УДК 004.052.42

ДОСЛІДЖЕННЯ ЗАВАДОСТІЙКОСТІ БІОМЕТРИЧНИХ ШАБЛОНІВ ДО ЗОВНІШНІХ ВПЛИВІВ ПІД ЧАС ПЕРЕДАЧІ МОБІЛЬНИМИ МЕРЕЖАМИ

А.О. Щербак, А.А. Астраханцев
Харківський національний університет радіоелектроніки

О.В. Щербак
Харківський національний університет Повітряних Сил імені Івана Кожедуба

Г.Є. Ляшенко
Харківський національний університет радіоелектроніки

Abstract *– The article is devoted to the study of the immunity of biometric templates to interference and fading during transmission over the LTE network. The widespread use of remote biometric authentication systems, primarily in remote mobile payment systems, determines the relevance of the chosen topic, and the development of mobile networks, and, first of all, the use of technologies that are more protected from attacks like LTE increases its practical focus. However, when authentication information is transmitted, even over a secure channel, it can be subject to interference and fading. That is why it is important to study their impact on the integrity of the biometric template that will be used to authenticate the user in the system. The paper analyzes the dependence of the quality of the authentication system on the parameters of the mobile communication channel (bit error rate, signal-to-noise ratio) and the parameters of the mobile device that transmits information (MIMO scheme, code rate, modulation scheme), which improves the quality of the remote biometric authentication systems by reasonably choosing the transmission parameters and taking into account the parameters of the communication channel.*

Анотація *– Стаття присвячена дослідженню стійкості біометричних шаблонів до завад та завмирань у разі передачі мережею LTE. Широке застосування систем віддаленої біометричної автентифікації, насамперед в системах віддалених платежів із мобільних пристроїв, зумовлює актуальність обраної теми, а розвиток мобільних мереж і в першу чергу застосування більш захищених від атак технологій, таких як LTE, підвищує її практичну направленість. Однак під час передачі автентифікаційної інформації, навіть по захищеному каналу, вона може піддаватися впливу завад та завмирань. Саме тому важливо дослідити їхній вплив на цілісність біометричного шаблону, який буде використовуватися для автентифікації користувача в системі. У роботі виконано аналіз залежності якості роботи системи автентифікації від параметрів каналу мобільного зв'язку (коефіцієнт бітових помилок, співвідношення сигнал/шум) та параметрів мобільного пристрою, який передає інформацію (схема MIMO, швидкість коду, алгоритм у модуляції), що дає можливість підвищити якість роботи системи віддаленої біометричної автентифікації через обґрунтований вибір параметрів передачі та врахування параметрів каналу зв'язку.*

Вступ

Віддалена біометрична автентифікація все частіше зустрічається в повсякденному житті, активно вона почала використовуватись у фінансових установах та банках [1]. Ідентифікація проводиться віддалено, на стороні компанії й дає змогу надавати фінансові послуги громадянам дистанційно, підтвердивши свою особистість за допомогою біометричних персональних даних, створюючи таким чином рівні можливості доступу до фінансових послуг незалежно від місця розташування користува-

ча. Також її почали впроваджувати в процедурах electronic Know Your Customer (e-KYC), щоб зробити e-KYC більш швидким і зручним для клієнтів.

Оскільки користувачі цих систем найчастіше під час проведення транзакцій використовують мобільні пристрої, підключені до мереж мобільних операторів зв'язку, то найбільш цікавими й актуальними стають сценарії проведення віддаленої автентифікації з урахуванням впливу зовнішніх чинників, що виникають у мобільних каналах зв'язку. На сьогодні найбільш поширеною технологією, використовуваною в мобільному зв'язку в Україні й за її межами, є технологія Long-Term Evolution (LTE). Тому математична модель фізичного рівня саме мережі LTE була обрана для проведення досліджень якості роботи системи віддаленої біометричної автентифікації.

Метою роботи є аналіз ефективності системи віддаленої біометричної автентифікації за умови її використання в каналах мобільного зв'язку із завадами.

Практична значущість полягає у виборі й обґрунтуванні параметрів передавача мобільного пристрою під час віддаленої біометричної автентифікації.

