SECTION 3. COMPUTER SCIENCE

DOI: 10.46299/ISG.2023.MONO.TECH.4.3.1

3.1 Proactive protection of 5G NR networks from jamming attacks

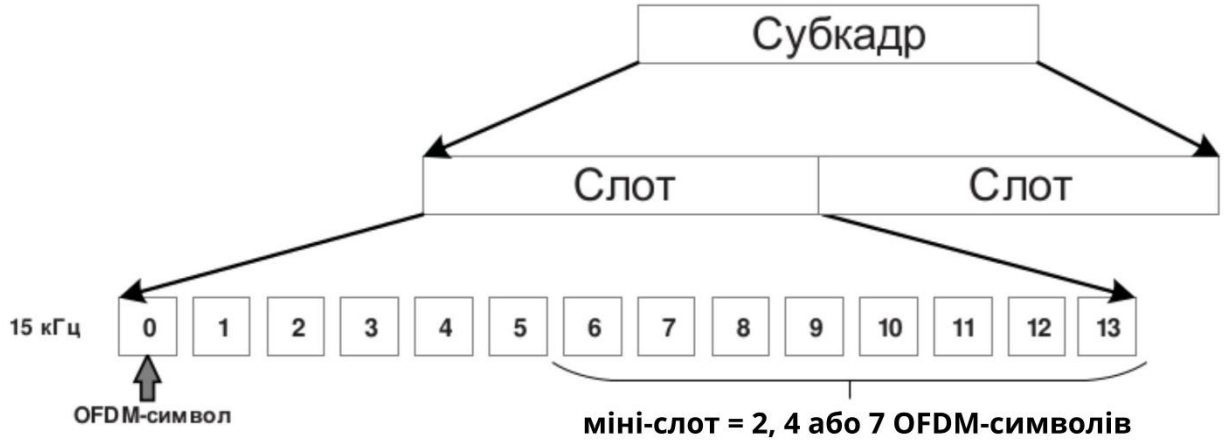
Розвиток технології зв'язку 5G, останнього досягнення в бездротових стільникових мережах, відкриває потенціал для підвищення швидкості передачі даних і надійного надання послуг. Задумана як каталізатор новаторських інновацій, таких як Інтернет речей (IoT - Internet of Things), автономні транспортні засоби та інтелектуальні міські центри, ця технологія знаходиться на порозі зміни нашого цифрового світу.

Щоб реалізувати це бачення, партнерська асоціація груп телекомунікаційних компаній *3GPP* (3rd Generation Partnership Project) випустила базову специфікацію нового радіо 5G у 2017 році, яка стане основою для наступного покоління мобільних мереж [96]. Розробка 5G NR (5G New Radio) є частиною постійного процесу розвитку мобільної широкосмугової мережі для задоволення вимог 5G, як зазначено в IMT-2020, подібно до розвитку бездротових технологій 3G та 4G. У минулих 3G і 4G основний акцент ставився на підключенні абонентів мережі, але у майбутньому 5G буде підключати все, це означає, що 5G NR буде підключати смартфони, автомобілі, лічильники, переносні пристрої та ін. Передбачається, що ціна за біт інформації відповідно буде нижча, нижчі будуть затримки при передачі даних, висока щільність обслуговування, яка становить більш мільйона користувачів на один квадратний метр, мінімальний час доставки пакету не більш 1 мс, надійність передачі інформації не менше 99,999% та максимальна енергоефективність. Завдяки новим вимогам, щодо затримки, надійності та безпеки, 5G NR буде масштабуватися для ефективного підключення великого різноманіття Інтернету речей (IoT) та зможе запропонувати нові типи критично важливих послуг. Архітектура 5G NR має п’ять основних принципів, що лежать в основі її дизайну: використання нових частот радіочастотного спектру, багатоелементні антенні решітки MIMO (multiple input multiple output - багатоелементні цифрові антенні

решітки), багатофункціональне підключення через різноманітний доступ до технології, гнучкі віртуалізовані мережі та посилений захист.

5G працює в широкому діапазоні радіочастот від 1 ГГц до 100 ГГц, що значно перевищує робочі частоти попередніх стільникових систем. Фізичний рівень базується на OFDM-модуляції (OFDM - orthogonal frequency-division multiplexing, мультиплексування з ортогональним частотним поділом) у низхідній лінії зв'язку. Для висхідної лінії зв'язку підтримується як OFDM, так і варіант під назвою OFDM з дискретним перетворенням Фур'є.

Структура субкадру 5G NR, наведена на малюнку 1, складається з 10 підкадрів, кожен з яких містить 14 символів OFDM, з тривалістю 10 мс.



