УДК 355.40

В.С. Наконечний

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ У МЕРЕЖАХ НОВОГО ПОКОЛІННЯ LTE

У статті розглянуто основні питання, пов'язані з інформаційною безпекою в мережах нового покоління. Відзначено важливість і гостра потреба у високоякісному та швидкісному сполученні. Визначено основні цілі створення стандарту LTE, його технологічні особливості, переваги та обмеження. Запропонований варіант відповіді на питання - чи не перетворяться мобільні мережі Інтернет з притаманними йому небезпеками і проблемами?

Ключові слова: Інтернет, інформаційні технології, інформаційна безпека, мобільна мережа, мережа нового покоління.

Введення

У розвинених країнах світу продовжується перехід до інформаційної сервісно-технологічної економіки, де значна частина ВВП забезпечується діяльністю з виробництва, обробки і розповсюдження інформації і знань. Економістами і політиками всього світу усвідомлено, що розвиток інформаційних технологій (IT) створює фундамент сучасної економіки держави і добробуту її людей.

В останні два-три роки в інформаційно-технологічної екосистемі бізнесу відбулися докорінні зміни, зумовлені збільшенням кількості пристроїв, їх обчислювальних потужностей, колосальним зростанням ємності і простотою використання знімних пристроїв пам'яті, перетворенням смартфонів у потужні мобільні комп'ютери, а також поширенням мобільних мереж нового покоління.

До недавнього часу Україна взагалі не знала, що таке швидкий 3G, не кажучи вже про LTE - стандарт зв'язку четвертого покоління, який вважається перспективним напрямком розвитку мобільних мереж. На думку експертів, з появою 4G в Україні почне формуватися абсолютно новий ринок з новими бізнес-моделями і новою логікою отримання доходів. Швидкість передачі даних LTE-мережі дозволить не тільки поліпшити якість надаваних послуг, але й розширить можливості для ведення онлайн-бізнесу. 4G – це наступний крок на шляху до «інтернету речей» (IoT). Це концепція, яка передбачає комунікацію між предметами побуту, товарами і технологіями без участі людини. Такий підхід зможе повністю змінити саму концепцію ведення бізнесу.

Без високошвидкісного мобільного Інтернету, доступного прямо тут і зараз, вже неможливо обійтися. Відеохостинги, потокові сервіси відтворення різних аудіо форматів, спілкування по FaceTime, ooVoo, Skype або іншими популярними месенджерами з функцією відео дзвінків – все це вимагає якісного високошвидкісного з'єднання. Варто лише раз спробувати можливості LTE – відмовитися від цього буде вже неможливо, та й непотрібно. За ним майбутнє!

Основна частина

Нові покоління мобільного зв'язку починали розроблятися практично через кожні десять років з моменту переходу від розробок першого покоління аналогових стільникових мереж в 1970-х роках (1G) до мереж з цифровою передачею (2G) у 1980-х роках Рис.1. У 1990-х роках почав розроблятися стандарт 3G, заснований на методі множинного доступу з кодовим поділом каналів (CDMA), він був впроваджений тільки в 2000-х роках. До четвертого покоління 4G відносяться перспективні технології, що забезпечують більш якісні послуги, із зменшенням затримок у передачі даних.

Мережі четвертого покоління LTE стали розроблятися в 2000 році і впроваджуватися в багатьох країнах починаючи з 2010 року. Якщо говорити в цілому, то кожне нове покоління мобільних мереж забезпечує кращу спектральну ефективність використання частотного ресурсу.

Який же приріст швидкості варто очікувати користувачам нових мереж?

За даними компанії HUAWEI Рис.1, мережі другого покоління 2G можуть забезпечити передачу даних до 114 Кбіт/с при використанні GPRS та до 472,6 Кбіт/с за технологією EDGE. Використовуючи 3G можна отримати швидкість до 21,6 Мбіт/с. У свою чергу, LTE забезпечує швидкість до 326,4 Мбіт/с від базової станції до користувача і до 172,8 Мбіт/с у зворотному напрямку.

