УНИВЕРЗИТЕТ СИНГИДУНУМ
Департман за последипломске студије

- МАСТЕР РАД -

АНАЛИЗА БЕЗБЕДНОСНИХ НЕДОСТАТАКА У 4G/LTE МОБИЛНИМ КОМУНИКАЦИОНИМ МРЕЖАМА

Ментор:
Проф. Др Младен Веиновић

Кандидат:
Александар Павић, дипл.инж.

У Београду, 2017. године

Садржај

Увод ... 3
Analysis of safety defects in 4G / LTE cellular network ... 4
Методологија научног истраживања ... 5
1. ЕВОЛУЦИЈА МОБИЛНИХ КОМУНИКАЦИЈА ... 8
1.1 Еволуција мобилних комуникационих система пре LTE ... 10
1.2 Основе 4G/LTE мобилних комуникационих мрежа ... 12
1.3 Развој LTE мрежа кроз статистичке показатеље ... 14
1.4 Стање LTE мрежа у Републици Србији ... 15
2 ТЕОРИЈСКИ АСПЕКТИ ВАЖНИ ЗА АНАЛИЗУ БЕЗБЕДНОСТИ LTE МОБИЛНИХ МРЕЖА ... 18
2.1 Основи архитектуре ... 18
2.2 Протоколи комуникације и комуникациони интерфејси ... 20
2.3 Секвенца успоставе позива VoLTE ... 22
3 МЕТОДЕ ЗАШТИТЕ КОМУНИКАЦИЈА И ТЕХНИКЕ ПРЕСРЕТАЊА САДРЖАЈА ... 24
3.1 Приступна инфраструктура мобилних мрежа четврте генерације ... 25
3.2 Имплементиране методе заштите комуникације у LTE мобилним мрежама ... 26
3.2.1 Принципи аутентификације и алгоритми енкрипције у мрежама старије генерације ... 27
3.2.2 Аутентификација и алгоритми енкрипције у 4G/LTE мрежама ... 28
3.3 Надзор мобилне телефоније ... 32
3.3.1 Пасивни систем надзора ... 33
3.3.2 Активни систем надзора ... 35
3.4 Безбедносни недостаци локацијских сервиса у LTE мрежама ... 37
3.4.1 Основе позиционирања мобилних уређаја ... 37
3.4.2 Диаметар протокол ... 39
3.4.3 Недостаци LTE локацијских сервиса ... 41
4 БЕЗБЕДНОСНИ АСПЕКТИ И НЕДОСТАТЦИ У 4G/LTE МОБИЛНИМ КОМУНИКАЦИОМ МРЕЖАМА ... 44
4.1 Увод ... 44
4.2 Захтеви и могућности LTE мобилних мрежа ... 44
4.3 Модел анализе ... 45
4.4 Општи безбедносни аспекти ... 45
4.4.1 Дистрибутивна мрежа и отворена архитектура ... 46

4.4.2 Децентрализована одговорност за безбедност ... 46
4.4.3 Комплексни бизнис модел у смислу инфраструктуре и размене сервиса ... 47
4.4.4 Минимализација трошкова безбедносне заштите ... 48
4.4.5 Превентивне мере ... 48
4.5 Мобилни уређаји ... 50
4.5.1 Физичка доступност мобилног уређаја ... 50
4.5.2 Недостатак безбедносних стандарда и контроле уређаја ... 51
4.5.3 Ризик од губитка приватних података ... 51
4.5.4 Безбедносни недостаци апликација ... 52
4.5.5 Превентивне мере ... 53
4.6 Приступна инфраструктура ... 55
4.6.1 Физички напад ... 56
4.6.2 Лажна базна станица ... 56
4.6.3 Пресретање саобраћаја ... 57
4.6.4 Повреда приватности ... 58
4.6.5 Превентивне мере ... 58
4.7 Језгро мреже (Evolved Packet Core (EPC)) ... 60
4.7.1 Неауторизовани приступ ... 61
4.7.2 DoS и DDoS напади ... 61
4.7.3 Злоупотреба ИП адресе претплатника ... 62
4.7.4 Превентивне мере ... 62
4.8 Сервисна мрежа ... 63
4.8.1 Неовлашћени приступ ... 64
4.8.2 Злоупотреба сервиса, крађа услуга ... 64
4.8.3 Неовлашћени надзор, преузимање сесија ... 65
4.8.4 Превентивне мере ... 65
Закључак ... 67
Литература ... 69
Списак слика ... 71
Списак табела ... 72
Списак скраћеница ... 73

Увод

LTE (*енг. Long Term Evolution*) мобилне комуникационе мреже су производ сталног развоја и унапређења савремених телекомуникација. Мобилни оператери условљени све већом потражњом за квалитетним телекомуникационим линковима који омогућавају пренос података у реалном времену. Повећање пропусног опсега и квалитета су основна начела развоја телекомуникација, а тако и мобилних мрежа четврте генерације. Живимо у времену када је готово незамисливо да немамо доступан широкопојасни интернет на сваком месту и у свако време. Основни комуникациони уређај је смартфон, мобилни уређај који омогућава приступ широкопојасној мрежи. Безбедност комуникација је веома важан сегмент савремених телекомуникација, поред аспекта брзине преноса података и капацитета линка који углавном највише интересују крајњег корисника, као и економске исплативости која највише интересује мобилног оператера који пружа услуге. Претплатник који свакодневно приступа интернету преко LTE мрежа и дели своје личне податке, банковне трансакције, садржаје преписки и садржаје из приватног живота у оквиру разних друштвених мрежа вреба велики број безбедносних ризика који могу да буду веома малициозни. Безбедност претплатника треба да буде један од основних постулата савремених комуникација, а паралелно са развојем технологија треба развијати и систем заштите који треба да буде адекватан и довољан за безбедно коришћење ресурса мобилне комуникационе мреже.

У овом раду су анализирани безбедносни аспекти мобилних мрежа четврте генерације како са становишта архитектуре телекомункационе инфраструктуре, тако и са аспекта већ постојећих протокола и технологија које су постале саставни део мобилних мрежа. Претплатник у оквиру LTE мобилних мрежа више није само један број телефона већ и IP (*енг. Internet Protocol*) адреса која обитава у комплексном екосистему који називамо интернет и самим тим преузима и све безбедносне ризике истог.

Циљ рада је изучавање савремених претњи по безбедност телекомуникација кроз анализу спектра већ познатих чињеница као и отварање нових непознатих безбедносних пропуста. Рад је структурно подељен на две целине. Прва се бави фундаментом LTE мрежа, њеном безбедносном структуром и могућностима пресретања комуникација. Друга целина се бави конкретном анализом различитих претњи које су последица архитектуре мреже и ризика преузетих са инкорпорацијом интернет протокола.

Кључне речи: LTE, безбедност LTE мрежа, пресретање комуникација, енкрипција, дијаметар, технике заштите мобилних комуникација, безбедносни аспекат LTE мрежа.

ANALYSIS OF SAFETY DEFECTS IN 4G / LTE CELLULAR NETWORK

LTE (*Long Term Evolution*) cellular network are the product of continuous development and improvement of modern telecommunications. Mobile opearators conditioned by the growing demand for high-quality telecommunications links that enable the transmission of data in real time. Increasing bandwidth and quality are the basic principles of development of telecommunications and mobile networks fourth generation. We live in a time when it is almost inconceivable that do not have broadband internet available anywhere and at any time. Basic communication device is a smartphone, a mobile device that provides access to the broadband network. In addition to the aspect of data transfer speeds and capacity of the link generally most interested end-users as well as the economic viability of the most interested in mobile operaterakoji provides services, an important segment of the communications security. The subscriber who daily access to the internet via LTE network and share their personal information, banking transactions, the contents of conversations and content private life in the context of various social networks lurks a large number of security risks can be very malicious. Security subscribers should be one of the basic principles of modern communications, parallel with the development of technology should be developed and the system of protection that should be adequate and sufficient resources for the safe use of mobile communications networks.

This paper analyzes the security aspects of mobile networks fourth generation both in terms of architecture, the telecommunication infrastructure, but also in terms of the existing protocols and technologies that have become an integral part of the mobile network. Subscriber within the LTE mobile network is no longer just a phone number, but also IP (*Internet Protocol*) address that resides in a complex ecosystem that we call the internet and therefore takes all the same security risks.

The aim of this paper is the study of modern threats to the security of the telecommunications spectrum analysis of already known facts as well as the opening of new, unknown security vulnerabilities. The paper is structurally divided into two parts. The first deals with the fundament LTE network, its security structure and interception of communications. The second part deals with specific analysis of the various threats that are a result of the network architecture and the risks assumed to incorporate the Internet Protocol.

Keywords: LTE, LTE network security, LTE interception, encryption, diameter, protection techniques of mobile communications, the security aspect of LTE networks.

МЕТОДОЛОГИЈА НАУЧНОГ ИСТРАЖИВАЊА

Предмет истраживања

Предмет истраживања мастер рада је безбедност комуникације у мобилним телекомуникационим мрежама четврте генерације LTE. С акцентом на анализи безбедносних ризика који су свакодневно присутни и који имају утицаја на све кориснике мобилне мреже четврте генерације, као и на пружаоце услуга мобилних комуникација.

Циљеви и задаци

Научни циљ овог мастер рада је систематизација знања о мобилним телекомуникационим мрежама четврте генерације, као и унапређење постојећих сазнања супституцијом чињеница која су стечена вишегодишњом праксом у наведеној области.

Друштвени циљ рада је систематизација сазнања из наведене области и приближавање тематике како експертима који се баве истом проблематиком, тако и обичном човеку који је основна јединка друштва.

Основни задатак овог мастер рада је анализирати познате безбедносне ризике у мобилним комуникацијама четврте генерације и створити услове за развој истраживања и генерисање нових чињеница које могу да буду од јавног интереса. Свакако да је сама актуелизација теме један од основних задатака јер подиже ниво свести крајњег корисника о безбедносним ризицима којима се свакодневно излаже употребом мобилних комуникационих уређаја.

Истраживачка хипотеза

Општа хипотеза при изради овог рада би била:

Анализа безбедносних ризика у мобилним телекомуникацием мрежама четврте генерације треба да обезбеди препоруке и унапреди методологију заштите мобилних телекомуникационих система.

Посебне хипотрезе при изради рада би биле:

- Комбиновањем познатих чињеница и супституција нових сазнања унапређују знање о LTE мрежама,
- Изучавање безбедносних ризика унапређује и развој метода за превенцију и спречавање настанка истих,

- Доступност савремених технологија обичном човеку чини систем телекомуникација рањивијим и зато је потребно анализирати безбедносне ризике и са становишта доступности технологија,
- Предлог мера и методологија унапређења заштите је једна од основа реализације безбедног окружења.

Методе истраживања и ток истраживачког процеса

Комплексност теме рада захтева комбиновање различитих метода истраживања као и комплексан ток истраживачког процеса. Наиме, како би се задовољили постулати објективности, поузданости, општости и систематичности истраживање је вршено основним, опште научним и методама прикупљања података.

Од основних метода коришћене су аналитичке и синтетичке методе. Од опште научних метода коришћени су хипотетичко дедуктивни и индуктивни модел. Прикупљање података вршено је следећим методама: компаративне, дескриптивне, статистичке, практична сазнања.