Малюнок 1. Структурна схема субкадра 5G NR

Для гнучкого розподілу ресурсів між висхідною та низхідною лінією зв'язку на фізичному рівні може використовуватися як мультиплексування з частотним поділом каналів (FDD - Frequency Division Duplex, дуплексний канал с частотним поділом), так і мультиплексування з часовим поділом каналів (TDD -Time Division Duplex, дуплексний канал с часовим поділом) [97]. Завдяки доступу до широкого спектру та застосуванню передових антенних технологій, таких як формування променя Massive MIMO, 5G досягає кращої пропускної здатності порівняно зі старими мережами. Massive MIMO використовує великі масиви з сотнями антенних елементів для точного просторового мультиплексування та керування променем. Це дозволяє фокусувати сигнали на конкретних

користувачів, одночасно зменшуючи перешкоди. 5G також об’єднує різноманітні типи підключення від мобільного широкосмугового зв’язку до надійних з’єднань з низькою затримкою. Програмне забезпечення мережі за допомогою SDN (software-defined networking - програмно-визначувана мережа) і NFV (network functions virtualization - віртуалізація мережевих функцій) забезпечує гнучкість дозволяючи оптимізувати потужності мережі до послуг, що надаються у відповідності з вимогами.

Працюючи у широкому діапазоні частот, 5G NR має широку смугу частот, що досягає 100 МГц нижче 6 ГГц, а вище цього порогу смуга частот становить 400 МГц. Центральне місце в архітектурі фізичного рівня 5G NR займають окремі канали для організації низхідної і висхідної передачі даних. Множина низхідних каналів включає в себе загальний низхідний канал (PDSCH - physical downlink shared channel), широкомовний канал (PBCH - Physical Broadcast Channel) і канал управління низхідною лінією (PDCCH - physical downlink control channel). Аналогічно, спектр каналів висхідної лінії зв'язку включає спільний канал висхідної лінії зв'язку (PUSCH - physical uplink shared channel), канал управління висхідною лінією зв'язку (PUCCH - physical uplink control channel) і канал довільного доступу (PRACH - physical random access channel).

Складність фізичного рівня 5G NR ще більше посилюється включенням масиву опорних сигналів і пілотних сигналів синхронізації - до них відносяться первинний сигнал синхронізації (PSS - primary synchronization signal) і вторинний сигнал синхронізації (SSS - secondary synchronization signal). Ці сигнали виконують критично важливу роль синхронізації між базовими станціями і користувацьким обладнанням (UE - user equipment), одночасно передаючи важливу ідентифікаційну інформацію про елемент мережі. Примітно, що PSS і SSS мають складні конфігурації послідовностей і підносійних, ретельно розроблені для полегшення диференціації базових станцій, навіть у сценаріях зі зниженим співвідношенням сигнал/шум (SNR - signal-to-noise ratio) [98].

Фундаментальний принцип 5G NR знаходить своє вираження в масштабованій нумерології NR, динамічній структурі, пристосованій для

узгодження з різноманітною множиною радіочастот, смуг пропускання і спеціалізованих послуг 5G. Це тягне за собою впровадження різних інтервалів між підносійними (SCS - subcarrier spcaing) - наприклад, 15, 30, 60 і 120 кГц, кожен з яких відповідає потребам макропокриття, малих сот, приміщень і частот діапазону міліметрових хвиль, відповідно. Взагалі архітектура мережі 5G NR тісно перекликається зі своєю попередницею 4G/LTE, прикрашеною тонкими нюансами.

Заглиблюючись у сферу кодування 5G NR, слід зазначити що в мережі 5G використовується гетерогенний підхід, при якому коди з низькою щільністю перевірки парності (LDPC - low-density parity-check) використовують у каналі передачі даних, тоді як полярне кодування використовується в каналі управління. Коди LDPC демонструють хорошу ефективність при виправленні помилок у процесі обробки невеликих пакетів даних. На противагу цьому, потенціал полярного кодування використовується для колосальних масивів даних, забезпечуючи продуктивність, яка впритул наближається до знаменитої межі Шеннона, хоча і краще підходить для сценаріїв передачі об'ємних даних.

Доповненням архітектури 5G NR є плавне впровадження технології масового багатоканального вводу-виводу (MIMO - multiple-input/multiple-out) - інновація, яка розширює як покриття, так і пропускну здатність, вдихаючи нове життя в саму суть бездротових стільникових мереж [99 - 102]. Складна взаємодія цих аспектів спільно вибудовує структуру 5G NR - архітектура, захищена від примарних атак "розумного" глушіння.