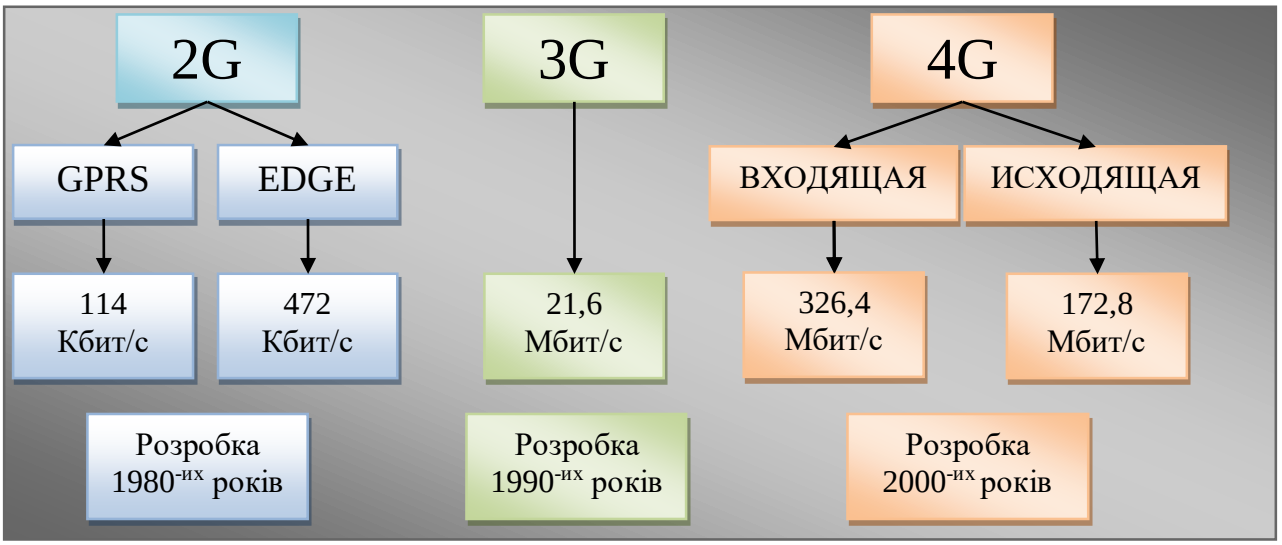

Рис.1. Рік розробки та швидкість передавання інформації в мережах різних поколінь

Метою створення стандарту LTE є:

– збільшення можливостей високошвидкісних систем мобільного зв'язку;

– зменшення вартості передачі даних;

– можливість надання широкого спектру недорогих послуг.

До числа основних технологічних особливостей LTE відносяться:

– Flexible Bandwidth – гнучкий вибір полоси каналу: 1.4, 3, 5, 10, 15, 20 МГц.

– Більш широкий вибір частотного діапазону для впровадження LTE: 700, 800, 900, 1800, 2100, 2300, 2600, 3500 МГц та ін.

– OFDMA технологія радіодоступу.

– 3 схеми модуляції QPSK, 16QAM, 64QAM. Вибір необхідної схеми модуляції залежно від конкретних радіоумов.

– Технологія MIMO (Multiple Input Multiple Output) – використання декількох антен для передачі даних.

– Carrier Aggregation – технологія агрегації частот для збільшення швидкості передачі даних.

– All IP архітектура і відсутність контролера.

Ще одна перевага LTE — варіативність частотних діапазонів, придатних для запуску (від 800 до 2600 МГц).

Однак поліпшення якісних і кількісних показників мереж нового покоління висуває й нові вимоги, пов'язані з підвищенням безпеки переданої інформації. Оскільки технологія 4G повністю заснована на протоколі IP, чи не перетворяться мобільні мережі в Інтернет з притаманними йому небезпеками і проблемами?

Для відповіді на це питання необхідно знання переваг LTE. Мобільний зв'язок четвертого покоління передбачає використання цілого спектру технологій, які раніше розвивалися паралельно. Всі вони внесли свій внесок у специфікацію LTE реалізованої в двох основних варіантах технологій: з дуплексним частотним поділом LTE-FDD (Frequency Division Duplex)

і часовим поділом LTE-TDD (Time Division Duplex) [1]. Опора на безліч різних технологій ускладнює пошук вразливостей в LTE, що добре з точки зору безпеки — злом радіоканалу для одних методів може спрацювати, а для інших — ні.