Научни ток мастер рада се одвијао од момента дефинисања основне хипотезе кроз систематизацију теоријских и практичних сазнања. Комбиновањем чињеница како из теоријских извора тако и имплементацијом практичних сазнања. Поред наведеног подаци и чињенице су упоређене са подацима релевантних институција које се баве изучавањем наведене тематике.

Структура мастер рада

Мастер рад под темом "*Анализа безбедносних недостатака у 4G/LTE мобилним комуникационим мрежама*" састоји се из увода, четири поглавља, закључка и списка коришћене литературе, слика и табела.

У првом поглављу *Еволуција мобилних комуникација,* биће описан историјски развој мобилних мрежа од самих почетака до савремених система који су дана у употреби. Тренутно стање развијености мобилних оператера у Републици Србији као и тенденције развија.

У другом поглављу *Теоријски аспекти важни за анализу безбедности LTE мобилних мрежа*, биће образложена структура мреже по најважнијим сегментима који су од интереса за ово истраживање. Преглед архитектуре, протокола и комуникационих интерфејса, као и секвенца успоставе позива су образложени у овом поглављу.

У трећем поглављу *Методе заштите комуникација и технике пресретања садржаја,* биће презентовани начини пресретања садржаја и идентификационих података мобилних уређаја као и методологија откривања и заштите.

У четвртом поглављу *Безбедносни аспекти и недостатци у 4G/LTE мобилним комуникационим мрежама,* који представља срж овог мастер рада биће размотрени безбедносни ризици и по свим сегментима мрежа у сладу са моделом анализи, као и методе превенције.

На крају у закључку су сублимирани сви резултати рада, као и конкретни закључци и смернице за наставак истраживања.

1. ЕВОЛУЦИЈА МОБИЛНИХ КОМУНИКАЦИЈА

Комуникација представља основу односа међу људима, тако да човек данас има потребу за брзом, свеобухватном и флуентном комуникацијом без обзира на место и време. Овакав вид комуникација свакако мора да буде мобилан и да пружа велики број сервиса. Давно је прошло време када су комуникације биле само пренос кратких порука и гласа као основе комуникације. Модерна комуникација представља скуп сервиса и услуга које су омогућене у оквиру WWAN (*енг. Wireless Wide Area Network*) мрежа чији су саставни део и мобилне комуникационе мреже.

Мобилна радио комуникација захтева да бар један од учесника у вези буде покретан, односно мобилан. Комуникације у правом смислу почеле су своју еволуцију од 24. маја 1844. године када је *Samuel Morse* тестирао први телеграфски систем на релацији Балтимор – Вашингтон у САД, а наведени датум се бележи као датум настанка електричних комуникација. Појаву бежичних телекомуникација условили су откриће осцилаторне природе електричних оптерећења (*Joseph Henry*), математичка интерпретација електромагнетних појава (*J.C. Maxvell*) и ка крају откриће и детекција електромагнетних таласа (*Heinrich Hertz*). Први патент из области бежичних комуникација регистровао је 1897. године *Gugielmo Marconi* и односи се на бежичну телеграфију. Док је права радио комуникација у јавном саобраћају изведена 1927. године.

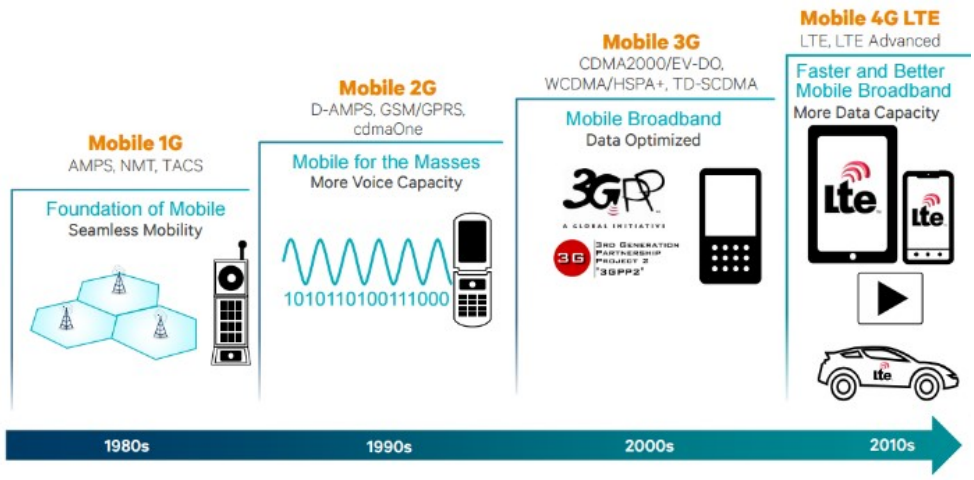
Мобилни комуникациони систем какав данас познајемо развија се кроз неколико генерација. Тренутно се активно користе системи друге, треће и четврте генерације. Док се системи пете генерације увелико развијају и тестирају.

Основа за почетак анализе и разматрања огледа се у Шаноновом закону (*Shannon's Law*) који описује техничке могућности и ограничења преноса података.

$$C = W \cdot n \cdot \log_2(1 + SNR) \qquad (1.1)$$

C представља капацитет канала преноса, *W* представља ширину канала, *n* представља коефицијент добитка антене, док *SNR* представља однос сигнал/шум. Једначином (1.1) у најкраћим цртама можемо описати све параметре које утичу на капацитет преноса у односу на искоришћење спектра и карактеристику антене.

На слици 1 приказана је еволуција система мобилних телекомуникација од аналогних 1G мрежа до савремених 4G мрежа кроз призму могућности и технологија.



Слика 1 Еволуција мобилних комуникационих система[1]

У табели 1 представљени су основни параметри мобилних комуникационих мрежа хронолошки по развоју кроз набрајање, капацитета, технологија, стандарда и типа приступне мреже.

Генерација мреже/Параметри	1G	2G	3G	4G
Почетак рада - Локација	1980-е - САД	1993 - Финска	2001 - Јапан	2009 - Јужна Кореја
Технологија	AMPS (Advanced Mobile Phone System), NMT, TACS	IS-95, GSM	IMT2000, WCDMA	LTE, WiMAX
Приступна мрежа	FDMA	TDMA, CDMA	CDMA	CDMA
Тип switching-a	Circuit switching	Circuit switching for Voice and Packet switching for Data	Packet switching except for Air Interface	Packet switching
Брзина преноса података	2.4 Kbps to 14.4 kbps	14.4 Kbps	3.1 Mbps	100 Mbps
Специјалне моћгућности	Први бежични мобилни систем	Дигитализована верзија 1G система	Дигитални широкопојасни систем са повећањем брзине преноса	Велике брзине преноса, потпуно IP систем
Карактеристике	Пренос аудиа	Више корисника на истом каналу	Мултимедијални садржаји, видео позив	Велика прзина преноса, стримовање садржаја у реалном времену
Могућност преноса	Аудио	Аудио и подаци	Аудио и подаци	Аудио и подаци
Интернет сервиси	Не	Ускопојани	Широкопојани	Широкопојасни велке брзине

[1] Преузето са https://www.qualcomm.com/media/documents/files/the-evolution-of-mobile-technologies-1g-to-2g-to-3g-to-4g-lte.pdf

Ширина канала преноса	Аналогини канал	25 MHz	25 MHz	100 MHz
Фреквенцијски опсези	800 MHz	GSM: 900MHZ, 1800MHz CDMA: 800MHz	2100 MHz	850 MHz, 1800 MHz
Тип канала	Ускопојани	Ускопојани	Широкопојасни	Ултра широкопојасни
Носећа фреквенција	30 KHZ	200 KHz	5 MHz	15 MHz
Предности	Једноставна архитектура мреже	Мултимедијални садржаји (SMS, MMS), приступ интернету, увођење SIM картица	Висока безбедност, интернационални роминг	Global mobility Велика брзина преноса, MIMO технологија
Мане	Лимитиране могућности, небезбедно, кратко трајање батерије, гломазни уређаји	Ограничена покривеност мреже, мали проток података	Велика потрошња енергије, слаба мрежна покривеност, висока цена лиценце за спектар	Комплексни хардверски захтеви, компликована имплементација мреже
Апликације	Позив	Позив, SMS, ограничен приступ интернету	Видео конференсинг, мобилна ТВ, GPS	Велики спектар апликација и уређаја, високе перформансе и хадрвера и софтвера

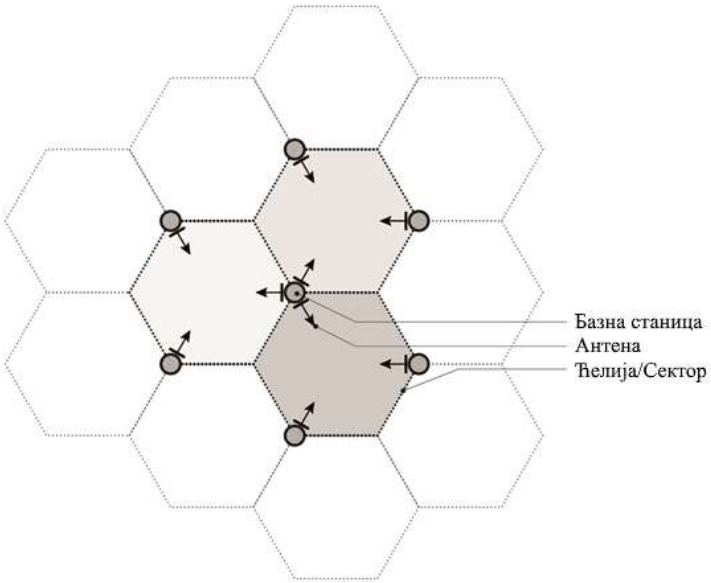
Табела 1 Преглед основних карактеристика мобилних комуникационих мрежа

Безбедносни аспекти у развоју мобилних мрежа еволуирали су као и мреже. Код мобилних мрежа прве генерације заштита није постојало. За комуникације је коришћен цео комуникациони канал, који је могао да се омета или слуша без ограничења. У наредним генерацијама доста труда је уложено у заштиту комуникације што ће бити детаљније објашњено у наредним поглављима.

1.1 Еволуција мобилних комуникационих система пре LTE

Први комерцијални бежични систем преноса уведен је у употребу још давне 1946. године. FCC (*енг. Federal Communication Commission*) је у САД-у одобрио систем компаније AT&T за бежичну комуникацију и то се сматра почетком ере данашње мобилне комуникационе мреже. Овај концепт је увео систем могућности употребе исте фреквенције на различитим локацијама (*cellular concept*) и на тај начин омогућио формирање посебних ћелија које користе исте ресурсе за комуникацију. Овај систем је финдамент данашњег модерног мобилног система телекомуникација.

Мобилни системи прве генерације увели су аналогни ћелијски пренос гласа, уз способност хандовер-а и роминг-а у оквиру мреже, али нису биле у могућности да функционишу на интернационалном нивоу [1].



Слика 2 Ћелијска структура мреже [1]

Аналогни системи преноса нису могли да задовоље растуће потребе система са готово ниједног аспекта па је већ средином осамдесетих година двадесетог века у Европи створен GSM (*енг. Global System for Mobile Communications*) пројекат који је за циљ имао унапређење мобилне мреже са становишта могућности и дигиталне технологије која је нудила доста више од постојеће аналогне. 1991. године уводи се први 2G систем који омогућава пренос мале количине података. Инкорпориране су дигиталне технологије вишеструког приступа TDMA (*енг. Time Division Multiple Access*) и CDMA (*енг. Code Division Multiple Access*) , које су увеле већу спектралну ефикасност, пренос података и обезбедиле како национални тако и интернационални роминг. У Европи је успостављен GSM систем, који је омогућавао пренос аудија, SMS (*енг. Short Message Service*) порука, GPRS (*енг. General Packet Radio Services*) сервис за пренос података брзином до 9.6 kbps.