Хоча 5G обіцяє суттєві переваги, його складність створює нові вразливості, якими можуть скористатися зловмисники. У мережах 5G, як і в будь-якій бездротовій стільниковій мережі, вразливості виникають через їхню залежність від відкритого простору комунікаційного середовища - необмеженої області вільного простору. Ця вразливість підкреслюється потенційною можливістю виникнення перешкод - явища, здатного значно погіршити продуктивність цих мереж, перешкоджаючи точному декодуванню сигналів на стороні приймача. У цьому контексті виникає тривожна перспектива:

зловмисники можуть скористатися цією вразливістю, здійснюючи атаки "глушіння", які здатні порушити зв'язок користувачів у певних бездротових каналах. Історичні передумови атак типу "глушіння" ("jamming") свідчать про їхнє попереднє використання на військових театрах бойових дій, що підтверджує їхню здатність спричиняти хаос у сучасних комунікаційних мережах [103, 104]. Ситуація ще більше ускладнюється сучасним поширенням доступних за ціною пристроїв для створення перешкод, а також можливістю здійснювати складні атаки за допомогою програмно-визначених радіоінструментів і навичок програмування, що значно підвищує потенціал для радіоатак.

Хитросплетіння таких атак з глушінням ґрунтується на їхній здатності маніпулювати самим ядром архітектури мережі 5G. В основі цих атак лежить цілеспрямована і добре відкалібрована стратегія перешкод, коли радіочастотні сигнали навмисно закриваються фальшивим шумом. Результатом є порушення когерентності переданих даних, що призводить до деградації сигналу і, зрештою, перешкоджає безперебійному потоку інформації. Це порушення може проявлятися у вигляді стрибків, затримок, зниження швидкості передачі даних і навіть повної втрати сигналу, що серйозно впливає на якість роботи користувачів.

Сучасні атаки з "розумним глушінням" відрізняються підвищеною складністю, що частково пояснюється технологічним розвитком самого ландшафту 5G. Фундамент 5G побудований на багатогранній архітектурі, що охоплює різні частотні діапазони, передові методи модуляції і складний набір методологій формування променя. Саме ці характеристики, що забезпечують покращену ефективність 5G, також створюють сприятливий ґрунт для зловмисних маніпуляцій. Зловмисники, озброєні поглибленим розумінням цих тонкощів, можуть організовувати атаки глушіння, націлені на певні частотні діапазони, або використовувати вразливості, притаманні алгоритмам формування променя. Такі атаки можуть бути налаштовані на різний рівень - від постановки шумоподібних перешкод в широкому діапазоні спектру використовуваних частот до вузькоспрямованих атак на критично важливі лінії зв'язку.

У відповідь на такі зростаючі загрози наукове співтовариство і галузеві експерти активно працюють над розробкою контрзаходів і оборонних стратегій для захисту мереж 5G від атак "розумного" глушіння. Розробляються вдосконалені алгоритми обробки сигналів, механізми виявлення аномалій та інтелектуальні методи аналізу спектру для швидкого виявлення та пом'якшення наслідків перешкод. Крім того, інтеграція можливостей когнітивного радіо, які дозволяють пристроям динамічно адаптувати параметри передачі, обіцяє підвищити стійкість мережі.

Серед безлічі викликів значне занепокоєння викликають генератори перешкод - бездротові пристрої, що використовуються зловмисниками для порушення безперебійного функціонування бездротових мереж стільникового зв'язку. Ця категорія охоплює різні типи генераторів перешкод, кожна з яких використовує різні стратегії для реалізації зловмисних намірів:

1) звичайні генератори перешкод - посідають чільне місце серед засобів, які створюють завади. Ці засоби, під виглядом звичайних пристроїв, здійснюють безперервне випромінювання радіочастотних сигналів, нехтуючи встановленими протоколами контролю доступу до середовища (MAC - medium access control). Такий підхід характеризується значним споживанням енергетичних ресурсів, що призводить до помітного виснаження заряду батареї хоста, який здійснює атаку. Таким чином, генерування таких перешкод накладає обтяжливі енергетичні витрати на пристрій, що здійснює атаку, ефективно висмоктуючи його запаси енергії і з часом роблячи його менш ефективним. Цікаво, що відмінною рисою цих звичайних генераторів перешкод є відсутність необхідності відстежувати діяльність підключених користувачів у мережі.