Якщо в 3G голосовий трафік і дані передавалися по двом різним мережам, то в мережах 4G весь трафік проходить через єдину архітектуру EPC (Evolved Packet Core) за протоколом IP. Ось чому в компанії Cisco вважають, що всі загрози безпеки інформації, що передається, пов'язані саме з протоколом IP.

З фізичної точки зору в мережах LTE використовуються:

– великі смуги частот;

– високорівнева модуляція сигналу;

– технологія MIMO.

Разом вони забезпечують адекватну завадостійкість, високі швидкості передачі даних і ємність мережі.

Важливою особливістю мережі 4G є те, що з її архітектури зникло поняття контролера радіомережі (RNC), який в 3G виконував основну функцію з управління комунікаційними ресурсами.

Базові станції в LTE стали більш інтелектуальними і самостійними - вони отримали можливість маршрутизувати трафік, що дозволило організовувати з'єднання між абонентами безпосередньо, минаючи ядро мережі. В результаті у зловмисників з'явилася можливість атакувати самі базові станції, які працюють тільки за протоколом IP, тому полегшується несанкціонований доступ до мережі і, отже, можуть бути використані класичні атаки на канальному рівні, широкомовні шторми й інші варіанти нападів.

Щоб звести до мінімуму атаки на конфіденційну інформацію, базова станція повинна забезпечити виконання таких важливих операцій, як кодування і розшифровку користувачів даних, а також зберігання ключів.

Для мінімізації шкоди, що наноситься в разі крадіжки інформації про ключі з базових станцій розроблені спеціальні заходи протидії:

– перевірка цілісності пристрою;

– взаємна аутентифікація базової станції оператора (видача сертифікатів);

– безпечні оновлення;

– механізм контролю доступу;

– синхронізація часу;

– фільтрація трафіку.

Існують чотири основні вимоги до механізмів безпеки технології LTE [2]:

– забезпечити як мінімум такий же рівень безпеки, як і в мережах типу 3G, не доставляючи незручностей користувачам;

– забезпечити захист від Інтернет-атак;

– механізми безпеки для мереж 4G не повинні створювати перешкод для переходу зі стандарту 3G на стандарт LTE;

– забезпечити можливість подальшого використання програмно-апаратного модуля UMTS (універсальна сім-карта).

Стандарт LTE виділяє п'ять основних груп безпеки це, насамперед:

– архітектура безпеки мережі повинна забезпечити користувачів надійним доступом до сервісів і захист від атак на інтерфейси;

– мережевий рівень повинен дозволяти вузлам мережі безпечно обмінюватися як даними користувачів, так і керуючими даними і забезпечувати захист від атак на провідні лінії;

– користувальницький рівень повинен забезпечувати безпечний доступ до мобільного пристрою;

– рівень додатків повинен гарантувати безпечний обмін повідомленнями;

– видимість і можливість зміни налаштувань безпеки повинна дозволяти користувачеві дізнаватися, чи забезпечується безпека і включати різні режими для її забезпечення.

В даний час віруси на комп'ютерах стали звичайною справою, троянців для Android стає все більше, отже, впровадження високошвидкісного стандарту LTE може принести в мобільні засоби зв'язку всі ті загрози, які ми зараз спостерігаємо в ситуації із звичайними комп'ютерами.

До числа основних очевидних загроз інформаційної безпеки в мережах LTE належать [3]:

– атаки DoS на мережу (Denial of Service). Ємність радіоканалу в LTE передбачається велика, але все ж вона має обмеження. Мережеві ресурси базової станції діляться між абонентами, і хоча є обмеження для монополізації смуги окремим користувачем, тим не менш, атака на відмову в обслуговуванні мережі цілком можлива;

– вірусні атаки. Хоча таким атакам піддаються пристрої, а не мережа, технологія LTE збільшує швидкість поширення шкідливих програм, оскільки сам цей стандарт є високошвидкісним;

– атаки на додаткові сервіси. Власне, LTE розроблялося не тільки для забезпечення доступу до Інтернету мобільних користувачів, а скоріше як платформа для впровадження нових відео, ігрових та багатьох інших послуг. Ці сервіси можуть бути уразливі для самих різноманітних атак — як з Інтернету, так і з мобільного мережі. Цілком можливо, що, атакувавши один з сервісів, зловмисники зможуть впровадити в клієнтські пристрої небезпечні програми.