2G мрежа се развијала преко 2,5G мреже која је у односу на основу имала GPRS сервис, касније и на EDGE (*енг. Enhanced Data for GSM Evolution*) мрежу која се још назива и 2,75G. Са EDGE технологијом почиње мобилни широкопојасни приступ, где се остварују брзине до 384kbps, техничком смислу она само модификује већ постојећу мрежу, али чини значајан напредак. У употребу се уводи савременије кодовање, повећава ефикасност преноса података по временском слоту, као и брзина преноса, која је већа када су радио услови бољи. Стандарди за развој мреже су били различити у различитим деловима света. Међутим мобилна интероперабилност требала је да омогући да претплатник може да равноправно употребљава свој телефон у свим деловима света. На тај начин уводи се појам сервиса у мобилне телекомуникације и он остаје основа за развој односно уводи стандарде који су важећи на планетарном нивоу, док технологије требају да омогуће употребу истих независно

ко их развија и употребљава. Стандардизација улази под окриље ITU (*енг. International Telecommunication Union*) која ће надање бити носилац стандардизације и развоја сервиса и система мобилних телекомуникација [1].

Нови концепт који је дефинисан почетком 90-их година 20. века је уједно и основа за трећу генерацију – 3G (*енг. Third Generation*) мреже које данас увелико користимо. ITU је дефинисала следеће захтеве за нову генерацију мобилних телекомуникација са акцентом на протоку података, по следећем:

- Висока мобилност (брзина ~ 120 km/h) – минимални проток од 144kbps у руралном окружењу;
- Потпуна мобилност (брзина мања од 120 km/h) - минимални проток од 384kbps у урбаном окружењу;
- Ограничена мобилност (брзина мања од 10 km/h) - минимални проток од 2Mbps унутар зграде или на мањем, ограниченом отвореном простору [2].

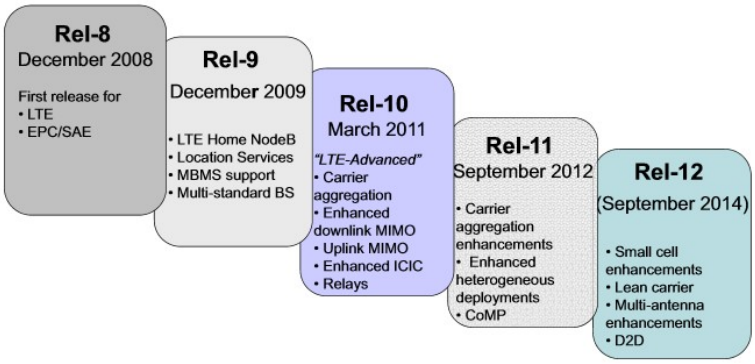
Трећа генерација сублимира више различитих стандарда који су дефинисани од стране ITU у оквиру партнерског пројекта 3GPP (*енг. 3rd Generation Partnership Project*). Усвојен је UMTS (*енг. Universal Mobile Telecommunications System*) као званична технологија за реализацију 3G мобилне мреже. Због потреба подршке великим брзинама преноса података преносни део приступне мреже је реализован у WCDMA (*енг. Wideband Code Division Multiple Access*) широкопојасној технологији у фреквенцијском FDD (*енг. Frequency Division Duplex*) или временском TDD (*енг. Time Division Duplex*) дуплексу. WCDMA-FDD се користи за веће покривање квалитетнијим сервисом (макро и микро ћелије), док за мање локалне зоне (микро и пико ћелије) WCDMA-TDD. Контролу транспорта врши ATM (*енг. Asynchronous Transfer Mode*) протокол.

Еволуцијом WCDMA настала је UMTS HSPA (*енг. High Speed Packet Access*) технологија која се огледа у два протокола. Први је HSDPA (*енг. High Speed Download Packet Access*) дефинисан у оквиру 3GPP *Release 5* и HSUPA (*енг. High Speed Upload Packet Access*) дефинисан у оквиру 3GPP *Release 6*. надање HSDPA терминали се могу поделити у 12 категорија са протоцима од 0.9Mbps до14.4Mbps. надање HSUPA уводи низ побољшања у односу на HSDPA, као што су боља покривеност на *uplink*-у за пренос података већим брзинама, до 5.76Mbps [3].

1.2 Основе 4G/LTE мобилних комуникационих мрежа

Мобилне мреже четврте генерације – 4G су продукт потражње тржишта за све већим могућностима у смислу капацитета преноса податак и приступа широкопојасном интернету.

ITU је у својим издањима од 2008. године отпочела активну спецификацију мобилних мрежа 4. генерације.

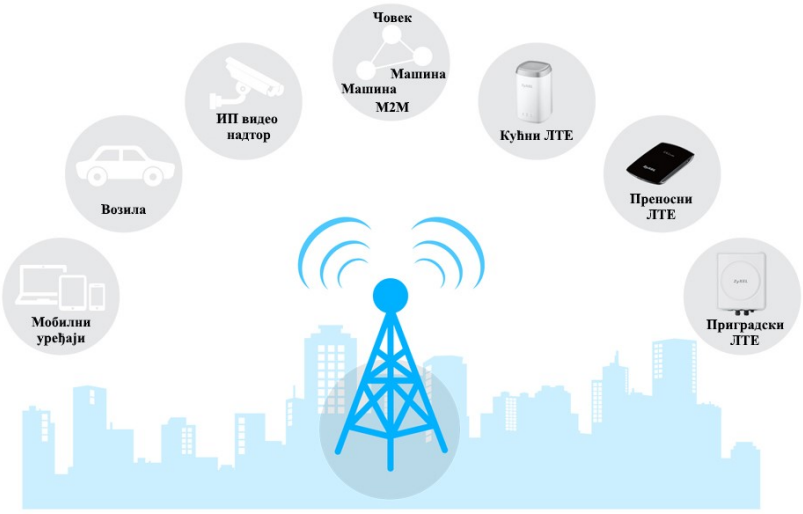


Слика 3 Спецификација захтева за LTE мреже у издањима 3GPP [1]

На слици 3 је приказана генеза захтева и развој мреже. Већ 2009. године у Јужној Кореји је успостављен први 4G функционалан систем комуникација, који је најавио брзу имплементацију нових технологија на глобалном нивоу.

У складу са захтевима ITU од 2008. године мобилне мреже 4. генерације треба да омогуће следеће могућности:

- Свеобухватну IP (*all IP*) мобилну подршку,
- Приступ са више различитих врста уређаја – мобилних уређаја (телефон, лаптоп, таблет, рачунар...),
- IP телефонија,
- QoS (*енг. Quality of Service*),
- Компатибилност са претходним генерацијама мобилних мрежа,
- Брзине преноса од 100Mbps за кориснике који се крећу великим брзинама до 1Gbps за стационарне кориснике,
- Динамичка расподела ресурса због подршке великом броју корисника,
- Промењљива ширина канала од 5-20MHz, опционо до 40 MHz,
- Непрекидна конекција на мрежу (*handover, roaming*),
- Мултимедијални сервиси високог квалитета [4].



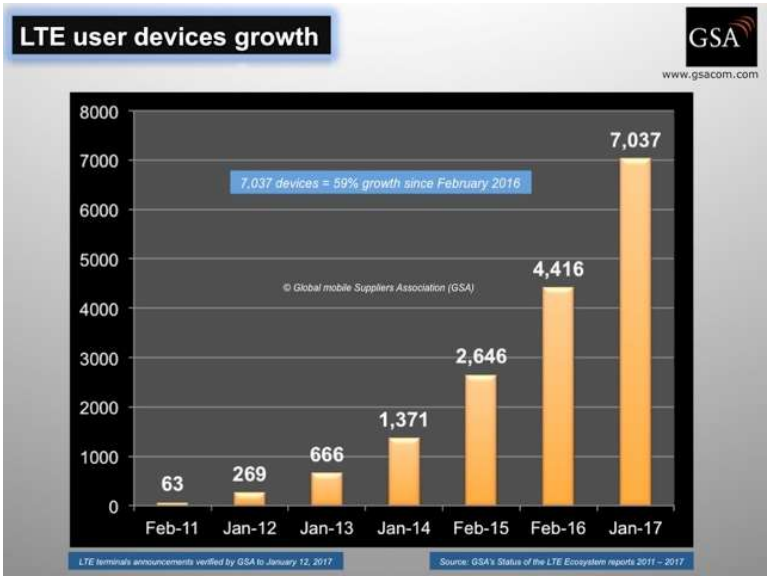
Слика 4 Могућности мобилних мрежа 4. генерације

4G мобилне мреже развијане су у два правца, WiMAX (*енг. Worldwide Interoperability for Microwave Access*) и LTE. WiMAX је серија стандарда IEEE 802.16e и први пут је имплементиран у Јужној Кореји 2007. Године. Други систем LTE је кроз 3GPP наставио развој већ постојећих система GSM/EDGE/UMTS/HSPA. Развијен је нови интерфејс E-UTRA (*енг. Evolved UMTS Terrestrial Radio Access*). Две наведене технологије нису биле заправо 4G мреже јер су омогућавале протоке далеко мање од 1Gbps и још се називају и 3.9G мобилним мрежама.

Да би се постигли захтевани стандарди развијен је програм IMT-Advanced (*енг. International Mobile Telecommunications-Advanced*) који је обухватио Mobile WiMAX Release и LTE Advanced. LTE Advanced је предложен од стране јапанске компаније NTT DoCoMo, стандардизован је 2011. године од стране 3GPP. Ради у фреквенцијским опсезима 800, 900, 1800, 2100 и 2600MHz (такође је дефинисана могућност коришћења опсега 450 и 3600MHz), са каналима ширине 5-20MHz, као и могућношћу проширења на 40MHz.

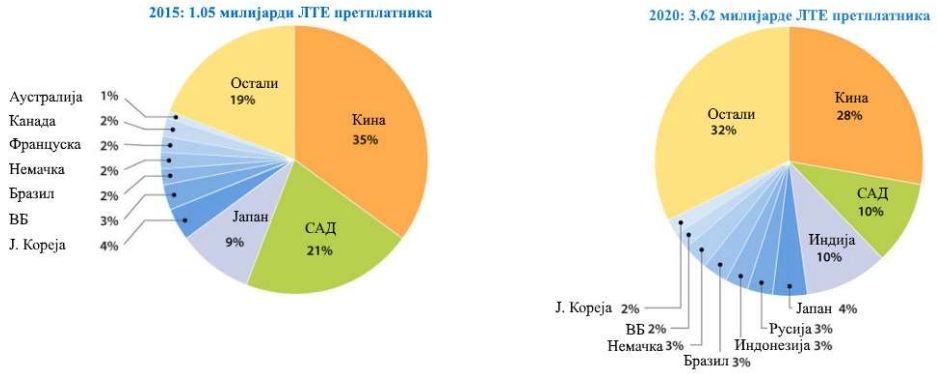
1.3 Развој LTE мрежа кроз статистичке показатеље

Развој LTE мрежа и повећање броја претплатника најбоље се може представити кроз број уређаја који пружају подршку. Наиме тренутно у употреби има преко 7000 уређеја који се користе у LTE мрежи, што имплицира милионски број корисника. На слици 5 која је преузета са сајта *gsacom.com* представљен је радст броја уређаја од 2011. до 2017. године, раст броја уређаја је готово експоненцијалан, што директно имплицира и раст тржишта.