Основна відмінність між звичайними генераторами перешкод та їхніми аналогами полягає в їхньому підході до динаміки мережі. На відміну від більш складних механізмів глушіння, які тонко аналізують поведінку зареєстрованих у мережі користувачів і реагують на неї, звичайні генератори перешкод працюють з відвертим ігноруванням таких нюансів. Така нерозбірливість є одночасно і

обмеженням, і відмінною рисою, що підкреслює складність протидії таким невибірковим перешкодам;

2) оманливі генератори перешкод, які ще також називають оманливими перешкодами, вводять дійсні бітові шаблони в канал зв’язку, змушуючи об’єкт-одержувач помилково зробити висновок, що передача походить із законного джерела. Виявлення таких ворожих атак є складним завданням через високу схожість між штучними та автентичними сигналами. Завдяки впровадженню автентичних послідовностей даних зловмисник-передавач успішно вводить одержувача в оману. Диференціація легітимної та оманливої передач залишається відкритою проблемою дослідження через порівнювані характеристики;

3) стохастичні перешкоди використовують стратегію періодичного блокування для досягнення економії енергії. Завдяки чергуванню між активним і неактивним станами, передавач зберігає енергію під час періодів простою. Під час активної фази в канал зв'язку вводяться перешкоди з попередньо визначеною тривалістю, перш ніж радіопередавач буде деактивовано. Вводячи випадкові перешкоди спорадичним чином, ефективність глушіння на одиницю потужності можна суттєво підвищити;

4) реактивні перешкоди, на відміну від активних перешкод, ґрунтуються на постановці адаптивних перешкод в каналі зв'язку. Замість того, щоб постійно передавати шуми, реактивні генератори перешкод контролюють канал і ініціюють блокування лише тоді, коли в ефірі виявляється транслювання, яке слід подавити. Ця селективна стратегія спрямована на підвищення енергоефективності шляхом усунення непотрібного споживання електроенергії під час періодів простою. Завдяки динамічному вибору частоти реактивні генератори перешкод ще більш мінімізують свій слід, вибираючи канали, які на даний момент проявляють активність. Однак реактивні підходи стикаються з проблемами швидкого виявлення цільових сигналів і активації перешкод до завершення прийому повідомлення;

5) перехідні перешкоди використовують вибірковий підхід обструкції шляхом націлювання на один діапазон частот під час кожної атаки. Коли легітимний передавач перемикає канали, щоб уникнути супротивної дії, генератор перешкод слідує за ним, переміщуючи фокус на нову частоту. У той час як таке адаптивне глушіння частоти забезпечує енергоефективне періодичне блокування, передавачі зі швидкими стрибками можуть потенційно спричинити надмірні витрати на комутацію та споживання ресурсів;

6) перешкоди для управління каналом мають на меті досягти повного блокування каналу зв'язку між законними передавачем та приймачем. Постійно займаючи канал, перешкоди зловмисників блокують доступ до мережі, що призводить до відмови в обслуговуванні. Безперервна передача сигналів перешкод від пристрою перешкод блокує використання каналу для зв'язку. Після ініціювання глушіння блокування керування каналом зберігається, доки генератор перешкод не припинить атаку. Ця стійка стратегія максимізує перебої в обслуговуванні, але вимагає значних витрат енергії;

У контексті вразливостей мережі 5G NR до атак типу "глушіння" слід віднести:

- вразливість PBCH (physical broadcast channel), яка існує у складній архітектурі базової станції, ґрунтується на деякій чіткій закономірності. Коли носійна частота розташована нижче 3 ГГц, символи розподіляються один від одного в межах двох слотів, тоді як цей розподіл розширюється до чотирьох слотів для носійних, що перевищують поріг 3 ГГц [105]. Цей шаблон розподілу створює значну вразливість, незалежно від частотного діапазону. Цікаво, що вразливість зберігається, незважаючи на обмеження поширення радіохвиль, притаманні високим частотам. Незважаючи на те, що високі частоти розповсюджуються на меншу відстань, що змушує ближче розташовувати джерела перешкод до мобільних станцій, складна конфігурація конструкції посилює сприйнятливість. Ця конструктивна особливість слугує каналом для селективних атак глушіння. Використовуючи невеликі робочі цикли, вибіркові перешкоди можуть ефективно націлюватися на PBCH. Що пояснюється