За останні роки було опубліковано низку наукових робіт [2-6], присвячених проблематиці спотворення інформації під час її передачі безпроводовими мережами унаслідок впливу різних чинників. У наведених [2-6] публікаціях здебільшого приділяється увага обчисленню коефіцієнта бітових помилок (Bit Error Rate, BER) залежно від співвідношення сигнал/шум (Signal-to-Noise Ratio, SNR). У даній роботі на відміну від інших публікації приділяється увага особливостям обробки чуттєвих до спотворень даних під час автентифікації за допомогою обчислення порогових значень спрацювання системи віддаленої біометричної автентифікації при різних рівнях зашумленості каналу зв'язку та оптимізації налаштувань передавача, а також шляхом вибору оптимальних за критерієм працездатність/швидкість елементів, серед яких: алгоритм модуляції, технологія конфігурації антен (Multiple Input Multiple Output (MIMO) та Single In Single Out (SISO)), алгоритм та ступінь завадостійкого кодування.

I. Опис процесу формування біометричних шаблонів

Автентифікація людини за відбитками пальців є найбільш розповсюдженою біометричною технологією [7] завдяки їхній відмінності, постійності, прийнятності й універсальності [8]. Більшість наявних методів порівняння відбитків пальців можна умовно поділити на три категорії: порівняння на основі кореляції, порівняння мінуцій та порівняння на основі гребенів папілярних ліній [9]. Метод порівняння відбитків пальців на основі мінуцій використовується в сучасній Automatic Fingerprint Identifcation System (AFIS), тому саме його було використано в даній роботі.

У якості бази даних зразків відбитків пальців, використовувалися відбитки, що були відскановані сканером DigitalPersona U.are.U 4000 з роздільною здатністю 500 пікселів на дюйм [10].

Для отримання біометричного шаблону спочатку із зображення відбитку пальця було отримано шаблон мінуцій за допомогою утиліти MINDTCT, що входить до

складу програмного забезпечення National Institute of Standards and Technology (NIST) Biometric Image Software (NBIS). MINDTCT – це система виявлення мінуцій. Додаток приймає на вхід зображення відбитку пальця та знаходить усі мінуції на ньому, присвоюючи кожній із них координати, орієнтацію, якість, після чого записує виявлені мінуцій у файл. За замовчуванням MINDTCT зберігає мінуції відповідно до стандарту American national standards institute / National Institute of Standards and Technology (ANSI/NIST), це значить, що точки мінуцій обчислюються на основі початку координат, розташованого в нижній лівій частині зображення. Детальний опис того, як працює MINDTCT можна знайти в офіційному посібнику від NIST «User's guide to NIST biometric image software (NBIS)» [11]. Треба зауважити, що різні AFIS представляють місце розташування мінуцій по-різному, саме тому MINDTCT має можливість зберігати їхні значення згідно зі стандартом ANSI INCITS 378-2004, який і був використаний у даній роботі. Відповідно до цього стандарту початок координат розташований у верхньому лівому куті зображення.

Далі отримані значення мінуцій перетворюються в біометричний шаблон за допомогою .Net DLL бібліотеки – Minutia Cylinder Codes software development kit (MCC SDK), який будує для кожної з мінуції локальну тривимірну структуру даних, так званий циліндр, побудований на основі взаємозв'язку незмінних відстаней і кутів даної та сусідніх мінуцій [12]. Дана бібліотека використовує лише координати та напрямок мінуцій у діапазоні $[0, 2\pi)$ і не бере до уваги її тип та якість. У якості параметрів запису шаблону були взяті стандартні значення. В результаті було отримано біометричний шаблон в двійковому форматі.

II. Опис імітаційної моделі

Біометричний шаблон передається через імітаційну модель мережі фізичного рівня стандарту LTE. Задля того, щоб з'ясувати, за яких параметрів мережі біометричний шаблон буде передано так, щоб на приймачі можна було правильно автентифікувати користувача через порівняння двох біометричних шаблонів, попередньо зареєстрованого еталонного біометричного шаблону, що збережений у системі та біометричного шаблону, що було передано через канал зв'язку.

Технологія LTE базується на трьох основних складових: використанні ортогональної модуляції з частотним поділом для кодування сигналів – Orthogonal Frequency-Division Multiplexing (OFDM), багатоантенних системах MIMO і безпосередньо архітектурі побудови ядра мережі – System Architecture Evolution (SAE). Дуплексне розділення каналів може бути як частотним Frequency Division Duplex (FDD), так і часовим Time-Division Duplex (TDD), що дає змогу операторам дуже гнучко використовувати частотний ресурс.