Є також проблеми і з самим стандартом [1].

1. Дуже гостро стоїть завдання взаємодії з не LTE мережами. Якщо трафік між користувальницьким обладнанням і базовою станцією шифрується (це вимога стандарту) і загроза порушення конфіденційності стає неактуальною, то взаємодія базової станції з радіоконтролером мережі 3G по умовчанню ніяк не захищене а, отже, це пролом для можливих атак з боку зловмисників.

2. Відсутність обов'язкової аутентифікації між ядром мережі і базовою станцією. Цю опцію оператор зв'язку для зниження своїх витрат щодо розгортання мережі LTE може і не задіяти зовсім.

Не можна забувати і про обмеження LTE. Наприклад, збільшення швидкості підключення зазвичай обертається зменшенням радіусу дії базової станції, який в середньому для 4G становить близько 5 км і залежить від використовуваного частотного діапазону [1]. Тому базових станцій в мережі стає більше, і вони розташовуються ближче одна до одної. В результаті тріангуляційний метод визначення місцезнаходження абонента за сигналами базових станцій працює точніше. З одного боку, це можна використовувати, наприклад, для контролю за переміщенням вантажів, оповіщення про надзвичайні ситуації та багато іншого. Але з іншого боку, сервіси геопозиціонування можна використовувати і для стеження за абонентом, що створює небезпеку нових загроз на особистість.

Ще одна особливість LTE в тому, що ця технологія орієнтована на підключення інтелектуальних пристроїв, з поширенням яких число потенційно небезпечних сервісів буде тільки зростати, що дозволить зловмисникам отримати доступ до конфіденційної інформації провайдера і побудувати нові витончені схеми інформаційних злочинів.

Враховуючи все вищевикладене, розробники мобільної технології LTE подбали про її захист істотно більше, ніж розробники Інтернету і тому мобільна мережа є більш надійною і безпечною, ніж всесвітня мережа. При цьому, в основному, захист покладено на більш інтелектуальні базові станції.

Всі функції захисту в LTE об'єднані стандартом і передбачають захист на декількох рівнях [4]: на рівні доступу до мережі, на рівнях мережевого і користувальницького доменів, на рівні додатків та на рівні відображення і конфігурацій рисунок 2.