просторовою близькістю символів, характеристикою, яка зберігається в усіх діапазонах частот. Така тонка вразливість, хоча і залежить від обмежень поширення частоти, підкреслює делікатну взаємодію між дизайном і сприйнятливістю. Стратегічні наслідки цієї вразливості багатогранні. Методології виявлення, що ґрунтуються на локалізації, є перспективними у визначенні походження перешкод, представляючи потенційний засіб протидії. Проте при зіткненні з мобільними перешкодами відбувається зміна алгоритму. У цьому випадку слід вийти за межі простого виявлення та використати постійний моніторинг переміщення перешкод. Такий підхід дозволяє передбачити майбутні позиції перешкод. Цікаво, що тривалість такого процесу моніторингу набуває першочергового значення, відкриваючи ключову детермінанту ефективності заходів із запобігання перешкодам. Часовий вимір виступає як центральний аспект. Збільшена тривалість моніторингу, хоч і пропонує зрозуміти моделі “мобільних” перешкод, ненавмисно надає розширене вікно можливостей для такого виду перешкод, тим самим посилюючи потенційну шкоду, завдану атакою;

- концепція CORESET (control resource set) - являє собою певний набір фізичних ресурсів, розташованих у сітці ресурсів низхідної лінії зв’язку 5G NR. Ці ресурси також включають набір параметрів, важливих для передачі фізичного каналу керування низхідним каналом (PDCCH). Навпаки, у структурі LTE подібний об’єкт, відомий як область PDCCH, займає початкові чотири символи OFDM у субкадрі. Однак виникає суттєва відмінність у тому, що в той час як LTE PDCCH рівномірно поширюється по всій смузі пропускання каналу, 5G NR CORESET обмежується певною областю в частотній області;

- глушіння каналу PDCCH у контексті 5G, представляє підвищену складність порівняно з аналогом у фізичному широкомовному каналі (PBCH). Щоб ефективно глушити PDCCH, зловмисник повинен знайти всі можливі місця розташування PDCCH. Такий підхід доволі складний, що обумовлено відсутністю інформації щодо частотної області CORESET. Незважаючи на це, зловмисник може перехопити та розшифрувати частотну область CORESET,

отримуючи таким чином перевагу у вибірковому націлюванні на підносійну, використовуючи робочий цикл, що залежить від параметра CORESET-time-duration. У цьому сенсі ключову роль відіграє час, необхідний для перехоплення та декодування CORESET;

- в PUCCH (physical uplink control channel) використовується модуляція зі стрибкоподібною зміною частоти всередині слота, що забезпечує певний ступінь захисту від вибіркових перешкод. Ефективність цього захисного механізму залежить від швидкості стрибків. Примітно, що ця інформація є загальнодоступною через прозорість стандарту 5G. Отже, обізнаний зловмисник може використати інформацію про перестрибування всередині слота, щоб ефективно порушити PUCCH з мінімальними витратами. Крім того, PUCCH використовує схеми модуляції, такі як M-PSK (m-ary phase shift keying) з полярними кодами або кодами повторення для виправлення помилок, що залежить від обсягу переданих бітів. Однак полярні коди, незважаючи на те, що вони широко використовуються, відомі своєю сприйнятливістю до атак з перешкодами;

- процедура випадкового доступу (RA — random access) є критично важливою передачею висхідної лінії зв'язку в 5G NR, що забезпечує початкову реєстрацію мережі та доступ до неї користувацького обладнання (UE - user equipment). Вона передбачає передачу обладнанню користувача послідовності преамбули по фізичному каналу випадкового доступу (PRACH - physical random access channel), який виділений для RA в структурі кадру NR. Після виявлення преамбули RA в PRACH базова станція використовує преамбулу для оцінки параметрів синхронізації, таких як випередження синхронізації, щоб скоригувати затримку розповсюдження. Крім того, базова станція розподіляє радіоресурси на низхідному і висхідному каналах для подальшого зв'язку з UE, який ініціював RA. Базова станція передає розрахункові часові параметри та інформацію про розподіл ресурсів до UE у визначеному вікні відповіді після отримання початкової преамбули [106]. Цей керуючий сигнал від базової станції до UE передається по низхідному фізичному каналу керування низхідною лінією

зв'язку (PDCCH), зіставленому з набором керуючих ресурсів (CORESET). Сама структура преамбули PRACH складається з послідовності Zadoff-Chu з низькими автокореляційними властивостями для забезпечення виявлення преамбули. Вона також містить тимчасовий ідентифікатор, що відповідає користувачеві, який отримує доступ. Незважаючи на безліч можливих частотних і часових розташувань преамбули PRACH, цілеспрямоване глушіння залишається можливим за наявності достатніх можливостей зловмисника. Крім того, випромінювання недійсних преамбул на PRACH, коли місцезнаходження невідоме, може порушити доступ через колізії з легітимними послідовностями. Це підкреслює необхідність застосування складних методів боротьби з перешкодами, адаптованих до критично важливого ресурсу PRACH в мережі 5G NR, щоб запобігти відмовам в обслуговуванні під час початкового доступу до мережі;

