Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Метод пошуку вразливостей безпеки інформації в мережах LTE
(тема)

Виконав: В'юхін Д.О.
(прізвище, ініціали)
студент 2 курсу, групи БДІРм-18-1
Спеціальність 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва освітньої програми)

Керівник д.т.н., проф. Северінов О.В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Халімов Г.З.
(підпис) (прізвище, ініціали)

2019 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 125 Кібербезпека
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна, або освітньо-наукова)

Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові *В'юхіну Данііілу Олександровичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Метод пошуку вразливості безпеки інформації в мережах LTE*
затверджена наказом по університету від "04" листопада 2019 р. № 1648Ст
2. Термін подання студентом роботи до екзаменаційної комісії
3. Вихідні дані до роботи *Теоретичні данні про LTE*
4. Перелік питань, що потрібно опрацювати в роботі
1. Основні поняття та принципи роботи мереж LTE.
2. Відомі атаки та статистика успішних відомих атак.
3. Проведення випробувань забезпечення безпеки інформації в мережах стільникового з'вязку.
4. Опрацювання отриманих даних.
5. Виведення методики виявлення вразливості в мережах LTE.
6. Підведення висновків що до забезпечення безпеки інформації в безпровідних мережах.
5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій *Презентаційний матеріал у вигляді слайдів*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	*Отримання завдання*	*9.09.19*	
2	*Пошук літератури*	*10.10.19-20.10.19*	
3	*Практичні випробування*	*20.10.19-05.11.19*	
4	*Збір даних за час випробувань*	*06.11.19-15.11.19*	
5	*Аналіз отриманих результатів*	*16.11.19-01.12.19*	
6	*Оформлення пояснювальної записки*	*02.12.19-12.12.19*	

Дата видачі завдання __09___ ____вересня___2019 р.

Студент _____
(підпис)

Керівник роботи (проекту) _____ __к.т.н., проф. Сєвєрінов О.В.____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до роботи містить: 67 сторінок, 13 джерел, 20 рисунків, 4 таблиці.

4G, 5G, безпека інформації в бездротових мережах, SS7, LTE, WIMAX, IMSI, GUTI, RRC.

В роботі розглянуто основні етапи розвитку безпровідних технологій передачі даних, статистику випадків атак на такі мережі, наведені дані про успішні атаки в процентах.

Також в роботі розглянуто, структура LTE-Advanced, її основні компоненти та рівень безпеки в мережі, приведені дані про проведені випробування та приклад пасивної атаки.

В кінці приведена методика в стислому виді про пошук та виявлення вразливостей в безпровідних мережах передачі даних LTE.

ABSTRACT

Explanatory note to the work contains: 67 pages, 13 sources, 20 figures, 4 tables.

4G, 5G, wireless security, SS7, LTE, WIMAX, IMSI, GUTI, RRC.

The main stages of development of wireless data transmission technologies, statistics of cases of attacks on such networks, the data on successful attacks in percentage are considered in the work.

The paper also examines the structure of LTE-Advanced, its main components and the level of security on the network, the data on the tests and the example of a passive attack.

At the end, a brief summary of how to find and detect vulnerabilities in LTE wireless networks is provided.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

4G	–	Четверте покоління рухомого (мобільного) радіозв'язку
5G	–	П’яте покоління рухомого (мобільного) радіозв'язку
IMT	–	International Mobile Telecommunication
LTE	–	Long Term Evolution
AT&T	–	American Telephone and Telegraph
АВН	–	Автоматичний визначник номеру
SMS	–	Short message service
MMS	–	Multimedia Messaging Service
UE	–	User Equipment
PDN	–	Packet Data Network
EPC	–	Evolved Packet Core
EPS	–	Evolved Packet System
QoS	–	Quality of Service
VoIP	–	Voice over IP
P-GW	–	PDN Gateway
GW	–	Gateway
S-GW	–	Serving Gateway
MME	–	вузол управління мобільністю
CN	–	Core Network
NAS	–	Non-Access Stratum (шар без доступу)
TFT	–	Traffic Flow Templates
FDD	–	Frequency Division Duplex
TDD	–	Time Division Duplex
RRC	–	Radio Resource Control
PCC	–	Primary Component Carrier
SCC	–	Secondary Component Carrier
MIMO	–	Multiple Input Multiple Output

TM	–	Transmission Mode
DSL	–	Digital subscriber line
WiMAX	–	Worldwide Interoperability for Microwave Access
SS	–	Subscriber Station
HA	–	Home Agent
NAP	–	Network Access Provider
NSP	–	Network Service Provider
ASN-GW	–	Access Service Network Gateway
SS7	–	Signaling System #7
IoT	–	internet of things
3GGP	–	The 3rd Generation Partnership Project
SAE	–	System Architecture Evolution
IMS	–	Information Management System
HSS	–	Сервер абонентських даних
VLR	–	Visitors Location Register
MSC	–	Mobile Switching Center
HLR	–	Home Location Register
AS	–	Access Stratum
eNodeB	–	Базова станція стандарту LTE
IMSI	–	Міжнародний ідентифікаційний номер абонента мобільного мережі
БС	–	Базова станція
MCC	–	Mobile Country Code
MNC	–	Mobile Network Code
MSIN	–	Mobile Subscriber Identification Number
EMM	–	EPS Mobility Management
S-TMSI	–	SAE Temporary Mobile Subscriber Identity
PLMN	–	Public Land Mobile Network
MMEI	–	MME Identity
M-TMSI	–	MME Temporary Mobile Subscriber Identity

GUTI	–	Globally Unique Temporary UE Identity
IDLE	–	Стан очікування підключення

ВСТУП

На сьогоднішній день найпоширеніша технологія безпровідного зв’язку четвертого покоління «4G», вона є найбільш швидкою на цей час. Але в світі вже починають переходити на наступне покоління «5G», і так як абонентів мобільного або бездротового радіоінтерфейсу становиться тільки більше від покоління до покоління то були проведені перевірки безпеки таких технологій.

Від мобільних радіоінтерфейсів потребують виконання наступних вимоги:

– фіксовані мережі повинні мати сумісність в рамках IMT;

– системи радіодоступу повинні мати можливість взаємодії з технологіями як минулих поколінь так і майбутніх;

– послуги високоякісного мобільного зв’язку;

– по всьому світу повинна бути надана послуга роумінгу;

– для підтримки розширених сервісів і програмних забезпечень підвищити пікові швидкості передачі даних.

Такі вимоги були к четвертому поколінню зв’язку, до п’ятого міжнародний комітет висував і розробляв більш підходящі під нові реалії. Після об’яви конкурсу на розробку та реалізацію таких технологій були сформовані наступні вимоги:

– вивести зв’язок на більш якісний рівень;

– підвищити середню швидкість передачі даних до стану – від 1 Гб/с;

– збільшити середню кількість одночасних підключень на км^2 – до 1 млн;

– зменшити затримку – до 1 мс;

– енергетична ефективність збільшена до високого значення;

– безпека для здоров’я людини.

Ці вимоги потрібні для того щоб був реалізований так званий «Інтернет речей».

З всього цього можна зробити висновок, що сучасні технології, які у самий ближчий час стануть повсякденністю, неможливі без гарантованого широкосмугового доступу, наприклад, дистанційні хірургічні операції та системи онлайн-консультування, що дозволить пацієнтам зв’язуватись з кращими фахівцями, а останні моментально отримувати карти хвороб своїх пацієнтів. Хмарні технології, без яких буде неможливе практично будь-який вид діяльності уже у найближчі роки, вимагають наявність надійних, швидких і володіючих високою пропускною здатністю каналів.

Предметом роботи – процес пошуку вразливостей безпеки інформації в мережах LTE.

Об’єктом роботи це безпека інформації в безпровідних мережах LTE.

Метою роботи є забезпечення безпеки інформації в мережах LTE на основі пошуку вразливостей засобів захисту.

У цій роботі задача провести перевірку безпеки інформації в безпровідних мережах передачі даних, та вироблення методики виявлення вразливостей у подібних технологіях.

1 ТЕХНОЛОГІЇ БЕЗДРОТОВОГО ЗВ’ЯЗКУ

1.1 Бездротові системи до мобільних телефонів

Від 1921 року історія бездротових мереж передачі даних починається в Детройті, на той час інформація передавалась лише в одному напрямку – від центральної станції до поліцейської машини. На стан у 1933 році такі станції могли не тільки посилати сигнали та інформацію, а й приймати повідомлення від патрульних, таке обладнання застосовувалось в місті Нью-Йорк.

До 1940 року використовували амплітудний спосіб передачі даних, на частотах від 2МГц які виділили на початку використання у 20-х роках, частоти 30-40 МГц та 4 канали стали застосовувати завдяки розвитку радіомереж від початку 1934 року.

Амплітудну технологія вирішили замінити тільки з 1940 року частотною модуляцією. Заміна успішно відбулась до 1946 року, перший міський рухомий радіотелефон з’являється у ті ж роки. Він працював на частотах в діапазоні 150 МГц та мав 11-ти канальну систему. Телефон з робочими частотами в діапазоні 450 МГц з’являється вже в 1956 році і має в наявності 12-ти канальний.

В телефонах такого типу використовували сімплексну систему, а комутація була ручною. Автоматичний вид розпочали випускати від 1964 року з робочим діапазоном частот 150 МГц, в 1969 році до доступних частот додали також смугу від 450 МГц відповідно.

В СРСР московський інженер Куприянович Л.І. у 1957 році, представив дослідний зразок рухомого автоматичного дуплексного мобільного телефону ЛК-1 та базової станції до нього. Цей телефон важив від 20 до 30 кілограм. Модель була удосконалена та допрацьована у 1958 році шляхом зменшення ваги до 0,5 кілограма ваги самого апарата та мінімізації розміру до пачки цигарок.

В Болгарії під час виставки «Інтероргтехніка-66» був представлений комплект із мобільних телефонів РАТ-0,5 і АТРТ-0,5 які могли поміщатися в

кишеню та РАТЦ-10 базової станції яка могла забезпечувати зв’язок для 10 абонентів.

Першу в світі повністю автоматизовану систему, під назвою «Алтай», розробили у кінці 50-х років у Вороніжському НІІ Зв’язку. В експлуатацію її ввели в 1963 році. До 1970 років робоча частота була 150 МГц, після тестувань цю систему встановили в 30 містах СРСР і для її роботи виділили діапазон частот 330МГц. Працювала вона наступним чином:

- Одна базова станція обслуговувала одне місто;
- на найвисоку будівлю міста встановлювалась БС;
- в радіусі 50-60 кілометрів був стійкий сигнал, десь навіть до 100 кілометрів.

Система «Алтай» дозволяла здійснювати дзвінки : в межах мережі, на міські телефони, так і міжміські та навіть за рубіж.

З відмінностями і у менших масштабах але по аналогічним сценаріям, бездротовий зв’язок розвивався і в інших державах. В Норвегії наприклад для морського мобільного зв’язку від 1931 року використовувалась міська телефонна мережа, у 1955 році берегових станції нараховувалось вже 27 станцій. Після другої світової війни почав розвиватись наземний мобільний зв’язок у вигляді приватних мереж з ручною комутацією.

Таким чином рухомий телефонний радіозв’язок до 1970 року, з одної сторони вже отримав достатньо широке розповсюдження, а з іншої сторони обмежене число каналів, жорстко визначені смуги частот він явно не встигав за швидко зростаючими потребами як користувачів так і операторів які надавали послуги технології бездротової передачі даних.

Вихід з положення був знайдено у виді системи стільникових мереж зв’язку, що дозволило за рахунок повторного використання частот різко збільшити ємність в системах з комірчастою структурою.

1.2 Стільникові системи

В 1971 почав своє існування мобільний зв’язок який ми знаємо, компанією “Bell System” в технічному докладі був наведений приклад такої технології. Саме від цього документу прийнято рахувати початок стільникових систем.

Федеральна комісія зв’язку США в 1974 році прийняла рішення для побудови та виділення у місті Чикаго тестової стільникової системи, у 1978 році на двох тисячах абонентах було проведено практичне випробовування тестової мережі.

У 1983 році першу комерційну автоматизовану систему ввела в експлуатацію компанія American Telephone and Telegraph (AT&T). В інших державах стільникові системи починають працювати від: 1978 року – в Канаді; 1979 – Японія; 1981 – Данія, Норвегія, Швеція, Фінляндія; 1982 – у Іспанії та Англії. Починаючи з 1997 року цей вид зв’язку обслуговував більше ніж 150 млн абонентів та був розповсюджений більш ніж в 140 державах усіх континентів.

До послуг які надають стільникові систем входять такі вимоги:

- голосовий дзвінок;
- автовідповідач;
- роумінг;
- автоматичний визначник номера (АВН), та антиАВН;
- прийом та передача коротких текстових повідомлень (SMS);
- прийом та передача мультимедійних повідомлень – зображень, мелодій та відео(MMS);
- доступ до інтернету;
- відеодзвінок та відеоконференція;
- визначення місцезнаходження мобільного телефона.

Розвиток поколінь бездротової системи зв’язку можна побачити в таблиці 1.

Таблиця 1.1 – Розвиток бездротових систем зв’язку

Початок розробки	1970	1980	1985	1990	<2000	2000	2015
Покоління	1G	2G	2.5G	3G	3.5G	4G	5G
Швид-кість передач	1,9 кбіт/с	9,6-14,4 кбіт/с	115 кбіт/с (перша фаза) 384 кбіт/с (друга фаза)	до 3,6 Мбіт/с	до 42 Мбіт/с	100 Мбіт-1 Гбіт/с	Від 1 Гб/с – 6,5 Гб/с
Мережа	PSTN	PSTN	PSTN, мережа пакетної передачі	мережа пакетної передачі	мережа пакетної передачі	мережа пакетної передачі	
Стандарти	AMPS, TACS, NMT	TDMA, CDMA, GSM, PDC	PPRS, EDGE(2.75 G), 1xRTT	WCDMA, CMDA 2000, UMTS	HSDPA, HSUPA, HSPA, HSPA+	LTE-Advanced, WiMax Release 2(IEEE 802.16m), WirelessMAN -Advanced	
Реалізація	1984	1991	1999	2002	2006-2007	2008-2010	2018

Сервіси що повинні були надавати різні покоління:

- 1G: аналоговий стандарт, речовий стандарт.;
- 2G: цифровий стандарт підтримка коротких повідомлень(SMS);

– 2.5G: більша ємність пакетів, пакетна передача даних, збільшення швидкостей мережі;

– 3G: ще більша ємність пакетів;

– 3.5G: збільшення швидкостей мереж 3G;

– 4G: більша ємність, IP-орієнтована мережа, підтримка мультимедії;

– 5G: середня кількість підключень – 1 млн на км^2, затримка – до 1 мс, висока енергетична ефективність.

