УДК 681.5 DOI: 10.31673/2412-4338.2019.042538

Катков Ю.І., Березовська Ю.В., Пшеничний Ю.С., Рижаков М.М., Прокопов С.В.
Державний університет телекомунікацій, Київ

АНАЛІЗ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ ПІД ЧАС ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ 4G/LTE

У статті розглядається проблема вразливості стільникових мереж 4G/LTE в критичних інфраструктурах. Технологічна революція в галузі мобільних бездротових широкосмугових стільникових мереж залучає Україну до необхідності впровадження нових технологій у процеси побудови цифрової економіки майбутнього. Однією з таких технологій є LTE. Показано, що вивчення внутрішніх і зовнішніх загроз, а також вразливість елементів стільникових мереж стандарту 4G/LTE для критичної інфраструктури є відносно новим і маловивченим, тому тема роботи є актуальною та практично затребуваною.

Поставлено завдання: під час розгляду рухомих бездротових широкосмугових стільникових мереж передачі даних стандарту 4G/LTE на основі аналізу функціонування її елементів визначити загрози для потенційно вразливих елементів. Для вирішення завдання виконано опис інноваційних механізмів впровадження мобільного зв'язку 4-го покоління, проаналізовано тенденції розвитку послуг перспективних областей застосування мобільного зв'язку стандарту 4G/LTE, розглянуто загрози для радіоінтерфейсу стільникових мереж стандарту 4G/LTE, що дозволяє визначити потенційну вразливість її окремих елементів.

На основі аналізу зроблено висновок, що впровадження мереж 4G / LTE неминуче зіткнеться з новими проблемами, зокрема: для більшості споживачів стандартні послуги LTE, ймовірно, будуть досить дорогими, тому такі мережі не будуть широко доступними тривалий час; смартфони та модеми LTE не зможуть продемонструвати свою функціональність, оскільки існуюча більшість телефонів та планшетів не матиме можливості використовувати значну частину спектру, який слід використовувати, оскільки вони не мають відповідних мікросхем; існує проблема з високим споживанням енергії акумуляторів кінцевих пристроїв і тривалим часом заряджання акумуляторів, що робить їх менш функціональними.

Ключові слова: *стільникові мережі стандарту 4G/LTE, вразливість, критична інфраструктура.*

Katkov Yu., Berezovska Yu., Pshenychnyi Yu., Ryzhakov M., Prokopov S.
State University of Telecommunications, Kyiv

ANALYSIS OF THREATS AND VARIABILITY AFTER IMPLEMENTATION OF 4G/LTE TECHNOLOGY

The article deals with the vulnerability of 4G/LTE cellular networks in critical infrastructures. The technological revolution in the field of mobile wireless broadband cellular networks attracts Ukraine to the necessity of introducing new technologies in the processes of building the digital economy of the future. One such technology is LTE. The article shows that the study of threats and vulnerabilities of 4G/LTE cellular network elements for critical infrastructures is relatively new and not well-known, so the topic of work is relevant and practically in demand.

In the article the task is set: when considering the mobile 4G/LTE mobile broadband cellular networks, based on the analysis of the functioning of its elements, identify the threats for potentially vulnerable elements. To solve the problem, the description of innovative mechanisms for the introduction of mobile communication of the 4th generation is performed, the analysis of trends in the development of services for advanced areas of application of mobile communications 4G/LTE standard, to consider the threats to the radio interface of 4G/LTE cellular networks, which allows to determine the potential the vulnerability of its individual elements.

Based on the analysis, it is concluded that the introduction of 4G/LTE networks will inevitably face new challenges, in particular: for most consumers, standard LTE services are likely

to be quite expensive, so such networks will not be widely available for a long time; LTE smartphones and modems will not be able to demonstrate their functionality because the existing majority of phones and tablets will not be able to use a significant portion of the spectrum to be used because they do not have the appropriate chips; there is a problem with high energy consumption of the batteries of the end devices and for a long time charging the batteries, which make them a little functional.

Keywords: *4G/LTE cellular networks, vulnerability, critical infrastructure.*

Катков Ю.И., Березовская Ю.В., Пшеничный Ю.С., Рыжаков Н.Н., Прокопов С.В.
Государственный университет телекоммуникаций, Киев

АНАЛИЗ УГРОЗ И УЯЗВИМОСТЕЙ ВО ВРЕМЯ ВНЕДРЕНИЯ ТЕХНОЛОГИИ 4G/LTE

В статье рассматривается проблема уязвимости сотовых сетей 4G/LTE в критических инфраструктурах. Технологическая революция в области мобильных беспроводных широкополосных сотовых сетей вовлекает Украину к необходимости внедрения новых технологий в процессы построения цифровой экономики будущего. Одной из таких технологий является LTE. Показано, что изучение внутренних и внешних угроз, а также уязвимость элементов сотовых сетей стандарта 4G/LTE для критической инфраструктуры является относительно новым и малоизученным, поэтому тема работы является актуальной и практически востребованной.

Поставлено задание: при рассмотрении подвижных беспроводных широкополосных сотовых сетей передачи данных стандарта 4G/LTE на основе анализа функционирования ее элементов определить угрозы для потенциально уязвимых элементов. Для решения задачи выполнены описание инновационных механизмов внедрения мобильной связи 4-го поколения, проанализированы тенденции развития услуг перспективных областей применения мобильной связи стандарта 4G/LTE, рассмотрены угрозы для радиоинтерфейса сотовых сетей стандарта 4G/LTE, позволяет определить потенциальную уязвимость ее отдельных элементов.

На основе анализа сделан вывод, что внедрение сетей 4G/LTE неизбежно столкнется с новыми проблемами, в частности: для большинства потребителей стандартные услуги LTE, вероятно, будут достаточно дорогими, поэтому такие сети не будут широко доступными длительное время; смартфоны и модемы LTE не смогут продемонстрировать свою функциональность, поскольку существующее большинство телефонов и планшетов не будет иметь возможности использовать значительную часть спектра, который следует использовать, поскольку они не имеют соответствующих микросхем; существует проблема с высоким потреблением энергии аккумуляторов конечных устройств и длительным временем подзарядки аккумуляторов, что делает их менее функциональными.

Ключевые слова: *сотовые сети стандарта 4G/LTE, уязвимость, критическая инфраструктура.*

Вступ. Технологічна революція в області стільникових мереж передачі даних залучає Україну до необхідності впровадження нових технологій в процеси побудови цифрової економіки майбутнього. Однією з таких технологій є LTE (англ. Long Term Evolution – довгострокова еволюція) – яка розглядається як наступний крок еволюційного розвитку технології UMTS. Її маркетингова назва “мережі 4G/LTE” – рухомі бездротові широкосмугові стільникові мережі передачі даних четвертого покоління (4G) [1, 2]. На основі технології LTE був побудований стандарт проміжного виду 4G/LTE, який став основним стандартом високошвидкісного бездротового зв’язку передачі даних проекту 3GPP для задоволення потреб у бездротовому доступі до послуг Triple Play в Інтернет, які вимагають високої якості передачі даних. Стандарт 4G/LTE є одночасно і платформою для наступних стандартів 4G/LTE/Advanced, LTE-Advanced Pro, IMT-Advanced [3].