Слика 5 Приказ раста броја LTE уређаја[2]

У различитим изворима могу се пронаћи пројекције броја претплатника у оквиру LTE мрежа, једно од интересантних је истраживање фирме Ovum, на слици 5 приказан је раст броја претплатника од 2015. До 2020. године. Може се закључити да и број корисника расте као и број уређаја који користе. Предњаче земље које су најмногољудније, али и технолошки најнапредније, пре свега НР Кина и САД.



Слика 6 Анализа броја претплатника у оквиру LTE мрежа као и предикција раста корисника за 2020. годину[3]

1.4 Стање LTE мрежа у Републици Србији

На основу Прегледа тржишта електронских комуникација у Републици Србији [5] у и Покривености сигналом мобилне телефоније у Србији [6], односно извештајима које

[2] Преузето са https://gsacom.com/

[3] Преузето са https://www.ovum.com/press_releases/global-lte-subscriptions-pass-1-billion/

квартално издаје Регулаторна агенција за електронске комуникације и поштанске услуге - РАТЕЛ можемо анализирати стање у мобилним комуникацијама четврте генерације. Услуге мобилне телефоније пружају пет оператера од тога три имају лиценце за коришћење електромагнетног спектра док два раде као виртуални оператери. Виртуални оператери Mundio mobile и Globaltel још увек немају значајније учешће на тржишту па неће бити анализирани у овом прегледу. Лиценце за коришћење електромагнетног спектра имају следећи оператери:

- Предузеће за телекомуникације Телеком Србија а.д. (МТС),
- Теленор,
- Вип мобиле.

Са око 9 милиона претплатничких бројеве колико је тренутно активно преглед тржишног удела је следећи: 47% Телеком Србија, 31% Теленор и 22% Вип мобиле. Не постоји податак колики проценат корисника користи мобилне уређаје који подржавају мреже 4. генерације.

За анализу безбедносних аспеката најважнији су подаци о Фреквенцијским опсезима у којим раде уређаји, базне станице и покривеност мреже. Наведени подаци су посебно важни када се анализира могућност пресретања комуникација и садржаја.

Оператери користе GSM, UMTS и LTE технологије за рад у следећим фреквенцијским опсезима:

- 791-821/832-862 MHz,
- 890-915/935-960 MHz,
- 1710-1780/1805-1875 MHz,
- 1900-1915 MHz,
- 1920-1965 MHz/ 2110-2155 MHz.

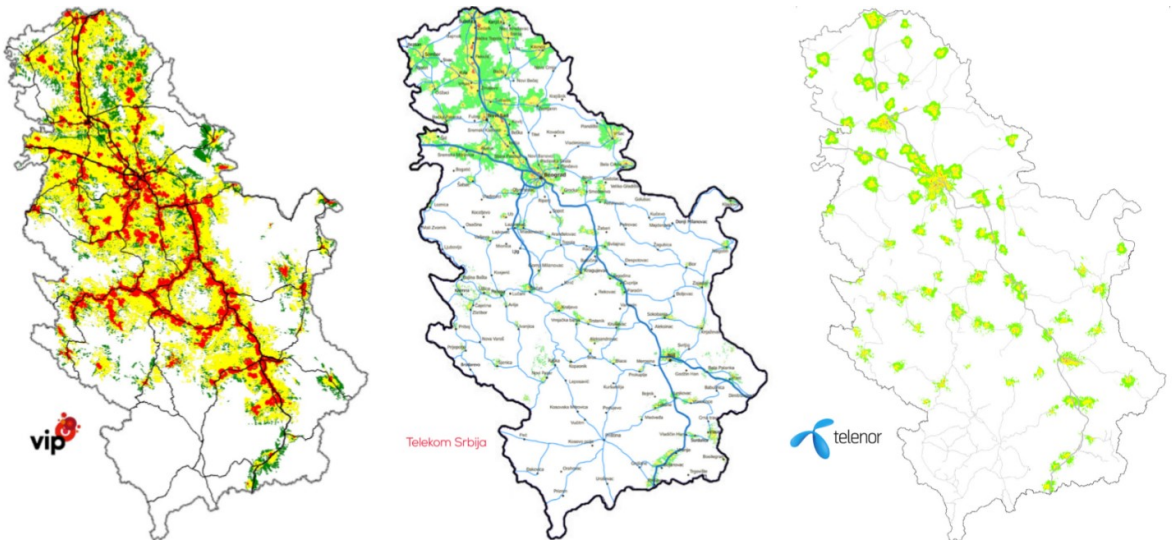
У оквиру LTE мрежа оператери имају велики број базних станица:

- Телеком Србија – 484,
- Теленор – 833,
- Вип мобиле – 1012.

Из наведеног се види да оператери имају различити приступ начину покривања територије базним станицама. Једни се фокусирају на локације где је већински насељено становништво док други покривају територију (главни путни правци, шира подручја ван градских језгара). На основу RSRP>-110dBm покривеност територије је заступљена по следећем:

- Телеком Србија – 15,64%,
- Теленор – 9,95%,

- Вип мобиле – 34,40%.



Слика 7 Упоредни приказ покривености територије Р. Србије сигналом LTE мобилне телефоније [6]

2 ТЕОРИЈСКИ АСПЕКТИ ВАЖНИ ЗА АНАЛИЗУ БЕЗБЕДНОСТИ LTE МОБИЛНИХ МРЕЖА

Познавање архитектуре мреже је основа за проучавање безбедносних проблема и могућих препорука како унапредити систем заштите.

Архитектура LTE мрежа у основи је дефинисана у 8. издању стандарда и унапређена од стране 3GPP (*Release 8*). Као што је претходно наведено ова мрежа није била у потпуности четврте генерације је није задовољавала основне захтеве већ је третирана као 3.9Г. Представљена је основа савремене мреже кроз еволуирани пакетни систем EPC (*енг. Evoluated Packet Core*). 3GPP у свом 10 издању (*Release 10)* представља први пут мобилну мрежу 4. генерације која се назива LTE Advanced. Ово је у ствари напредни LTE стандард и он треба да обезбеди следеће [1]:

- радну брзину преноса података за долазни канал (*DL – Down Link*) до 1Gbps, а за одлазни канал (*UL – Up Link*) до 500 Mbps,
- фреквенцијски опсег од 70 MHz-а за DL и 40 MHz за UL,
- двоструко већа брзина преноса података на рубу ћелије у односу на LTE,
- просечна брзина преноса података по кориснику 3 пута већа у односу на LTE.

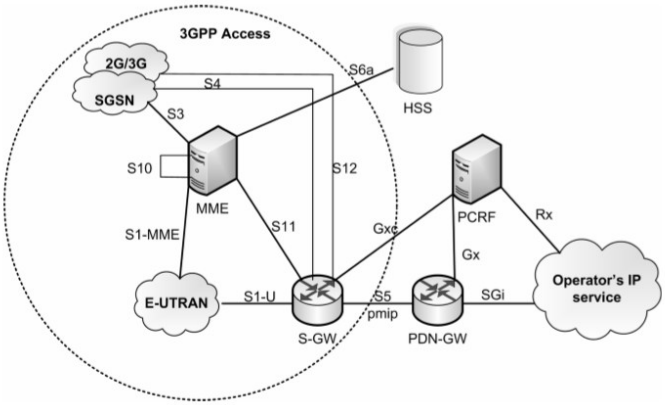
Обзиром на пакетни систем размене података, који је потпуно еволуирао у односу на претходне генерације мобилних мрежа посебна пажња треба да се обрати на пренос говора преко LTE напредних мрежа. Напредне LTE мреже захтевају и одговарајућу архитектуру, односно еволуирану архитектуру система SAE (*енг. System Architecture Evolution*). Пренос говора у складу са пакетском структуром мреже је могућ коришћењем VoLTE (*енг. Voice over LTE*) који представља коришћење VoIP (*енг. Voice over IP*) или прелазак на 2G/3G мреже ради успоставе позива.

Поред наведеног важно је додати да се кодовање и пренос сигнала врши адаптивним модулационим техникама, квадратурном амплитудском модулацијом QAM-N (*енг. Quadrature Amplitude Modulation*) која се прилагођава квалитету преносног линка. Такође се користе и технике вишеструког приступа применом ортогоналног мултиплексирања OFDMA (*енг. Ortogonal Frequency Division Multiple Access*), што укључује технике вишеслојног преноса MIMO (*енг. Multiple Input Multiple Out*) .

2.1 ОСНОВИ АРХИТЕКТУРЕ

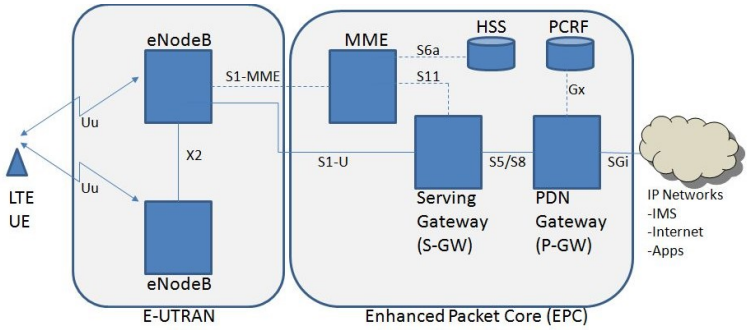
Референтни модел архитектуре мреже је основа за даље проучавање и анализу, дефинише функционалне целине и референтне тачке интероперабилности целина. Систем се састоји од

две целине: приступна мрежа и језгро мреже. Приступна мрежа се назива E-UTRAN (*енг. Evolved UMTS Terrestrial Radio Access Network*), док је језгро мреже назива еволуирано пакетно језгро, EPC. Наведене целине представљају EPS (*енг. Evaluated Packet System*).



Слика 8 LTE референтни модел [7]

LTE мрежа је E2E IP (*енг. End To End IP*) што значи да комплетан саобраћај између мобилног уређаја (*UE - Eser Equipment*), до јавне комуникационе мреже, PDN (*енг. Public Data Network*), преноси се по IP протоколу у оквиру EPS-а који пружа приступ ка спољним мрежама, управља функцијама безбедности (аутентификација, додела сигурносних кључева), ажурира претплатничке информације, тарифира, врши наплату и организује мобилност ка другим мрежама. E-UTRAN обавља све функције које су у вези са радио приступом за активне терминале. Састоји се од базних станица, *eNB* (*енг. e Node B*) [7].



Слика 9 Функционална шема LTE архитектуре мреже[4]

На слици 9 је приказана функционална шема архитектуре мреже. Основне компоненте мреже представљају мобилни уређај, UE и базна станица, eNB која омогућава радио канал за пренос података. Када говоримо у језгру мреже, EPC исто је састављено од више елемената. Један од одновних елемената је MME (*енг. Mobility Management Entity*) компонента која

[4] Преузето са http://rcrlte.wpengine.com/wp-content/uploads/2013/01/Network-diagram.jpg

управља сесијама и контролише различите функције. У њему се одвијају и безбедносне функције које су задужене за аутентификацију и проверу идентитета претплатника. Незаобилазна је функција QoS која прати параметре квалитета сервиса. Такође врло важна функција је и праћење локације корисника у тренуцима када корисник није активан.