1.3 Технологія – стандарт LTE Advanced

LTE Advanced — була розроблена та стандартизована 3GPP як головне поліпшення стандарту Long Term Evolution (LTE). Міжнародний союз електрозв'язку надав назву та сертифікат специфікації 3GPP 10 версії – «IMT-Advanced», таким чином стільникові мереж четвертого покоління отримали офіційний статус. Технологією 4G признані тільки визначені версії LTE, усі попередники не входять до стандарту. Цю систему розробляли також для того щоб користувачі мали доступ до сервісів які вимагають постійного доступу до Інтернету, та самої технології Інтернет за допомогою протоколів IP.

Міжнародний союз електрозв'язку в секторі стандартизації електрозв'язку в якості кандидата у кінці 2009 року на офіційно представив систему 4G. У Марті 2011 року відбулось офіційне завершення конкурсу та затвердження LTE — Advanced як частину технології бездротової технології передачі даних наступного покоління.

В Женеві у 2012 році розвиток стандарту WiMAX набув офіційного статусу стандарту бездротового зв’язку четвертого покоління і назву WiMAX — 2. Таким чином офіційне признання стандарту бездротового зв'язку четвертого покоління 4G, і його існування, відбулось саме на цій конференції.

Перелік основних елементів та назва інтерфейсів які входять то технології LTE —Advanced зображено на схемі з рисунку 1.1.

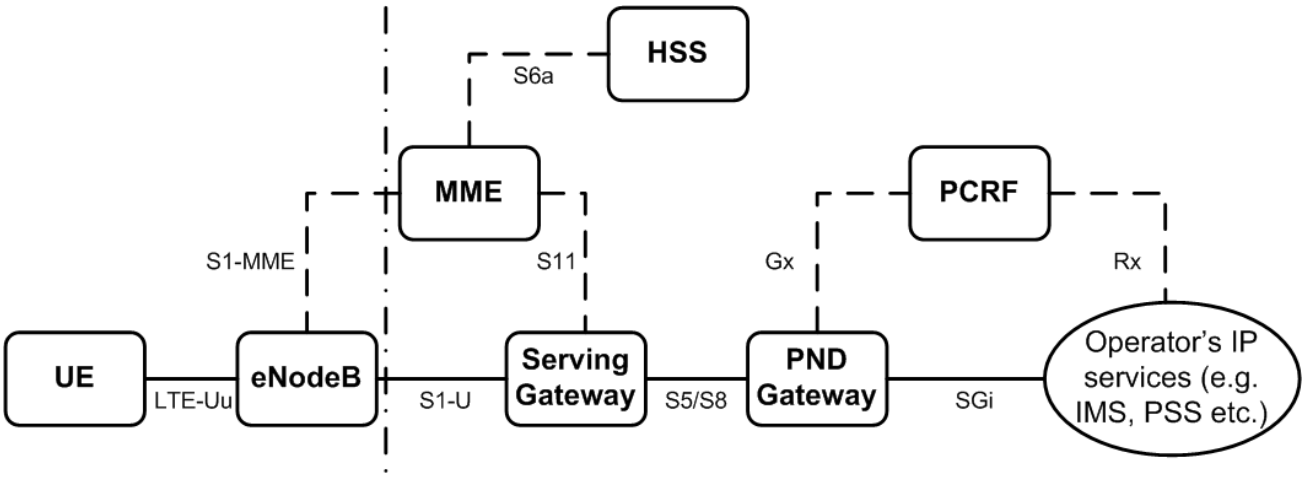

Рисунок 1.1 — Структура LTE Advanced

Саме для можливості встановлення з'єднання комутаційних пакетів між абонентськими станціями (User Equipment, UE) і мережею передачі даних (Packet Data Network, PDN) за допомогою IP протоколів і розроблялась система LTE. Під технологія радіо доступу розуміється термін LTE, під терміном EPC (Evolved Packet Core) розуміється опорна мережа оператора. Для утворення EPS (Evolved Packet System) потрібне використання разом як LTE так і EPC.

Для забезпечення доставки IP пакетів між шлюзом (gateway, GW) і PND до UE використовується концепція EPS потоків (EPS bearers) яка входить до EPS. На ділянці між GW і UE потік IP пакетів – це потік з певними параметрами якості обслуговування (Quality of Service, QoS). Може бути створено декілька EPS потоків, для користувача, щоб надати різні QoS (наприклад, VoIP і FTP потоки) або для надання з'єднання різних.

Нижче наводиться список основних елементів мережі:

- PDN Gateway (P-GW)
- Serving Gateway (S-GW)
- Mobility Management Entity (MME)

MME (Mobility Management Entity)

Контрольним вузлом що пропускає через себе весь сигнальний трафік між UE і Core Network (CN) через себе є MME. За передачу контрольного трафіку UE

і CN, використовується також протокол під назвою NAS (Non-Access Stratum). Виконання функцій MME можна поділити на дві безлічі:

– Управління потоками (Bearer Management). В дану область відносять рівень управління сесіями (session management layer) протоколу NAS, під час його роботи здійснюється створення, підтримка і видалення потоків.

– Управління підключеннями (Connection Management) У рамках цієї функціональності здійснюється підключення абонентів до мережі і створення правил шифрування і кодування між UE і мережею. Ці дії виконуються на рівні підключень або управління мобільністю протоколу NAS.

S-GW (Serving Gateway) — при знаходженні UE в холостому режимі (idle mode) зберігає всю інформацію про його потоки. Також займається тимчасовим накопиченням даних які біли надіслані до UE, у той час коли MME запускав процедуру пейджінга (paging) UE, для створення потоків (на радіо каналів) до UE.

S-GW здійснює крім перерахованих функцій, ще і деякі адміністративні функції у візитній мережі, такі як: збір інформації для здійснення списань по рахунку.

P-GW (PDN Gateway) — робота цього пристрою полягає у дотриманні параметрів QoS, виділенні IP адреси для UE, і здійсненні списань по рахунку на основі набору правил, отриманих з PCRF (Policy Control and Charging Rules Function). P-GW також виконує фільтрацію отриманих IP пакетів в різні клієнтські потоки з конкретним набором параметрів QoS використовучи при цьому TFT (Traffic Flow Templates).[1]

1.3.1. Характеристики LTE Advanced

Основними вимогами для зв’язку між базовою станцією і мобільною станцією є: пропускна здатність до 1Гбіт/с та спектральна ефективність до 30 біт/с/ГЦ на радіоканалі. Для реалізації цих вимог в стандарт LTE Release 10 додали ряд розширень, основні з яких:

– В LTE-Advanced для найпростішої реалізації збільшення пропускної здатності та використання більш широкого каналу використовують метод «об’єднання несучих» (Carrier Aggregation). Також для забезпечення сумісності з попередниками та розширення каналу Release 10 (Release 9 і Release 8) застосовується метод об’єднання кількох несучих, що функціонують по протоколам Release 9/8. Такий тип об’єднань можливий при використанні любого виду дуплексу: FDD (Frequency Division Duplex) і TDD (Time Division Duplex). Несучі можуть об’єднуватися в різних розмірах(20 МГц, 15 МГц, 10 МГц, 5 МГц, 3 МГц, 1,4 МГц), сумарна кількість не повинна перевищувати п’яти. Завдяки цим технічним рішенням сумарна ширина каналу в LTE-Advanced має можливість досягати 100 МГц. Об’єднанні несучі можуть займати як безперервний частотний діапазон(contiguous), так і бути розташовані в різних частотних діапазонах(non-contiguous). Це все залежіть від стільникового оператора зв’язку, які частоти він має в своїй підтримці. Треба також зазначити, що об’єднання несучих в низхідному каналі і висхідному може бути різним, але в той самий час кількість об’єднання несучих в висхідному каналі не може перевищувати кількості в низхідному каналі. Release 10 – завдяки визначеним та стандартизованим комбінаціям несучих має можливість об'єднання до п'яти пар несучих. Визначили комбінації пар для і для висхідного каналу, а від початку роботи Release 12 були визначили для низхідних каналів трійки несучих. В даній технології сектором (cell) є кожна несуча, область покриття якої значно відрізняється від різниці використаних частот для несучих (особливо помітна різниця в разі використання non-contiguous). Мобільна станція, при використанні об’єднаних несучих, виконуючи підключення тільки до одного сектору по протоколу RRC, має назву Primary Cell (або PCC - Primary Component Carrier). Всі інші сектора по відношенню до цієї мобільної станції називаються Secondary Cell (або SCC - Secondary Component Carrier).

– Інший спосіб для збільшення пропускної здатності буде через збільшення спектральної ефективності. Для цього використовують декілька як прийомних антен, так і передавальних (MIMO, Multiple Input Multiple Output).

MIMO можна використовувати в декілька способів, але не всі з них можуть збільшити пропускну здатність. В цій роботі буде використано просторове мультиплексування (Spatial Multiplexing) – саме цей варіант MIMO дозволяє досягати більш високої пропускної здатності. В LTE-Advanced додали підтримку для низхідних каналів (від базової станції до мобільних станцій) з назвою MIMO 8x8, і в висхідну частину (від мобільної станції до базової станції) з назвою MIMO 4x4. Для цього ввели нові режими передач (TM, Transmission Mode) і додали нові категорії мобільних станцій. Нові режими передачі відрізняються від визначених раніше (Release 8/9) в таких аспектах:

- число потоків даних (Layers), тобто скільки різних потоків даних може передаватися одночасно;
- використання різних портів (antenna ports);
- використання різних пілотних сигналів (CRS, DM-RS);
- різна попереднє кодування (precoding).

Також в LTE-Advanced додається підтримка вузлів ретрансляції (Relay). Використання таких вузлів дозволяє закрити "дірки" в покритті і поліпшити радіо умови для користувачів, що знаходяться на кордонах стільники. Вузли ретрансляції з'єднуються з базовою станцією, яка в цьому випадку називається Donor eNB (DeNB), за допомогою телефону, який називається Un-інтерфейс. При цьому, може використовуватися той же частотний діапазон, що і для обслуговування мобільних станцій (в цьому випадку станції ретрансляції називаються як Type 1 RN), або різні частотні діапазони (Type 1a RN).

1.4. Технологія – стандарт WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) IEEE 802.16 — це стандарт який забезпечує широкосмуговий зв'язок безпровідним мережам на значні відстані зі швидкістю кабельних з'єднань. [2]

Саму назву технологія «WiMAX» отримала на однойменному форумі WiMAX Forum. Форум був створений не комерційною організацією з назвою

“WiMAX Forum”. Сама компанія починає працю від 2001 року, з метою розвитку і просування стандарту «WiMAX». Вони описують дану технологію як: “технологію засновану на стандарті, для надання бездротового високошвидкісного доступу до мереж, шляхом виділення DSL і альтернативним лініям.

Вона вирішує наступні завдання:

– виділення альтернативних ліній та DSL для забезпечення широкосмугового бездротового доступу до мереж;

– надання телекомунікаційних послуг та стабільної швидкісної (до 3 Мбіт/с) передачі даних;

– з’єднання різних сегментів Інтернету через Wi-Fi;

– дозволяє створювати не прив’язані до географічних положень точок доступу.

Технологія WiMAX дозволяє замінювати Wi-Fi точки доступу, та надавати не тільки доступ до Інтернету, а й покривати більшу площу. Завдяки цим властивостям стандарт може використовуватися як «магістральний канал», DSL лінії та локальних мереж якого виступають його продовженням. Такий набір можливостей дозволяє швидко створювати масштабовані мережі в містах.

1.4.1. Фіксований і мобільний варіант WiMAX

В процесі створення бездротової мережі, під основою технології, WiMAX розробники намагались поєднати різні ринкові ніші, та знайти оптимальне вирішення для декількох станів: рухомого і фіксованого, на жаль поєднати всі вимоги та потреби в рамках одного рішення не вийшло. І не зважаючи на те що деякі з вимог збігаються технологія WiMAX має в своїй реалізації дві окремі версії. Їх прийнято вважати різними стандартами. Із-за націленості на різні сфери обслуговування специфікації WiMAX по різному визначають робочий діапазон частот, смуги пропускання мають відмінності, випромінювання має різну потужність, способи кодування відмінні, при використанні повторних радіочастот використовуються різні показники та принципи, модуляція, методи

передачі даних та доступу також відмінні. Тому при однаковій назві стандарту, перевагах що надаються та схожості в робочих версіях (802.16d і 802.16e), ці системи практично не сумісні між собою.

Основна різниця полягає у тому, що фіксований WiMAX не має змоги обробляти та обслуговувати мобільних абонентів зі швидкістю переміщення до 150 км/год. Мобільність включає в себе функцію «безкоштовного» перемикання між БС або роумінгу, при пересуванні пристрою в мережі стільникової системи. Окремі випадки дозволяють використовувати WiMAX версію мобільного обслуговування для фіксованих користувачів.[2]

1.4.2. Широкосмуговий доступ в WiMAX

Технології 802.16 дозволяють надавати послуги у важкодоступні території, поширювати свою мережу на нових абонентів при менших затратах на обслуговування обладнання (у порівнянні з провідниковими) та більш високі швидкості передачі даних. Тому багато телекомунікаційних компаній роблять вибір у сторону використання WiMAX. Також у сторону вибору можна назвати більшу простоту використання бездротових мереж перед кабельними. Великою перевагою WiMAXa в порівнянні із всіма іншими технологіями називають його легку масштабованість як простоту розгортання так і мінімізацію часу встановлення, ці опції дуже важлива при надзвичайних подіях. Так наприклад, в Індонезії (Aceh) після цунамі 2004 року, таку систему встановлювали для тих хто вижив. Її встановили як оперативну заміну всій комунікаційній системі що вийшла з ладу щоб відновити зв’язок з іншими регіонами та рятівниками.

В сумі, для телефонних операторів, такі переваги дозволяють надавати свої послуги високошвидкісного доступу до Інтернету як приватним особам, так і бізнес-структурам по зниженим цінам.

