лінії, а також попереджають перегрів клієнтських пристроїв в місцях, де сигнал знаходиться на межі повного зникнення.

Найефективніші MIMO-антени - ті, які на друкованій платі [19]. Патчі можуть мати X-поляризацію (універсальну) або яскраво виражену вертикальну і горизонтальну. У розділі «Антени GSM, 3G, 4G і Wi-Fi» представлені різні варіанти обладнання.

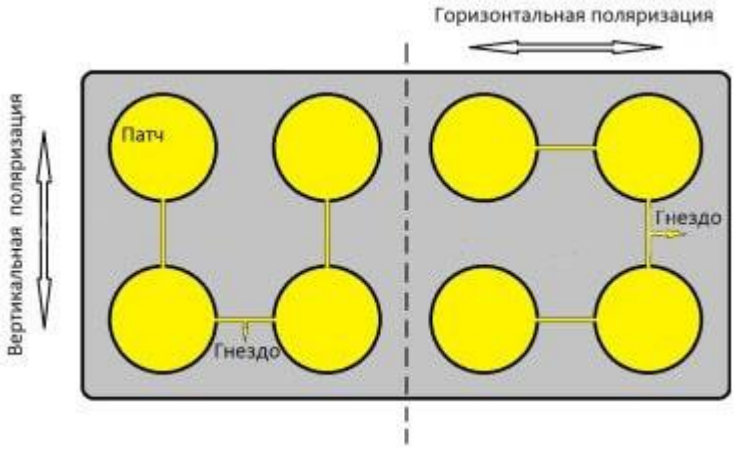

Рис. 2.7 MIMO-антена на друкованій платі

Переваги MIMO

Основний плюс технології - підвищення швидкості мобільного інтернету, проте не потрібно думати, що показники виростуть у кілька разів. Як показує практика, швидкість підвищується на 25-35%.

Друга перевага - MIMO може застосовуватися для прискорення LTE, а також Wi-Fi, 3G і WiMAX.

За рахунок двох і більше незалежних потоків інформації стабільність з'єднання значно зростає. Якщо це MIMO-антена, то підключення другого кабелю покращує якість прийому сигналу в кілька разів.

За допомогою MIMO мобільні оператори отримують можливість підвищити пропускну здатність мережі, не вдаючись до розширення каналу. Єдине - пристрої абонентів повинні підтримувати технологію.

MIMO - відносно молода розробка: перші конфігурації з'явилися тільки в 1984 році. Сьогодні фахівці шукають шляхи для одночасного запуску 64 потоків даних. Можливо, в майбутньому вдасться досягти колосальних швидкостей передачі даних.

2.4 Перспективи застосування технології MIMO у військових системах радіозв'язку

Для реалізації MIMO необхідно забезпечити рознесення антен на відстані, достатні для забезпечення достатнього рівня некорельованості просторових каналів [16]. Таким чином, зі зменшенням робочої частоти зростає і відстань між антенними елементами. Тому для портативних (носимих) радіостанцій, на відміну від стаціонарних та рухомих (автомобільних), у традиційному діапазоні, що використовується військовими СРЗ (від 30 до 110 та навіть 512 МГц) реалізувати багатоантенну систему складно. Тому можна розглядати наступні варіанти з'єднань у військових СРЗ: MIMO – між двома рухомими станціями; MISO – при передачі від рухомої до портативної; SIMO – при передачі від портативної до рухомої; SISO – при обміні між двома портативними. У той же час, у більш високому діапазоні частот (понад 1 ГГц), принаймні ранцеві радіостанції цілком можуть бути оснащені багатоантенними системами.

Технологія MIMO, яка була розроблена для боротьби з багатопроменевістю та підвищення пропускної спроможності радіоліній в умовах щільної міської забудови, не передбачає можливість ефективної роботи в умовах впливу навмисних завад без застосування додаткових технічних заходів.

Цифрові антенні решітки. Одним з найбільш ефективних методів підвищення завадозахищеності СРЗ з MIMO є використання адаптивних антенних решіток.