Відомо, що основне призначення технології LTE – це безшовний перехід від існуючих мереж загального користування другого покоління, побудованих за технологією GSM (2G/GSM), і третього покоління, побудованих за технологією UMTS (3G/UMTS) до мереж IMT-Advanced, метою яких є підтримка постійно зростаючого трафіку даних і кількості

кінцевих пристроїв. Також мережі за стандартом 4G/LTE мають спадкоємність: операторам існуючих стільникових мереж 2G/GSM і 3G/UMTS, які сьогодні є найбільш розповсюдженими стільниковими мережами, не потрібно будувати нову мережу, а необхідно модернізувати існуюче вузлове обладнання, яке було зроблено за технологіями WCDMA, HSDPA, HSUPA до стандарту 4G/LTE/Advanced [3–4].

Не зважаючи на початок впровадження мереж п'ятого покоління 5G, майбутнє якого ще примарно, впровадження мереж 4G/LTE/Advanced вже реальне та остається одним із перспективних напрямків розвитку стільникових мереж сучасності. В Україні основні оператори українського ринку мобільного зв'язку (Київстар, Vodafone Україна та Lifecell) отримали можливість будувати мережі 4G/LTE в українських містах. Вони вважають, що впровадження мереж 4G/LTE дозволить операторам: зменшити капітальні та операційні витрати; знизити сукупну вартість володіння мережею; розширити свої можливості в області конвергенції послуг і технологій; підвищити доходи від надання послуг передачі даних. Але впровадження мереж 4G/LTE має не тільки переваги. Тому під час впровадження мереж 4G/LTE є необхідність знати про потенційні загрози та вразливі елементи, які можуть створити критичні ситуації інформаційної інфраструктури.

Постановка завдання. Звідси виникає завдання розглянути четверте покоління рухомих бездротових широкосмугових стільникових мереж передачі даних побудованої за стандартом 4G/LTE. Необхідно на основі аналізу функціонального призначення елементів мережі 4G/LTE визначити потенційні загрози та вразливі (критичні) елементи. Для вирішення завдання за допомогою методів теоретичного рівня (вивчення та узагальнення, абстрагування, формалізації та аналізу) виконати опис факторів критичності в інноваційних механізмах впровадження мобільного зв'язку 4G/LTE. Об'єктом дослідження є стільникові мережі 4G/LTE, предметом дослідження – теоретичні, методичні та практичні аспекти критичності функціонування мереж 4G/LTE.

Аналіз останніх досліджень і публікацій. До теперішнього моменту накопичено значний обсяг теоретичного і практичного матеріалу з різних аспектів розвитку мереж 4G/LTE. Значний внесок у розвиток теорії та практики закладений в роботах таких дослідників, як S.R. Hussain, O. Chowdhury, S. Mehnaz, E. Bertino, L. Gordon, S. Sesia, I. Toufic, M. Baker, M. Wang, Yu. Yang, A. Osseiran, F. Boccardi, V. Braun, K. Kusume, S. Mjlsnes, R. Olimid, A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, J. Seifert, P. Marsch, M. Maternia, M. Schellmann, H. Schotten, В.Б. Толубко, В.О. Тихвинский, С.В. Терентьев, Н.А. Соколов та багато інших. У роботах цих авторів, наприклад, у [3–5] – концептуальному осмисленню піддаються окремі питання специфіки стільникових мереж 4G/LTE та формування світового ринку послуг в умовах економічного зростання, розглядаються особливості функціонування елементів стільникових мереж 4G/LTE. Аналіз вітчизняної та зарубіжної літератури щодо аспектів критичності функціонування стільникових мереж 4G/LTE дозволяє зробити висновок про недостатність науково обґрунтованих уявлень і висновків про потенційні загрози, особливості впливу загроз на функціонування таких мереж, наявність вразливих елементів, а також про можливі наслідки, що ускладнює проведення комплексних заходів з оптимізації процесів створення та просування мереж 4G/LTE. Таким чином, у зв'язку з тим, що вивчення вразливості стільникових мереж 4G/LTE є відносно новим і маловивченим стаття є актуальною та практично затребуваною.

Аналіз потенційних викликів та вразливості елементів мережі стандарту 4G/LTE. *Основні характеристики специфікацій мережі стандарту 4G/LTE*. Для визначення потенційних загроз та вразливих (критичних) елементів мережі стандарту 4G/LTE стисло розглянемо основні характеристики специфікацій технології LTE. Відомо, що високі темпи зростання потреб у нових послугах Triple Play наштовхнулося в поколінні 2G/GSM і 3G/UMTS на такі недоліки: необхідність синхронізації в приймачах кодових послідовностей; значні труднощі щодо реалізації когерентної обробки прийнятих сигналів; необхідність швидкого регулювання потужності передавачів мобільних кінцевих пристроїв і базової станцій; залежність дальності зв'язку від швидкості передачі та швидкості пересування

абонента; непостійність покриття (“дихання”) стільнику, що в свою чергу знижує якість зв’язку, а при перевантаженні стільнику створює значні труднощі до адаптивного управління мережею в реальному часі.

У мережах стандарту 4G/LTE ці недоліки були враховані, але це вимагало вдосконалення архітектури та технічних можливостей обладнання мережі. Про це більш докладно можна прочитати в [6–10]. Для вирішення нашого завдання стисло визначимо основні риси. Стандарт 4G/LTE визначає архітектуру мережі, яка включає в себе мережу радіодоступу E-UTRAN (Evolved Universal Terrestrial Radio Access Network) і вдосконалене пакетне ядро EPC (Evolved Packet Core), що показано на рисунку 1 [8].

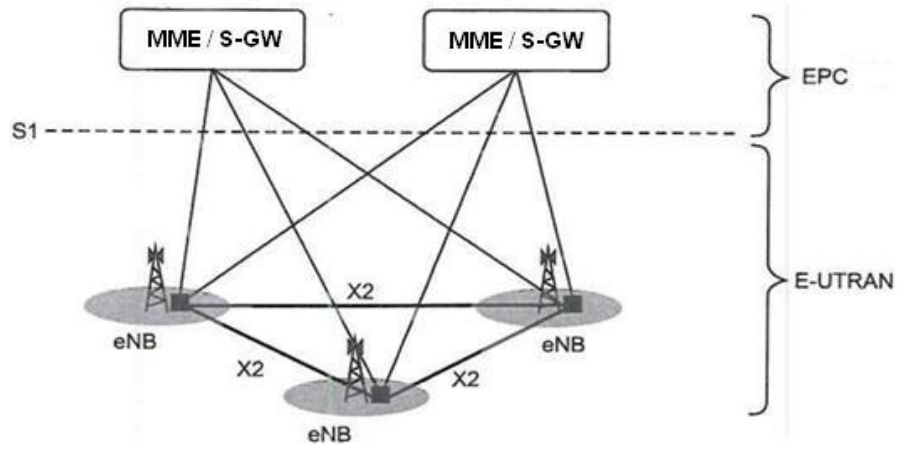

Рис. 1. Архітектура мережі LTE [8]

На рисунку 1 наведено архітектуру мережі LTE, яка побудована як сукупність базових станцій eNB (Evolved NodeB або eNodeB), де сусідні eNB з’єднані між собою інтерфейсом X2. До EPC за допомогою інтерфейсу S1 підключені eNB. Робота EPC основана на технології Internet Protocol (IP) – це міжмережевий протокол маршрутизації мережевого рівня стека TCP/IP, який об’єднує окремі мережі передачі даних у всесвітню мережу Інтернет. Невід’ємною частиною протоколу IP є адресація. Таку структуру відносять до All-IP Network (AIPN). Також показана взаємодія елементів в архітектурі E-UTRAN: S-GW (Serving Gateway) – обслуговуючі шлюзи, які містять програмне забезпечення процесу управління по протоколу ММ (MME – Mobility Management Entity). Нагадуємо, що у мережі LTE радіо-інтерфейс між UE і eNB здійснений на основі технології OFDMA (Orthogonal Frequency Division Multiplexing – мультиплексування з ортогональним частотним поділом каналів). Для максимальної швидкості передачі використовується технологія MIMO (англ. Multiple Input / Multiple Output – множинний вхід / множинний вихід). При використанні технології MIMO і ширині каналу 20 МГц максимальна швидкість передачі даних може досягати 300 Мбіт/с у низхідному каналі й 170 Мбіт/с у висхідному. Для мереж LTE в якості антен можна використати звичайні панельні антени з крос-поляризацією мереж GSM і UMTS. Але для їхньої роботи в LTE необхідно модернізувати ці панельні антени [8–9].