1.4.3 Обладнання користувача

WiMAX обладнання може бути різного розміру та випускається різними виробниками, його розміри дозволяють встановлювати обладнання в

приміщені(його розміри не перевищують розміри DSL-модемів) або поза ними(пристрої розміром із ноутбук). Ще одна перевага даної технології в тому що при установці такого устаткування в приміщені – не потребує навичок. Також треба зазначити що обладнання встановлене в приміщені працює на значно менших відстанях у порівнянні з професійно встановленими зовнішніми пристроями. Виходячи з цього – такі пристрої будучи встановленими в приміщеннях, потребують більшої кількості грошей що будуть вкладені в розвиток внутрішньої мережі, так як буде передбачено набагато більша кількість точок доступу.

Після реалізації мобільної версії WiMAX розробники роблять все більший акцент у розвиток мобільних пристроїв. У список таких винаходів входять: звичайні телефонні трубки (схожі на звичайний сматрфон), і комп'ютерна периферія (PC card та USB радіомодулі).[3]

1.4.4. WiMAX принцип роботи

Основні частини в мережі WiMAX включають в себе : БС, абонентську станцію, обладнання що дозволяє зв'язати станції між собою та надавати послуги від операторів для роботи сервісів і доступу до Інтернету.

Базова станція для з'єднання з обладнанням абонента використовує діапазон високих частот від 1,5 да 11 ГГц. Передача або обмін даних при ідеальних умовах може досягати 70 Мбіт/с, забезпечення прямої видимості від приймача до базової станції при цьому не обов'язкова.

Для вирішення проблеми «останньої милі» і надання офісам та мережам доступу в мережу WiMAX використовують наступним чином. Встановлюють з'єднання (в прямій видимості), при цьому діапазон частот який використовується знаходиться від 10 до 66 ГГц, завдяки чому досягається швидкість передачі даними може бути 120 Мбіт/с. Одна з базових станцій повинна бути підключена до мережі провайдера через класичну дротову систему, але чим більше базових станцій буде підключено таким чином – тим швидше та більш надійно в цілому буде відбуватися обмін даними.

За структурою сімейства мереж стандарту IEEE 802.16, схожа з GSM мережами. Принцип їх дії також схожий на такий тип мереж – базові станції можуть посилати сигнал, до пристроїв, на відстань до десяти кілометрів. Вежі базових станцій не обов'язково будувати – їх установка можлива і на дахах будинків, але при дотриманні вимоги прямої видимості такої ж вежі.[3]

1.4.5. Режим роботи

В мережах Wi-Fi типу щоб передати інформацію через точку доступу (Access Point), на канальному рівні (MAC), всі станції абонентів повинні «змагатися за увагу» таких точок. Такий вид передачі даних може викликати ситуацію у якій віддалені станції не мають змоги передати інформацію, у той час як більш близькі абоненти передають її з перевагою. На жаль такий недолік системи робить застосування таких сервісів як – Voice over IP (VoIP) невигідним, так як він схильний переривати обмін від недостатнього з'єднання.

Що до мереж у яких засовується стандарт WiMAX, він використовує на канальному рівні алгоритми планування. У кожного підключеного до базової станції обладнання користувача є виділений під нього слот, недоступний іншим абонентам.

WiMAX Forum розробив архітектуру для WiMAX, яка змогла визначити такі аспекти роботи :

- автентифікація;
- взаємодія з мережами іншого типу;
- розподіл мережевих адрес;
- інше.

У наведеному нижче рисунку 1.2 зображена архітектура WiMAX стандартів.[3]

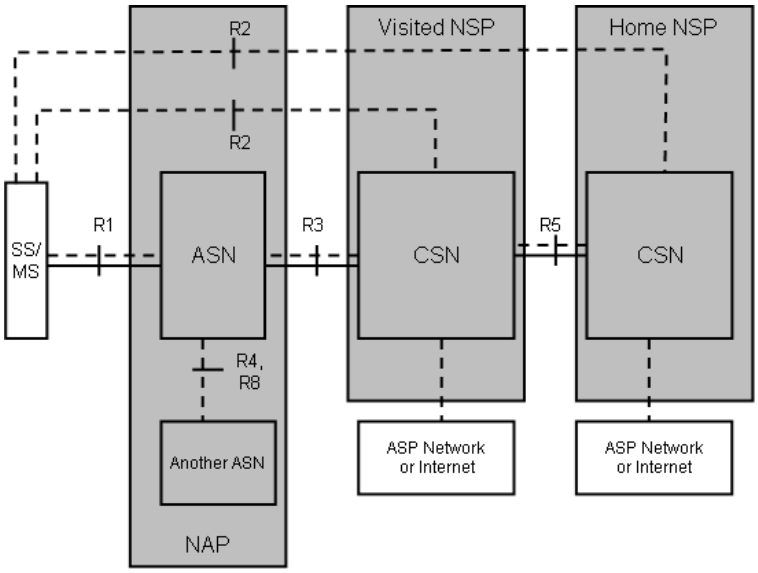

Рисунок 1.2 — Архітектура WiMAX

– станція передплатника (Subscriber Station (SS))/мобільна станція (Mobile Station(MS));

– мережа доступу (the Access Service Network(ASN));

– базова станція (Base station(BS));

– шлюз (the ASN Gateway(ASN-GW)) ;

– мережа забезпечення послуг (the Connectivity Service Network(CSN));

– Home Agent (HA) (частина CSN);

– NAP (a Network Access Provider);

– NSP (a Network Service Provider).

Крім основних функцій встановлення та підтримки з’єднань та роз’єднань, базова станція виконує обробку сигналізації, а також розподіляє свої ресурси для користувачів. Частина функцій входить до шлюзу (ASN).

Шлюз (ASN) об’єднує трафік та повідомлення, сигналізаційні повідомлення від базових станцій та пересилає отримані пакети з даними в мережу CSN.

Home Agent (HA) – відповідальний за можливість роумінгу в мережах. Також забезпечує правильний обмін даними між операторами зв’язку.

Також не можна забувати що архітектура WiMAX дуже гнучка, має можливість масштабування, і не прив’язана к якоїсь одної конфігурації.

Роботу над наступною версією IEEE 802.16n (WiMAX – 3) почалась майже відразу після утвердження IEEE 802.16m. Над цим проектом почала своє дослідження група з назвою PAR (Project Authorization). Новий стандарт здатний буде забезпечувати новий рівень швидкостей обміну даних в мережах, починаючи від 10 Гбіт/с для фіксованого варіанту технології і до 1 Гбіт/с для мобільних абонентів. WiMAX Forum має надію що WiMAX, третьої версії, буде прийнятий в найближчі роки.

Міжнародний орган IEEE утвердив розширення IMT до стандарту IEEE 802.16m. Розширення до стандарту IEEE 802.16m надає доступ до швидкісного інтернету (до 100 Мбіт/с). Додатком до швидкостей йде поліпшення до системи черги пакетів MIMO (багатоканальний вхід - багатоканальний вихід), оновлені магістральні канали дозволяють обслуговувати інтереси декількох операторів, з’являється можливість вносити внесок кожного абоненту в обслуговування розташованих поблизу «кооперативних комунікацій». Новий стандарт пропонує підтримку фемтостільників, само організованих мереж та ретрансляторів. WiMAX 2 впровадили до систем обслуговування найбільші індустріальні організації та держави.

За останніми відкритими даними компанії ABI Research, зараз більше 3 млрд. жителів Землі працюють та живуть в зоні покриття бездротових високошвидкісних мереж зв’язку. Це дає інформацію про те що технології широкосмугових бездротових мереж які можуть надавати доступ до Інтернету будуть розвиватися великими темпами і надалі. У таблиці 1.1 приведена порівняльна інформація про розвиток технології WiMAX ті стандартів що входять до неї.

Таблиця 1.2 – Порівняльна таблиця стандартів WiMAX

Технологія	Стандарт	Варіант дії	Максимальна швидкість	Радіус покриття	Діапазон частот
WiMAX	802.16d	WMAN	До 75 Мбіт/с	25-80 км	1,5-11 ГГц
WiMAX	802.16e	Mobile WMAN	До 40 Мбіт/с	1-5 км	2.3-13.6 ГГЦ
WiMAX – 2	802.16m	WMAN,	До 1 Гбіт/с,	1-5 км	20 ГГц
		Mobile WMAN	до 100 Мбіт/с		
WiMAX – 3	802.16n	WMAN,	До 10 Гбіт/с,	В розробці	В розробці
		Mobile WMAN	до 1 Гбіт/с		

Приведена інформація дала зрозуміти, що технології бездротової технології будуть поширюватися і розвиватись далі на все більш зростаючу аудиторію користувачів так як вже на теперішній час надає високі швидкості передачі даних та стабільні інтернет послуги. Але незважаючи на розвиток, в таких мережах є вразливості. І наявність вбудованих методів захисту потребує детального розгляду та перевірок. Виходячи з цього необхідно провести аналіз даної технології на предмет забезпечення безпеки інформації абонентів так і неперервності зв’язку.

У наступних розділах буде розглянуто структуру таких систем, її основні недоліки і типи загроз як користувачам таких мереж, так і компаніям що надають послуги стільникового зв’язку.

2 АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ІНФОРМАЦІЇ ДЛЯ ТЕХНОЛОГІЇ 4G

2.1. Дослідження погроз безпеки і атак у мережі SS7

Широке поширення мобільних мереж зв'язку четвертого покоління спростило доступ до швидкісного інтернету для мільярдів користувачів. Однак не тільки смартфони, планшети і комп'ютери масово підключаються до 4G. Висока швидкість передачі даних і мінімальні затримки в LTE-мережах дозволяють використовувати їх для побудови інфраструктури інтернету речей. За прогнозами аналітиків, до 2022 року число IoT-пристроїв, підключених до стільникових мереж, збільшиться з 400 млн до 1,5 млрд. За даними на 2015 рік користувачів стільникових систем в тому чи іншому вигляді нараховувалось 1.37 млрд.[19] Таким чином, захищеність систем «розумного міста», самоврядних «підключених автомобілів» і інших IoT-технологій буде тісно пов'язана з питаннями безпеки сучасних (4G) і перспективних (5G і LTE-M) мереж мобільного зв'язку.

У даній роботі була проведена робота по аналізу захищеності сигнальних мереж 4G. У всіх досліджених мережах телефонних-операторів були виявлені уразливості, обумовлені фундаментальними недоліками ядра пакетної мережі Evolved Packed Core. Виявлені проблеми дозволяють відключати одного або групу абонентів, перехоплювати інтернет-трафік і SMS-повідомлення, виводити з ладу обладнання оператора і здійснювати інші нелегітимні дії. Процес експлуатації вразливостей в мережах 4G не вимагає від зловмисника важкодоступних інструментів або високого рівня кваліфікації.

Незважаючи на появу мереж нового покоління 4G, що використовують іншу систему сигналізації – Diameter, проблеми безпеки SS7 будуть залишатися актуальними ще довгий час, так як оператори зв'язку все ще повинні забезпечувати підтримку стандартів 2G/3G і взаємодія між мережами різних

поколінь. Більш того, дослідження доводять, що протокол Diameter схильний тим же загрозам, що і SS7.

Для мереж четвертого покоління 3GGP розробив нову архітектуру ядра мережі – System Architecture Evolution (SAE). Базовим елементом нової архітектури являється ядро пакетної мережі Evolved Packet Core (EPC). У порівнянні з мережами попередніх поколінь структура ядра EPC стала простіше (рисунок. 2.1), що збільшило пропускну здібність і знизило затримки сигналу при передачі призначених для користувача даних та службової інформації. Зокрема, зник важливий компонент - мережа з комутацією каналів. Мережі 4G побудовані за принципом All IP Network, що дозволяє передавати в пакетної середовищі не тільки дані, але й голосові виклики. Однак до сих пір не всі оператори реалізували необхідні технології (наприклад, IMS для VoIP) для передачі голосу засобами 4G. В таких випадках при здійсненні виклику апарат абонента примусово перемикається у 2G/3G і може зіткнутися з уразливими, про які буде іти мова пізніше.

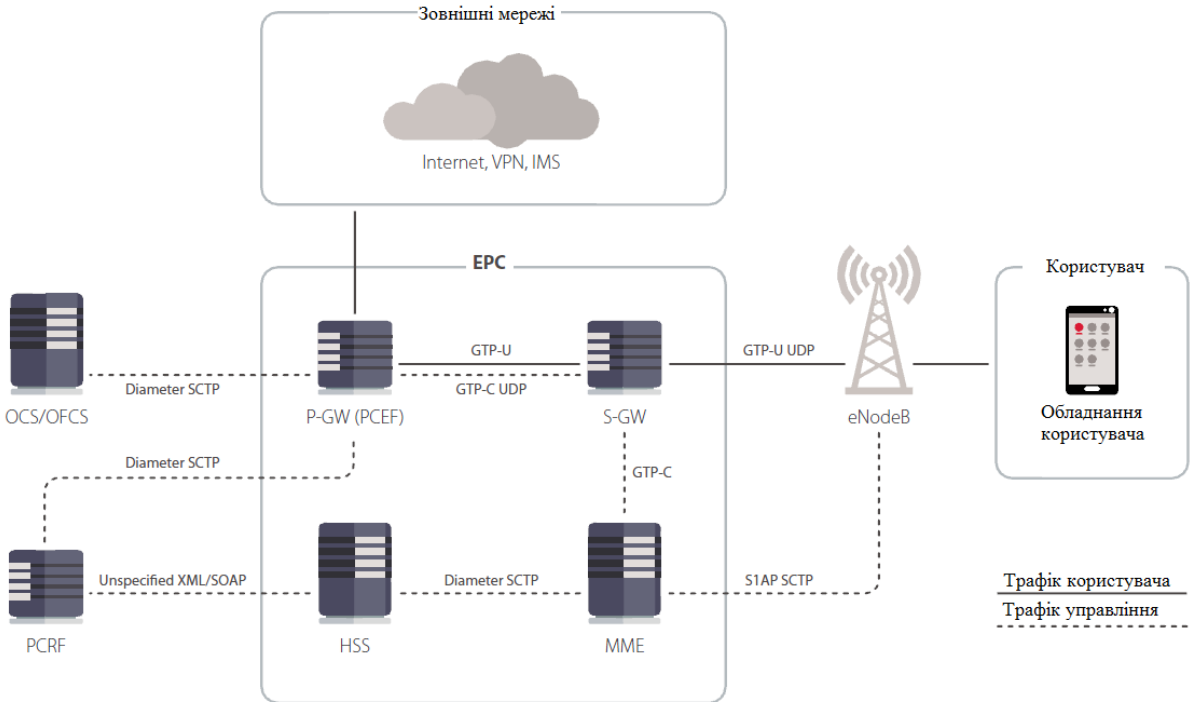

Рисунок 2.1 — Структура ядра пакетної мережі EPC

Основними компонентами ядра пакетної мережі є такі елементи:

– сервер абонентських даних (HSS) являє собою велику базу даних і призначений для зберігання інформації про абонентів. Фактично HSS замінює собою бази VLR, HLR, AUC и EIR, які використовувалися в мережах 2G / 3G;

– обслуговуючий шлюз (S-GW) забезпечує передачу і обробку даних користувача між призначеними для користувача пристроями (UE) і підсистемою базових станцій мережі LTE (eNodeB) оператора;

– пакетний шлюз (P-GW) керує потоками даних, які передаються в зовнішні пакетні мережі, по суті являючись в мережі оператора точкою входу і виходу для користувача трафіку. При поєднанні з PCEF - елементом мережі, що відповідає за застосування правил тарифікації - забезпечує коректну роботу розрахункових систем і застосування тарифних правил;

– вузол управління мобільністю (MME) забезпечує можливість перемикання між базовими станціями і роботу у роумінгу. Крім того, MME відповідає за аутентифікацію користувача пристроїв (UE), взаємодіючі з HSS, а також за вибір шлюзу S-GW.

