АНАЛІЗ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ 5G З ТЕХНОЛОГІЄЮ MASSIVE MIMO

Поповська Є.О., Марчук В.С.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна.

E-mail: yelyzaveta.popovska@nure.ua
volodymyr.marchuk@nure.ua

Abstract

Advanced MIMO technology - massive MIMO is implemented in modern 5G wireless telecommunication systems. Base stations use antenna arrays with hundreds or even thousands of elements. Multi-beam antenna arrays make it possible to increase the bandwidth and spectral efficiency of the communication system. Each of the rays of the directional diagram serves its own group of users. This technology is usually implemented in the range of millimeter radio waves. The use of this range makes it possible to design antenna arrays of rather small sizes with a large number of antenna elements. 5G networks have many advantages over the previous generation of 4G. But at the same time, such networks have a number of security problems. The paper analyzes the main security problems of 5G networks with massive MIMO technology and ways to reduce them.

Multiple-input-multiple-out (MIMO) – дуже важлива технологія для безпроводових мереж. Вона використовується для одночасного відправлення та прийому кількох сигналів по тому самому радіоканалу. При фіксованій смузі пропускання в радіоканалі формується декілька просторових каналів. MIMO відіграє велику роль у мережах WI-FI, 3G, 4G та 4G LTE-A.

MIMO, в основному, використовується для досягнення високої спектральної ефективності та енергоефективності, але вона не відповідає сучасним вимогам пропускної спроможності та надійності підключення. Ці показники у MIMO досить низькі. Щоб вирішити цю проблему, було використано безліч технологій MIMO, таких як однокористувацьке MIMO (Single-User MIMO, SU-MIMO), багатокористувацьке MIMO (Multi-User MIMO, MU-MIMO) та мережеве MIMO (Network MIMO). Однак, ці нові види MIMO також не задовольняли вимогам кінцевих користувачів.

Massive MIMO (mMIMO) – це вдосконалена технологія MIMO. Така технологія впроваджується в мережах 5G. На базових станціях використовуються антенні решітки з сотнями і навіть тисячами елементів. Ці антенні решітки дають можливість збільшити пропускну спроможність і спектральну ефективність. Класичні антенні решітки збільшують ступінь концентрації радіохвиль в головному напрямку, зменшуючи ширину діаграми спрямованості головного її пелюстка. Згідно формули Шенона збільшення рівня сигналу по відношенню до потужності шуму плюс завада в точці прийому дає можливість збільшити швидкість передачі інформації. Використання декількох просторових каналів в системах MIMO дає можливість збільшити пропускну здатність, що буде сумою пропускних здатностей окремих каналів. Більш того в системах з технологією mMIMO антенні решітки побудовані таким чином, що формують у просторі багато променів навколо базової станції. Це дає можливість забезпечити обслуговування груп користувачів кожним з променів. Чим більше променів тим більше користувачів обслуговується. Таким чином маємо два процеси: збільшення пропускної здатності за рахунок створення просторових каналів і збільшення кількості користувачів за рахунок використання багатопроменевості.

В наш час, розвиток технології Інтернету речей (Internet of Thing – IoT) потребує мереж з високою пропускною здатністю. У традиційних мережах зв'язку зі звичайними, як правило, трьох-секторними антенами збір даних з інтелектуальних датчиків в мережах IoT є складним завданням,

оскільки це призводить до збільшення затримки, зниження швидкості передачі даних та надійності. Ця проблема вирішується в системах з багатопроменевими антенними системами в технології mMIMO. Технологія mMIMO здатна забезпечити передачу даних, зібраних з сотен різних датчиків, в реальному часі в центральні точки моніторингу.

Найбільша ефективність в 5G досягається при використанні міліметрового діапазону – це діапазон FR2 (рис.1) [1].

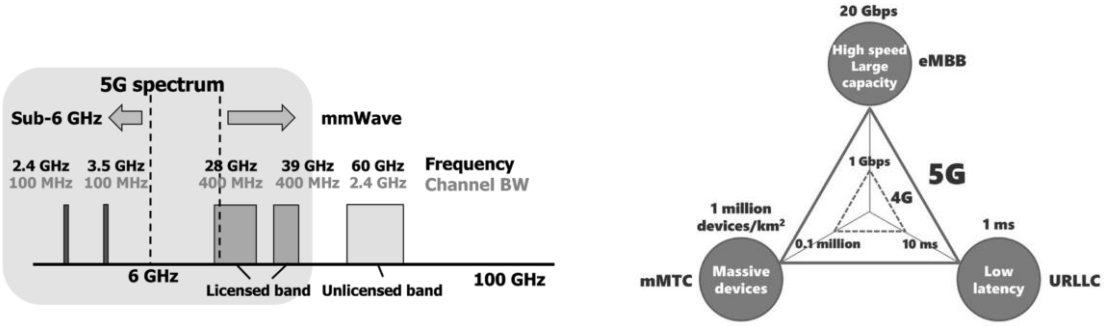

Рис. 1. Спектри систем 5G і діаграма переваг 5G над 4G

Основні особливості технології 5G: пропускна здатність в 20 разів може перевищувати показники систем 4G і досягати 20 Гбіт/с, затримка зменшується з 10 мс до 1 мс, а щільність користувальницьких пристроїв збільшується з 0,1 до 1 мільона на 1 кв.км.