Следећа компонента представља базу података о кориснику и назива се је HSS (*енг. Home subscriber server*), састоји се из два дела HLR (*енг. Home Location Register*) и AuC (*енг. Authentication Center*). Овде се чувају информације о идентификацији корисника у облику IMSI (*енг. International Mobile Phone Subscriber*) или MSISDN (*енг. Mobile Subscriber Integrated Services Digital Network*) бројева, информације о корисничком пакету који плаћа и QoS информације. Поред наведених у HSS су и информације о аутентификацији и ауторизацији претплатника, као и локацији и активном S-CSCF (*енг. Serving - Call Session Control Function*). SGW (*енг. Signaling Gateway*) обавља конверзију протокола и обезбеђује интерфејс ка сигнализационој равни CS (*енг. Circuit switching*) мреже, тачније представља терминал између PS (*енг. Packet switching*) и E-UTRAN. PDN GW (*енг. Public Data Network Gateway*) представља спојну тачку EPC и екстерне IP мреже, уједно рутира податке у оба смера. Обавља и додатне функције као што су алокација IP адреса/ IP префикс, као и функције безбедности, контроле и тарифирања. PCRF (*енг. Policy and Charging Rules Function*) је компонента се бави проблемом сигурности и заштите као и постављањем QoS параметара за сваку сесију, функције врши у оквиру две секције PDF (*енг. Policy Decision Function*) који је задужен за безбедност и CRF (*енг. Charging Rules Function*) [7].

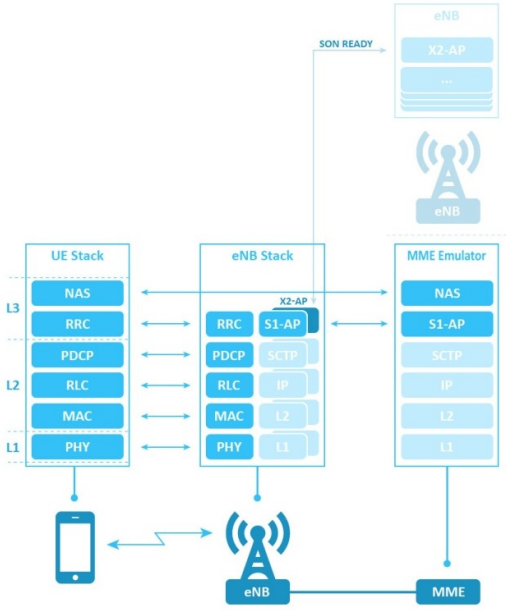
2.2 ПРОТОКОЛИ КОМУНИКАЦИЈЕ И КОМУНИКАЦИОНИ ИНТЕРФЕЈСИ

Приступање капацитетима мобилне мреже уређајима који нису саставни део мреже и који представљају специјалну опрему намењену прикупљању података могућа је једино ако се користе већ постојећи протоколи комуникације који се користе у редовном одвијању саобраћаја, како претплатника са мрежном инфраструктуром тако и интерних чинилаца мреже. Протоколи могу да се користе за декодовање пресретнутог саобраћаја или за директно преузимање података како од мрежне инфраструктуре тако и са мобилних уређаја.

На слици 10 приказани су протоколи комуникације по нивоима који су синхронизовани у зависности од нивоа. Најзначајни међу њима су:

- Физички слој – L1, он преноси све информације од транспортног нивоа у етар. Организује адаптацију линка, контролу снаге, прелаз са ћелије на ћелију и остале функције.

- Транспорни слој – L2, у ком MAC (*енг. Media Access Control*) подслој који подешава логички канал за RLC (*енг. Radio Link Control*), такође подешава HARQ (*енг. Hybrid Automatic Repeat-reQuest*) корекцију грешака, приортете у каналу између мобилних уређаја. RLC преноси PDCP (*енг. Packet Data Convergence Protocol*) и PDU (*енг. Protocol Data Unit*), може да ради у три режима рада. PDCP врши две функције, за RRC (*енг. Radio Resourse Control*) омогућава транспорт података са шифровањем и заштитом, док за IP врши транспорт пакета са заштитом и компресијом.
- Мрежни слој – L3, између осталог брине о емитовању информација о систему који се односе на приступни слој и транспорт NAS (*енг. Non-access stratum*) порука, позивање, успостављање и прекид везе, управљање кључевима за енкрипцију сигурности, прелазак са једне на другу базну станицу, мерења везана за inter-RAT (*енг. Radio Access Technology*) функционалност и остало.



Слика 10 Комуникациони протоколи по нивоима[5]

Посебно је важан NAS протокол који је директна веза између мобилног уређаја и MME, као и IP протокол.

Протоколи комуникације своје функције врше кроз два интерфејса, односно кориснички и контролни план:

- S1 интерфејс – се може описати кроз две функционалности кориснички S1-U *(S1 user plane)* и контролни план S1-MME *(S1 control plane).* Први обавља

[5] Преузето са https://www.is-wireless.com/wp-content/uploads/2013/06/protocol_stack_v12-06.jpg

комуникацију између базне станице (*eNode-B*) и S-GW, други обавља комуникацију између базне станице и MME. Потпуно је базиран на IP протоколу.

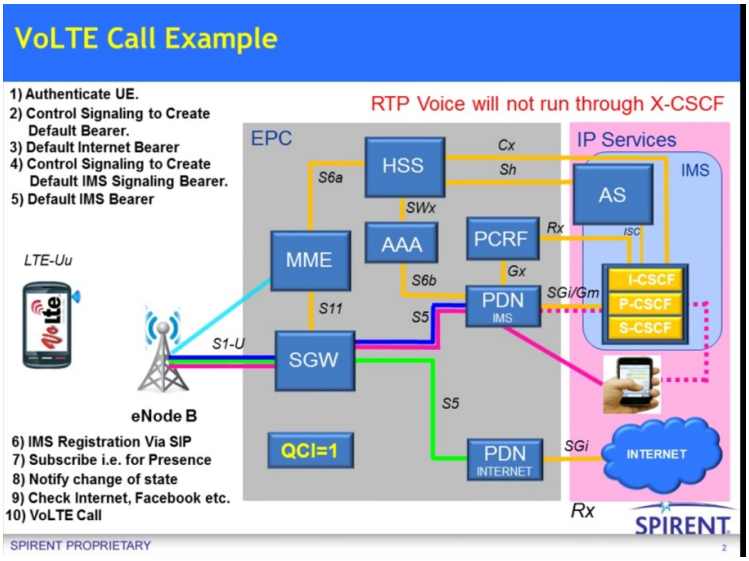
- X2 интерфејс – се такође може описати кроз две функционалности, кориснички X2-U *(X2 user plane)* и контролни план X2-CP *(X2 control plane).* Обавља комуникацију између базних станица и посебно је значајан код приступа мрежи од стране лажних базних станица и осталих малициозних уређаја. Базиран је на SCTP (*енг. Stream Control Transmission Protocol*) протоколу [7].

2.3 СЕКВЕНЦА УСПОСТАВЕ ПОЗИВА VOLTE

Аутентификација мобилног уређаја на мрежу је критичан и комплексан моменат је посебно важан са становишта безбедности. У том поступку се врши размена идентификационих података уређаја са мрежом и може се злоупотребити од стране лажних базних станица за прикупљање идентификационих података о мобилном уређају. Овај поступак ће бити накнадно образложен у наредним поглављима.

Посебан изазов у комуникационим мрежама 4. генерације представља пренос комуникационих сервиса, пре свега говора, SMS порука. Један од најважнијих параметара безбедне комуникације је пренос говора и SMS порука у реаланом времену. Наиме у старијим генерацијама пренос је вршен комутацијом кола преко PSTN (*енг. Public Switched Telephone Network*) мрежа. У IP системима подаци треба да се дела на комутационе пакете и тако транспортују преко мобилне мреже у реалном времену. Овакви сервиси су већ развијени у оквиру различитих интеренет сервиса који се односе на VoIP али имајуману јер не могу да гарантују квалитет преноса говора. У мобилним мрежама квалитет мора да постоји и управо због тога је развијен VoLTE. Пренос овог вида података је реализован преко SIP (*енг. Session Initiation Protocol*) и RTP (*енг. Realtime Transfer Protocol*) протокола у стандардним VoIP системима.

У LTE комуникацијама за пренос говора се користи IMS (*енг. IP Multimedia Subsystem*) говорни сервис. Овај сервис мора да обезбеди квалитет минимално као у 2G/3G мрежама и више. На овај начин се успоставља мултимедијална сесија у реалном времену. IMS технологија је базирана на SIP протоколу. Успостављање позива је приказано кроз секвенцу од 10 корака на слици 11. Успостава позива обухвата велики број корака са различитим сигурносним процедурама, тако да је за сада готово немогуће пресретање овог вида комуникације, односно садржаја комуникација.



Слика 11 VoLTE секвенца успостављања позива[6]

[6] Преузето са http://www.3glteinfo.com/wp-content/uploads/2013/01/Voice-over-LTE-VoLTE-Signalling.png

3 МЕТОДЕ ЗАШТИТЕ КОМУНИКАЦИЈА И ТЕХНИКЕ ПРЕСРЕТАЊА САДРЖАЈА

Пресретање саобраћаја мобилних комуникација постоји од када и сама комуникација. Паралелно са методама пресретања развијале су се и методе заштите комуникација. У почетку се комуникација одвијала без заштите и могла је да буде пресретнута без било каквих софистицираних уређаја. Убрзо је било јасно да је потребно заштити претплатнике од малициозних намера како појединаца тако и од разних интересних група. Како су напредовале генерације мрежа тако се развијала и заштита односно методе заштите и пресретања. Сигурно је да произвођачи опреме морају да имплементирају захтеване стандарде, али исто тако случајно или намерно увек постоје одређени безбедносни пропусти који се накнадно откривају и побољшавају новим верзијама софтвера и фирмвера. Ти безбедносни пропусти су врата за приступ у мрежу од стране оних који делују ван ингеренција мобилних оператера. Да би неки уређај могао да приступи мрежи мора да буде компатибилан са стандардима који су имплементирани и као такав не сме да остави траг свога деловања. На тај начин долазимо и до основне поделе пресретања саобраћаја у зависности од активности уређаја [21]:

- Активно пресретање,
- Полуактивно (хибридно) пресретање,
- Пасивно пресретање.

Свака од наведених метода има своје предности и мане као и технолошке изазове које треба да испуни да би била функционална. Методолошки гледано све технике пресретања користе систем приступа "*MtM – Man in the Middle*", где се уређај за пресретање налази између мрежне инфраструктуре и мобилног уређаја који је циљ напада.

Поред наведене постоји још различитих подела техника напада у зависности од начина приступа мобилном уређају, може се издвојити техника нарушавања безбедности *frameworka* уређаја, и то по следећем:

- Хардверске технике (преправка уграђеног хардвера уређаја),
- Типске технике (прикупљање података из етра преко *WiFi* мреже или *backdoor),*
- Корисничке технике (малициознне апликације које заобилазе системе заштите) [9].

Могућности пресретања саобраћаја мобилних комуникација су различите и зависе од више параметара, од којих су најважнији следећи:

- Генерација мобилне мреже,

- Врста пресретања (комплетна комуникација или само идентификатори мобилног уређаја),
- Техничке и тактичке могућности.