Специфікація LTE дозволяє забезпечити швидкість завантаження до 326,4 Мбіт/с, швидкість віддачі до 172,8 Мбіт/с, а також досягати високих агрегатних швидкостей передачі даних: 100 Мбіт/с для низхідного з’єднання і 50 Мбіт/с для висхідного. Затримка в передачі даних може бути знижена до 5 мілісекунд. LTE підтримує смуги пропускання частот від 1,4 МГц до 20 МГц і підтримує як частотне розділення каналів (FDD), так і тимчасовий поділ (TDD) [6–8]. Радіус дії базової станції LTE залежить від потужності випромінювання й теоретично не обмежений, а максимальна швидкість передачі даних залежить від радіочастоти та віддаленості від базової станції. Теоретична межа для швидкості в 1 Мбіт/с – від 3,2 км (2600 МГц) до 19,7 км (450 МГц) [6–8].

Подальшим розвитком система LTE є LTE Advanced. LTE Advanced – це технологія,

яка дозволяє агрегацію (об'єднання) в один канал кілька несучих частотних діапазонів (від 450 МГц до 5 ГГц) [3–4]. Так, наприклад, оператор, який використовує LTE Advanced, застосовує агрегацію трьох несучих 1800 + 2600 + 800 МГц з сумарною шириною смуги до 35 МГц (20 + 10 + 5), що дозволяє досягти швидкості до 260 Мбіт/с. Вона була розроблена для того, щоб надати користувачам доступ до всіляких мультимедійних сервісів мережі Інтернет за допомогою протоколу IP.

Мережа LTE (LTE Advanced) складається з множини вузлів. Усі вузли мережі прийнято ділити на дві категорії: вузли, що відносяться до мережі радіодоступу (radio access) та вузли опорної мережі (core network). Ключовим елементом, що визначає ефективність будь-якої радіомережі, є алгоритми й механізми, які використовуються для передачі даних між базовою станцією (БС, в англомовній літературі – eNodeB) і мобільними станціями (МС, в англомовній літературі – UE) [10, 11].

Аналіз потенційних викликів мережі стандарту 4G/LTE. Тепер на основі характеристик мережі стандарту 4G/LTE розглянемо критичні моменти (загрози або виклики), які супроводжують процес впровадження мереж стандарту 4G/LTE/(LTE Advanced).

1. Несумісний роумінг 4G/LTE (LTE Advanced). Відомо, що існують кілька стандартів у поколіннях 2G і 3G, основними з яких є GSM / WCDMA / HSPA і CDMA 2000 1X EV-DO. Між ними організувати роумінг складно. Навіть якщо у вас є пристрій, який підтримує ці мережі, немає ніякої гарантії, що ви зможете використовувати 4G/LTE (LTE Advanced) за кордоном. Це відбувається тому, що в різних країнах використовуються різні діапазони для послуг 4G, так що якщо ви їдете за кордон, вам доведеться повернутися до використання мереж 3G. *Загроза у тому, що немає ніякої гарантії, що ви зможете використовувати 4G/LTE (LTE Advanced) скрізь*.

2. Не можливість у мережі LTE одночасно працювати з двома даними з мережі LTE і мережі WCDMA. Абонентських пристроїв, що можуть працювати одночасно з двома даними мережами різних стандартів GSM / WCDMA / HSPA і CDMA 2000 1X EV-DO, дуже мало. Недолік у тому, що абонент, маючи пристрій, який підтримує тільки WCDMA, не зможе отримати ніяких послуг у мережі LTE, яка побудована на базі CDMA 2000. *Загроза у тому, що абонентські пристрої не можуть працювати одночасно з двома даними мережами різних стандартів LTE (LTE Advanced) і GSM / WCDMA / HSPA і CDMA 2000 1X EV-DO.*

3. Невигідно обслуговувати абонентів, які використовують абонентські пристрої попередніх поколінь 2G або 3G. Наступний недолік стосується, перш за все, операторів, яким через деякий час після запуску мережі стандарту 4G/LTE в комерційну експлуатацію стане невигідно обслуговувати абонентів, які використовують абонентські пристрої попередніх поколінь 2G або 3G, так як операторам потрібно буде обслуговувати всі мережі, що досить затратно. Але і для абонентів, які використовують пристрої, що підтримують LTE, голосовий виклик не буде працювати. Справа в тому, що для голосового зв'язку в попередніх поколіннях використовується комутація каналів, а LTE повністю основана на комутації пакетів і працює по протоколу IP. Незважаючи на те, що є методи вирішення цієї проблеми, а саме: по-перше, відступ до комутації каналів при голосовому виклику, по-друге, це впровадження технології VoLGA. У першому випадку виникає проблема в тривалому часі встановлення з'єднання. В другому – технологія VoLGA (передача голосу зверху LTE за допомогою мережі загального доступу) – це найбільш доцільне рішення на сьогоднішній день, тому що відкату до комутації каналів не відбувається. Але якщо абонент виїжджає за межі мережі LTE і опиняється в зоні дії мережі попереднього покоління, то поточний виклик перерветься, і йому доведеться здійснювати повторний дзвінок [12]. *Загроза у тому, що передача голосу зверху LTE не буде працювати з відповідною якістю.*

4. Примусове витіснення абонентів мережі GSM внаслідок скорочення базових станцій в мережі LTE. Базова станція LTE (LTE Advanced) по радіусу дії перевершує базові станції 2G і 3G мереж, тому для скорочення витрат у процесі модернізації обладнання оператори можуть піти на скорочення числа працюючих раніше базових станцій за рахунок збільшення

радіусу покриття. Це в кінцевому підсумку вплине на місткість мережі в цілому, на якість надання послуг зокрема, а також на кількість абонентів. *Загроза у тому, що у абонентів з мережі GSM або UMTS не буде бажання підключення до мережі LTE (LTE Advanced).*

5. Скорочення місткості мережі LTE під час одночасного обслуговування активних абонентів LTE і абонентів мереж 2G і 3G. Відомо, що базова станція стандарту 4G/LTE може обслуговувати одночасно до 200 активних абонентів, але не варто забувати про те, що та ж сама базова станція повинна підтримувати і абонентів мереж 2G і 3G, що помітно скорочує місткість мережі. Це обумовлено тим, що базовій станції одночасно доводиться працювати і в режимі комутації каналів, і в режимі комутації пакетів, що на короткочасні інтервали може значно знижувати якість послуг, які надаються, наприклад, втрата пакетів, і, як наслідок, повторна передача даних, що реалізована по протоколу HARQ (Hybrid Automatic Repeat Query). Але при максимальному завантаженні мережі протокол HARQ може не справлятися з виправленням помилок, і в такому випадку повторна передача пакетів реалізується за допомогою протоколу ARQ, що пов'язано з великими накладними витратами і підвищує час затримки передачі пакетів. Для голосового виклику VoLGA це буде призводити до катастрофічних помилок, де є обмеження на втрату пакетів. *Загроза у тому, що абоненти мережі LTE (LTE Advanced) будуть незадоволені якістю голосового виклику VoLGA.*