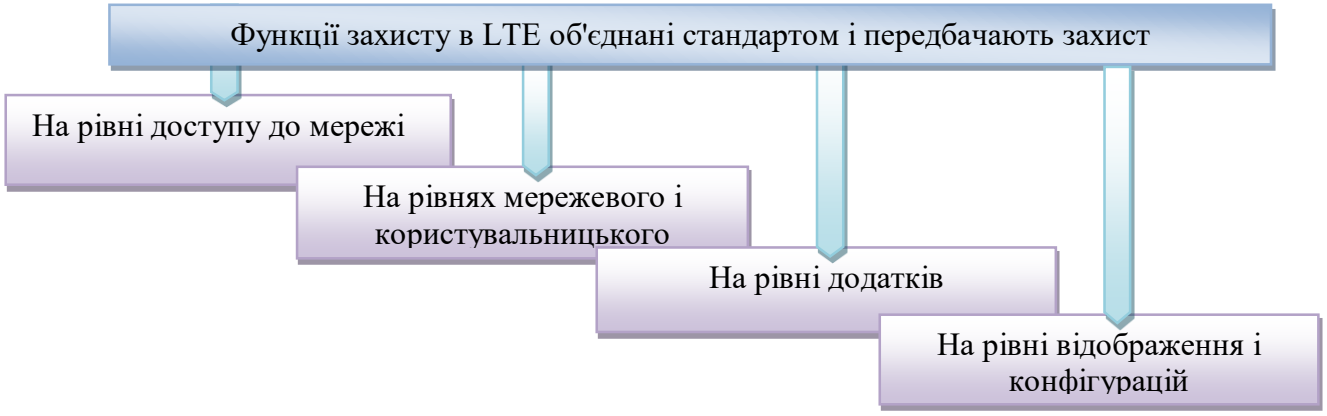

Рис. 2 Функції захисту в LTE

Кожен з цих рівнів передбачає аутентифікацію і авторизацію всіх пристроїв, чого немає в Інтернеті. Технологія LTE передбачає використання не тільки IP-адреси, але і системи розповсюдження ключів шифрування для всіх пристроїв, підключених до мережі з можливістю переходу зі 128 до 256-бітові ключі і введення нових алгоритмів, зберігаючи зворотну сумісність. Крім алгоритмів шифрування і забезпечення комплексної безпеки в мережах 4G використовуються додаткові алгоритми, які навіть за умови того, що один з них буде зламаний, решта забезпечать безпеку мережі LTE.

Крім того, в LTE зберігаються і методи аутентифікації користувачів по прив'язці до SIM карти, як в традиційному мобільному зв'язку. Користувач може заблокувати доступ до телефону з PIN-кодом.

Аналітична компанія OpenSignal представила результати дослідження стану середньої доступної швидкості мобільних мереж в різних країнах. Дані були зібрані від понад 800 тисяч користувачів зі всього світу рисунок 3 [5].

Глобальним лідером по швидкості мобільного Інтернету стала Південна Корея, де швидкість з'єднання становить 41 Мбіт/с. Друге місце посідає Сінгапур з 31 Мбіт/с. Трійку замикає Угорщина з показником 26 Мбіт/с. Україна ж знаходиться на досить низькому 67 місці зі швидкістю з'єднання 5,78 Мбіт/с, значно поступаючись більшості європейських країн.

Враховуючи величезну економічну і політичну важливість запровадження в Україні технологій 4G, Президент Порошенко підписав указ про початок роботи по їх впровадженню у нашій країні.

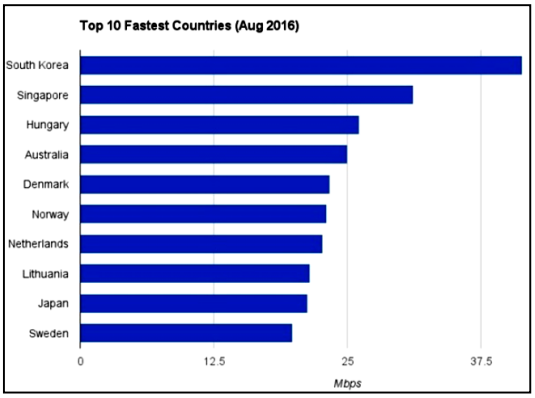

Рис. 3. Результати дослідження середньої доступної швидкості мобільних мереж у різних країнах світу (за даними компанії OpenSignal)

Висновки

Таким чином, фахівці з безпеки спільно з розробниками LTE постійно відстежують появу нових загроз безпеки і роблять усі необхідні кроки для забезпечення цілісності і конфіденційності переданих даних.

І ми горді тим, що вже сьогодні результатом плідної співпраці всіх НПП Державного університету телекомунікацій з його стін, випускаються висококваліфіковані професіонали в галузі інформаційних технологій, кібербезпеки та захисту інформації, знання і практичні навички яких високо оцінені провідними компаніями галузі. Кращі науково-педагогічні працівники нашого Університету приймають активну участь у реалізації державної політики у сфері кібербезпеки, криптографічного та технічного захисту інформації, а також стандартизації в рамках технічного комітету ТК-107.

Література

1. [Електронный ресурс]. Режим доступу: http://pro-spo.ru/mobilnye-texnologii-i-telefony/4058-lte-zhdat-li-novyx-ugroz?device=xhtml

2. [Електронный ресурс]. Режим доступу: http://amonitoring.ru/article/detail.php?ELEMENT_ID=56.

3. [Електронный ресурс]. Режим доступу: http://www.osp.ru/nets/2012/06/13032673/.

4. [Електронный ресурс]. Режим доступу: http://pro3gsm.com/zashhita-lte/.

5. [Електронный ресурс]. Режим доступу: http://opensignal.com/reports/2016/08/global-state-of-the-mobile-network/

Надійшла 23.11.2016 р. Рецензент: д.т.н., проф. Вишнівський В.В.