Поред наведеног могу се дефинисати и неколико врста напада, од којих су најзначајнији: прислушкивање, клонирање мобилне мреже, преузимање контроле над уређајем или делом мрежне инфраструктуре, крађа података са мобилног уређаја, слање лажних података и сигнала, крађа корисничких података и други.

Све технике пресретања имају за циљ да угрозе претплатнике, а да онај ко врши пресретање података буде невидљив у систему. Наравно постоје и институције које легално уз прибављену дозволу надлежних судова могу да пресрећу садржај мобилне телефоније уз употребу техничких средстава.

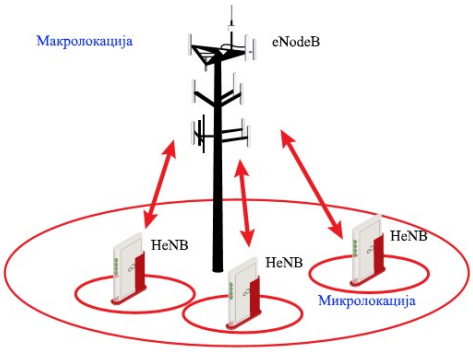
Да би се пресретање саобраћаја операционализовало потребно је познавати различите параметре како мобилне мреже тако технологија које се користе, као и техника заштите комуникације.

3.1 ПРИСТУПНА ИНФРАСТРУКТУРА МОБИЛНИХ МРЕЖА ЧЕТВРТЕ ГЕНЕРАЦИЈЕ

Приступна инфраструктура у LTE и напредним LTE мрежама налази се у E-UTRAN сегменту мреже и физички се огледа у базним станицама или eNode B. Мобилни уређај приликом првог регистровања на мрежу мора да да своје идентификаторе. Технологија приступа је принципијално иста за све типове мрежа. Наравно еволуција мрежа је условила да се са порастом генерације укључују и нове методе, пре свега размене кључева и вишеструке идентификације. У основи најважнија су два параметра то су IMSI и IMEI (*енг. International Mobile Equipment Identity*) бројеви. Први је идентификатор SIM (*енг. Subscriber Identity Module*) картице, док је други идентификатор мобилног уређаја. Важни параметри који су такође битни за пресретање саобраћаја су и TMSI (*енг. Temporary Mobile Subscryber Identity*) идентификатора и MAC адреса мрежног уређаја (*WiFi - Wireless Fidelity* или *LAN - Local Area Network*) чија ће употреба накнадно бити образложена.

Базне станице као физички порт за приступ мрежи могу бити различитог карактера. Углавном се препознају као антенски системи на антенским стубовима или на доминантним објектима, међутим постоје просторије које оне не могу да се покрију сигналом, тако да се користе мале базне станице (*femtocells, picocells, microcells)*. Овај тип базних станица у LTE мрежама се назива HeNB (*енг. Home eNodeB*) и има исте могућности као и стандардна базна станица само има умањене перформансе по питању покривености. За разлику од мрежа

претходних генерација у којима су овакве базне станице служиле само као репликатори сигнала, HeNB је потпуно функционално равноправна са осталим базним станицама [8].



Слика 12 Приступна инфраструктура

Поред инфраструктуре мобилне мреже као приступна инфраструктура може да се користи и WiFi који данас има сваки мобилни уређај. Приликом пресретања мобилних комуникација у активном или полуактивном режиму пресретања уређај за пресретање је уствари клонирана базна станица, у зависности од карактеристика може да буде класична или мала базна станица. Директан приступ мрежи се врши преко X2 интерфејса. У табели 2 приказани су технички параметри базних станица у различитим условима употребе.

	Карактеристике базне станице			
	У затвореном простору	**Микроћелија**	**Урбана средина**	**Велика брзина кретања**
Тип уградње	Indoor Hotspot	Urban Micro	Urban Micro	Rural Micro
Модел канала	InH	UMi	UMa	Uma
Носећа фреквенција	3.4 GHz	2.5 GHz	2.0 GHz	0.8 GHz
Даљина између базних станица	60 m	200 m	500 m	1732 m
Брзина терминала	3 km/h	3 km/h	30 km/h	120 km/h
Распоред корисника	100% унутра	50% унутра, 50% напољу	100% унутра	100% напољу
Висина антене БС	6 m	10 m	25 m	35 m
Појачање антене БС	0 dBi	17 dBi	17 dBi	17 dBi
Излазна снага БС	21 dBm/20MHz	44 dBm/20MHz	49 dBm/20MHz	49 dBm/20MHz
Излазна снага МУ	21 dBm	24 dBm	24 dBm	24 dBm

Табела 2 Техничке карактеристике базних станица [1]

3.2 Имплементиране методе заштите комуникације у LTE мобилним мрежама

Основни метод заштите транспорта саобраћаја у мобилним мрежама је енкрипција садржаја. Постоји више различитих врста енкрипције који су се примењивали током еволуције мобилних комуникационих система. Ако сагледамо саме почетке у аналогним системима није било енкрипције већ је комплетан садржај био отворен и могао је без

препрека да се преслушава у реалном времену. Врло брзо су произвођачи мобилних уређаја увидели да је потребно да се заштити комуникација и на тај начин је уведена енкрипција.

Постоје државне институције које имају могућност да законски, уз одобрење надлежног суда врше лоцирање претплатника, повлачење задржаног саобраћаја, преглед остварених комуникација са и без увида у садржај комуникација [10]. Овакво коришћење ресурса је регулисано на државном нивоу у оквиру законских одредби и једино државне институције могу да користе за своје потребе.

Систем заштите мобилним мрежама четврте генерације треба да анализирамо кроз процес аутентификације, ауторизације и енкрипције, односно приступа, веродостојности и интегритета [11]. Комбинацијом сва три параметра систем треба да обезбеди да корисник сигурно користи ресурсе мреже.

3.2.1 Принципи аутентификације и алгоритми енкрипције у мрежама старије генерације

Ауторизација и екнрипција су основни процеси у заштити комуникације, да би се комуникација између мобилног уређаја и мрежне инфраструктуре одвијала сигурно потребно је да се ови процеси у потпуности испоштују.

Сама аутентификација је прво била једносмерна а затим је унапређена и захтева да се оба чиниоца идентификују како би могла да равноправно размењују податке. Ово је основна тачка безбедности јер штити и претплатника и мобилног оператера од неовлашћеног упада. Такође је основна тачка за неовлашћени приступ садржају комуникације или идентификационим параметрима мобилног уређаја. Важно је познавати све типове енкрипције и аутентификације јер управо манипулација мобилним уређајем односно са наметањем одређеног вида енкрипције или прелазак на одређени ниво генерације мреже омогућава и приступ мобилном уређају. Зато ће у наредним пасусима бити појашњени основни типови алгоритама енкрипције и техника пријављивања на мрежу.

Процес екрипције саобраћаја је еволуирао као и мобилне мреже. Почеци озбиљнији системи заштите јављају се у 2G мрежама, односно имплементиран је GSM проткол [12]. Кратком анализом основних сегмената мреже можемо лако утврдити да постоји неколико елемената који су важни за заштиту. Прво и основно је SIM картица која је повезана са јединственим IMSI бројем који је састављен од 15 цифара и јединствен је на глобалном нивоу. Састоји се од MCC (*енг. Mobile Country Code*), MNC (*енг. Mobile Network Code*) и MSIN (*енг. Mobile Subscriber Identification Number*) бројева. Са друге стране мобилни уређај је опремљен са IMEI бројем који је уникатни за сваки појединачни уређај. Ова два параметра

мобилног уређаја и SIM картице су задржани у оквиру свих генерација мобилних мрежа и имају једнако важну улогу у аутентификацији. Поред наведених у SIM картици је сачувано неколико других важних бројева и то A3 алгоритам аутентификације, кључ A8 алгоритма и 128 битни K_i кључ. Пријављивање на мрежу се врши једносмерно од мобилног уређаја ка базној станици без повратне провере. Базне станице, односно неколико суседних контролише контролер BSC (*енг. Base Station Controller*) и он је спрега између мобилног уређаја и MSC-а (*енг. Mobile Switching Center*) у ком се налазе VLR (*енг. Visitor Location Register*), HLR и AuC који проверавају кључеве и све податке од мобилног уређаја и омогућавају приступ мрежи. Ово су у најкраћим цртама елементи GSM протокола који су одговорни за пријављивање на мрежу.

Приступ односно аутентификација се одвија преко A5 енкрипционог алгоритма. Процес комбинује 128-битни стохастички код који генерише AuC са кључем K_i из SIM картице и генерише 32-битни одговор. AuC такође генерише и A8 K_c 64-битни кључ који је везан за сесију у току. У зависности од мреже он се мења после сваке сесије или после одређеног времена. Уколико се сви кључеви слажу комуникација може нормално да се одвија, мобилни уређај добија нови TMSI број, у супротном мобилни уређај не може да приступи мрежи.

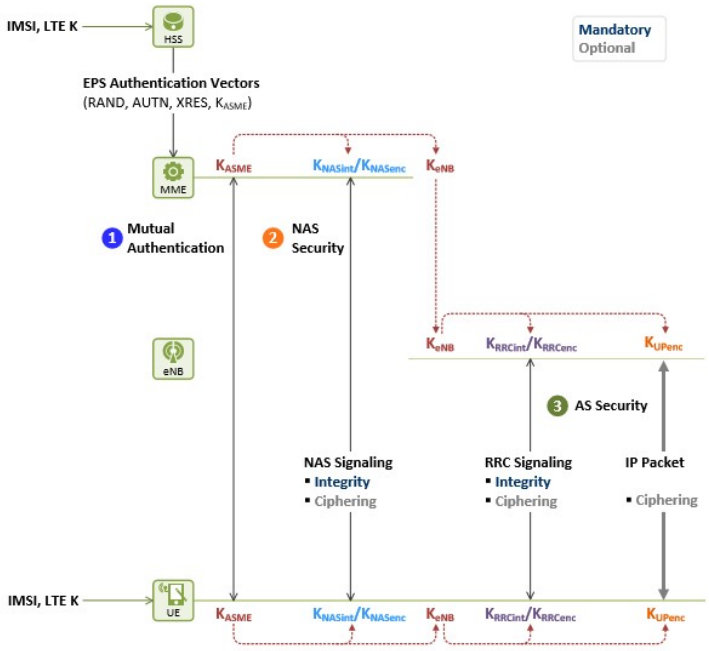
Постоји неколико врста A5 алгоритама. Најпростији је A5/0 и он уствари нема никакву енкрипцију, следећи је A5/1 који је масовно у употреби међутим може релативно лако да се дешифрује јер су кључеви садржани у Rainbow табелама. A5/2 алгоритам је слабији од A5/1 и више се не користи у пракси. Најновија верзија је A5/3 и он је базиран на Касуми алгоритму који је основа енкрипције за 3G мобилне мреже. Напредан је и веома тешко се дешифрује. Поред наведених постоје и алгоритми за енкрипцију података GEA (*енг. GPRS encryption algorithm*), у више верзија GEA1, GEA2 и GEA3. Који су еволуирали као и A5 алгоритми у складу са генерацијом мреже.