Кожен вузол EPC може забезпечувати не тільки функції перевірки і фільтрації мережевих пакетів по їх вмісту (DPI), але і різні функції законного перехоплення, які використовуються правоохоронними органами.

Щороку експерти проводять десятки робіт з аналізу захищеності сигнальних мереж SS7. В ході перевірок моделюються дії потенційного порушника, який, як передбачається, здійснює атаки з міжнародної або національної мережі, зовнішньої по відношенню до оператора. Зловмисник має можливість відправляти в тестову мережу запитання протоколів програм, які можуть привести до реалізації різних загроз як щодо самого оператора, так і його абонентів, якщо оператор не вживає достатніх заходів захисту. Для емуляції шкідливого вузла використовується спеціальне обладнання (Рисунок 2.2).

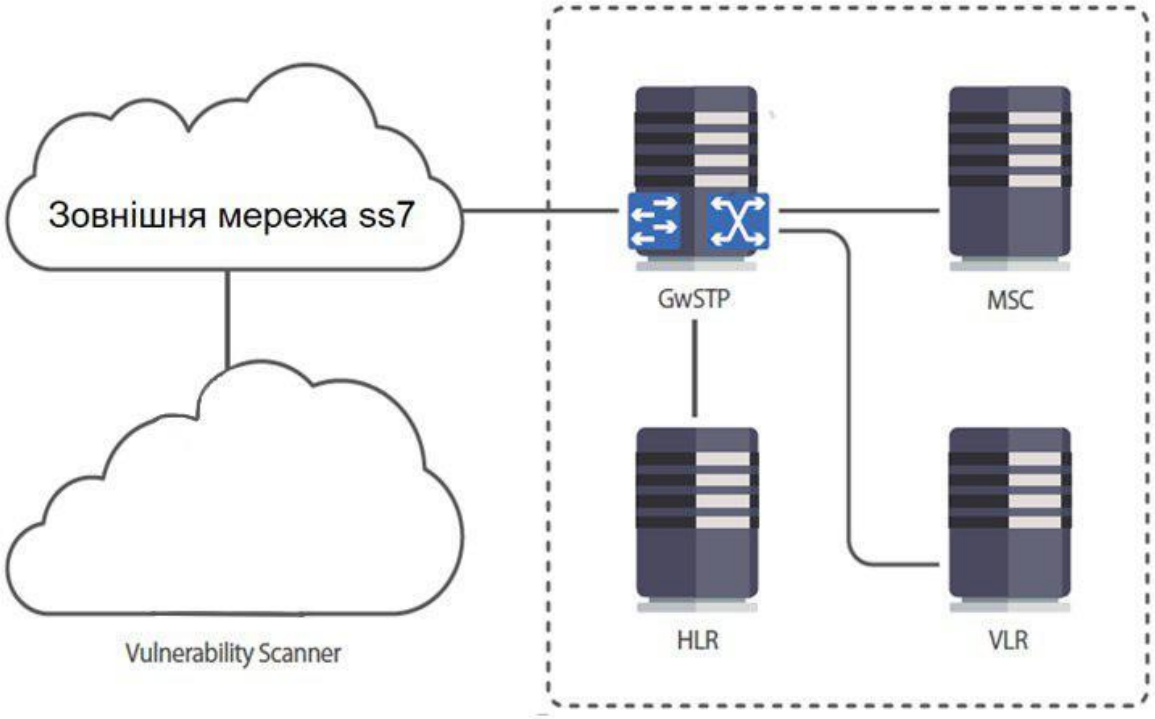

Рисунок 2.2 — Схема робіт з аналізу захищеності мереж SS7

Для дослідження було вибрано 24 найбільш інформативних проектів по аналізу захищеності мереж SS7 у 2016-2018 роках, у ході яких проводився максимально повний перелік перевірок.

Були виявлені наступні загрози, які може реалізувати зловмисник, експлуатуючи недоліки захищеності мереж операторів мобільного зв'язку:

- розкриття інформації про абонента
- розкриття інформації про оператора
- перехоплення трафіка абонента
- шахрайство
- відмова в обслуговуванні

Кожна з перерахованих загроз несе як репутаційні, так і фінансові ризики для оператора. Безпосередню небезпеку для абонента представляють загрози шахрайства, перехоплення трафіку, відмови у обслуговуванні і розкриття

розташування, які можуть привести до значних грошових втрат, порушення приватності і доступності абонентів мережі.

Під розкриттям інформації про абонента розуміється витік ідентифікаторів IMSI, розкриття місця розташування абонента, а також іншої інформації, таку як стан балансу або деталей профілю. Розкриття інформації про мережу оператора загрожує витоком даних про конфігурацію мережі SS7.

На даний момент відомі такі техніки перехоплення абонентського трафіку у мережах SS7, які дозволяють прослуховувати або перенаправляти на сторонні номера вхідні та вихідні голосові виклики, а також перехоплювати SMS користувачів.

Атаки з метою шахрайства можуть здійснюватися як щодо оператора, так і по відношенню до абонентів. Наприклад, зміна платіжної категорії для дзвінків у роумінгу або обхід системи тарифікації можуть принести шкоду оператору зв'язку, а переказ коштів з рахунку, перенаправлення викликів на платні номери або підписка на платні сервіси - користувачам мережі.

Рівень обізнаності операторів про проблеми захищеності мереж SS7 поступово зростає, у зв'язку з чим оператори починають впроваджувати засоби захисту від атак. Якщо в 2016 році кожна досліджена мережа була схильна до всіх видів загроз, то за останні два роки позначилися позитивні зміни у загальному рівні захищеності мереж. В таблиці 2.1 можна побачити такі зміни.

Таблиця 2.1 Долі вразливих мереж за типами загроз

Тип загрози	2016	2017	2018
Розкриття інформації про абонента	100%	100%	100%
Розкриття інформації про мережу оператора	92%	63%	60%
Перехоплення трафіка абонента	100%	89%	80%

Шахрайство	85%	78%	71%
Відмова в обслуговуванні	100%	100%	100%

Помітно знизилися ризики витоку інформації про мережу оператора, шахрайства і перехоплення абонентського трафіку. Проте кожна досліджена мережа, як і раніше, схильна до вразливостей, які дозволяють отримати інформацію про абонентів або викликати відмову у обслуговуванні.

Розглянемо частки успішних спроб атак, які експерти змогли реалізувати у рамках робіт з аналізу захищеності (Рисунок 2.3).

Рисунок 2.3 — Долі успішних атак за типами загроз

Як видно, в першу чергу оператори вживають заходів, спрямованих на зниження ризику розкриття інформації про мережу та абонентах, оскільки ці відомості служать вихідними даними для реалізації безлічі інших атак. У порівнянні з 2016 роком частка успішних атак, спрямованих на розкриття інформації про мережу оператора, знизилася майже втричі, і в два рази рідше удавалось отримати дані про абонентів мережі. Способи захисту від такого роду атак досить прості, а на ринку інформаційної безпеки існують готові рішення,

але при цьому уразливі для розкриття інформації про абонентів і раніше 100% мереж, що говорить про недостатню ефективність існуючих рішень.

Для інших видів загроз відсоток успішно здійснених атак змінився не так значно. Причина полягає у тому, що впровадження систем фільтрації і блокування трафіку не може компенсувати архітектурні проблеми SS7, для мінімізації цих ризиків необхідний інший підхід.

Можна виділити наступні причини, за якими можлива реалізація тих чи інших загроз:

– відсутність перевірки реального місце розташування абонента
– неможливість перевірки приналежності абонента мережі
– недоліки конфігурації SMS Home Routing
– відсутність фільтрації повідомлень

Як показують результати, порушник може проводити більшість атак, експлуатуючи уразливості, які пов'язані з відсутністю перевірки реального місця розташування абонента та його приналежності мережі оператора (Рисунок 2.4).

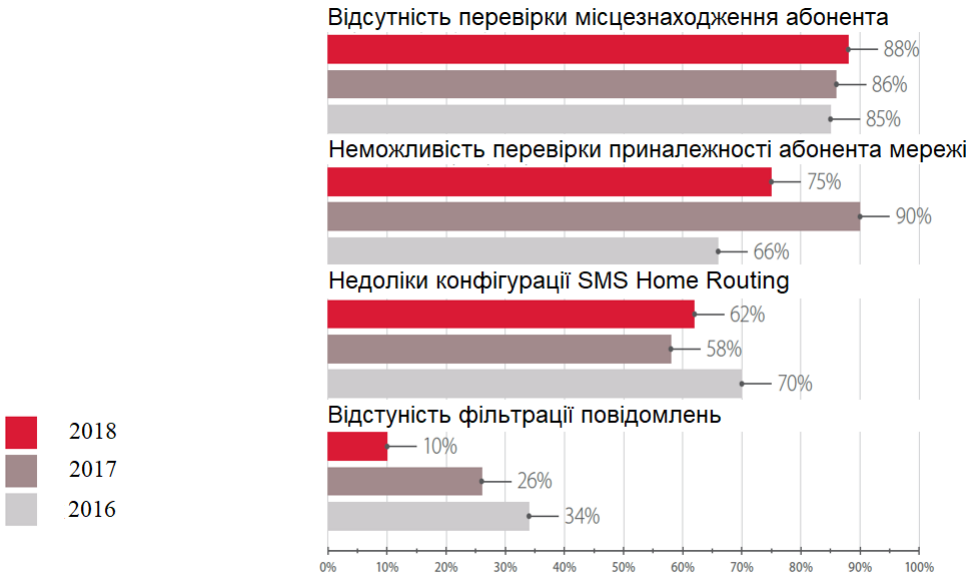

Рисунок 2.4 — Вразливості (долі успішних атак)

Зокрема, можливі атаки, спрямовані на розкриття місця розташування абонента, перенаправлення або перехоплення виклику, перехоплення SMS, зміна платіжної категорії або профілю абонента. Відсутність перевірки

місцерозташування відноситься до сигнальних повідомлень, що приходять в домашню мережу абонента з мережі, в зоні дії якої перебуває абонент в роумінгу. Якщо сигнальне повідомлення складено коректно, немає можливості перевірити його справжність тільки за отриманими параметрами. Потрібна додаткова перевірка, чи дійсно абонент знаходиться в тій мережі, звідки прийшов сигнальний трафік (Рисунок 2.5).

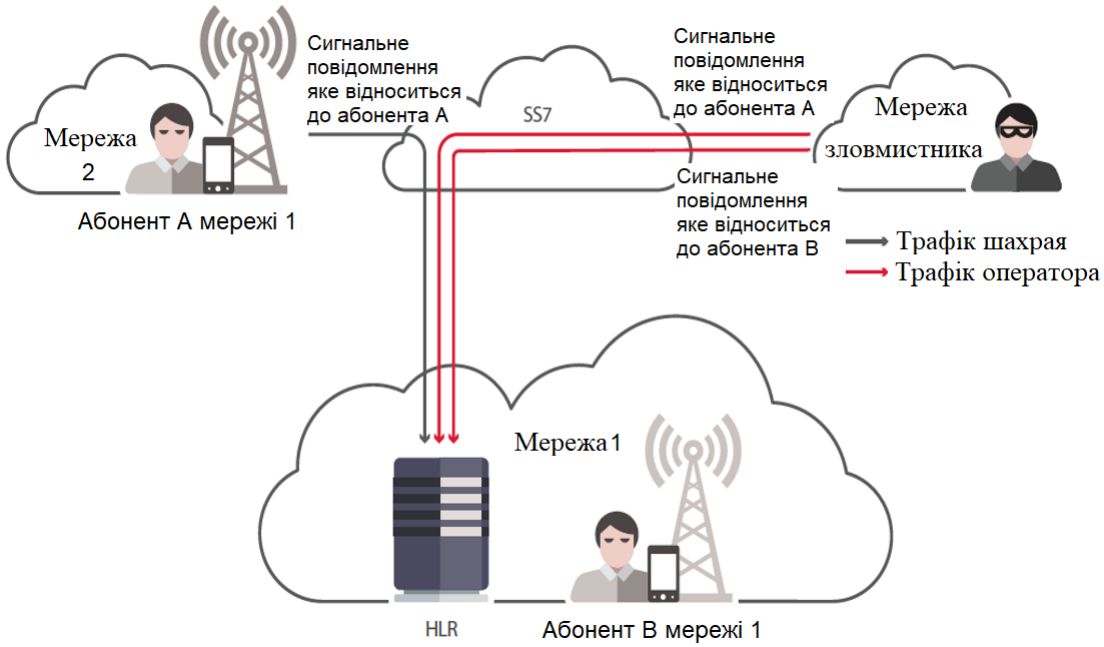

Рисунок 2.5 — Відсутність перевірки реального місцерозташування абонента

Складність перевірки приналежності абонента мережі пов'язана з сигнальними повідомленнями, що направляються оператором зв'язку на адресу своїх абонентів, які перебувають у роумінгу, з іншою мережею, в якій ці абоненти на даний момент зареєстровані. Для визначення нелегітимного трафіку потрібно перевіряти відповідність джерела повідомлення і ідентифікатора абонента. Якщо адреса джерела та ідентифікатор абонента відповідають одному оператору, то повідомлення легітимне. Але якщо відповідності не знайдено, це ще не означає фальсифікацію повідомлення, так як адреса джерела може бути змінена, наприклад, транзитним оператором. З повною упевненістю можна говорити про нелегітимність даного виду сигнального трафіку, якщо він

надходить з зовнішніх мереж і спрямований на адресу абонентів домашньої мережі(Рисунок 2.5).