Але використання міліметрового діапазону призводить до зменшення радіусу соти приблизно до 100 м на відміну від 5G діапазону FR1 (радіус приблизно 200 м). Для систем 4G цей радіус збільшується до 1 км.

Було проведено аналіз безпеки мереж 5G.

Суттєве збільшення пропускної здатності і щільності терміналів користувачів збільшує розмір поверхні атаки. Використання мереж 5G в технології IoT призводить до зменшення рівня захищенності всієї мережі. Це пояснюється з одного боку дуже великою кількістю датчиків в таких мережах, що збільшує кількість точок через які зловмисники можуть проникати в мережу, а з іншого боку більшість цих датчиків інтелектуальні – мають програмне забезпечення. Як правило, ці датчики дешеві, мають спрощену структуру і в них використовуються спрощені протоколи для організації обміну інформацією з центром управління. Такі протоколи мають великий рівень і кількість вразливостей. Більш того вони не мають антивірусного забезпечення, а якщо і мають, то воно не оновлюється. Не оновлюється також і програмне забезпечення самих датчиків.

Проаналізуємо найбільш вразливі протоколи в технології IoT [2]. Протокол DDS, що реалізує операції читання та запис, є досить примітивним. Дані не видаляються з локального кеша DDS і можуть бути прочитані. Спеціалізований протокол передачі CoAP є спрощеним протоколом для пристроїв з обмеженим ресурсом і дуже зручний для проведення DDoS атак і IP-спуфінгу. Протокол.XMPP має певні проблеми з безпекою, пов'язані з недостатністю шифрування даних, що передаються між користувачами. Окрім того протокол MQTT має проблеми з налаштуванням бо не має паролю для входу.

Зменшення радіусу соти в мережі 5G, особливо в міліметровому діапазоні FR2 призводить до значного збільшення кількості базових станцій. Наслідком цього є поява можливостей як фізичного взлому так і програмних атак на апаратуру міні базових станцій, що, як правило, не охороняються.

Захист від глушіння сигналу є важливим аспектом технології mMIMO в 5G мережі.

Антени mMIMO можуть бути розташовані на значній відстані одна від одної, що допомагає знизити вплив глушіння. Це забезпечує кращу просторову роздільність і поліпшує ефективність передачі та приймання сигналу.

У технології mMIMO можуть використовуватися різні частотні діапазони для передачі сигналу з різних антен. Це дозволяє знизити вплив глушіння, оскільки сигнали на різних частотах менше взаємодіють між собою.

Технологія mMIMO може змінювати потужність сигналу та напрямок випромінювання з різних антен. Це дозволяє змінювати фокусування сигналу та уникнути глушіння з інших джерел.

У технології mMIMO використовуються алгоритми обробки сигналу, які можуть відділяти бажані сигнали від небажаних і компенсувати вплив глушіння.

Глушіння сигналу mMIMO, котре можна класифікувати як DoS атаку, в мережах 5G можливе при певних умовах.

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.

Існують різні техніки та механізми для боротьби з міжсимвольною інтерференцією. До них входять алгоритми еквалізації сигналу, фільтрації, корекції часової затримки та інші методи обробки сигналу, які допомагають відновити оригінальні символи та знизити вплив міжсимвольної інтерференції на якість приймання сигналу.

Збільшення кількості антен в mMIMO. Дане рішення дозволить боротися з можливим глушінням сигналу мережі шляхом збільшення сили самого сигналу та одночасно поліпшить якість самої мережі завдяки збільшенню пропускної здатності в прилеглому секторі чи зоні дії антен. Також необхідно обов'язково вводити до активної роботи алгоритми еквалізації сигналу, фільтрації, корекції часової затримки та інші методи обробки сигналу заради протидії можливій інтерференції, котра може виникнути в mMIMO випадково чи завдяки зловмисникам.

Література

1. Ning Guan. Expected Application Spaces and Supporting Technologies in 5G. URL: https://www.fujikura.co.jp/eng/rd/gihou/backnumber/pages/__icsFiles/afieldfile/2022/03/02/51e_01.pdf

2. IoT Protocols and their Architecture. URL: https://www.elprocus.com/iot-protocols-and-its-architectures/