6. Критичність до значної кількості одночасно працюючих абонентських пристроїв. Якщо в зоні покриття мережі 4G/LTE (LTE Advanced) кількість смартфонів і планшетів збільшиться, це може призвести до великого навантаження на мережу тому, що хоча 4G і пропонує широкосмуговий доступ і більш високу швидкість в теорії, але в реальності зростання кількості планшетів і смартфонів у зоні покриття мережі 4G/LTE (LTE Advanced) зможе перевантажити навіть таку сучасну мережу. *Загроза у тому, що абоненти будуть шукати іншого оператора в той же зоні покриття.*

7. Неможливість забезпечення максимальних швидкостей завантаження/віддачі. Раніше було сказано, що специфікація LTE дозволяє забезпечити швидкість завантаження до 326,4 Мбіт/с, швидкість віддачі до 172,8 Мбіт/с. Але ці значення досягаються тільки в смузі пропускання, що дорівнює 20 МГц, при низькій завантаженості мережі. В реальних умовах мережі, що будуть модернізовані на основі мереж 2G/GSM і 3G/UMTS з набагато меншою пропускною здатністю (до 5 МГц), отже, швидкість при низхідному з'єднанні не буде перевищувати 5–20 Мбіт/с, що в середньому вище швидкості, яку можуть забезпечити HSPA і EV-DO Rev.B, але можна порівняти зі швидкістю, яку забезпечує WiMAX. А так як WiMAX вже використовується кілька років, і зона покриття WiMAX мережі постійно зростає, то під час початку запуску мережі LTE для абонента не буде сенсу переходити в цю мережу. А якщо врахувати те, що зона обслуговування LTE спочатку буде значно меншою зони обслуговування WiMAX, і те, що доведеться споживачу купувати новий пристрій з підтримкою даної технології – це може позначитися на доходах оператора, який побудував мережу, і, як наслідок, на перспективу розвитку самої мережі. *Загроза у тому, що абоненти не будуть підключатися до оператора мережі 4G/LTE (LTE Advanced) тому, що є WiMAX у тій же зоні покриття.*

8. Значне енергоспоживання абонентськими пристроями внаслідок використання багато антенної передачі (режим MIMO). Відомо використання багато антенної передачі даних (MIMO) в мережі LTE покращує технічні характеристики і розширює можливості в плані обслуговування абонентів. Але варто зазначити, що використання багато антенної передачі в абонентському пристрої значно підвищує його енергоспоживання, що є вагомим недоліком, тому що кінцеві пристрої, що підтримують LTE – це, в основному, мобільні пристрої, які мають обмежений ресурс в акумуляторах (комунікатори, нетбуки, ноутбуки, інтернет-планшети). Звідси підвищене енергоспоживання негативно вплине на час автономної роботи цих пристроїв. *Загроза у тому, що час роботи абонентських пристроїв значно скорочується.*

9. Проблема через доплерівські зрушення або нестабільності генераторів

абонентських пристроїв. У LTE існує проблема через доплерівські зрушення або нестабільність генераторів абонентських пристроїв. Це пов'язано з тим, що в технології LTE для сигналів первинної синхронізації використовується крок сітки піднесучих частот дрібніший, ніж для всіх інших сигналів (близько 1 кГц). Це призводить до більших обмежень на доплерівські зрушення і підвищеним вимогам щодо високої стабільності генераторів абонентських станцій. Тривалість елементарної посилки становить 800 мкс, а набір OFDM піднесуть дорівнює 839 (з захисними інтервалами в частотній смузі становить 864 піднесуть, що для інформаційного сигналу LTE відповідає 72 піднесучих). Тобто, розніс піднесучих частот становить 1,25 кГц, а загальна смуга сигналу PRACH = 1,25 × 839 = 1048,75 кГц. Звідси виникає проблема через доплерівські зрушення або нестабільності генераторів абонентських пристроїв, тому що обробка з пошуком і підстроюванням по частоті в сукупності з пошуком допустимих зрушень у синхропослідовностях ZC по трудомісткості для процесорів нездійсненна. Тому, як тільки частотні зрушення досягають близько 600 Гц, встановити синхронізацію з сигналами запитів PRACH система LTE не може. Можна оцінити теоретично максимальні швидкості, на яких такі зрушення виникнуть, наприклад, якщо зрушення близько 600 Гц, то при несучій частоті 2,6 ГГц отримуємо швидкість руху 250 км/год. У реальних умовах критичні стани виникають вже на швидкостях приблизно 120 км/год. Для компенсації цього недоліку застосовується стандарт McWiLL, що підвищує вартість обладнання. *Загроза у тому, що задекларована швидкість руху абонентів або не буде виконана, або необхідно докупати обладнання більшої вартості, що підвищить вартість послуг для абонентів.*

10. Вплив радіусу стільника на показники продуктивності каналів. Відомо, що згідно з вимогами до системи LTE радіус стільників від 5 до 30 км. При радіусі стільника в 5 км всі вимоги до показників продуктивності (спектральної ефективності, пропускної спроможності та роботи з мобільними абонентами) повинні підтримуватися. При радіусі стільника в 30 км допускається погіршення в показниках продуктивності. Але практично це означає, що швидкість каналів зі збільшенням радіусу зменшується. *Загроза у тому, що швидкість каналів змінна і залежить від радіусу покриття.*

11. Сукупність технології OFDMA і MIMO породжує суттєві недоліки. Сукупність технології OFDMA і MIMO породжує наступні суттєві недоліки. По-перше, дана сукупність технологій дуже чутлива до синхронізації по частоті, а, по-друге, в результаті застосування технології MIMO технологія OFDMA дуже критична до показника відношення пікової потужності до середньої потужності PAPR (Peak to Average Ratio) [13]. Мова йде про те, що, стандарт LTE під час застосування технології передачі MIMO дозволяє істотно збільшити пікову швидкість передачі даних і значення спектральної ефективності. У вимогах до LTE значення спектральної ефективності вказані як 5 біт/с/Гц для низхідного каналу і 2.5 біт/с/Гц для висхідного каналу (що відповідає швидкостям передачі даних в 100 Мбіт/с і 50 Мбіт/с). При цьому високі показники продуктивності повинні підтримуватися для мобільних користувачів, які прямують зі швидкістю до 120 км/год. Але якщо відношення пікової потужності до середньої потужності PAPR буде:

а) *низьким*, то це в свою чергу призведе до того, що підсилювач сигналу, який використовується, буде працювати в нелінійних ділянках своєї характеристики. Тому його ефективність буде низькою, що досить критично для пристроїв з обмеженим запасом енергії (мобільних терміналів);