У мобилним мрежама треће генерације потпуно је уведен Касуми алгоритам за енкрипцију који уводи Misty1 секвенцу која је отпорна и на линеарну и диференцијалну крипто анализу и уводи F8 функцију за секвенцијално шифровање и F9 функцију за потврду интегритета података. Такође у 3G мрежна аутентификација корисника је двосмерна што значи да се врши размена кључева приликом аутентификације корисника са обе стране, што је значајно унапређење безбедности у мрежи.

3.2.2 Аутентификација и алгоритми енкрипције у 4G/LTE мрежама

Мобилне мреже четврте генерације у складу са измењеном архитектуром и значајно унапређеним могућностима нуди и нове начине безбедности за своје кориснике. Као и у

претходним мрежама основа безбедности је у аутентификацији корисника, која омогућава кориснику да се региструје на мрежу. Поред аутентификације развијен је низ заштитних мера кроз NAS и AS (*eng. Access Stratum*) које омогућавају сигуран трансфер података путем радио линка [13].



Слика 13 Концепт заштите у LTE мрежама [13]

На слици 14 је представљен концепт безбедности који се може сврстати у три целине:

- Аутентификација корисника – представља узајамну идентификацију мобилног уређаја и мобилне мреже у најширем смислу,
- NAS заштита – представља заштиту интегритета (верификацију) и кодовање (енкрипцију/декрипцију) размене података између мобилног уређаја и MME,
- AS заштита – представља заштиту интегритета (верификацију) и кодовање RRC између мобилног уређаја и eNB, као и кодовање садржаја комуникације између истих [13].

3.2.2.1 LTE АУТЕНТИФИКАЦИЈА

Аутентификација је процес који одређује да ли претплатник који покушава да приступи мрежи има неопходне акредитиве. На слици 13 може се видети да је аутентификација двострана и да се одвија размена одређених вектора који су састављени од појединачних елемената. У LTE мрежама аутентификација се још назива и EPS AKA (*енг. EPS Authentication and Key Agreement*). Ова врста аутентификације се одвија у два корака. Прво, HSS генерише EPS вектор аутентификације (RAND (*енг. RANDom number*), AUTN (*енг.*

Authentication Token), XRES (*енг. Expected Response*), K_{ASME}) који се преноси до MME. Затим у другом кораку MME одабира један од аутентификацијских вектора који користи за међусобну аутентификацију са мобилним уређајем и са истим дели исти кључ (K_{ASME}) за аутентификацију. ASME (*енг. Access Security Management Entity*) је целина која прима кључеве највишег нивоа од HSS-*а.* K_{ASME} је кључ највишег нивоа и кад се изврши аутентификација мобилни уређај и MME исти кључ користе током комуникације. Да би се избегла евентуална манипулација кључем исти се не доставља преко радио E-UTRAN већ у оквиру аутентификационог вектора са више других параметара који су претходно наведени.

3.2.2.2 NAS ЗАШТИТА

NAS заштита је развијена да обезбеди сигурну размену сигналних порука између мобилног уређаја и MME преко радио линка. Омогућава заштиту интегритета (верификацију) и кодовање (енкрипцију/декрипцију) размене података. За обе функције користи различите кључеве, с тим што је провера интегритета обавезна, а кодовање размене података опциона функција која не мора да се имплементира.

3.2.2.3 AS ЗАШТИТА

AS заштита омогућава безбедну размену података између мобилног уређаја и eNB преко радио линка. Обједињује проверу интегритета и кодовање података сигналних порука RRC у оквиру контролног плана и кодовање ИП пакета у корисничком плану. У оба случаја се користе различити кључеви, с тим да је провера интегритета обавезна док је кодовање опционо.

AS кључеви, KRRCint, KRRCenc и KUPenc, се генеришу у KeNB и код мобилног уређаја и код eNB. KRRCint и KRRCenc се користе за проверу интегритета и кодовање података контролног плана, док KUPenc се користи за кодовање корисничког плана. Провера интегритета и кодовање се врши коришћењем PDCP протокола.

Мобилни уређај може да генерише KeNB из K_{ASME}, међутим K_{ASME} се не преноси на eNB, уместо мобилног уређаја за њега KeNB генерише MME и истом прослеђује.

3.2.2.4 АЛГОРИТМИ ЕНКРИПЦИЈЕ

Критичан моменат и место за извршење напада, односно пресретање комуникације је простор између мобилног уређаја и покушаја аутентификације. У претходним одељцима је приказан поступак аутентификације и може се рећи да је сам вектор аутентификације као и распоред размене кључева веома сложен и сигуран систем. Евентуално декриптовање

садржаја комуникација у LTE мрежама захтева обезбеђење више различитих кључева у зависности од степена заштите.

У складу са [15] процес предаје захтева за приступање мобилног уређаја који се састоји од: IMSI, врсте алгоритма енкрипције који је заступљен, као и поруке KSI_{ASME}=7 која означава да мобилни уређај нема кључ за аутентификацију. У самом захтеву нападач већ може да сазна IMSI број претплатника који шаље захтев за идентификацију. На овај начин се може сазнати део идентификационих података али не и садржај комуникација по извршеној аутентификацији јер нападач не поседује кључеве за декрипцију планова комуникације.

Алгоритме енкрипције делимо у две категорије [14]:

- EPS алгоритам енкрипције EEA (*енг. EPS Encryption Algorithms*) и
- EPS алгоритам интегритета EIA (*енг. EPS Integrity Algorithms*).

EEA		**EIA**	
EEA0	Нулти алгоритам енкрипције	EIA0	Нулти алгоритам заштите интегритета (*дозвољен само у неауторизованим хитним позивима*)
128-EEA1	SNOW 3G	128-EIA1	SNOW 3G
128-EEA2	AES	128-EIA2	AES
128-EEA3	ZUC	128-EIA3	ZUC

Табела 3 Алгоритми енкрипције [15]

Сваки мобилни уређај има и одређене типове и верзије ових алгоритама које подржава и приликом интеграције са мрежом он те податке дели са истом. У табели 3 приказане су врсте алгоритама које су у употреби. Исти се стално развијају и унапређују.

Пошто MME прими захтев од мобилног уређаја исти се прослеђује до HSS и у том захтеву се налазе следећи параметри: IMSI, SN ID (PLMN ID), n *(број аутентификационих вектора)*, тип мреже. По пријему захтева HSS генерише RAND и SQN (*енг. Sequence Number*), затим генерише XRES, AUTN, CK (*енг. Cipher Key*) и IK (*енг. Integrity Key*) користећи EPS AKA алгоритам са LTE кључем (K), SQN и RAND. Груписањем свих наведених података генерише кључ највишег нивоа $K_{ASME.}$

Затим се комплетна процедура одвија у супротном смеру HSS доставља одговор MME. Потом MME доставља вектор аутентификације у виду захтева мобилном уређају са вектором KSI_{ASMEi}, RANDi, AUTNi, док се XRESi користи касније. На самом крају процеса мобилну уређај одговара MME да је аутентификација успешна или није.

После компликованог процеса аутентификације можда је боље безбедносни аспект представити у облику неопходних кључева који у крајњи продукт система енкрипције. У

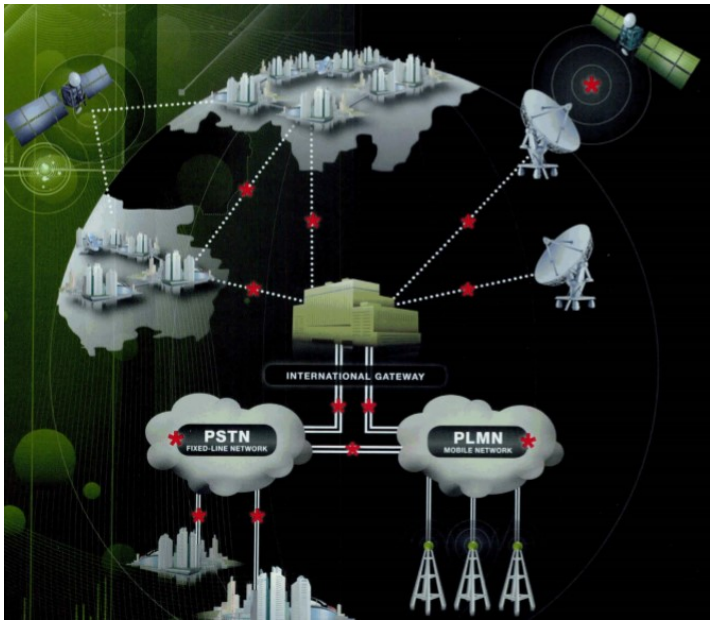
табели 4 су приказани LTE безбедносни кључеви који се користе у интеракцији мобилног уређаја и мобилне мреже.

Кључ	Дужина	Локација	Извор	Опис
K	128 bita	USIM, HSS/AuC	-	LTE кључ
CK	128 bita	USIM, HSS/AuC	K	Кључ кодовања
IK	128 bita	USIM, HSS/AuC	K	Кључ интегритета
K_{ASME}	256 bita	UE, HSS, MME	CK, IK	MME основни кључ

Табела 4 LTE безбедносни кључеви [13]

3.3 НАДЗОР МОБИЛНЕ ТЕЛЕФОНИЈЕ

Појам надзора мобилне телефоније датира од саме појаве мобилних уређаја, међутим то је само један од сегмената који се односи на мобилне комуникације. Систем надзора комуникација односно комплетне телефоније је најшири појам и он обухвата све комуникационе системе који су у употреби. Системом надзора обухваћене су сателитске, мобилна и фикса телефонија, оптички системи преноса, као и остали комерцијални системи преноса. Мониторисањем интернационалних комуникационих протокола као што су SS7 (*енг. Signaling System 7*) и дијаметар могуће је са удаљених локација, на интернационалном нивоу мониторисати комуникације и кориснике услуга. Мониторинг бежичних комуникација се врши на микролокацији и то принципима напада "човек у средини" (*MtM – Man in the Middle*) употребом специјализованих техничких средстава.



Слика 14 Централизовани систем надзора комуникација[7]

[7] Преузето са http://www.documentcloud.org/documents/711299-brochure484.html

Јавне комуникационе мреже су подељене на две мреже и то фиксне - земаљске PSTN и мобилне комуникационе мреже. Један од најважнијих и најексплоатисанијих система преноса су мобилне комуникације, које дају велики број података како у реалном времену, тако и задржаних података који могу накнадно да се анализирају. Надзор мобилне телефоније може да се подели на следеће целине у складу са примењеним техникама и коришћеним сервисима:

- Пасивни систем надзора,
- Активни систем надзора,
- Хибридни систем надзора,
- Позиционирање мобилних уређаја,
- Сондирање телекомуникационог етра.

Системи надзора мобилних комуникација четврте генерације и поред великог броја безбедносних пропуста су прилично ограничени и даље недоступни уколико се разматра искоришћење могућности које су везане за сервисе и инфраструктуру четврте генерације.

У наставку ће посебно бити објашњени пасивни и активни системи надзора као и могућности позиционирања. Хибридни системи су све више у употреби јер омогућавају комбиновање више технологија и техника пресретања, а самим тим и дају шири спектар информација и могућности. Већина могућности биће објашњена кроз пасивни и активни систем надзора. Сондирање телекомуникационог етра је савремена технологија која омогућава прецизније позиционирање, наиме заснива се на уградњи посебних сонди које прате стање у простирању сигнала базних станица и на тај начин употребом посебних софтвера и хардвера омогућавају веома прецизно позиционирање на националном нивоу употребом само могућности инфраструктуре мобилних оператера.