Для моделювання фізичного рівня мережі LTE побудовано модель з FDD режимом передачі даних у середовищі MATLAB і Simulink, ця модель представлена в роботі [13].

Досліджувана модель фізичного рівня LTE складається з передавача, моделі каналу та приймача. Ланцюг обробки сигналу на передавачі являє собою комбінацію логічного (Downlink Shared Channel, DLSCH) та фізичного каналів (Physical Downlink Shared Channel, PDSCH). Стек обробки повністю визначений у документах, розроблених 3rd Generation Partnership Project (3GPP), що описують мультиплексування й канальне кодування [14], а також фізичні канали й модуляцію [15]. Модель каналу передбачає наявність завмирань та адитивного білого гаусового шуму (additive white Gaussian noise, AWGN). Приймач виконує обробку даних у каналах (DLSCH і PDSCH).

Обробка в логічному каналі DLSCH включає в себе приєднання коду Cyclic Redundancy Check (CRC) для виявлення помилок, сегментування даних на більш дрібні фрагменти (підблоки), здійснення операцій канального кодування на основі турбокодування, виконання операції узгодження швидкості, яка вибирає кількість вихідних біт відповідно до бажаної швидкості кодування й перетворення кодових блоків у кодові слова.

У фізичному каналі PDSCH кодові слова спочатку піддаються операції скремблювання, а потім модуляції, результатом якої є потік модульованих символів. Модель підтримує такі алгоритми модуляції: QPSK, 16QAM, 64QAM. Наступний етап включає використання технології MIMO, у якій один потік модульованих символів розділяється на кілька підпотоків, призначених для передачі через кілька антен. Останній крок у ланцюгу обробки пов'язаний із передачею на декількох несучих. У низхідному каналі операції з декількома несучими ґрунтуються на схемі модуляції Orthogonal Frequency Division Multiplexing (OFDM).

На рис. 1 представлено структурну схему імітаційної моделі, яка відображає ланцюг обробки сигналу, що застосовується до транспортних блоків, що надходять від рівня MAC до рівня PHY.