- численні дослідження продемонстрували вразливість до атак на завади в системах MIMO, які розгортаються в 5G NR. Орієнтуючись на процедури оцінки каналу, зловмисник може серйозно вплинути на продуктивність методів MIMO, які покладаються на точну інформацію про стан каналу (CSI - channel status information). Наприклад, реалізації MIMO, засновані на розкладанні сингулярних значень (SVD - singular value decomposition), чутливі до атак, які підривають можливості багатопотокової передачі [107]. Аналогічно, були розроблені стратегії для порушення широко використовуваної схеми просторово-часового блокового кодування (STBC - space time block code) для MIMO з двома антенами. Ефективність таких атак, що порушує завадостійкість каналів MIMO, було підтверджено за допомогою теоретичного аналізу, моделювання та реальних експериментів. Важливо, що принципи атаки застосовні навіть при збільшенні масштабу, до MIMO з більшою кількістю антен. До того ж точна інформація CSI має фундаментальне значення для досягнення високого коефіцієнта формування променя і просторового мультиплексування, що гарантується MIMO. Таким чином, оцінки завадостійкості каналу можуть значно зменшити ці переваги продуктивності. Тому адаптивні алгоритми оцінки

стійкості каналу до завад є необхідними для того, щоб методи MIMO з великою кількістю антен забезпечували очікувані переваги над звичайною MIMO при наявності перешкод. Однак слід зазначити, що це відкрита дослідницька проблема, яка вимагає методів, що або протистоять завадам, або виявляють і виключають завадостійкі пілотні сигнали при оцінці CSI для попереднього кодування і просторової обробки сигналів. Рішення для захисту від масивних завад MIMO мають вирішальне значення в міру розгортання мереж 5G NR, які все більше покладаються на ці технології для забезпечення високих вимог.

Стандарт 3rd Generation Partnership Project (3GPP) для фізичного рівня 5G NR визначає використання як полярних кодів, так і кодів LDPC для кодування каналів. Полярні коди використовують явище поляризації каналу для класифікації підканалів на надійні та ненадійні набори. Інформаційні біти виділяються для більш надійних підканалів, тоді як на ненадійних передаються заздалегідь визначені біти. Це дозволяє уникнути зайвих витрат енергії на каналах з високою ймовірністю помилок. Однак, обмеження полярних кодів включають досягнення пропускної здатності лише для великих довжин блоків і високу складність кодування/декодування. Коди LDPC можуть забезпечити майже повну пропускну здатність, але страждають від складності декодування, яка експоненціально зростає при великих довжинах блоків. У 5G NR полярні коди є кращими для каналів управління, що вимагають низької затримки, тоді як коди LDPC використовуються для каналів передачі даних, що вимагають високої надійності [108]. На жаль, дослідження продемонстрували вразливість обох схем кодування до завадоподібних атак, які збільшують перешкоди та шум. Полярні коди демонструють надзвичайно високу частоту бітових помилок в умовах завад, особливо при низьких рівнях SNR близько 0 дБ [109]. Коди LDPC також стикаються з погіршенням ефективності виправлення помилок, коли завади зменшують ефективний коефіцієнт кодування. Це створює проблеми в гарантуванні стійкого і надійного контролю NR і передачі даних в умовах протидії перешкодам. Для вирішення такого роду проблем, методи завадостійкого кодування, такі як перемежування з випадковим вибором блоків,

можуть допомогти підвищити стійкість до перешкод [110]. В той же час, перспективні ітеративні алгоритми декодування продовжують досліджувати, з точки зору їх більшої стійкості до різного роду перешкод.

Науковцями та інженерами проводиться широке дослідження методів виявлення та пом'якшення наслідків атак з використанням завад на мережі 5G NR. Методології виявлення завад можна розділити на порогові, статистичні та засновані на машинному навчанні [111-113]. Порогові підходи відстежують такі показники, як коефіцієнт доставки пакетів, коефіцієнт бітових помилок і співвідношення сигнал/шум, щоб виявити аномалії, які вказують на наявність перешкод. Однак їхня ефективність обмежена проти адаптивних перешкод, а динаміка бездротового зв'язку може спричинити велику кількість хибних спрацьовувань. Статистичні методи використовують статистичний аналіз даних для розрізнення заглушених сигналів, досягаючи вищої точності для постійних перешкод. Останнім часом значну увагу приділяють машинному навчанню, де для виявлення завад застосовують класифікатори, такі як “випадковий ліс”, машини опорних векторів і глибокі нейронні мережі. Глибинне навчання демонструє високі показники виявлення, але вимагає більшої кількості наборів даних. Більшість моделей навчаються на імітованих даних, які не можуть бути узагальнені до реальних атак.