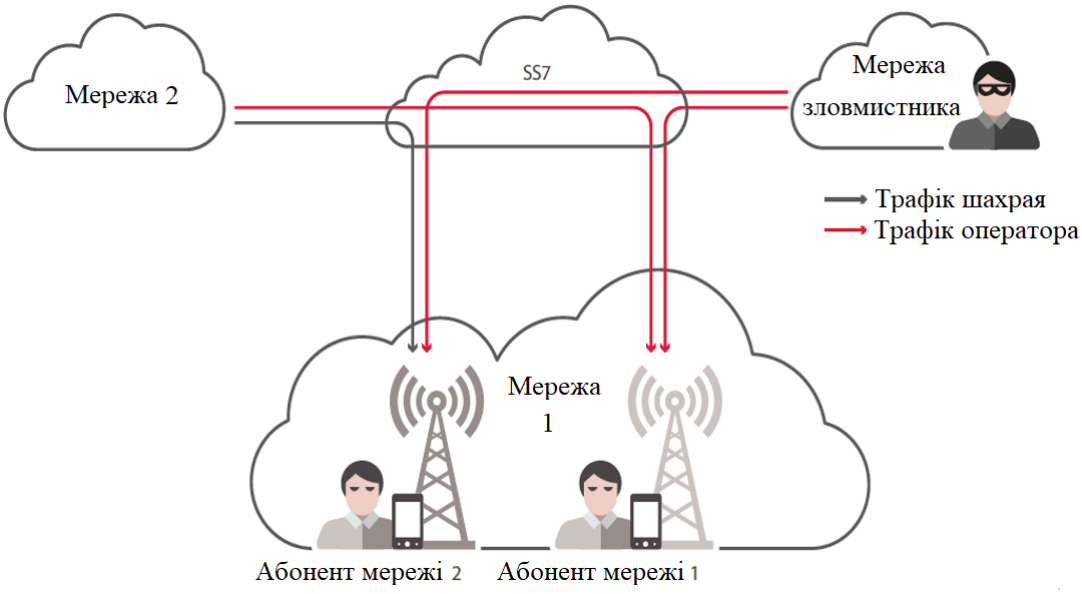

Рисунок 2.6 — Відсутність перевірки приналежності абонента мережі

SMS Home Routing - апаратно-програмний комплекс, призначений для приховування реальних ідентифікаторів абонентів і адрес мережевого обладнання - використовується у 85% досліджених мереж, однак некоректна настройка дозволяє здійснювати атаки у обхід механізму захисту. У мережах, де система SMS Home Routing була відсутня, були успішні абсолютно все спроби отримати ідентифікатори абонентів і інформацію про мережі.

Для проведення атак використовуються стандартні повідомлення, призначені для виконання службових операцій. Ці повідомлення повинні проходити перевірку на кордоні або всередині мережі оператора, щоб припинити нелегітимні запити. Одна і та ж атака може бути здійснена декількома методами, при цьому успішність різних методів неоднакова.

Оператори активно впроваджують системи фільтрації і блокування сигнального трафіку: у 2017 році вони функціонували вже у третини досліджених мереж. Як результат, атаки, що експлуатують уразливості, пов'язані

з відсутністю фільтрації повідомлень, на сьогоднішній день успішні лише у 10% випадків, що у три рази краще за показники попередніх років.

2.2 Витік інформації про абонента

Першим заходом щодо зниження вірогідності проведення більшості атак є зниження ризику розкриття IMSI -унікальних ідентифікаторів абонентів. У порівнянні з 2015 роком дізнатися IMSI за телефонним номером абонента у минулому році вдавалося приблизно у 4 рази рідше.

З рисунку 2.7 видно, що на сьогоднішній день визначити місце розташування абонента можливо у 75% мереж, при чому кількість успішних атак з використанням різних методів становить 33%, що є значно кращим показником порівняно з даними попередніх років.

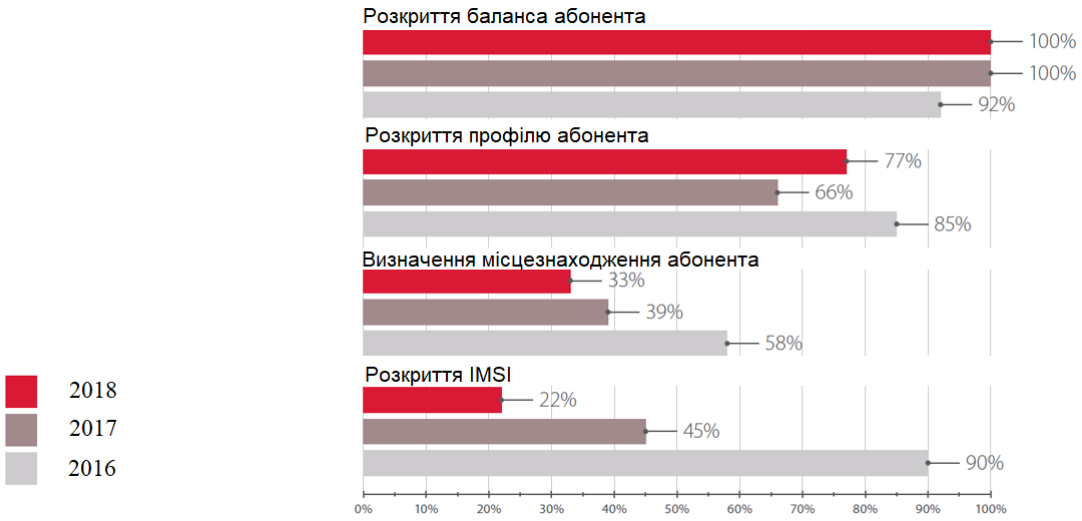

Рисунок 2.7 — Долі успішних атак по типам загроз, зв’язаних з отриманням інформації про абонента

Розкриття інформації про абонента може бути реалізовано чотирма методами, успішність яких показана на рисунку 2.8.

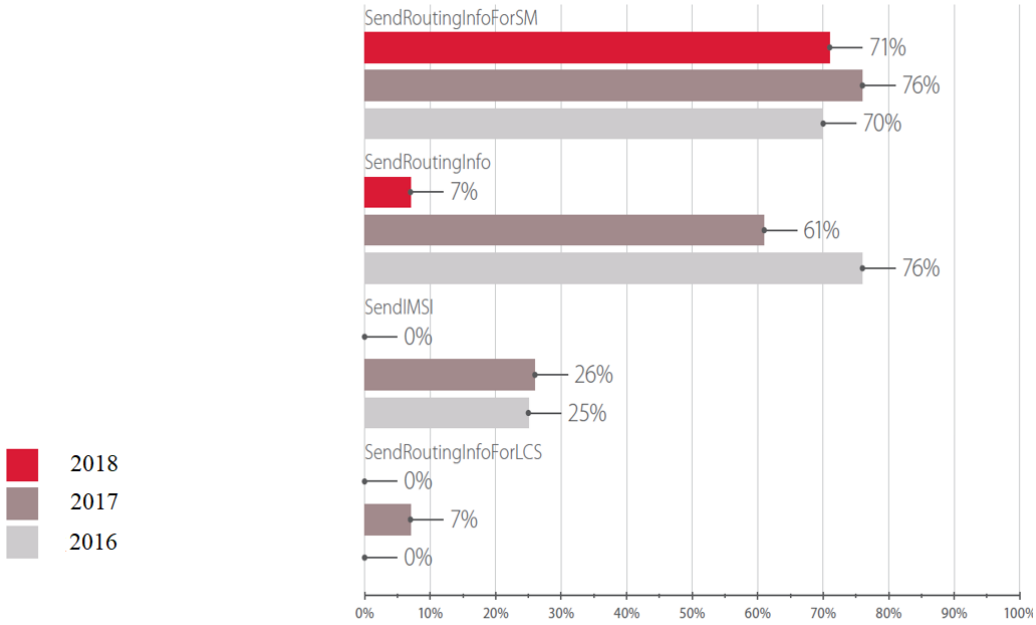

Рисунок 2.8 — Методи які використовуються для отримання IMSI абонента (долі успішних атак)

Зниження частки успішних атак методами SendRoutingInfo і SendIMSI зв’язано з використанням коштів фільтрації у мережах операторів. Повідомлення SendRoutingInfo використовується для отримання маршрутної інформації про абонента при вхідний голосовий виклик і має передаватися тільки у межах домашньої мережі оператора. Повідомлення SendIMSI для запиту IMSI абонента за його телефонним номером у даний час практично не використовується операторами, проте обробляється у мережах мобільного зв'язку для того, щоб повністю забезпечити відповідність стандартам.

Метод SendRoutingInfoForLCS, що служить для запиту інформації сервісами, яким для коректного функціонування потрібні дані про місцезнаходження абонента, був успішно введений в експлуатацію лише у двох мережах з усіх, що були досліджені, що також пов’язано з ефективною фільтрацією повідомлень.

Повідомлення SendRoutingInfoForSM використовується для отримання маршрутної інформації, необхідної для доставки вхідного SMS. Для запобігання поширенню реальних ідентифікаторів абонентів та адреси мережевих елементів, повідомлення, що надійшло із зовнішньої мережі, має перенаправлятись в

системі SMS Home Routing та повертати віртуальні дані, проте незважаючи на широке використання системи SMS Home Routing, часто можна зіштовхнутись з некоректною конфігурацією граничного мережевого обладнання (STP / FW), що призводить до того, що запит надсилається до HLR в обхід пристрою SMS Router та повертає справжній IMSI абонента і дані про конфігурацію мережі оператора.

В більшості випадків визначити місце розташування абоненту вдавалось шляхом використання методу ProvideSubscriberInfo, що пов'язано з недоліками в архітектурі мережі SS7. Повідомлення ProvideSubscriberInfo має оброблятися тільки у тому випадку, якщо джерело повідомлення і ідентифікатор абонента відповідають одному і тому ж оператору. У зв'язку з особливостями архітектури мереж SS7 неможливо визначити чи належить абонент до мережі оператора, для захисту від атак, які спрямовані на цю вразливість SS7, використовуються системи фільтрації трафіку.

У 2016 році припускалось, що операторам відомі атаки методом AnyTimeInterrogation, що за допомогою телефонного номеру абоненту визначає його місце розташування, а також були відомі відповідні методи захисту, так як не було зафіксовано жодної вдалої атаки, проте протягом наступних двох років були знайдені мережі з повною відсутністю фільтрації цього повідомлення.

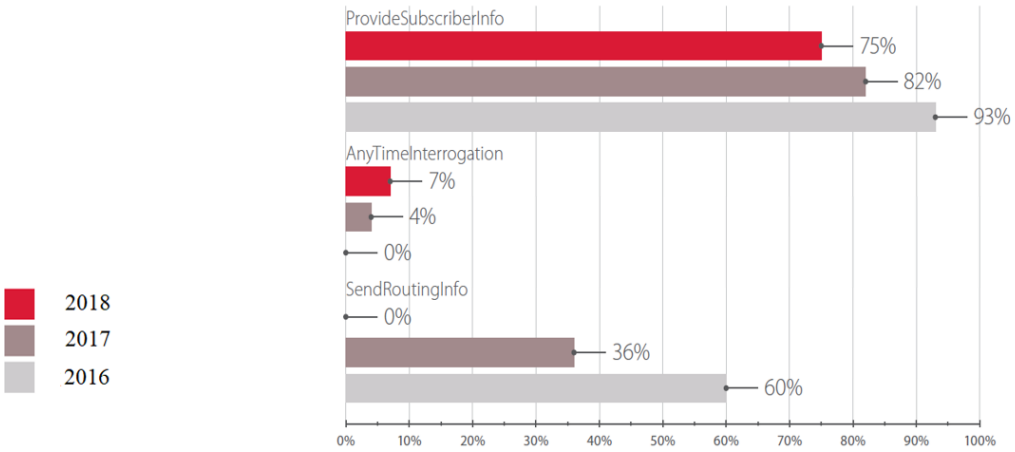

Рисунок 2.9 — Засоби що використовуються для визначення місцерозташування абонента (долі успішних атак)

Захист від загроз розкриття балансу та деталей профілю абоненту не має високого пріоритету, бо вони не несуть безпосередньої небезпеки, а також забезпечення захисту від більшості методів, що використовуються, можливо лише за допомогою постійного моніторингу та фільтрації сигнального трафіку. Реалізувати відповідні атаки можна у кожній дослідженій мережі, для цього використовуються наступні повідомлення:

- Restore Data
- Interrogate SS
- Process Unstructured SS
- Update Location
- Any Time Subscription Interrogation

У ході робіт з аналізу захищеності вдавалося здійснити атаки усіма методами крім AnyTimeSubscriptionInterrogation.

2.3 Витік інформації про оператора

На рисунку 2.10 зображено, що при проведенні перевірок вдалося здійснити більше половини атак, що були пов’язані з некоректними конфігураціями SMS Home Routing, які в свою чергу дозволяли отримати відомості про конфігурацію мережі. Незважаючи на це оператори змогли значно знизити ймовірність розкриття такої інформації.

Зростання числа успішних атак методом Send Routing Info For SM в 2017 році викликано тим, що досліджувались кілька мереж, у яких система SMS Home Routing була відсутня.