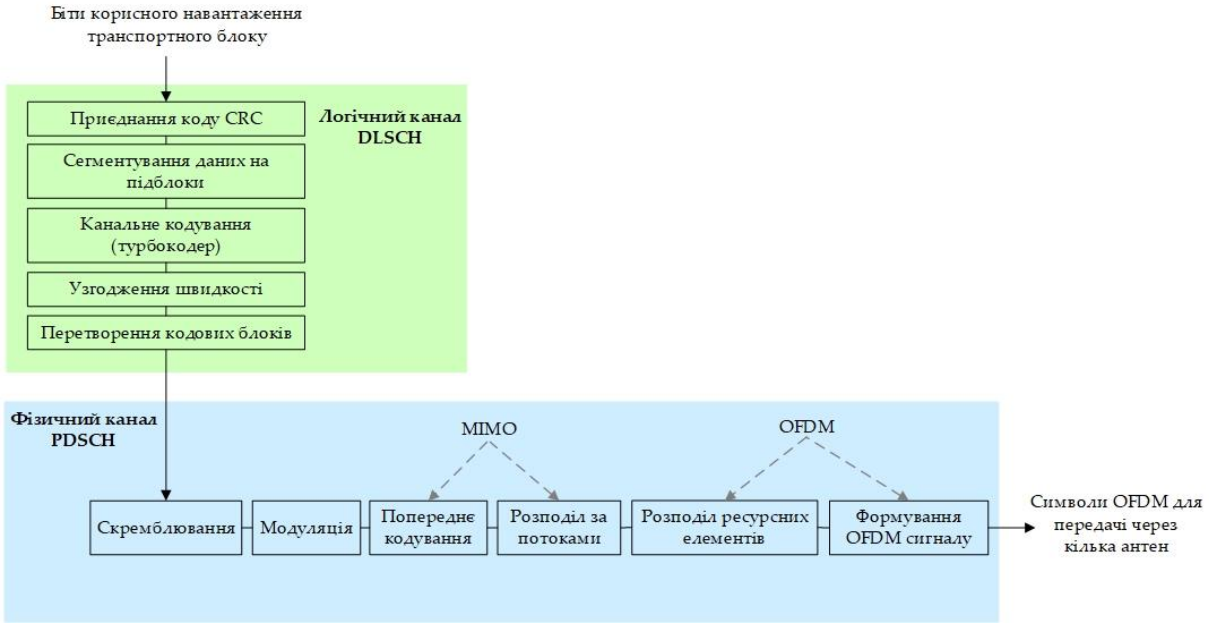

Рис. 1. Ланцюг обробки сигналу для каналів DLSCH та PDSCH

Моделювання каналу виконується за допомогою комбінування багатопроменевого каналу MIMO із затуханням та каналу з AWGN. Типові параметри каналів MIMO включають конфігурації антен, профілі багатопроменевого завмирання, максимальні доплерівські зсуви (maximum Doppler shift – MDS) і рівні просторової кореляції в антенах, як на стороні передавача, так і на стороні приймача. Канал AWGN, як правило, характеризується значеннями співвідношення сигнал/шум або дисперсії шуму. На приймальній стороні ланцюг обробки сигналів застосовується до прийнятих символів, які пройшли через модель каналу і виконуються операції, зворотні тим, що виконуються на передавачі.

Після передачі біометричного шаблону через модель фізичного рівня LTE його було порівняно з оригінальним. Для порівняння двох біометричних шаблонів було використано бібліотеку MCC SDK. У цій бібліотеці запропоновано метод оцінювання для об'єднання локальної схожості в унікальну загальну оцінку, що позначає загальну схожість двох відбитків пальців. Для порівняння біометричних шаблонів були взяті стандартні значення, надані бібліотекою. Оцінка схожості може набувати значень від 0 (біометричні шаблони зовсім не збігаються) до 1 (біометричні шаблони ідеально збігаються).

III. Результати дослідження завадостійкості біометричних шаблонів до зовнішніх впливів під час передачі

У роботі проведено багатобічний аналіз впливу параметрів передавача на працездатність роботи системи віддаленої біометричної автентифікації за умови наявності в каналі зв’язку доплерівських зсувів та завад. Для цього був оцінений поріг спрацювання системи, за умови застосуванні модуляції 16QAM і MIMO 2x2 для швидкості коду 1/2 (табл. 1). Відсутні значення в таблиці вказують на те, що система порівняння біометричних шаблонів не прийняла шаблон, через наявність великої кількості помилкових біт.

Результати досліджень (табл. 1) показали, що зростання максимального доплерівського зсуву у разі зниження співвідношення сигнал/шум суттєво погіршує якість роботи системи. Як наведено в табл. 1, у разі відсутності доплерівського зсуву порогом спрацювання системи є значення SNR = 6,4 дБ, але у разі появи та зростання MDS поріг спрацювання збільшується до 7,8 дБ, тобто наявність у каналі доплерівського зсуву буде вимагати збільшення потужності передавача або використання більш завадостійких кодів та алгоритмів модуляції.

Першим чинником, вплив якого на якість роботи був досліджений – це швидкість коду, яка характеризує співвідношення кількості символів на вході завадостійкого кодера до кількості символів на виході. Зменшення швидкості коду зазвичай дає можливість покращити завадостійкість, але знижує ефективну швидкість передачі даних.

Таблиця 1. Аналіз порогу спрацювання системи віддаленої біометричної автентифікації залежно від рівня максимального доплерівського зсуву та співвідношення сигнал/шум (SNR)

Максимальний доплерівський зсув, Гц	0	10	40	80
SNR, дБ	Оцінка схожості			
6,2	–	–	–	–
6,3	–	–	–	–
6,4	1	–	–	–
6,5	1	1	1	–
6,6	1	1	1	–
6,7	1	1	1	–
6,8	1	1	1	–
6,9	1	1	1	–
7	1	1	1	–
7,1	1	1	1	–
7,2	1	1	1	–
7,3	1	1	1	–
7,4	1	1	1	–

Як показали результати дослідження, зменшення швидкості коду (рис. 2) для підвищення завадостійкості дає можливість майже вдвічі покращити пороги спрацювання для системи віддаленої біометричної автентифікації.