б) *великим*, то це в свою чергу призведе до того, що необхідне використання дорогих і неефективних підсилювачів потужності, які пред'являють високі вимоги до лінійності, а це впливає на зростання вартості терміналів і швидкості розряду батареї. Таку можливість надає у висхідному каналі LTE інша версія OFDM під назвою SC-FDMA, яка менш критична до нелінійної характеристики підсилювача потужності. Відмінність SC-FDMA від OFDMA полягає в тому, що в SC-FDMA використовується додаткова обробка сигналу для зниження PAPR. У SC-FDMA для такої додаткової обробки сигналу використовується перетворення Фур'є. Так само, як і в низхідному каналі, в висхідному каналі можуть використовуватися

види модуляції: QPSK, 16QAM, 64QAM. *Загроза у тому, що показник продуктивності мережі 4G/LTE (LTE Advanced) дуже критичний до показника відношення пікової потужності до середньої потужності PAPR, а це означає або втрату якості каналів, або підвищення вартості послуг.*

12. Обмеження частотного і тимчасового дуплексу для ширини радіоканалу під час забезпечення двобічної передачі даних між БС і МС. Для забезпечення двобічної передачі даних між БС і МС за допомогою технології LTE підтримується як частотний (FDD), так і тимчасової дуплекс (TDD). Для частотного дуплексу визначено 15 парних частотних діапазонів (частоти від 800 МГц до 3.5 ГГц), а для тимчасового – 8. При цьому, ширина радіоканалу може бути різною. Можливі наступні значення: 1,4; 3; 5; 10; 15 і 20 МГц. Тому в низхідному каналі систем множинного доступу в LTE використовуються OFDMA, а в висхідному каналі – SC-FDMA (Single Carrier Frequency Division Multiple Access – множинний доступ з частотним поділом на базі однієї несучої). Це є причиною обмеження частотного і тимчасового дуплексу для ширини радіоканалу [14]. *Загроза у тому, що якість обслуговування залежить від навантаження на радіоканал під час забезпечення двобічної передачі даних між БС і МС, а це означає наявність можливості відмови в доступі до послуг мережі під час перенавантаження.*

13. Критичність "економіки частотного діапазону". Розподіл мереж LTE в світі за діапазонами за даними 400 найбільших мереж LTE наведено на рисунку 2 [15].

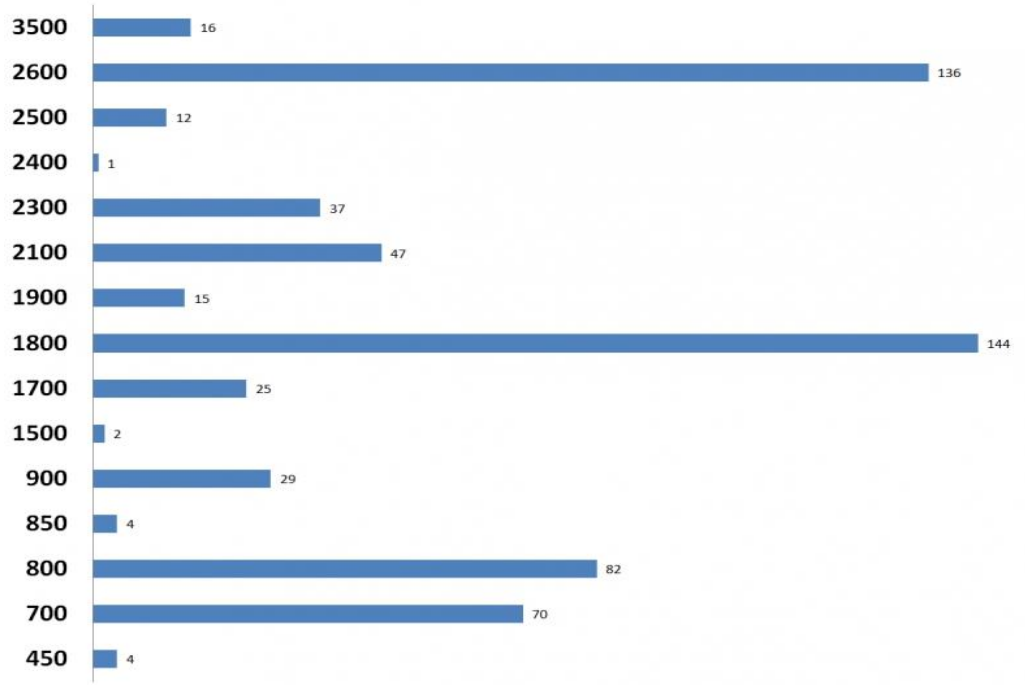

Рис. 2. Розподіл мереж LTE в світі за діапазонами [15]

З рисунка 2 бачимо, що найбільш популярним є діапазон 1800 МГц. Причини такої активності наступні:

–по-перше, це "економіка частотного діапазону". Відомо, що відповідно до законів фізики чим менша частота діапазону, тим більша буде відстань розповсюдження. Тому при однаковій потужності випромінювання LTE-1800 МГц має радіус дії (площу покриття) базової станції, що працює на частотах 1800 МГц, в чотири рази більше, ніж у обладнання, що працює на частотах 2500–2700 МГц. Радіус дії базової станції LTE залежить від потужності випромінювання та теоретично не обмежений, а максимальна швидкість передачі даних залежить від радіочастоти і віддаленості від базової станції. Теоретична межа базової станції – кінцевий пристрій для швидкості в 1 Мбіт/с – від 3,2 км (2600 МГц), 6,8 км (1800 МГц), 13,4 км (800 МГц) й до 19,7 км (450 МГц) [16]. Можна підвищити потужність випромінювання для збільшення радіусу покриття, але це призведе до збільшення вартості

експлуатації. Звідси використання обладнання LTE-1800 МГц дозволяє в найкоротші терміни розгортати мережі, тому що одну і ту ж територію можна покрити меншою кількістю базових станцій. Тут слід підкреслити, що застосування LTE у діапазоні 700–800 МГц може здатись ще корисніше тому, що, як відомо, істотне зменшення частоти хоча і збільшує радіус покриття, але кількість користувачів, які можуть користуватися одночасно послугами LTE мережі у діапазоні 700–800 МГц значно скорочується внаслідок недостатності смуги частот для організації каналу зв'язку, яка потрібна для формування ресурсних елементів. Також на цих частотах зменшується бітрейт – кількість ресурсних блоків, що призначається певному користувачу, в яких використовується відповідна ступінь модуляції. Практично, це означає скорочення швидкості в каналах для певного виду послуг (аудіо, відео, даних), що впливає на якість обслуговування. Тому діапазон 1800 МГц – найбільш використовуваний в світі, він поєднує в собі високу ємність і великий радіус дії;

–по-друге, це "ефект проникнення". Відомо, що відповідно до законів фізики менша частота має більшу здатність проникнення та розповсюдження крізь перешкоди. Тому сигнал базових станцій LTE-1800 МГц краще проникає в закриті приміщення, краще огинає перешкоди, ніж сигнал, що працює в більш високих діапазонах, наприклад, LTE-2600 МГц. Але необхідно пам'ятати, що на кінцеву швидкість впливають також інші чинники: погодні умови (дощ призводить до розсіювання сигналу), число користувачів (чим їх більше, тим середні швидкості менші).