Антенними решітками (АР) прийнято називати випромінюючі системи у вигляді великого числа дискретних випромінювачів, розташованих упорядкованим чином [21]. Структурна схема АР, представлена на рис. 2.8. Потужність з виходу передавача надходить на діаграмоутворюючу схему (ДУС), де за командами управляючого пристрою здійснюється її розподіл у потрібній пропорції між випромінювачами решітки, а також забезпечення необхідних фазових зсувів між струмами в них. Для вирішення цієї задачі в ДУС застосовуються дільники потужності, фазообертачі, комутатори, атенюатори та інші елементи.

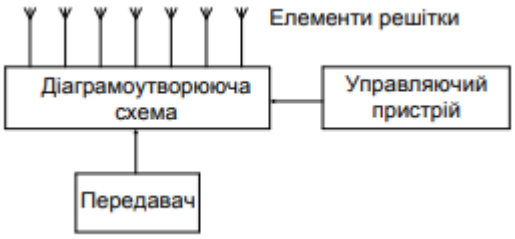

Рис. 2.8 Структурна схема антенної решітки

Адаптивні антенні решітки (ААР) – антенні решітки, параметри яких (у першу чергу, характеристика направленості) автоматично змінюються таким чином, щоб забезпечити якнайкращі умови прийому корисного сигналу на фоні змінних зовнішніх впливів (завад), або передачі сигналу, виходячи із задач, що вирішуються радіоелектронним засобом (наприклад, якщо це радіостанція – сформувати максимум діаграми направленості (ДН) у напрямку на кореспондента та мінімуми – у напрямках на інших користувачів, найближчих до неї).

Одним із найбільш перспективних напрямів розвитку цього виду антенної техніки є цифрові антенні решітки, які виконують діаграмоутворення за допомогою цифрової обробки сигналу, що забезпечує можливість адаптивного формування багатопроменевої діаграми направленості. ЦАР дозволяють реалізувати значно вищий рівень завадозахищеності в порівнянні з ФАР за рахунок формування більш глибоких провалів у ДН у напрямках на джерела завад та точнішого вимірювання просторових напрямків кореспондентів, а також забезпечують більшу швидкодію.

Режим MIMO, по суті, відповідає роботі ЦАР з формуванням множини променів на прийом і передачу.

Обробка прийнятих сигналів в ЦАР ділиться на 2 етапи: входження в зв’язок і передача даних. У кожному з вказаних режимів застосовуються свої алгоритми обробки сигналів. В режимі входження в зв’язок спочатку аналізується завадова обстановка в каналі зв’язку шляхом пеленгації джерел активних завад для подальшого віднімання відгуків завадових сигналів з результуючих напруг вторинних каналів. Пеленгація може бути реалізована за допомогою методів спектрального оцінювання:

– оптимальний (максимальної правдоподібності);

– квазіоптимальні (MUSIC, Кейпона, ESPRIT);

– класичні (максимуму діаграми направленості, багато імпульсний та ін., засновані на електронному скануванні діаграмою направленості в просторі).

Важливою особливістю функціонування ЦАР є цифрове формування променів характеристики направленості, яке дозволяє ефективно реалізувати динамічну оптимізацію зони покриття на основі оперативного перенацілювання цифрових приймальних променів за групами кореспондентів в залежності від їх розташування на місцевості. Сузір'я приймальних променів може синтезуватися, наприклад, за алгоритмами швидкого перетворення Фур'є і представляє собою, по суті, сукупність „просторово-частотних фільтрів", кожний з яких виділяє строго визначений набір сигналів і подавлює інші, які одночасно приймаються в широкому просторовому секторі, як завади.

При цьому суттєво покращується якість зв'язку в умовах багатопроменевого поширення радіохвиль, а також різко підвищується завадозахищеність системи у випадку інтенсивної радіопротидії.

Експерименти підтверджують можливість подавлення активної шумової завади у восьмиелементній ЦАР більш ніж на 30 дБ, причому не тільки по бічних, але і у основному пелюстку ДН, при середньоквадратичному відхиленні коефіцієнтів підсилення аналогових приймальних каналів 0,5 дБ і величині фазових помилок не більше 3º.