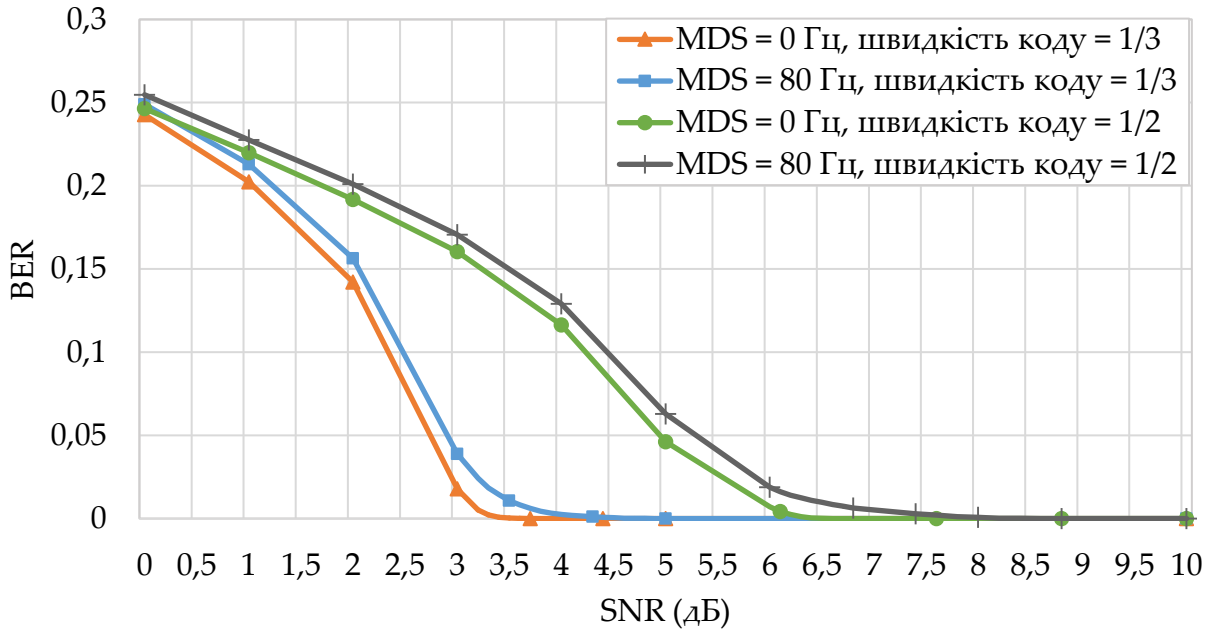

Рис. 2. Залежність коефіцієнта бітових помилок (BER) від співвідношення сигнал/шум (SNR) за умови використання швидкості коду 1/2 та 1/3 при модуляції 16QAM та різних рівнях доплерівських зсувів (0 та 80 Гц)

Так, судячи з рис. 2, за умови відсутності впливу доплерівських зсувів поріг спрацювання системи покращується з SNR = 6,4 дБ при швидкості коду 1/2 до

SNR = 3,4 дБ при швидкості коду 1/3, а сам вплив навіть максимальних значень доплерівських зсувів незначно погіршує пороги спрацювання (зі значення SNR = 6,4 дБ при MDS = 0 Гц до значення SNR = 7,8 дБ при MDS = 80 Гц) у порівнянні з впливом швидкості коду. Базуючись на цьому, можна зробити висновок про доцільність використання саме швидкості 1/3 при будь-яких значеннях індикатору стану каналу (Channel Quality Indicator – CQI).

Наступний чинник, який можна вибирати та змінювати на боці передавача – алгоритм модуляції. У технології LTE залежно від індикатору стану каналу можуть використовуватися три основні алгоритми модуляції (табл. 2). CQI може приймати значення від 1 до 15, де значення «1» відповідає найгіршій якості, а рівень «15» відповідає найкращим мережним умовам.

Таблиця 2. Залежність вибору алгоритму модуляції від індикатору стану каналу

CQI	1	4	5	6	7	8	9	10	11
Модуляція	QPSK	QPSK	QPSK	QPSK	16 QAM	16 QAM	16 QAM	64 QAM	64 QAM
Біт/символ	2	2	2	2	4	4	4	6	6

Результати дослідження показали (рис. 3), що алгоритм QPSK навіть за умови найгірших параметрів каналу забезпечує значення BER на рівні $3{,}5\cdot10^{-6}$, у той час як алгоритми 16QAM та 64QAM можуть забезпечити лише $1\cdot10^{-5}$ та $1{,}5\cdot10^{-3}$ відповідно для значень SNR, що відповідають порогу спрацювання системи. Базуючись на отриманих результатах, можна зробити висновок, що в системі віддаленої біометричної автентифікації навіть за умови високих показників SNR не рекомендується використовувати 64QAM.