Таким чином, можна зробити висновок, що чим нижче частота, тим більший радіус покриття і поліпшена якість проходження крізь міську забудову, але менша ємність самої мережі та, відповідно, швидкості в ній залежить від числа користувачів. Це дозволяє забезпечувати високошвидкісною мережею LTE-1800 МГц віддалені населені пункти, автомобільні траси, а також зони з частотними обмеженнями. Для кращої роботи в мережах 4G/LTE кінцевий пристрій (телефон) повинен підтримувати як мінімум частоти: 1800 і 2600 МГц (діапазони b3 і b7). *Загроза у тому, що в різних країнах діапазони b3 і b7належать різним користувачам (військовим, різним службам) тому використання залежить від програм конверсії радіочастотного спектру.*

14. Не повна сумісність інтерфейсу LTE та GSM/UMTS. Бездротовий інтерфейс LTE є несумісним з 2G і частково несумісним з 3G, через низку технологічних відмінностей, які мають антенні пристрої базових станцій та масові кінцеві пристрої. В системах LTE для отримання високих пікових швидкостей передачі даних застосовують удосконалені антенні рішення, що були розроблені для впровадження HSPA (eHSPA) в поколінні 3G. Удосконалені антенні рішення є ключовими компонентами для досягнення цілей високошвидкісного доступу з високою завадостійкістю під час багато променевому прийманні радіовипромінювання. Сутність цих рішень основане на застосуванні багатошарових антенних рішень, таких як 2x2 або 4x4 MIMO. Але розширене покриття зручніше забезпечувати за рахунок використання бімформінга (beamforming).

Технологія бімформінгу – це формування фазовими решітками такого променю, який здатний розпізнавати місце розташування встановленого пристрою і пускає сигнал прямо на цей пристрій. Бімформінг покращує енергетичні показники радіоканалу, що дозволяє обладнанню використовувати більш швидкісні види модуляції, це збільшує канальну швидкість передачі даних, знижується ймовірність повторного запиту пошкоджених пакетів. Зростає швидкість і зменшується латентність у мережі. Дана технологія дозволяє значно збільшити якість сигналу на прийомі, що забезпечить стабільну роботу, при великих відстанях від базової станції. Але бімформінг під час збільшення кількості одночасних клієнтів, збільшує час затримки сигналів, що викликано часом обробки по черзі координат клієнтів. Крім того, виникають ще два істотних недоліки: по-перше, надзвичайно короткі хвилі, що використовуються в цих технологіях, ледве проходять крізь стіни, коли багато променеві сигнали можуть огинати перешкоди, а, по-друге, зі збільшенням частоти молекули кисню починають поглинати електромагнітну енергію (особливо в 60-гігагерцовому діапазоні). Ці мінуси не дозволяють масово застосовувати бімформінг. Хоча для організації

зв'язку з високо швидкими об'єктами в повітрі (наприклад, з дронами) з використанням технологій штучного інтелекту бімформінг може застосовуватися. Що стосується масових кінцевих пристроїв, то старі моделі не мають функцій пристроїв, які притаманні пристроям кінцевим LTE. Попит створення мобільних пристроїв LTE сумісних з пристроями 2G і 3G показав їх малу фінансову ефективність тому, що зменшувався перелік отримання послуг або їх якість. Тому системи LTE працюють на окремій частоті самостійно. *Загроза у тому, що є не повна сумісність інтерфейсу LTE та GSM/UMTS, а це означає неможливість багатьом абонентам використовувати послуги мереж LTE.*

15. Знижений час життя абонентського пристрою (фактори User Inactivity Timer; background mode; Handover, Redirection, Reselection; Voice over LTE). Відомо, що при слабкому покритті мобільної мережі мобільний пристрій витрачає більше енергії на підтримку радіосигналу, тому що він працює з підвішеною потужністю випромінювання. З ростом ємності акумуляторів величина цієї енергії стала несуттєвою. Однак еволюція типів мереж накладає додаткові механізми, які можуть виснажити батарею мобільного пристрою без участі користувача. Розглянемо механізми, які можуть знизити час життя телефону в залежності від обраної LTE мережі *(час розрядки без урахування дій користувача)*:

1. *Фактор User Inactivity Timer*. Мобільний пристрій, який зареєстровано в LTE мережі, може перебувати в двох станах: RRC_CONNECTED і RRC_IDLE [17].

RRC_CONNECTED (Radio Resource Control) – це канал управління радіоресурсами. У режимі RRC_CONNECTED створюється конфігурація параметрів, яка задана на рівні eNB і записана в повідомлення RRC Connection Reconfiguration. Цей режим забезпечує двостороннє з'єднання між рівноправними об'єктами управління радіоресурсами на стороні обладнання користувача і UTRAN. У RRC_CONNECTED стані є встановлений активний радіоканал між мобільним пристроєм і вишкою. Енергоспоживання в стані RRC_CONNECTED в середньому становить 300 mA. Відповідальність за перемикання з RRC_CONNECTED в RRC_IDLE покладено на мережу. User Inactivity Timer – це час між останнім переданим пакетом даних і звільненням радіоканалу (сигнал RRC connection release генерує мережу). Величина User Inactivity Timer не описана в стандарті 3GPP, тому виробники обладнання для мереж встановлюють цей час за результатами власних спостережень. Зазвичай, цей час коливається в межах від 10 с до однієї хвилини. Відомо, що чим більша величина User Inactivity Timer – тим рідше мережі потрібно звільняти / виділяти канал для передачі даних; чим менша величина User Inactivity Timer – тим менше часу знадобиться мобільному пристрою для підтримки радіоканалу [19]. Тобто чим більша величина User Inactivity Timer, тим менші втрати енергії.

Слід відмітити, що в мобільних пристроях є спеціальний режим енергозбереження – *режим cDRX (Connected Mode Discontinuous Reception),* який у режимі RRC_CONNECTED допомагає скоротити енергоспоживання в проміжки часу, коли дані не передаються. Відомо, що 95 % енергії зберігається в стані RRC_CONNECTED, коли не ведеться активна передача даних; 20 % – 40% зберігається в разі активних інтернет сервісів; 14 % – при активному використанні інтернету користувачем. Протягом цього часу функція cDRX циклічно вмикає і вимикає приймач, щоб зберегти енергію. Параметри cDRX встановлюються і контролюються мобільним пристроєм, але мережа при цьому повинна підтримувати cDRX технологію [17].

RRC (Radio Resource Control) – протокол верхнього рівня, який є частиною інтерфейсу Iub. Рівень RRC забезпечує з'єднання сигналізації до верхніх рівнів з метою підтримки обміну інформаційними потоками між процесами верхнього рівня. Сигнальне з'єднання використовується для передачі повідомлень між призначеним для користувача обладнанням і основною мережею, щоб передати інформацію верхнього рівня. Для кожної локальної області мережі сигнальне з'єднання може обслуговувати в кожен момент тільки один виклик для одного UE. У RRC входять наступні протоколи: прикладні протоколи RRC; протоколи управління каналом зв'язку (RLC); протоколи управління доступом до середовища (MAC – Media Access Control). Також відомо, що RRC виконує наступні функції: розподіляє заявки за рівнями на стороні користувацького обладнання або на стороні мережі UTRAN; виконує

широкомовні функції – широкомовне управління, доставку широкомовних повідомлень; оповіщає призначені для користувача термінали (UE) про стан мережі та радіоресурсів; розсилає інформацію по радіомережі; розсилає інформацію всім рівням мережі; здійснює встановлення, реконфігурацію і звільнення RRC-з'єднання між UE і UTRAN; здійснює встановлення, реконфігурацію й звільнення радіоносіїв; здійснює призначення, реконфігурацію та звільнення радіоресурсів для RRC-з'єднання; забезпечує функції мобільності з'єднання; формує UE-повідомлення про результати вимірювання; здійснює управління потужністю; управляє шифруванням; здійснює вибір і перевибір первинного стільнику; забезпечує збереження достовірності інформації [18].