Поява 5G NR відкриває нові можливості і ставить нові виклики для захисту від завад у бездротових системах зв'язку наступного покоління. Використання високочастотного діапазону міліметрових хвиль вище 30 ГГц забезпечує покращений захист, оскільки ефективний діапазон дії перешкод обмежений збільшенням втрат на шляху проходження сигналу. Однак, цілеспрямоване створення перешкод поблизу базових станцій або користувацького обладнання залишається можливим [99]. Методи розширення спектра, такі як розширення спектра з прямою послідовністю (DSSS - direct sequence spread spectrum) і розширення спектра зі скачкоподібною перебудовою частоти (FHSS - frequency hopping spread spectrum), можуть ще більше підвищити стійкість до перешкод [111].

DSSS розширює смугу пропускання сигналу шляхом множення вузькосмугових даних на широкосмуговий псевдошумовий (PN — pseudo-noise) код, забезпечуючи покращення обробки сигналу з обмеженою смугою пропускання [112]. Але DSSS має недоліки, такі як вищі вимоги до пропускної здатності та складність реалізації. Вона також чутлива до злому PN-коду. Розширення спектра зі стрибками частоти (FHSS) досягає стійкості шляхом швидкої стрибкоподібної зміни носійної частоти за псевдовипадковим шаблоном [113-117]. Ефективність залежить від швидкості стрибків відносно ефективності генератора перешкод. Повільне перемикання дозволяє створювати перешкоди протягом одного стрибка, а швидке перемикання викликає проблеми з синхронізацією. Надійно встановити шаблони стрибків є складним завданням за допомогою засобів сканування. Були запропоновані адаптивні схеми FHSS, адаптовані для 5G, але вони потребують подальшого аналізу.

Методи теорії ігор можуть моделювати проблему боротьби із завадами як змагальну гру між легальними користувачами і завадами для визначення оптимальних стратегій, таких як стрибки частоти [118-120].

Інші підходи пропонують використання каналів синхронізації - метод боротьби з перешкодами, який має на меті відновити зв'язок між законними користувачами, використовуючи закономірності в роботі перешкод [121, 122]. Для того, щоб уникати перешкод за допомогою стрибкоподібної зміни частоти, канали синхронізації встановлюються на каналі з перешкодами шляхом вибіркової передачі під час емпірично визначених періодів відсутності перешкод. Це дозволяє уникнути накладних витрат, пов'язаних зі стрибкоподібною перебудовою частоти, за рахунок переривчастого зв'язку. Створення ефективного каналу синхронізації опирається на точне виявлення завад як необхідний крок. Аналізуючи канал з перешкодами у часі, можна виявити часові патерни атак противника. Це дає змогу зробити висновок про робочий цикл постановника перешкод і визначити інтервали часу, коли він неактивний. Тоді законний передавач може обмежити передачу, щоб узгодити її з цими періодами відсутності перешкод, уникаючи інтервалів коли присутні перешкоди у каналі.

Однак точність каналу синхронізації сильно залежить від процесу виявлення завад. Помилкові моделі поведінки завад призведуть до того, що можливості передачі під час фактичної відсутності перешкод будуть помилково класифіковані як перешкоди. А переривчастий характер зв'язку може знизити пропускну здатність. Адаптивні завади також потенційно можуть ідентифікувати шаблони каналів синхронізації і змінювати свою стратегію для порушення зв'язку. Загалом, хоча канали синхронізації є альтернативою стрибкоподібній перебудові частоти, їхня ефективність залежить від точного виявлення і аналізу завад. Канали синхронізації можуть бути більш ефективними проти реактивних завад з регулярними періодами відсутності перешкод у каналі, ніж проти постійних перешкод. Необхідні подальші дослідження для розробки надійних конструкцій каналів синхронізації, стійких до навчання і динамічності противника. Це включає методи перевірки правильності моделей завад і швидкої адаптації синхронізації передачі при виявленні відхилень. Класифікація станів перешкод на основі машинного навчання може допомогти забезпечити надійність каналів синхронізації в умовах складних атак.