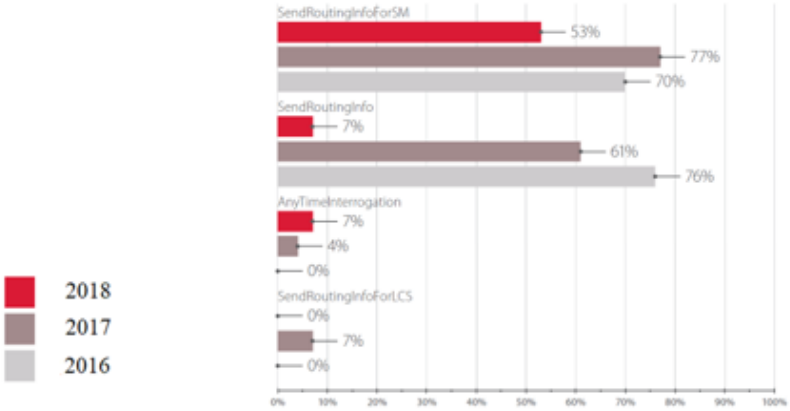

Рисунок 2.10 — Методи використовувані для отримання інформації про конфігурацію мережі SS7(долі успішних атак)

2.4 Перехоплення трафіку абонента

Ризик перехоплення призначеного для користувача трафіку як і раніше залишається достатньою високим. Переважна більшість спроб перехопити SMS абонентів виявилися успішними. На сьогоднішній день за допомогою SMS передається вкрай важлива інформація – паролі для двофакторної автентифікації, які відправляють сервіси, що надають послуги дистанційне банківського обслуговування, інтернет-платежів та ін., витік якої може як нанести значного впливу на репутацію оператору зв’язку, так і стати приводом для клієнтів для розірвання договору, в тому числі для компаній з великими обсягами трафіку.

З рисунку 2.11 видно, що перехопити та перенаправити вхідні та вихідні дзвінки абонентів вдавалось більш ніж у половині випадків.

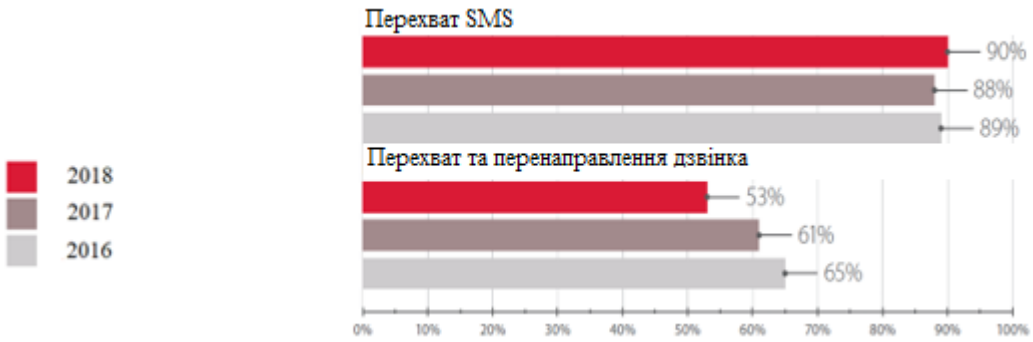

Рисунок 2.11 — Методи які використовують для перехоплення та переадресації трафіка абонента (долі успішних атак)

Під перенаправленням дзвінків розуміється лише передача виклику на номер зловмисника, що в свою чергу дає йому змогу встановити з'єднання таким чином, аби він мав змогу прослухати розмову абонента.

Повідомлення UpdateLocation служить для оповіщення HLR про зміну абонентом обслуговуючого комутатора. Перехоплення вхідних SMS або викликів здійснюється за допомогою формування та відправлення зловмисником фальшивого запиту на реєстрацію абонента в мережі. При надходженні дзвінка мережа оператора відправляє запит в фальшиву мережу для отримання роумінгового номера абонента. Зловмисник може відправити у відповідь номер власної АТС і в цьому випадку вхідний трафік надійде на його обладнання, після відправлення повторного запиту на реєстрацію абонента, зловмисник може перенаправити виклик на номер абонента, в результаті чого розмова буде перенаправлятись через обладнання зловмисника. В основі метода RegisterSS, що використовується для перехоплення вхідних дзвінків, лежить принцип схожий на раніше описаний метод, проте головною його відмінністю є те, що встановлюється безумовна переадресація на номер АТС зловмисника.

Високий відсоток успішних атак пов'язаний з відсутністю перевірки реального місця розташування абонента. Для зниження ймовірність атак, в основу яких покладені раніше розглянуті методи, необхідно забезпечити постійний моніторинг сигнального трафіку і аналіз підозрілої активності для

виявлення підозрілих вузлів, побудови списків заборонених і довірених мереж, негайного блокування запитів із заборонених джерел.

Вхідні дзвінки також можуть прослуховуватись за схемою в основу якої покладено те, що спеціально сформоване повідомлення InsertSubscriberData замінює у профілі абонента, яке зберігається у базі даних VLR, адресу платформи для тарифікації викликів. При отриманні запиту за новою адресою зловмисник спочатку перенаправляє вихідний дзвінок на підконтрольне йому обладнання та лише потім на абонента.

Таким чином зловмисник отримує можливість прослуховувати будь яку розмову абонента.

2.5 Шахрайство

Відомо широкий спектр методів, що можуть бути використані злочинцями з метою отримання фінансової вигоди за рахунок оператора або коштів абонентів мережі. Ці методи поділяються на чотири категорії:

- нелегітимна переадресація вхідних або вихідних дзвінків
- експлуатація USSD – запитів
- маніпулювання SMS
- зміна профілю абонента

2.5.1 Нелегітимна переадресація вхідних або вихідних дзвінків

Зловмисник може переадресовувати голосові виклики абонентів на платні номера або на сторонній номер з метою уникнення тарифікації. Кошти за з’єднання будуть списані з рахунку абонента у разі установки безумовної переадресації на номер шахрая, або за рахунок оператора зв’язку – у разі реєстрації абонента у помилковій мережі і підміни його роумінгового номера.

Переадресація викликів дозволяє відтворювати і інші шахрайські схеми. Так, наприклад, якщо абонент здійснює вихідний дзвінок до банку, то переадресувавши його на власний номер і представившись співробітником

служби роботи з користувачами банку, шахрай може дізнатися конфіденційну інформацію, необхідну для підтвердження особистості, зокрема паспортні дані та кодове слово. Також можлива зворотна ситуація: шляхом переадресації вхідних дзвінків зловмисник може видавати себе за абонента, наприклад для підтвердження банківських операцій.

Рисунок 2.12 — Долі успішних атак направлених на переадресацію голосових повідомлень абонента

Перенаправлення викликів здійснюється за використанням вже згаданих методів UpdateLocation, RegisterSS, InsertSubscriberData, а також методу AnyTimeModification, за допомогою якого можна редагувати профіль абонента, змінювати його данні (зауваження – жодна атака методом AnyTimeModification не привела до потрібного результату).

2.5.2 Експлуатація USSD-запитів

Зловмисник може перевести гроші з рахунку абонента або партнерів оператора, експлуатуючи можливість відправки підроблених USSD-запитів за допомогою методу ProcessUnstructuredSSRequest. Іншим варіантом використання є метод UnstructedSSNotify, що використовується для відправки повідомлень абонентам від імені різноманітних сервісів, включаючи повідомлення і від самого оператора. Злочинець може відправити підроблену

інформацію від довіреної сервісу, яка містить інструкції, що потрібно виконати абоненту: відправити SMS на платний номер для підключення послуги, зателефонувати за фальшивим номером банку завдяки підозрілим операціями на карті або перейти по посиланню для оновлення мобільних додатків.

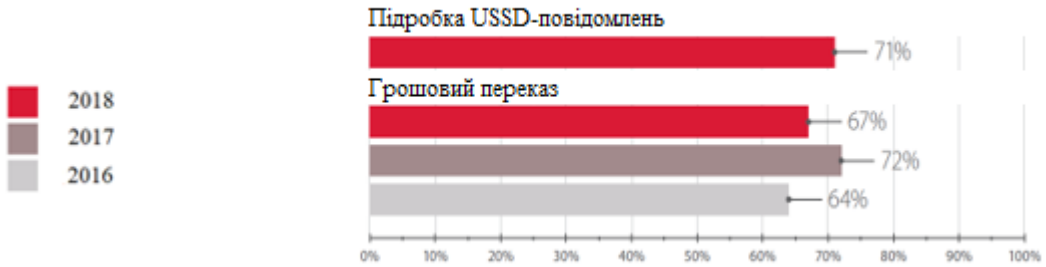

Рисунок 2.13 — Загрози пов’язанні з підробкою USSD-запитів (долі успішних атак)

2.5.3 Маніпулювання SMS

Рекламну або фішингову розсилку повідомлень можна організувати, відправляючи підроблені SMS від ідентифікаторів довільних абонентів або сервісів використовуючи методи MT-ForwardSM і MO-ForwardSM. Метод MT-ForwardSM призначений для доставки вхідних повідомлень і може застосовуватися зловмисниками для формування підроблених вхідних SMS. Несанкціоноване використання методу MO-ForwardSM відправляє вихідні повідомлення від імені та за кошти абонентів мережі. У 2017 році усі мережі, де проводилися даного типу перевірки в ході аналізу захищеності, виявились схильні до вразливостей, пов'язаних з недостатнім аналізом сигнального трафіку, що дозволяють відправити підроблені повідомлення.

2.5.4 Зміна профілю абонента

Інформація про платформу тарифікації і глобальні послуги зберігається у профілі абонента. Для обходження системи тарифікації у реальному часі необхідно видалити O-CSI підписку абонента, що використовується для здійснення абонентом вихідних дзвінків, або підмінити адресу платформи

тарифікації на фіктивність. Для запобігання нетарифікованих викликів у параметрах O-CSI вказується, що при недоступності платформи необхідно завершити виклик. Проте цей параметр можна підмінити таким чином, щоб виклик тривав без звернення до платформи. В результаті легітимна платформа не отримуватиме інформацію про виклики і не буде виробляти тарифікацію.

Рисунок 2.14 — Долі успішних атак направлених на внесення змін у профіль абонента

Атаки методами InsertSubscriberData і DeleteSubscriberData були успішні, але здійснені більш ніж у 80 % випадків, а спроби атак методом AnyTimeModification не приводили до результатів.

2.6 Відмова в обслуговуванні

На сьогоднішній день атаки, націлені відмову у обслуговуванні окремих абонентів, можливі у кожній дослідженій мережі. виявлені недоліки пов'язані з архітектурними проблемами протоколів (неможливість перевірки приналежності абонента мережі і відсутність перевірки реального місцеположення абонента) і дозволяють успішно проводити атаки наступними методами:

- UpdateLocation
- RegisterSS
- IncertSubcriberData

– PurgeMs

Всі спроби атак приводили до відмови у обслуговуванні абонентів, за виключенням методу InsertSubscriberData (83% успішних атак). З цією ж метою може бути використаний і метод AnyTimeModification, однак параметри безпеки всіх досліджених мереж перешкоджали проходженню цих запитів.

Крім можливості здійснювати голосові виклики і обмінюватися SMS, абонент може позбутися доступу у інтернет під час проведення атаки методом InsertSubscriberData.

Незважаючи на те, що розглянуті порушення функціонування мережі направленні і зачіпають у кожному випадку тільки одного абонента, який не виключений і масовий збій у обслуговуванні, якщо зловмисник має базу ідентифікаторів абонентів або може підібрати ідентифікатори перебором.

Такі збої в обслуговуванні можуть бути критичними для пристроїв, які відносяться до інтернету речей. Це ринок який стрімко розвивається, нараховує мільярди пристроїв, для роботи яких потрібен доступ до телекомунікаційних мереж. Періодичний вихід з ладу систем розумного будинку, систем відеоспостереження, пристроїв, які відстежують розташування автомобіля або зупинка промислових процесів підприємства може привести до значного відтоку клієнтів.

При проведенні досліджень ми встановили, що середній час недоступності абонента після такої атаки становить понад три години, а у деяких випадках при виконанні запиту на порушення доступності змінюється поточний профіль абонента у базі даних, і встановлене обладнання не здатне відновити профіль, навіть коли абонент перезавантажує пристрій. Це траплялося при атаках на порушення доступності методами PurgeMS і InsertSubscriberData.

При видаленні з HLR адреси VLR, у якому у даний момент зареєстрований абонент, за допомогою процедури PurgeMS, ініційованої якимось третім вузлом, відбувається наступне. Вхідні дзвінки не можуть маршрутизовуватись на обслуговуючий абонента VLR/MSC, оскільки у HLR адреса реєстрації відсутня.

При цьому вихідні дзвінки абоненту доступні, оскільки реєстраційний запис у VLR не змінювалася.

Відновлення реєстрації у HLR звичайним способом – перезавантаженням телефону (або іншого пристрою) - не працює, так як VLR не ініціює процедуру UpdateLocation щодо HLR, вважаючи, що у реєстраційних даних абонента немає змін.

В результаті відновити реєстрацію, а відповідно, і доступність абонента для вхідних викликів, можна тільки при реєстрації у зоні дії іншого обслуговуючого MSC, наприклад якщо спочатку вручну вибрати мережу іншого оператора, а потім знову вибрати домашню мережу. Інший варіант - перемістится у зону дії іншого MSC домашньої мережі.

У цьому розділі розглядались найпоширеніші загрози та вразливості мобільних та бездротових систем до яких також належить і технологія 4G.

Такі системи як виявилось мають досить критичний недолік у самій архітектурі мережі що дозволяє зловмиснику проводити успішні атаки як на абонентів такої системи так і на операторів зв’язку, що може призвести до втрати особистої інформації користувача або матеріальних втрат як абонента мережі так і оператора мобільного зв‘язку. Різні успішні атаки будуть представлені у наступному розділі.