У режимі RRC_IDLE застосовуються установки за замовчуванням, що розсилаються широкомовно, наприклад, об'єкти, на яких проводяться вимірювання, періодичність відправлення результатів вимірювання, отримання конфігурації параметрів, зіставлення об'єктів вимірювання з формою звіту, показники вимірювань і коефіцієнти фільтрації для проведення оцінки подій та надання звітності, періодичність проведення вимірювань, відсутність передачі. У стані RRC_IDLE мобільний пристрій зареєстровано в EMM (mobility management), проте воно не має активної сесії. У цьому стані мобільний пристрій може бути викликаний для передачі даних або ініціювати передачу UL (upload) трафіку через запит на виділення радіоресурсів. Енергоспоживання в стані RRC_IDLE у середньому становить 4 mA. Звідси стає зрозумілим, що будь який акумулятор мобільного пристрою буде розряджатися, наприклад, більшість бюджетний мобільних пристроїв мають акумулятор ємністю близько 2000 мА*год, який розрядиться через 6 годин. Тому проблема енергоспоживання мобільними пристроями стає досить актуальною.

2. *Фактор background mode (режим періодичних коротких опитувань інтернет-сервісів)*. Коли користувач активно не користується інтернетом, робота мобільного пристрою в мережі полягає у періодичних коротких опитуваннях інтернет-сервісів. Корисний обмін даними відбувається в межах секунди. Тоді корисне енергоспоживання становить <10 % від усього. Кількість запитів на годину для різних сервісів в background режимі: новини (Flipboard, Daily news та ін.) 4–6 операцій/год; соціальні мережі 1–4 операцій/год; миттєві повідомлення (Skype, Hangouts, Viber тощо) 2–12 операцій/год; географічні сервіси 2–3 операцій/год. Режим періодичних коротких опитувань інтернет-сервісів виконується в режимі RRC_CONNECTED. Це означає додаткові затрати енергії акумулятора [17].

3. *Фактор Handover, Redirection, Reselection*. Дані технології відповідають за перемикання мобільного пристрою між вишками в межах однієї мережі. Під час тільки одноразової дії процесу використовується близько 4 мА. У стані RRC_IDLE мобільний пристрій проводить вимірювання потужності сигналу з різних вишок. Якщо результати цих вимірювань відповідають критеріям переходу, мобільний пристрій переключиться на відповідну вишку і залишається в стані RRC_IDLE. Redirection – відбувається, коли мобільний пристрій спершу перебував у стані RRC_CONNECTED. У цьому стані мобільний пристрій також проводить вимірювання доступних вишок і звіт відсилає в мережу. Якщо існує можливість більш оптимального зв'язку, мережа перемикає радіоканал з однієї вишки з мобільним пристроєм на іншу. У разі Handover, вишка, на яку перемикається мобільний пристрій, вже підготовлена, тоді як у разі Redirection – мережа висилає дані про частоту, на якій знаходиться відповідна вишка. Handover можливий тільки, якщо існує фізичний інтерфейс між двома вишками. Існує три шляхи перемикань пристрою між вишками: *Handover команда* – вимагає налаштувань для всіх вишок оператора, що можливо тільки в разі, якщо існує фізичний інтерфейс між вишками; *Redirection команда* – вимагає налаштувань для всіх вишок оператора (на відміну від попереднього – необхідна лише частота на яку слід переключитися), мобільний пристрій сам проведе підключення; *RRC connection release команда*, яка переведе мобільний пристрій в RRC_IDLE стан і телефон сам вибере оптимальну вишку і проведе процедуру підключення.

4. *Фактор VoLTE (Voice over LTE).* IMS (IP Multimedia Subsystem) у разі VoIP/LTE реалізований на AP рівні. Відповідно, AP процесор мобільного пристрою повинен бути під

навантаженням. Для VoLTE IMS модуль розташований в модемі, тому навіть при дзвінку, AP процесор може перебувати в сплячому режимі. Це дозволяє значно заощадити заряд батареї: 33 % енергії зберігає в порівнянні зі Skype дзвінком; 0 % рівносильно дзвінку в WCDMA мережі [20].

На даний момент на території СНД голосові послуги в LTE мережах виконуються через функцію CSFB (Circuit Switched FallBack). Мобільний пристрій отримує сигнал про вхідний дзвінок, перемикається в мережу нижчого рівня (WCDMA / GSM) приймає дзвінок і потім виконує приєднання до LTE мережі. Перемикання / пошук вимагають додаткових витрат енергії. Таким чином, швидкість розрядки акумулятора мобільного пристрою в значній мірі залежить від якості мережі в якій пристрій зареєстровано. Для погано налаштованих мереж середньостатистичний LTE-телефон може розрядитися за 8 годин без втручання користувача. *Загроза у тому, що фактори User Inactivity Timer; background mode; Handover, Redirection, Reselection; Voice over LTE значно зменшують корисне використання мобільного пристрою і створюють незручності для заряджання акумуляторів.*

Висновки. Огляд можливостей стандарту 4G/LTE (LTE Advanced) показує впровадження нових телекомунікаційних, інформаційних та інтелектуальних технологій, які можуть здійснювати підтримку нових послуг. Однак розробка мереж на основі стандарту 4G/LTE (LTE Advanced) неминуче зіткнеться з новими технічними критичними проблемами, які створюють наступні загрози:

1. Немає ніякої гарантії, що можна використовувати 4G/LTE (LTE Advanced) у будь-якому місці;
2. Абонентські пристрої не можуть працювати одночасно з двома даними мережами різних стандартів LTE (LTE Advanced) і GSM / WCDMA / HSPA і CDMA 2000 1X EV-DO;
3. Передача голосу поверх LTE не буде працювати з відповідною якістю;
4. У абонентів з мережі GSM або UMTS не буде бажання підключення до мережі LTE;
5. Абоненти мережі LTE будуть незадоволені якістю голосового виклику VoLGA;
6. Абоненти будуть шукати іншого оператора в тій самій зоні покриття;
7. Абоненти не будуть підключатися до оператора мережі 4G/LTE (LTE Advanced) тому, що є WiMAX в тій самій зоні покриття;
8. Час роботи абонентських пристроїв значно скорочується;
9. Задекларована швидкість руху абонентів не буде виконана, або необхідно докупати обладнання більшої вартості, що підвищить вартість послуг для абонентів;
10. Швидкість каналів змінна і залежить від радіусу покриття;
11. Показник продуктивності мережі 4G/LTE (LTE Advanced) дуже критичний щодо показника відношення пікової потужності до середньої потужності PAPR, а це означає або втрату якості каналів, або підвищення вартості послуг;
12. Якість обслуговування залежить від навантаження на радіоканал під час забезпечення двобічної передачі даних між БС і МС, а це означає наявність можливості відмови в доступі до послуг мережі під час перенавантаження;
13. У різних країнах діапазони b3 і b7 належать різним користувачам (військовим, різним службам) тому використання залежить від програм конверсії радіочастотного спектру;
14. Є не повна сумісність інтерфейсу LTE та GSM/UMTS, а це означає неможливість багатьом абонентам використовувати послуги мереж LTE;
15. Фактори User Inactivity Timer; background mode; Handover, Redirection, Reselection; Voice over LTE значно зменшують корисне використання мобільного пристрою і створюють незручності для заряджання акумуляторів.