Особливий інтерес представляє застосування технологій MIMO та ЦАР у військових мобільних радіомережах MANET (Mobile Ad-Hoc Network). Відомими недоліками роботи таких мереж з використанням ненаправлених антен є наступні: складність забезпечення сучасних вимог до якості обслуговування при великій кількості ретрансляцій, непостійність пропускної спроможності радіоканалу, залежність пропускної спроможності від відстані між рухомими радіостанціями, потужності передачі, кількості сусідніх вузлів та рівня створюваного ними трафіка.

Встановленню зв'язку в мобільних радіомережах з направленими антенами передує попереднє виявлення засобу радіозв'язку (ЗРЗ), що веде передачу, приймальним. Далі визначається напрямок приходу сигналу при роботі на прийом і

відбувається формування ДН з основним пелюстком у відповідних напрямках (φ12 та φ21) при роботі на передачу і прийом обома станціями, як показано на рис. 2.9.

Кожен мобільний радіовузол повинен забезпечувати ретрансляцію пакетів на різних (можливо, декількох) інформаційних напрямках, а також здійснювати подавлення завадових сигналів (також, можливо, з декількох просторових напрямків). Тому виникає завдання розробки математичних моделей, які дозволять врахувати вказані умови, а також розробки методик оперативного управління параметрами СРЗ.

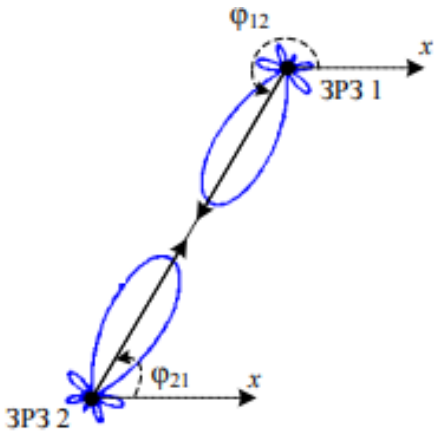

Рис. 2.9 Приклад орієнтації ДН засобів радіозв’язку на радіолінії

РОЗДІЛ 3
ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БЕЗПРОВОДОВИХ СИСТЕМ З ТЕХНОЛОГІЄЮ MASSIVE MIMO

3.1 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 [22]. В цьому діапазоні досить високий рівень загасання сигналів у вільному просторі. Радіус зони дії базової станціїї суттєво зменшується, як можна побачити на рис. 3.1.