Також, як стратегія боротьби з перешкодами, досліджуються безпілотні літальні апарати (БПЛА). В основному вони виконують роль повітряних ретрансляторів, коли наземна інфраструктура порушується через перешкоди [123]. У цьому контексті БПЛА забезпечують альтернативний шлях зв'язку "повітря-земля", якщо наземна базова станція зазнає сильних перешкод. Мобільність і гнучкість розгортання БПЛА дозволяє відновлювати зв'язок навколо зон з перешкодами. Для динамічного визначення оптимального позиціонування та маршрутизації ретранслятора БПЛА було запропоновано методи глибокого навчання з підкріпленням. Проблема боротьби з перешкодами формулюється як марковський процес прийняття рішень, а логіка управління БПЛА вивчаються за допомогою глибоких Q-мереж або методів градієнта для максимізації стійкості зв'язку [124]. Досліджуючи різноманітні середовища перешкод за допомогою моделювання, БПЛА можуть навчитися інтелектуальним методикам для маневрів ухилення та уникнення перешкод.

Однак існують значні труднощі на шляху до ефективної боротьби з перешкодами на основі БПЛА за допомогою навчання з підкріпленням. БПЛА мають власні вразливості до перешкод через відкриті повітряні лінії зв'язку. Їх залежність від живлення від батареї також обмежує тривалу роботу. Доступність БПЛА як ретрансляторів також може бути обмежена в складних умовах з інтенсивними перешкодами. Крім того, навчання з глибоким підкріпленням залежить від отримання великих навчальних даних про різні сценарії перешкод. Навчання на основі моделювання має бути доповнене реальними даними про завади. Вивчені методики також потребують перевірки на ефективність і стійкість до непередбачуваних jamming атак.

Методи обробки сигналів MIMO представляють перспективний напрямок для зменшення впливу перешкод, що в свою чергу надає змогу зменшити збої в мережах 5G [125]. Використовуючи просторову селекцію, що забезпечується великими антенними решітками, методи формування променя можуть вибірково зменшувати перешкоди, зберігаючи при цьому зв'язок. Це забезпечує стійкість до перешкод без модифікації каналу зв'язку. Однак ефективність придушення завад залежить від отримання точних оцінок каналів перешкод для побудови фільтрів подавлення перешкод.

Розробниками запропоновано вдосконалені конструкції приймачів для оцінки характеристик каналу з перешкодами [126]. Явно оцінюючи як бажаний сигнал, так і канали завад, можна отримати лінійні приймальні фільтри для придушення сигналу перешкод. Однак, ефективність залежить від чистоти пілотного сигналу перешкоди і динамічності каналу. У цьому сенсі використання ітеративного уточнення оцінок каналів завад може бути необхідним проти складних атак.

Повсюдне використання програмного забезпечення в мережі 5G за допомогою SDN (software-defined networks) і NFV (network function virtualization) створює нові можливості для інтелектуального і динамічного уникнення завад за допомогою управління радіоресурсами. Такі методи, як управління потужністю, формування променя і планування, можуть бути адаптовані в режимі реального

часу на основі мережевих умов для пом'якшення впливу перешкод [127]. Наприклад, спільні алгоритми управління потужністю і планування були розроблені для оптимізації QoS в умовах дії завад з невідомим розташуванням [127]. Формулюючи оптимізаційні задачі для максимізації корисності та дотримання обмежень QoS, можна розподіляти ресурси для обходу перешкод.

Інтеграція глибокого навчання з програмним управлінням може ще більше підвищити швидкість реагування та якість оптимізації. Глибокі нейронні мережі дають можливість вивчати складну поведінку перешкод, щоб передбачати їх місцезнаходження та закономірності. На основі прогнозів завад розробляються алгоритми проактивного розподілу ресурсів. Однак ефективність глибокого навчання значною мірою залежить від отримання великих об'ємів даних про перешкоди в різних середовищах і типах атак.

Незважаючи на багатообіцяючі можливості, інтелектуальний захист від завад за допомогою планування і глибокого навчання має певні проблеми. Складність оптимізації зростає в геометричній прогресії при великих розмірах мережі. Адаптація в реальному часі може бути ускладнена затримками обчислень. Віртуалізація мережі також збільшує сферу дії атаки. Моделі прогнозування завад повинні використовувати ансамблеві підходи і змагальне навчання для підвищення надійності та узагальнення. Загалом, поєднання програмно-визначених мереж з машинним навчанням вимагає продовження досліджень для повної реалізації адаптивних і стійких комунікацій в умовах дедалі витонченіших перешкод. Тому важливо підкреслити важливість подальших досліджень у розробці ефективних методів боротьби з перешкодами, спеціально пристосованих до викликів, що виникають в мережах 5G NR. Ці методи повинні враховувати мінливий характер jamming атак і забезпечувати надійний захист, щоб гарантувати безпеку і надійність мереж 5G перед обличчям складних загроз перешкод.