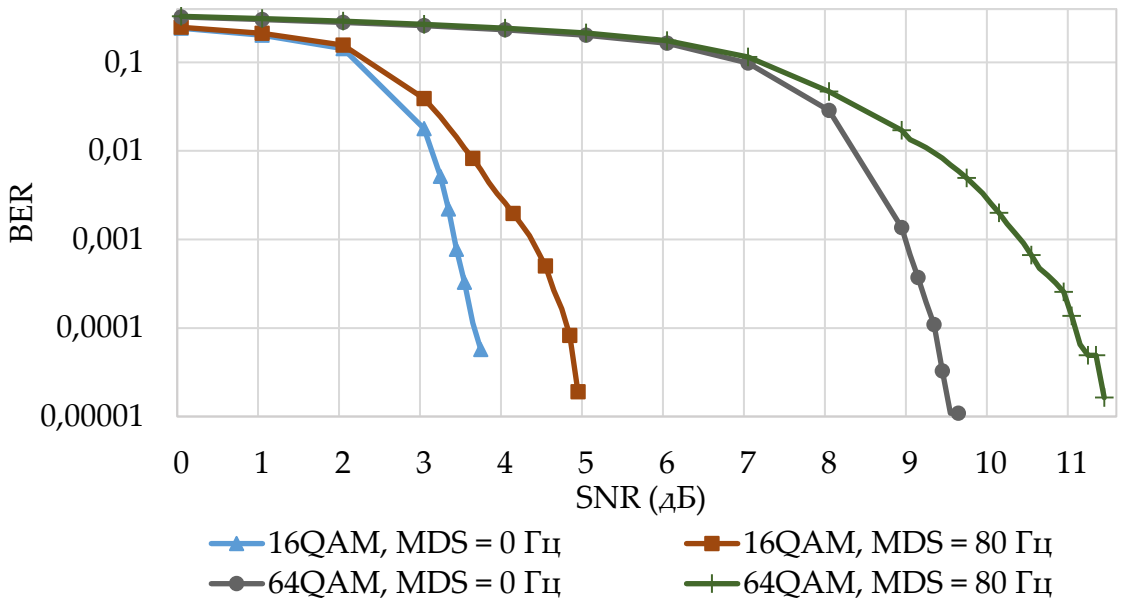

Рис. 3. Залежність коефіцієнта бітових помилок (BER) від співвідношення сигнал/шум (SNR) за умови використання алгоритмів модуляції 16QAM і 64QAM при швидкості коду 1/3 та різних рівнях доплерівських зсувів (0 та 80 Гц)

Ще одним чинником, який може впливати на якість роботи системи та може бути відкоригований на боці передавача, є налаштування багатоантенного прийому та передачі (MIMO). У роботі був оцінений вплив застосування більш складних схем MIMO 2x2 та 4x4 на завадостійкість у порівнянні з відсутністю використання MIMO (схема 1x1). Результати досліджень, що наведено на рис. 4, показують, що застосування MIMO також дає можливість майже вдвічі підвищити завадостійкість і таким чином покращити пороги спрацювання автентифікаційних даних.