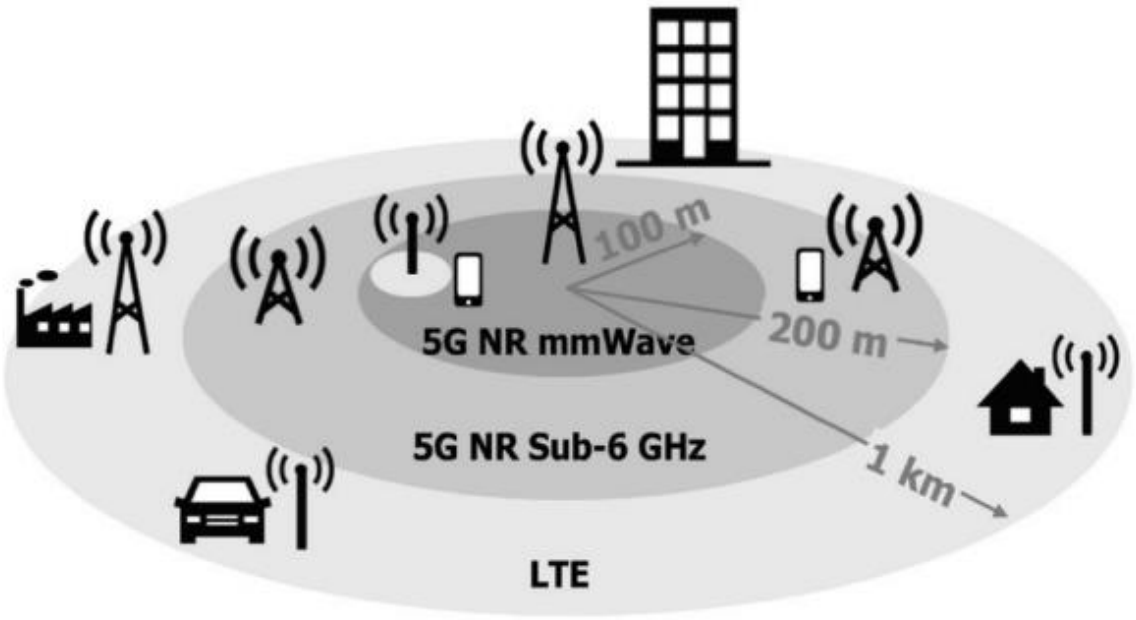

Рисунок 3.1 – Зони дії базової станції телекомунікаційних систем різних поколінь

Для вирішення цієї проблеми запропоновано використовувати реконфігуруємі інтеллектуальні поверхні Reconfigurable Intelligent Surfaces (RIS). Ці поверхні працюють як пасивні відбиваючі поверхні, але з ефектом фокусування – концентрації енергії в заданих напрямках. На рисунку 3.2 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, 55 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.

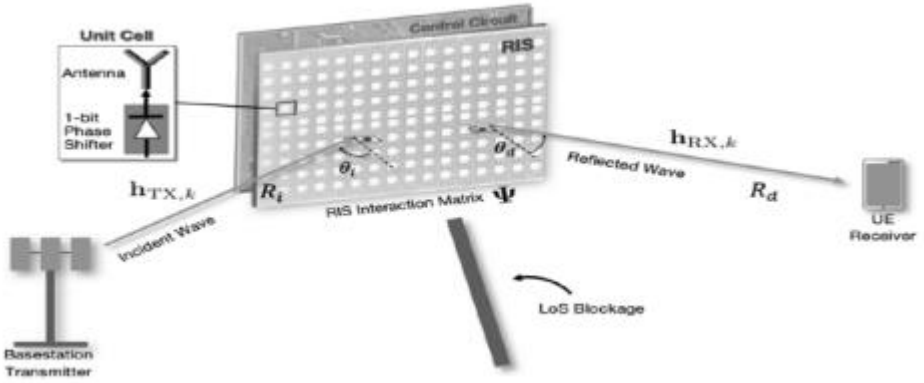

Рисунок 3.2 – Схема інтеллектуальної поверхні RIS

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.

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.

3.2 Забезпечення безпеки на основі захищеного Internet протоколу.

Протокол IPsec заведено використовувати у не сервісно-орієнтованих інтерфейсах між базовою станцією gNB і ядром 5G [15]. 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.

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.

3.3 Забезпечення безпеки на рівні транспортного протоколу.

Серед сервісно-орієнтованої архітектури усі інтерфейси на основі послуг мають бути захищені за допомогою Transport Layer Security (TLS) [23].

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.

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 ecdsa_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.

3.4 Атаки прикладного рівня.

Атаки прикладного рівня можуть бути або DoS, або DDoS-загрози [24]. 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.

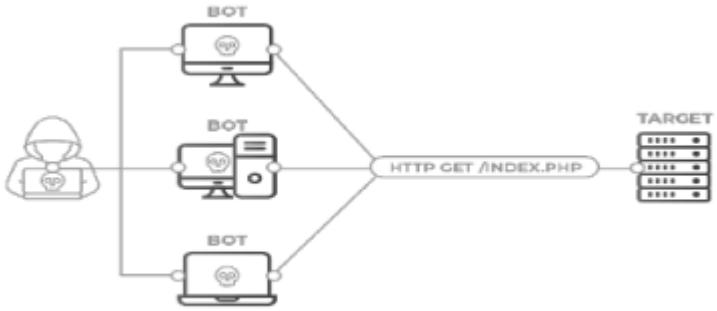

Рисунок 3.1 – Атака HTTP-флудом

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 41 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.

ВИСНОВКИ

На основі проведеного в роботі аналізу сучасної технології високошвидкісного зв’язку MIMO можна зробити такі висновки:

1. Використання технології MIMO в системах радіозв’язку дозволяє значно збільшити частотну ефективність (пропускну здатність) системи. Так застосування в системі двох передавачів і двох приймачів призводить до двократного зростання пропускної здатності при тій же смузі частот, виділеної для роботи системи.

2. 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.

3. 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.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кучеренко О. С. Безпека бездротових мереж на базі технології Wi-Fi // Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Радіофізика та електроніка. - 2017. - Вип. 29. - С. 3-8.