3 ПЕРЕВІРКА ВРАЗЛИВОСТЕЙ БЕЗПРОВІДНИХ МЕРЕЖ ЗВ’ЯЗКУ

3.1 Спрощена архітектура LTE Advanced

Для зменшення подробиць які не стосуються безпеки інформації та системи через яку будуть проведені атаки, розглянемо спрощену архітектуру бездротової технології передачі інформації. (Рисунок 3.1)

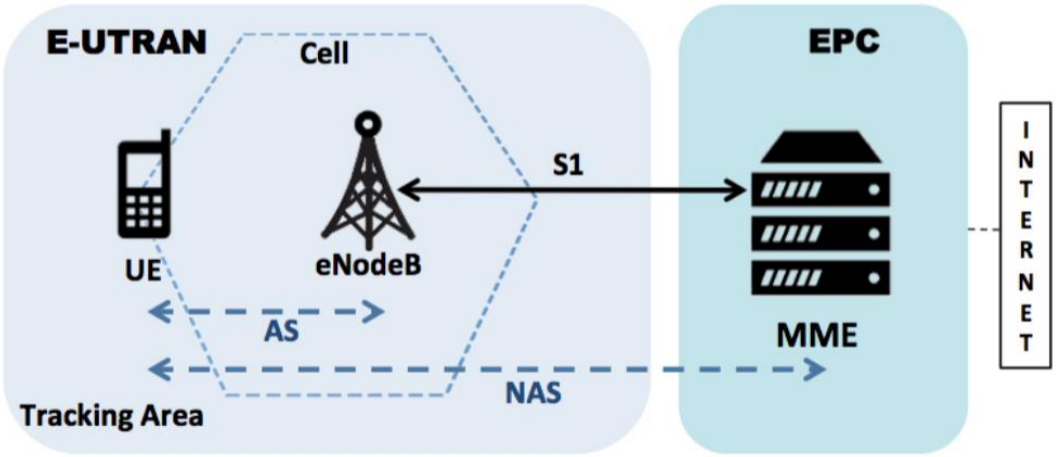

Рисунок 3.1 – Спрощена архітектура LTE

На рисунку 3.1 можна побачити наступні елементи мережі:

- UE (User Equipment);
- AS (Access Stratum);
- Cell (мережа);
- eNodeB (центральна вежа зв’язку);
- NAS (шар без доступу);
- Tracking Area (TA);
- EPC (Evolved Packet Core);
- Mobility Management Entity (MME)(вузол управління мобільністю);
- E-UTRAN.

Обладнання користувача (UE) відноситься до пристрою зв’язку яким може бути: смартфон, планшет і всі пристрої що мають в собі універсальній модуль ідентифікації користувача(Universal Subscriber Identity Module (USIM))[8]. Такі пристрої повинні також мати міжнародний мобільний ідентифікатор абонента(International Mobile Subscriber Identity (IMSI)), ця інформація використовується для ідентифікації абонента в мережах LTE(за термінологією 3GPP). USIM спочатку проходить процедуру автентифікації, а потім приймає учать у генеруванні криптографічних ключів які формують основу для ієрархії ключів – які використовуються в системах сигналізації та передачі абонентських даних між UE та БС.

Як можна побачити на рисунку 3.1 E-UTRAN складається з БС. Він керує радіозв’язком UE, та полегшує зв'язок між UE та EPC, в технології LTE базова станція називається «розвиненою» eNodeB. Для обміну сигнальними повідомленнями між UE та eNodeB, використовується протокол доступу Access Stratum (AS). Такі повідомлення включають до себе допис протоколів управління радіо ресурсів (RRC) До інших функцій eNodeB можна додати також :

- пошуковий дзвінок UE;
- безпровідний захист;
- можливість з’єднання даних фізичного рівня;
- передачу обслуговування.

Mobility Management Entity (MME) у EPC, забезпечує функціональні можливості базової мобільної мережі за допомогою мережі повністю заснованої на IP та призначеної для технологій LTE. [10] MME у той же час відповідає за:

- розподіл ресурсів UE;
- автентифікацію UE при підключенні до мережі;
- налагодження цілісності безпеки;
- шифрування для сигналізації;
- відстеження UE на макро-рівні.

Набір протоколів відповідальний за зв'язок між UE та MME, має назву шар без доступу (NAS).

В безпровідних мережах LTE, зони обслуговування оператора поділені географічно і далі на регіони, відомі як Tracking Area (TA), вони аналогічні областям місцезнаходження в GSM мережах та керуються MME. Крім того кожна TA містить групу «осередків» кожна з яких в свою чергу керується eNodeB. Мобільна сота (eNodeB) транслює специфічну інформацію для оператора, наприклад :

- код зони відстежування (TAC);
- мобільний код держави (MCC) ;
- мобільний код мережі (MNC) ;
- ідентифікатор соти, шляхом повідомлення блока системної інформації (SIB).

Всі данні допомагають UE ідентифікувати свого обслуговуючого оператора стільникової мережі та ініціювати з’єднання з мережою. Підключаючись до мережі UE починає процедуру CONNECTED, після проходження якої отримує доступ до послуг, згідно свого тарифу, та на основі свого підпису починає роботу процедура оновлення місцеположення в мережі TrackingAreaUpdate (TAU) інформуючи таким чином мережу о своїй мобільності в обслуговуючій області.

3.2 Безпека в LTE

Оскільки в безпровідних мережах LTE є IMSI, і він є постійним, то його передачу намагаються звести до мінімальних значень по зображенням безпеки та конфіденційності. Заміть нього зазвичай використовують глобальний тимчасовий ідентифікатор (GUTI).[9] Він визначається UE та може змінюватись з визначеною періодичністю, для забезпечення тимчасової незв’язаності графіку з одним і тим же користувачем. Для узгодження між взаємної автентифікації між UE та мережою застосовується протокол Автентифікації та Узгодження Ключів

(АКА). Цей протокол забезпечує також цілісність та конфіденційність для наступних повідомлень NAS та AS.

В парі безпеку NAS та AS [11] створюють так звану безпеку EPS. Вона встановлюється між UE та eNodeB та MME, під час процедур EMM (EPS Mobility Management) [12] та включає до себе:

- в узгодження ключів;
- бажані криптографічні алгоритми;
- інші значення.

До ідентифікатора IMSI входять наступні частини:

- MCC
- MNC
- MSIN (Mobile Subscriber Identification Number) – назначається оператором зв’язку та визначає номер пристрою абонента, Може буди довжиною 9-10 цифри (якщо MNC містить 3 цифри, та 2 відповідно)

На рисунку 3.2 можна побачити його побудову

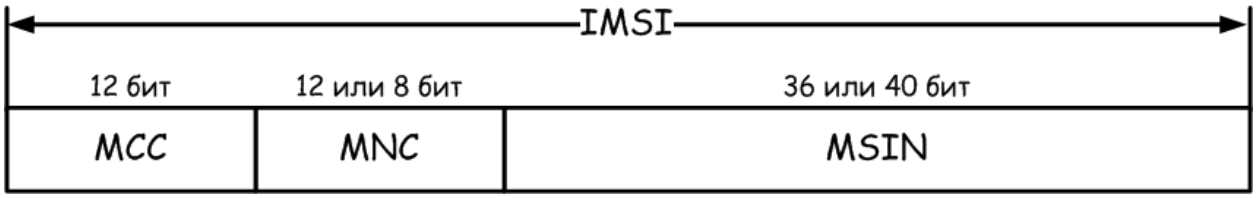

Рисунок 3.2 – побудова IMSI

3.3 Пейджинг в LTE

До процедури пошуку (пейдженгу) відноситься процес, коли MME необхідно знайти UE в визначеній області, та доставити послугу (наприклад послугу вхідного виклику). Оскільки MME може і не знати точного eNodeB, до якого в даний момент підключений UE він генерує пошукове повідомлення і посилає його по всім eNodeB у TA. Одночасно з цим MME починає запуск таймер пошукового повідомлення (T3413) і очкує відповіді від UE до скінчення

початого таймеру. Таким чином, всі eNodeB, які присутні в виділеній TA, передають пейджингове повідомлення RRC для визначення місце розташування UE. Такі повідомлення містять ідентифікатори UE, сере них:

– STMSI;

– IMSI;

– S-TMSI.

S-TMSI є частиною тимчасового ідентифікатора (SAE Teorary Mobile Subscriber Identity) та входить до GUTI. На рисунку 3.3 зображено схему його пакетів та протоколів що входять до нього.

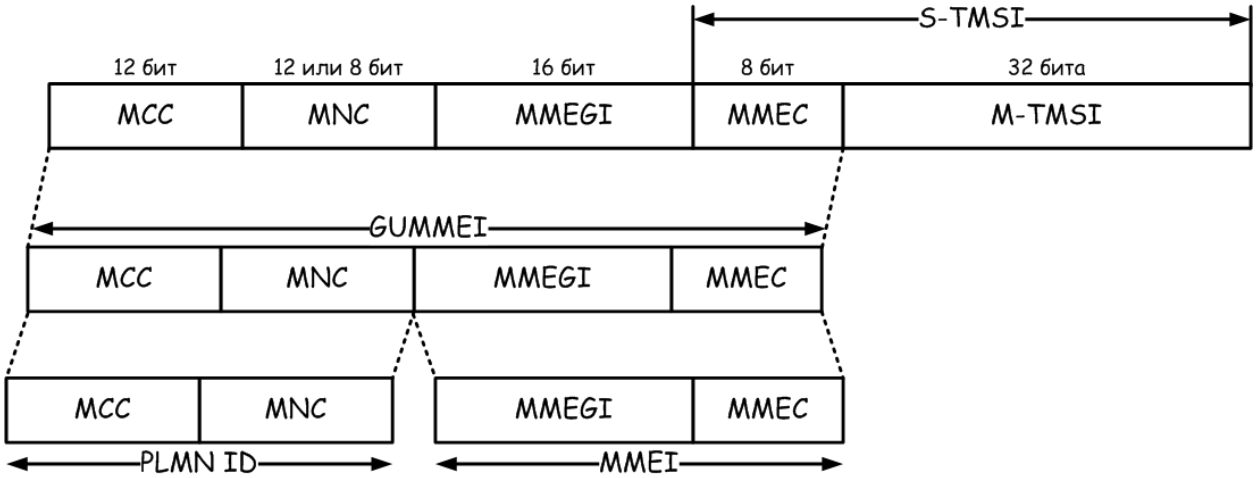

Рисунок 3.3 – Глобальний тимчасовий ідентифікатор (GUTI)

Згідно технічному опису в GUTI входять:

– PLMN(Public Land Mobile Network) – ідентифікатор глобальної мережі;

– MMEI (MME Identity) – згідно з PLMN визначає місце MME в мережі;

– M-TMSI – в рамках MME визначає eNodeB.

Далі для спрощення буде використовуватися GUTI коли посилання потрібно буде на одну з його частин (наприклад STMSI). Далі на рисунку 3.4 буде показана процедура пошукового виклику LTE, які більш ретельно описана в спеціальних розділах специфікації LTE.[12][13][14]

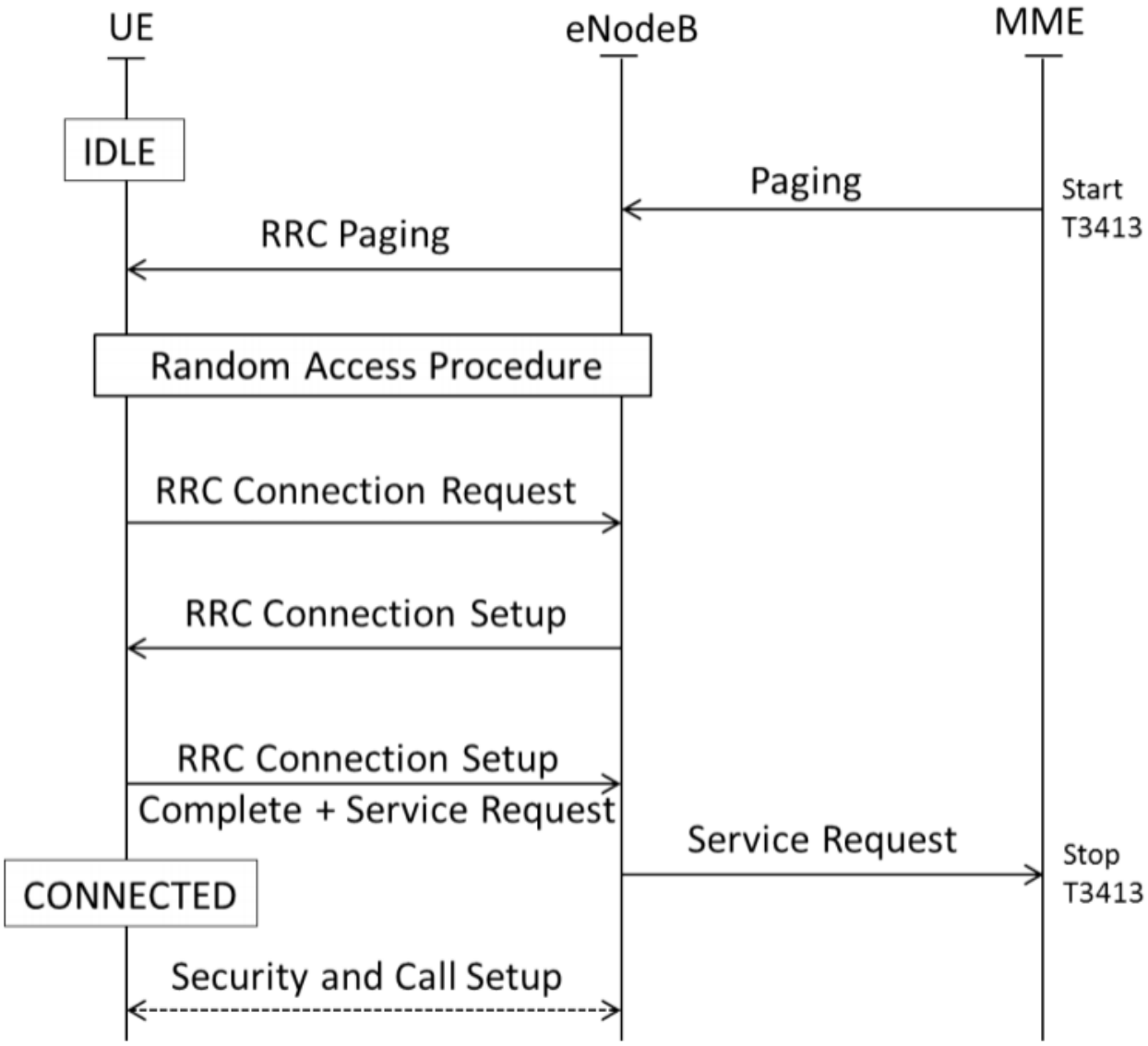

Рисунок 3.4 Виконання пошуку UE в мережах LTE

UE у стані IDLE декодує повідомлення пошуку RRC від eNodeB. Після чого починається «Налаштування з'єднання RRC» що включає до себе налаштування радіоресурсів для обміну сигнальними повідомленнями. Після отримання такого повідомлення про налаштування UE завершує процедуру трьохсторонню процедуру встановлення зв'язку, відправляючи повідомлення «Налаштування з'єднання RRC завершено» разом с цим відправляється повідомлення «Запит на обслуговування». В цей момент UE покидає стан IDLE та отримує новий статус CONNECTED. ENodeB посилає повідомлення із запитом на обслуговування MME, що в свою чергу, зупиняє таймер пошукового

виклику. Крім того, eNodeB встановлює протоколи безпеки та починає надавати мережеві послуги абоненту.