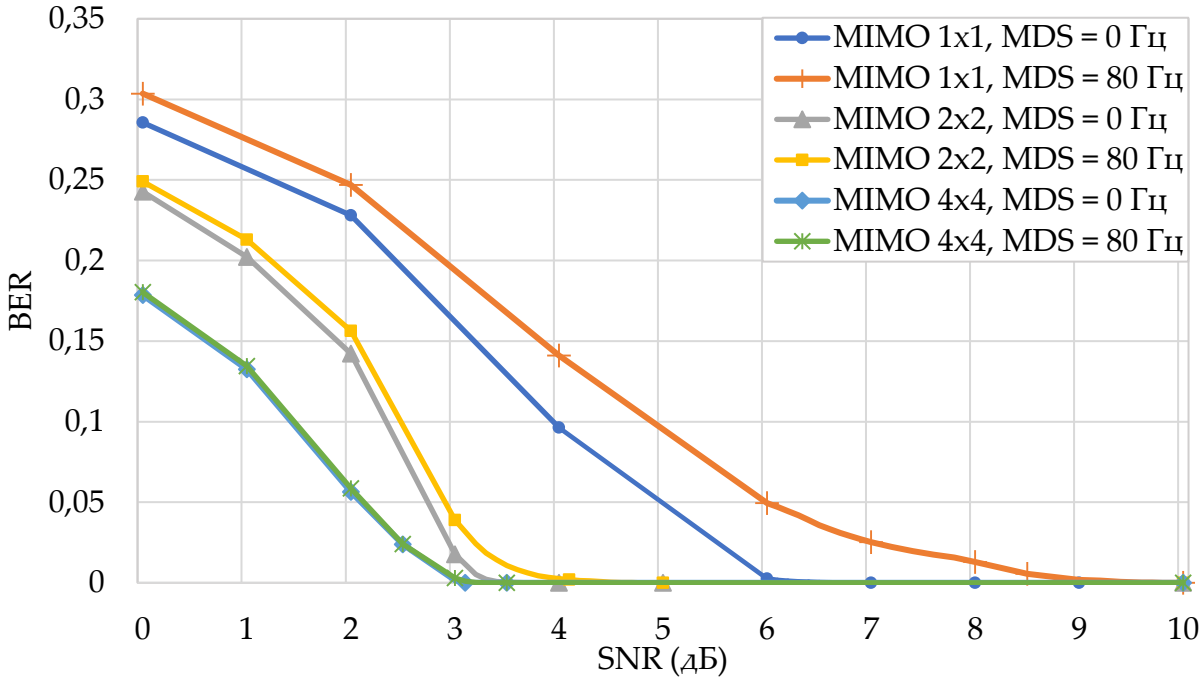

Рис. 4. Залежність коефіцієнта бітових помилок (BER) від співвідношення сигнал/шум (SNR) за умови використання багатоантенної технології MIMO при швидкості коду 1/3 і модуляції 16QAM та різних рівнях доплерівських зсувів (0 та 80 Гц)

Висновки

Результати роботи показали, що якість роботи системи віддаленої біометричної автентифікації може бути істотно покращена за допомогою застосування додаткових засобів завадостійкості та використання адаптивних налаштувань на стороні передавача. На основі отриманих результатів дослідження можна зробити висновок, що найкращий компроміс між завадостійкістю та швидкістю при проведенні віддаленої біометричної автентифікації в мережі LTE забезпечує модуляція 16QAM. Проте, квадратурну амплітудну модуляцію 64QAM не бажано використовувати під час проведення транзакцій. Висновки базуються на тому, що у разі відсутності впливу доплерівських зсувів поріг спрацювання системи з використанням модуляції QPSK становить SNR = 0 дБ, з модуляцією 16QAM SNR = 3,4 дБ, а з 64QAM значення SNR дорівнює 9 дБ.

Застосування декількох антен для передачі та прийому сигналу (MIMO 2x2 та 4x4) поліпшило якість каналу. Так, наприклад, для значення BER, що дорівнює 0,14, за умови використання антенної конфігурації – 1x1 (MDS = 80) SNR становить 4 дБ, а для MIMO 4x4 (MDS = 80 Гц) для того ж самого значення BER SNR дорівнює 1 дБ. Це чітко вказує на перевагу використання технології MIMO 4x4. Пороги спрацювання системи віддаленої біометричної автентифікації такі (при MDS = 0 Гц):

MIMO 1x1 SNR = 6,1 дБ;

MIMO 2x2 SNR = 3,4 дБ;

MIMO 4x4 SNR = 3,1 дБ.

Крім модуляції та антенної конфігурації, було визначено, що швидкість коду також впливає на значення BER. Поріг спрацювання системи зменшився майже вдвічі від SNR = 6,4 дБ для швидкості коду 1/2 до SNR=3,4 дБ для 1/3.