2. Хоменко А. П., Мельник Л. В., Осаволюк Л. І. Використання технології Wi-Fi у бездротових системах зчитування інформації // Інформаційні технології в освіті та науці. - 2019. - Т. 1. - С. 81-85.

3. "Технологія Bluetooth: принципи роботи та використання" - автор Ігор Гавриїльович Худяк

4. "Bluetooth та бездротові технології зв'язку" - автор Олександр Заліско

5. Ільченко М.Ю. Сучасні телекомунікаційні системи / Ільченко М.Ю., Кравчук С.О. –К.: НВП „Видавництво „Наукова думка” НАН України”, 2008.

6. SIM900 GSM/GPRS RS232 Modem - User Manual," [Online]. Available: https://www.rhydolabz.com/documents/gps_gsm/sim900_rs232_gsm_modem_opn.pdf

7. Свердлова, А. А. Огляд сучасних технологій бездротового зв'язку.

8. Беделл, П. "Мережі. Бездротові технології"/ П. Беделл // М.: НТ Пресс, 2008. - 448с.

9. Вишневський, В.М. Широкосмугові бездротові мережі передачі інформації / В.М. Вишневський, А.І. Ляхов, С.Л. Кравець, І.В. Шахновіч // М.: Техносфера, 2005. - 591с.

10. Стрельников, А. Ю. Технологія бездротової передачі даних Wi-Fi / А.

Ю. Стрельников, С. А. Страмоусова // Молодий вчений. – 2016.– №9-4 (113). – с. 67-69.

11. "GSM 900 или GSM 1800 []," [Online]. Available: https://www.gsmsota.com.ua/blog/novosti/gsm-900-ili-gsm-1800/.

12. "Wi-Fi Working Principle," [Online]. Available: https://www.elprocus.com/how-does-wifi-work/.

13. "Bezdrotova merezha ZigBee, yiyi perevahy ta osoblyvosti,shcho potribno dlya toho, shchob sformuvaty personal' numerezhu ZigBee [Бездротова мережа ZigBee, її переваги та особливості, що потрібно для того, щоб сформувати персональну мережу ZigBee]," [Online]. Available: http://ipkey.com.ua/uk/faq/966-zigbee.html.

14. "Besprovodnyye seti ZigBee i Thread [Беспроводные сети ZigBee и Thread]," [Online]. Available: http://www.wless.ru/technology/?tech=1.

15. 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.

16. Performance analysis of MIMO-OFDM for LTE tactical communication systems in jamming environment / [S. Malisuwan, J. Sivaraks, N. Tiamnara, N. Suriyakrai] // International journal of advances in electronics and computer science. – Volume-3, Issue-1. – Jan., 2016.

17. Кувшинов О.В. Аналіз характеристик систем радіодоступу з технологією MIMO /О. В. Кувшинов, Д. А. Міночкін // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – Вип.№ 3 – К.: ВІКНУ, 2006. – С. 51– 56.

18. Redl, Siegmund M. An introduction to GSM / Siegmund M. Redl, Matthias K. Weber, Malcolm W. Olipfant / Artech House Boston, London, 1995 https://books.google.com.ua/books/about/An_Introduction_to_GSM.html?id=9Ud4QgAACAAJ&redir_esc=y

19. Cellular and PCS/PCN Telephones and Systems. An Overview of technologies, Economics, and Services / By Lawrence Harte and Steve Prokup / APDG Publishing: www.cybercom.net/ - apdg ,1996.
https://www.wirelessnetworksonline.com/doc/cellular-and-pcspcn-telephones-and-systems-an-0001
https://www.amazon.co.uk/Cellular-PCs-Pcn-Telephone-Systems/dp/0965065812

20. "Fundamentals of MIMO Communication" авторства David Tse і Pramod Viswanath

21. "MIMO: From Theory to Implementation" авторства Alain Sibille

22. E. Balevi, A. Doshi, and J. G. Andrews, “Massive MIMO channel estimation with an untrained deep neural network”, IEEE Transactions on Wireless Communications, vol. 19, no. 3, pp. 2079–2090.

23. "Сучасні підходи до захисту транспортних протоколів" - В. Іванов

24. "Що таке атака прикладного рівня".
https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-ddos-attack