Список використаної літератури

1. 3GPP, «LTE», 2017. https://www.3gpp.org/technologies/ keywords-acronyms/%2098-lte (10.05.2019).
2. 3GPP Specification: 23.402. Architecture Enhancements for non3GPP Accesses 2013.

http://www.3gpp.org/DynaReport/23402.htm (10.05.2019).

3. S.R. Hussain, O. Chowdhury, S. Mehnaz, E. Bertino, "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE," in Proceedings of the Network and Distributed Systems Security (NDSS REDIRECTION), 2018.

4. H. Lin, "LTE: Forcing Targeted LTE Cellphone into Unsafe Network," in Hack In The Box Security Conference (HITBSecConf), 2016.

5. U. Meyer and S. Wetzel, "On the Impact of GSM Encryption and Manin-the-Middle Attacks on the Security of Interoperating GSM/UMTS Networks," in Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE International Symposium on, vol. 4. IEEE, 2004.

6. 3GPP. ETSI TS 26.300, "Evolved Universal Terrestrial Radio Access and Evolved Universal Terrestrial Radio Access Network; Overall description; Stage 2," 2017. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/36300.htm (10.05.2019).

7. LTE: как работает. https://habr.com/ru/company/beeline/ blog/129694/ (10.05.2019).

8. 3GPP. TS 36.331, "Evolved Universal Terrestrial Radio Access (EUTRA); Radio Resource Control (RRC); Protocol specification", 2017.

9. 3GPP. TS 24.301, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3", 2017.

10. 3GPP. TS 24.008, "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3", 2017.

11. A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems," Proceedings of the Network and Distributed System Security Symposium (NDSS), 2016.

12. C.-Y. Li, G.-H. Tu, C. Peng, Z. Yuan, Y. Li, S. Lu, and X. Wang, "Insecurity of Voice Solution VoLTE in LTE Mobile Networks," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015.

13. Описание физического уровня LTE http://anisimoff.org/lte/phy_description.html (10.05.2019).

14. Основні характеристики LTE http://jak.bono.odessa.ua/ articles/osnovni-harakteristiki-lte.php. Дата перегляду 10 травня 2019.

15. Операторы предпочитают LTE 1800. https://nag.ru/ articles/article/27771/operatoryi-predpochitayut-lte-1800.html (10.05.2019).

16. LTE в 450 МГц и не только. [Електронний ресурс].https://mobile-review.com/articles/2013/lte-450.shtml (10.05.2019).

17. Как выбранная LTE сеть влияет на энергопотребление телефона, или недостатки LTE сетей в СНГ. https://habr.com/ru/post/237947/ (10.05.2019).

18. Behrouz A. Local Area Networks. First Edition**.** Mc Graw-Hill Forouzan Series, 2002.

19. MCE-T Q.1741.

20. H. Kim, D. Kim, M. Kwon, H. Han, Y. Jang, D. Han, T. Kim, and Y. Kim, "Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015.

References

1. 3GPP, (2017), *"LTE"*. *https://www.3gpp.org/technologies/keywords-acronyms/98-lte* (10.05.2019).

2. 3GPP Specification: 23.402. Architecture Enhancements for non3GPP Accesses 2013. *http://www.3gpp.org/DynaReport/23402.htm* (10.05.2019).

3. Hussain S.R., Chowdhury O., S. Mehnaz, and E. Bertino, "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE," in Proceedings of the Network and Distributed Systems Security (NDSS REDIRECTION), 2018.

4. Lin H. (2016) "LTE: Forcing Targeted LTE Cellphone into Unsafe Network," in *Hack In The Box Security Conference (HITBSecConf)*.

5. Meyer U., and Wetzel S., (2004) “On the Impact of GSM Encryption and Manin-the-Middle Attacks on the Security of Interoperating GSM/UMTS Networks,” in *Personal, Indoor and Mobile Radio Communications, 2004. 15th IEEE International Symposium on vol. 4. IEEE,*.

6. 3GPP. ETSI TS 26.300, “Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2”, 2017. *http://www.3gpp.org/ftp/Specs/html-info/36300.htm* (10.05.2019) .

7. LTE:How does it work. https://habr.com/ru/company/beeline/blog/129694/ (10.05.2019).

8. 3GPP. TS 36.331, *“Evolved Universal Terrestrial Radio Access (EUTRA); Radio Resource Control (RRC); Protocol specification”*, (2017).

9. 3GPP. TS 24.301, *“Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3”*, (2017).

10. 3GPP. TS 24.008, *“Mobile radio interface Layer 3 specification; Core network protocols; Stage 3”*, (2017).

11. Shaik A., Borgaonkar R., Asokan N., Niemi V., and Seifert J.-P., (2016)“Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems,” *Proceedings of the Network and Distributed System Security Symposium (NDSS)*.

12. Li C.-Y., Tu G.-H., Peng C., Yuan Z., Li Y., Lu S., and Wang X., (2015) “Insecurity of Voice Solution VoLTE in LTE Mobile Networks,” in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM*.

13. Description of the physical layer LTE *http://anisimoff.org/lte/phy_description.html* (10.05.2019)

14. Main characteristics LTE. *http://jak.bono.odessa.ua/articles/osnovni-harakteristiki-lte* (10.05.2019).

15. Operators prefer LTE 1800. *https://nag.ru/articles/article/27771/operatoryi-predpochitayut-lte-1800.html* (10.05.2019).

16. LTE v 450 MGts and not only. *https://mobile-review.com/articles/2013/lte-450.shtml* (10.05.2019).

17. How does the chosen LTE network affect the power consumption of the phone, or the disadvantages of LTE networks in the CIS. *https://habr.com/ru/post/237947/* (10.05.2019).

18. Behrouz A. Forouzan. (2002) *“Local Area Networks.”* First Edition. Mc Graw-Hill Forouzan Series. Print.

19. MSE-T *Q.1741*.

20. Kim H., Kim D., Kwon M., Han H., Jang Y., Han D., Kim T., and Kim Y., (2015) “Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations,” in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*.

Автори статті (Authors of the article)

Катков Юрій Ігорович – к.т.н., доцент, доцент кафедри комп’ютерних наук (Katkov Yu. – PhD, Associate Professor, Associate Professor at the Department of Computer Science). Phone: +380(67)789 34 78. E-mail: kyi12@bigmir.net.

Березовська Юлія Володимирівна – аспірант Державного університету телекомунікацій (Berezovska Yu. – Postgraduate Student at the State University of Telecommunications). Phone: +380(50) 559 98 19. E-mail: krasabereza@gmail.com.

Пшеничний Юрій Сергійович – студент групи ІМЗ-51 Державного університету телекомунікацій (Pshenychnyi Yu. – Master Student Group IMZ-51 at the State University of Telecommunications). Phone: +380(98) 716 99 29. E-mail: moyaposhta21@gmail.com.

Рижаков Микола Миколайович – аспірант Державного університету телекомунікацій (Ryzhakov M. – Postgraduate Student at the State University of Telecommunications). Phone: +380(98) 442 00 68. E-mail: nykolay.ryjakov@gmail.com.

Прокопов Сергій Васильович – к.т.н, доцент, доцент кафедри комп’ютерних наук (Prokopov S. – PhD, Associate Professor, Associate Professor at the Department of Computer Science). Phone: +380 (50) 735 99 72. E-mail: psvhome@ukr.net.