Отже, як рекомендації з використання систем віддаленої біометричної автентифікації в мережах мобільного зв'язку треба використовувати параметри передавача із застосуванням схем MIMO 2x2 і 4x4, кодів 1/3 та модуляції 16QAM. У цьому випадку можна досягти найкращих результатів зі спрацювання системи. За умови найгірших мережних умов пріоритет треба віддавати застосуванню схеми MIMO 4x4, модуляції QPSK та використанню кодів 1/3.

Результати роботи пропонується застосувати до створення нового класу обслуговування та формування вимог щодо його пріоритетної передачі й забезпечення необхідних характеристик, у тому числі завадостійкості.

Список літератури:

1. *Моногарова, А. А., Курзанов, И. Д., Николайчук, О. А.* (2009), "Биометрия как способ удалённой идентификации в банковском секторе", Научный формат, No. 3(3), С. 83-90.

2. *Mousavi, H., Amiri, I., Mostafavi, M., Choon, C.* (2019), "LTE physical layer: Performance analysis and evaluation", Applied Computing and Informatics, No. 15(1), P. 34-44. **DOI**: https://doi.org/10.1016/j.aci.2017.09.008

3. *Nandal, V., Nandal, D.* (2017), "Improving the BER in LTE System using various Modulation Techniques over Different Fading Channel", International Journal for Research in Technological Studies, No. 4(8), P. 5-9.

4. *Lal, M., Arora, H.* (2011), "BER performance of different modulation schemes for MIMO systems", International Journal of Computer Science and Network Security, No. 11(3), P. 62-79.

5. *Якименко, С. И., Молоковский, И. А.* (2018), "Использование возможностей MatLAB для моделирования и анализа физических каналов LTE", Автоматизация технологических объектов и процессов. Поиск молодых: сборник научных трудов XVIII научно-технической конференции аспирантов и студентов, С. 1-5, режим доступу: http://masters.donntu.org/2018/fkita/yakymenko/library/article1.htm

6. *Ghosh, S.* (2015), "Performance Evaluation of Different Coding and Modulation Scheme in LTE Using Different Bandwidth and Correlation Levels", Wireless Personal Communications, No. 86(2), P. 563-578. **DOI**: https://doi.org/10.1007/s11277-015-2945-6

7. *Kanjan, N., Patil, K., Ranaware, S., Sarokte, P.* (2017), "A Comparative Study of Fingerprint Matching Algorithms", International Research Journal of Engineering and Technology, No. 4(11), P. 1892-1896.

8. *Jain, A., Ross, A., Prabhakar, S.* (2004), "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, No. 14(1), P. 4-20. **DOI**: https://doi.org/10.1109/TCSVT.2003.818349

9. Maltoni, D., Cappelli, R. (2008), "Fingerprint Recognition", Jain A.K., Flynn P., Ross A.A. (eds) Handbook of Biometrics. Springer, Boston, MA, P.23-42. **DOI**: https://doi.org/10.1007/978-0-387-71041-9_2

10. Neurotechnology (2007), "Fingerprint samples were scanned with DigitalPersona U.are.U 4000 scanner at 500 ppi", available at: http://www.neurotechnology.com/download/UareU_sample_DB.zip (last accessed 20.10.2020)

11. *Watson, C. I., Garris, M. D., Tabassi, E., Wilson, C. L., McCabe, R. M., Janet, S., Ko, K.* (2007), User's Guide To NIST Biometric Image Software (NBIS), 207 p. **DOI**: https://doi.org/10.6028/NIST.IR.7392

12. *Cappelli, R., Ferrara, M., Maltoni, D.* (2010), "Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition", IEEE Transactions on Pattern Analysis and Machine Intelligence, No. 32(12), P. 2128-2141. **DOI**: https://doi.org/10.1109/TPAMI.2010.52

13. *Zarrinkoub, H.* (2014), Understanding LTE with MATLAB: From Mathematical Modeling to Simulation and Prototyping, John Wiley & Sons, Chichester, 512 p.

14. LTE; Evolved Universal Terrestrial Radio Access (E-UTRA) (2012), Multiplexing and channel coding (3GPP TS 36.212 version 10.6.0 Release 10), European Telecommunications Standards Institute, Sophia Antipolis, 80 p.

15. LTE; Evolved Universal Terrestrial Radio Access (E-UTRA) (2011), Physical channels and modulation (3GPP TS 36.211 version 10.0.0 Release 10), European Telecommunications Standards Institute, Sophia Antipolis, 104 p.