В LTE процедур пейджингу покращили для зменшення навантаження сигналізації та швидкий пошук місцезнаходження UE, використовуючи техніку з навою Smart Paging.[16][17][18] Вона відповідає специфікаціям LTE та складається з вибіркового вибору направлення пейджингових повідомлень через eNodeB, в зону де останній раз «бачили» останній раз. Якщо відповідь не отримана то пошук продовжується по всім ТА.

3.4 Види атак та модель зловмисника

Атаки та види зловмисника можна поділити на категорії:

- пасивний;
- напівпасивний;
- активний.

Пасивний порушник здатний прослуховувати радіомовні канали LTE, для досягнення цього він повинен мати доступ до апаратних при строїв (наприклад універсальному програмному забезпеченню переферійних пристроїв радіозв’язку (USRP)) та відповідному програмному забезпеченню необхідному для спостереження та декодування повідомлень радіомовної сигналізації.

Напівпасивний порушник, окрім обладнання і програмного забезпечення для пасивної атаки, повинен бути здатен ініціювати сигнальні повідомлення для користувачів, використовуючи інтерфейси та дії які законно доступні в LTE або в системах бездротової передачі даних більш високого рівня. Наприклад такий порушник здатен ініціювати пейджингове повідомлення для користувачів, відправляючи повідомлення через соціальні мережі або ініціювати вхідний дзвінок. Вважається що опонент знає о особистості жертви. Таким чином під загрозою можуть бути ідентифікатори в соціальних мережах (Facebook, WatsApp)[20][21] або мобільний номер абонента. Такий тип атаки вважається «чесним, але зацікавленим», «напівлегальною» моделлю порушника.

Активний зловмисник може встановлювати та використовувати шахрайські eNodeB для встановлення шкідливого впливу на UE. Можливості які необхідні для такого включають:

- знання специфікацій обладнання LTE (USRP);
- вміння видавати себе за частину мережі;
- встановлення шахрайських пакетів до UE.

Такий порушник аналогічний «зловмисній» моделі порушника.

3.5 Обладнання необхідне для атаки

Для реалізації атаки в безпровідних мережах необхідно мати:

- eNodeB;
- MME;
- UE.

Зі сторони мережі можна використати USRP B210, підключений до головного комп’ютеру/ноутбуку, він буде працювати як eNodeB.

USRP – це визначаємий програмний радіопристрій, який може бути підключено до головного комп'ютера і використовуватися програмним забезпеченням на основі хоста для передачі / прийому даних по радіоканалу.

Зі сторони UE можна обрати будь, які популярні смартфони або телефони, але в них повинна бути підтримка LTE мереж.

Все це буде імітувати технологію LTE, на яку можна імітувати атаки.

3.6 Приклад атаки збору даних

Було проведено вимірювання в мережах LTE, для розуміння розподілу GUTI інтелектуальний пейджинг та відображення області відстежування та розмірів осередків з метою вивчення технічно-економічних аспектів атак визначення місцеположення. Перед вимірювання розподілу GUTI та Smart

Paging роздивимось наступні тимчасові обмеження для процедур пейджингу в LTE мережах:

– пейджингові повідомлення відправляються тільки якщо абонент знаходиться в стані IDLE;

– якщо UE зберігає мовчання в часі 10 секунд під час з'єднання, eNodeB звільняє виділені ресурси і UE переходить в стан IDLE;[14]

– зміна або перерозподіл GUTI повністю залежить від конфігурації оператора.

Використані методи розподілу ті перерозподіл GUTI застосовуються декількома операторами. Зокрема ця перевірка зможе показати – чи є GUTI дійсно тимчасовими на практиці.

В ході перевірки були ідентифіковані NAS та записані GUTI для кожного "оператора" для подальшого аналізу. Крім того, зміна тимчасового ідентифікатора можна було перевірити в інженерному режимі на декількох обраних телефонах.

Були отримані такі результати:

– З двома періодичностями (один раз в годину, або один раз в 12 годин) відбувається від'єднання та підключення UE, коли воно було нерухомим, таке відбувалось з усіма «операторами». Стаціонарне UE не змінювало свій GUTI на строк до трьох діб або при переміщені між TA в межі міста.

– Коли UE переміщався по місту в протягом трьох діб, але з'єднаним з мережею, то ніяких змін в GUTI не відбувалось в жодній з мереж «оператора».

– Якщо UE було відключено на одну добу, то при включенні було відразу нове значення GUTI. У випадку одного з «операторів» новопризначений GUTI відрізнявся від старого тільки однією шістнадцятирічною цифрою. Це означає що GUTI були обрані не випадково.

Виходячи з результатів спостереження, зробили висновок, що GUTI має тенденцію залишатись незмінним, навіть коли UE переміщаєтеся в межах міста строком до трьох діб. Це означає що так звані тимчасові ідентифікатори на ділі

виявляються не такими, в жодній із мереж. Це дозволяє реалізувати пасивні атаки. В таблиці 3.1 приведена поведінка GUTI, операторів та Smart Paging за результатами перевірки

Таблиця 3.1 результати тестування GUTI

Активність	Smart Paging		Зміна GUTI (всі «оператори»)
	на вежу	на ТА	
Повідомлення Facebook	Так	Відсутня	Відсутня
SMS	Так	Відсутня	Відсутня
Дзвінок VoLTE	Відсутня	Так	Відсутня
Від’єднання та підключення UE кожну годину	–	–	Відсутня
Від’єднання та підключення UE кожні 12 годин	–	–	Відсутня
Звичайна процедура TAU	–	–	Відсутня
Періодична процедура TAU	–	–	Відсутня

4 МЕТОД ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В БЕЗДРОТОВИХ МЕРЕЖАХ ТИПУ LTE

4.1 Підготовка до перевірки

Для проведення перевірок та пошуку вразливостей в безпровідних мережах треба з початку:

- прочитати описання технології що буде проходити перевірку
- мати обладнання для імітування безпровідної мережі і потрібних протоколів
- вміти посилати сигнальні повідомлення в обидві сторони
- знати минулі вразливості (якщо вони були), для початку перевірки і старту атаки
- мати обладнання для обробки отриманих даних (як апаратних, так і програмних)
- після обробки результатів повідомити заказника

4.2 Проведення випробувань

Для проведення випробувань, треба визначити наступне:

- об’єкт випробувань;
- мету випробувань;
- загальні положення;
- обсяг випробувань;
- умови та порядок проведення випробувань;
- матеріально-технічне забезпечення;
- звіт.

Таким чином визначеним об’єктом випробувань становиться безпровідна мережа типу LTE, і забезпечення безпеки інформації абонента.

Метою випробувань буде пошук вразливостей які можуть призвести до порушенню безпеки інформації та загрози конфіденційності як абонента, так і оператора.

Обсяг випробувань – залежить від радіусу дії базової станції на якій вона функціонує.

Умови і матеріально-технічне забезпечення: в наявності пристрій який може імітувати мережу LTE, повинні бути робочі протоколи обміну даними, можливість посилати сигнальні повідомлення, пристрій обробки отриманих пакетів.

Порядок проведення випробувань буде наступним:

1) Встановлення макету безпровідної мережі.
2) Налаштування мережі.
3) Підключення абоненту до макету БС.
4) Імітування процесу обміну, з’єднання між базовою станцією та користувачем.
5) Обробка отриманих пакетів.
6) Пошук ідентифікаторів які допоможуть визначити ціль атаки та показати місцезнаходження абоненту в радіусі дії базової станції.
7) Використовуючи отримані ідентифікатори можна як починати перехоплювати трафік жертви, так і шпигувати за нею в пасивному стані.

Після отримання результатів пишеться звіт на знайдену вразливість в бездротовій мережі передачі даних та пропозиції як ці вразливості можна закрити.

ВИСНОВОК

В процесі написання роботи було розглянуто історичні відомості про розвиток та становлення безпровідних мереж. В таблицях наведені приклади порівнянь різних поколінь таких технологій. Також приведена статистика відомих атак на безпровідні мережі типу LTE, зібрані дані дають інформацію про те що кількість атак не буде зменшуватись так як на стільникову технологію переходить все більше людей. Швидкості в таких мережах все зростають, а методи захисту стають все більш застарілими.

Було проведено практичне випробування на предмет пошуку вразливості яка може впливати на роботу мережі, безпеці інформації абонента, конфіденційності даних та можливості роботи базових станцій під впливом шахраїв.

Отримані під час випробовування дані дають зрозуміти – що безпека інформації в мережах безпровідного доступу знаходиться під загрозою, і не зважаючи на те що працівники та розробники в сфері технологій намагаються зменшити ризики та підвищити рівень захисту в них, під загрозою все ще знаходиться і абонент що користується такими мережами, і базова станція що передає, приймає, обробляє отримані пакети інформації, і нарешті під загрозою є провайдер який надає послуги та тарифи користувачам.

На сьогоднішній день шахраї можуть компрометувати провайдерів шляхом зміни тарифів та абонентської плати, вираховувати місцезнаходження базових станцій (вони знаходяться в відкритому доступі) намагатись підробити та перенаправити сигнал з вежі до зловмисників. В широті можливостей злодіїв знаходиться також перевантаження базових станцій запитами через DDoS атаками, що призводить до відключення можливості надавання послуг абонентам. Перехоплені тимчасові ідентифікатори містять в собі інформацію про міжнародний номер абонента, який є секретним та використовується для початку процедури генерації ключів, що може впливати на конфіденційність

повідомлень які надходять та надсилаються користувачу, таким чином можна читати повідомлення та прослуховувати дзвінки.

Таким чином для безпеки інформації загрозою являється передача пакетів в відкритому виді. На жаль без такого виду передачі неможлива робота цієї технології.

Для позбавлення недоліків та вразливостей таких мереж необхідно с початку переглянути системи обміну, зашифровувати важливі та критичні частини пакетів або забезпечити зашифрований зв'язок між базовою станцією та абоненту. Такий вибір на жаль не є оптимальний так як тоді ціна обслуговування буде вище ніж необхідність захисту повідомлення.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЬ

1. LTE-Advanced [Электронный ресурс]. – Режим доступу URL: 3gpp.org/technologies/keywords-acronyms/97-lte-advanced (дата запиту 01.10.2019)

2. 1MA167: IEEE 802.16m Technology Introduction стр.6 [Электронный ресурс] – Режим доступу URL: rohde-schwarz.com/ru/applications/white-paper_230854-15513.html (дата звернення 01.10.2019)

3. WiMAX [Электронный ресурс] – Режим доступу https://uk.wikipedia.org/wiki/WiMAX

4. WiFi-Based IMSI Catcher [Электронный ресурс]. – Режим доступу URL: blackhat.com/docs/eu-16/materials/eu-16-OHanlon-WiFi-IMSI-Catcher.pdf (дата звернення 05.10.2019)

5. Технология 4G [Электронный ресурс] – Режим доступу URL: anisimoff.org/lte/lte.html (дата запиту 01.10.2019)

6. Thomas Porter, Michael Gouch [2007] “How to Cheat at VoIP Security”

7. Опис використання мобільними телефонами протоколу SS7. Tobias Engel [2008] [Электронный ресурс] – Режим доступу URL: events.ccc.de/congress/2008/Fahrplan/attachments/1262_25c3-locating-mobile-phones.pdf (дата звернення 03.06.2019)

8. 3GPP. Characteristics of the Universal Subscriber Identity Module (USIM application) 3GPP TS 31.102 version 12.5.0 Release 12. [Электронный ресурс] – http://www.3gpp.org/dynareport/31102.htm (дата звернення 07.10.2019)

9. 3GPP. Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003 version 12.5.0 Release 12). [Электронный ресурс] – http://www.3gpp.org/ dynareport/23003.htm (дата звернення 07.10.2019)

10. 3GPP. Network Architecture ; Specification 3GPP TS 23.002 version 12.7.0 Release 12. [Электронный ресурс] – http://www.3gpp.org/ DynaReport/23002.htm (дата звернення 02.10.2019)

11. 3GPP. System Architecture Evolution (SAE); Security architecture; (3GPP 33.401 version 12.14.0 Release 12). [Электронный ресурс] – http://www.3gpp.org/dynareport/33.401.htm (дата звернення 07.10.2019)

12. 3GPP. Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 Specification 3GPP TS 24.301 version 12.8.0 Release 12. [Электронный ресурс] – http://www.3gpp.org/dynareport/24301.htm (дата звернення 03.10.2019)

13. 3GPP. evolved universal terrestrial radio access (E-UTRA); user equipment (UE) procedures in idle mode; Specification 3GPP TS 36.304 version 12.4.0 Release 12. [Электронный ресурс] – http: //www.3gpp.org/dynareport/36304.htm (дата звернення 07.10.2019)

14. 3GPP. Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (EUTRAN); overall description; stage 2, Specification 3GPP TS 36.300 version 12.4.0 Release 12. [Электронный ресурс] – http://www.3gpp.org/ dynareport/36300.htm (дата звернення 03.10.2019)

15. Идентификаторы UE в LTE [Электронный ресурс] – http://anisimoff.org/lte/ue_ids.html (дата звернення 07.10.2019)

16. Melih Tufan. Packet Networks Portfolio. [Электронный ресурс] – http://www.ericsson.com/ericsson/investors/doc/2011/apforum/ericsson apac forum 150911 packet networks.pdf (дата звернення 010.10.2019)

17. David Nowoswiat. Managing LTE core network signaling traffic. [Электронный ресурс] – http://www2.alcatel-lucent.com/techzine/ managing-lte-core-network-signaling-traffic/ (дата звернення 10.10.2019)

18. Nokia Networks. Voice over LTE (VoLTE) Optimization. [Электронный ресурс] – http://networks.nokia.com/sites/default/files/document/ nokia volte optimization white paper 071114.pdf (дата звернення 10.10.2019)

19. ABI. LTE Subscriber Base to Grow to 1.4 Billion Globally by Year-end 2015. [Электронный ресурс] – https://www.abiresearch.com/ press/lte-subscriber-base-to-grow-to-14-billion-globally/ (дата звернення 10.10.2019)

20. Facebook Inc. Facebook Messenger. [Электронный ресурс] – https: //www.messenger.com/features (дата звернення 10.10.2019)

21. WhatsApp Inc. WhatsApp Messenger. [Электронный ресурс] – http: //www.whatsapp.com (дата звернення 10.10.2019)