3.3.1 Пасивни систем надзора

Пасивни систем надзора мобилних комуникација је и даље један од највећих изазова за развој система. Наиме пасивни системи пресретања података у етру заснивају се пре свега на разбијању система енкрипције у комуникацији између мобилног уређаја и базне станице. У претходним поглављима објашњене су методе енкрипције и алгоритми којима су подаци заштићени.

На слици 15 приказано је у најширем смислу како се изводи пресретање мобилних комуникација. Уређај за пресретање треба да буде позициониран у простору између мобилног уређаја и базне станице са којом комуницира, као би се могли мониторисати и *uplink* и *downlink* комуникације, у супротном подаци о комуникацији неће бити потпуни.

Наравно поред надзора једног уређаја који је мета мониторише се и велика количина саобраћаја која представља саобраћај других претплатника.

Уређај за пасивно пресретање састоји се од одређеног броја пријемника који се користе за надзор доступних канала комуникације, система за разбијање кључева којим су закључани алгоритми енкрипције и апликативног нивоа за управљање и аналитику.



Слика 15 Принцип пасивног надзора мобилних комуникација

Хардвер који се користи је углавном на бази софтверски дефинисаног радија који се данас увелико употребљава и омогућава флексибилност по питању технологије и начина употребе.

Системи пасивног пресретања у свом фундаменталном смислу по информацијама које су доступне из јавних извора користе се само у мрежама друге генерације и то за декрипцију кључева алгоритама A5/1 и A5/2 који се највише користе. Данас велики број мобилних оператера своје комуникације шифрује са A5/3 алгоритмом за који постоје индиције да је разбијен и може се видети да одређени произвођачи нуде уређаје који декриптују и овај алгоритам. За мреже више генерације не постоје поуздане информације да се могу пасивним путем пресретати комуникације, односно да су развијени системи.

Да би се могле пресрести комуникације мобилних уређаја који су у мрежама треће и четврте генерације потребно је користити хибридни систем пресретања, који ће активним методама принудити мобилни уређаја да пређе на 2G мрежу и да промени алгоритам енкрипције. Када се изврши промена алгоритма енкрипције уређај може да се стандардним методама мониторише [12].

Системи за пасивни мониторинг имају једну предност која се огледа у потпуној пасивности односно није видљива у електромагнетном спектру и не може се открити

уређајима. Против овог система мониторинга тешко је предузет контра мере или се заштити. Могућа решења се огледају у домену забране мобилном уређају да користи мреже старије генерације, међутим обзиром на слабу покривеност мобилним мрежама више генерације ван градских средина исти корисници би се нашли у проблему да немају мрежу и не могу да комуницирају. Поред наведеног велики број савремених мобилних уређаја и поред забране употребе рецимо 2G мреже ће у недостатку мрежа новије генерације како би одржа континуитет комуникације прећи на 2G мрежи и опет постати рањив.

Системе за пресретање нуди велики број произвођача али са приближно истим карактеристикама, такође постоје и *opensource* решења која служе за развој и изучавање могућности пресретања, један од понуђених решења је доступан на сајту *OpenBTS.org*. Међутим исти да би се користио потребно је поседовати одређени хардвер који је такође јавно доступан.

3.3.2 Активни систем надзора

Основни уређај за активни надзор је *IMSI Catcher*. Овај уређај активно учествује у етру и учествује у комуникацији са мобилним уређајима. Основна идеја овог уређаја је била да се дође до идентификационих података корисника мобилног уређаја како би се добијени подаци експлоатисали у оквиру других поступака и мера које користе државне институције из домена безбедности. Основна намена овог уређаја одавно је превазиђена тако да овај уређај данас може да обезбеди веома много информација о мобилном уређају, као и функционалности које су некада биле незамисливе. Експанзија развоја условљена је пре свега тражњом тржишта и развојем мобилних комуникација.



Слика 16 Принцип активног надзора мобилних комуникација

Принцип рада уређаја је приказан на слици 16, наиме уређај првобитно скенира спектар у окружењу и анализира комплетно доступну инфраструктуру мобилних оператера. Када се заврши скенирање уређај се конфигурише тако што клонира једну од базних станица која није из директног окружења већ је оптимално удаљена тако да мобилни уређај неће да види базну станицу која је клонирана. Одабрана базна станица ће бити суседна одређеном броју базних станица које мобилни уређај види као суседне и на тај начин ће моћи да обави своју основну функцију у етру. Већина уређаја данас поседује аутоматски систем за одабир оптималних базних станица за клонирање.

IMSI Catcher својим радом симулира стварну базну станицу и у оквиру мреже одређеног оператера у веома кратким интервалима интерконектује се са мобилним уређајима тако што од истих захтева идентификационе параметре. Уређај емитује веома високом снагом и на тај начин привлачи мобилне уређаје да се идентификују на истом, јер мобилни уређај увек тражи базну станицу из окружења са најјачим сигналом и на исту се повеже. Технички гледано IMSI Catcher се понаша као регуларна базна станица, што значи да је мобилни уређај принуђен да пошаље енкрипционе параметре истој.

Иницијализација конекције отпочиње слањем сигурносних параметра мобилног уређаја IMSI Catcher-у, који одговара захтевом за идентитетом, на шта мобилни уређај одговара идентификационим параметрима. Мобилна мрежа затим захтева размену кључева у оквиру RAND сесије међутим пошто исти не поседује кључ уређај не одговара на захтев. IMSI Catcher прослеђује RAND захтев ка мобилном уређају који поседује исправан кључ који враћа у оквиру SRES (*енг. Signed Response*) сесије и на тај начин је отворен канал везе између мобилног уређаја и IMSI Catcher-а.

Захтев за идентификационим подацима ка истом уређају може да се понавља неограничен број пута са је потребно да се промени LAC (*енг. Local Area Code*) код у 2G и 3G мрежама или TAC (*енг. Tracking Area Code*) код у LTE мрежама. Поред овог броја уређај може да проследи и друге параметре као што су IMEI и TMSI који су битни код осталих врста експлоатације мобилног уређаја. Идентификационе податке мобилног уређаја који је мета једноставно може добити уколико корелишемо податке са више локација где се претходно налазио.

Савремени IMSI Catcher-и омогућавају велики број финкционалности поред основне, најраспрострањеније су следеће:

- Лоцирање уређаја директно преко IMSI Catcher-а или коришћењем гониометра *uplink-a* мобилног уређаја (*direction finder*),
- Лоцирање уређаја упућивањем захтева да се проследи тачна GPS локација,
- Укључење микрофона телефона,

- Манипулација мрежом и енкрипцијом, ометање уређаја тако да са 4G мреже пређе на 3G или 2G мрежу,
- Дисконектовање мобилног уређаја са мреже,
- Упућивање позива или SMS поруке,
- Упућивање "тихог" позива (*silent call*) и остало.

Обзиром на распрострањеност ових уређаја постепено су се развијали системи и механизми детекције истих. IMSI Catcher у етру може да се распозна по неколико следећих параметара [12]:

- Коришћење радне фреквенције ван дозвољеног опсега,
- Нестандардне базне станице на одређеној локацији,
- Базне станице са измењеним параметрима и могућностима,
- Ометање у радиофреквентном спектру,
- Промена генерације мреже на мобилном уређају,
- Одсуство енкрипције,
- Цурење информација о суседним ћелијама базних станица,
- Кратко радно време базне станице,
- Учестало мењање локалног просторног кода.

Распознавање наведених параметара тешко је без специјализованих уређаја који прате све промене у радио спектру по питању мобилне телефоније, као и специјалних мобилних уређаја који су опремљени посебним апликацијама за детектовање лажних базних станица.

3.4 Безбедносни недостаци локацијских сервиса у LTE мрежама

3.4.1 Основе позиционирања мобилних уређаја

Лоцирање мобилних уређаја, односно претплатника употребом локацијских сервиса мобилних мрежа (*LBS – Location Based Services*) је веома важан сегмент услуга које омогућавају мобилне комуникације. Током еволуције мрежа развијено је више технологија које са различитим параметрима могу да лоцирају мобилни уређај са одређеним степеном прецизности. Државне агенције и службе су легални корисници ових сервиса и исте константно имплементирају нове могућности које нуде савремене технологије. Најпознатији сервис који користе локацијске сервисе су 911 и 112 који омогућавају прослеђивање хитних позива службама као што су ватрогасци, полиција, хитна помоћ и остали. На пример захтеви за стандард E911 у САД је да мање од 67% мерења не сме да да грешку мању од 50 метара, док 95% мерења мора да има грешку мању од 150 метара [17]. Приликом активирања ових

сервиса систем сам омогућава да се употребом локацијских сервиса лоцирају мобилни уређаји са којих је извршен позив.

Постоји неколико могућности за лоцирање у оквиру LTE мрежа. У LTE мрежама локацијски сервиси се називају LCS (*енг. Location Services*). Локација може да се одређује на основу величине ћелије, адаптивних техника антене, естимацији пропагације сигнала, временске прецизности, покривености базне станице. Оператер може да одабере коју технику да имплементира у зависности од финансијских могућности и захтева крајњих корисника. Позиционирање мобилног уређаја обухвата два корака:

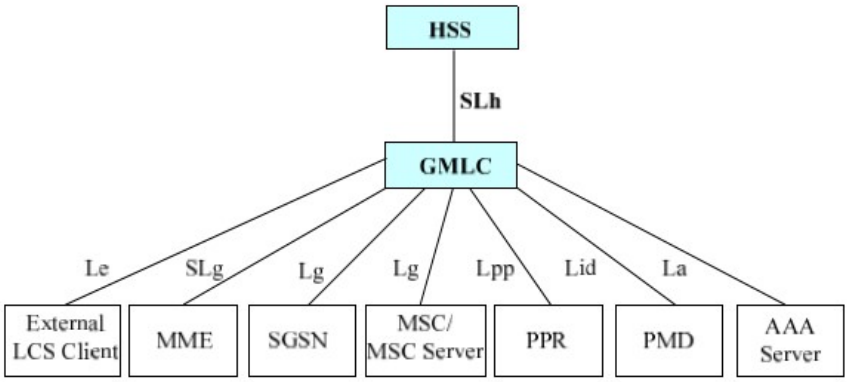
- Мерење сигнала и
- Естимацију позиције.

Основни елеменат локацијских сервиса у LTE мрежама је GMLC (*енг. Gateway Mobile Location Centre*). У овај центар се рутирају сви захтеви и у истом се и обрађују. Он комуницира са PPR (*енг. Privacy Profile Register*), односно регистром приватних профила где се проверава да ли је захтев ауторизован. У комплетан процес позиционирања укључени су и MME и HSS у складу са својим функцијама [16]. Постоји неколико стандардних метода које могу да унапреде систем позиционирања коришћењем додатних техничких могућности мобилног уређаја, и то:

- ECID (*енг. Enhanced Cell ID*) метода,
- A-GNSS (*енг. Assisted - Global Navigation Satellite System*) метода,
- OTDOA (*енг. Observed Tome Differencial of Arrival*) метода [17].

Поред наведених метода постоје и два протокола која су намењен за извршење LBS сервиса. Први је SUPL 2.0 (*енг. Secure User Plane Location*) који подржава технике као што је *WiFi* позиционирање, други је нови протокол који се јавља од Release 9 и назива се LPP (*енг. LTE Positioning Protocol*), исти представља нови протокол уведен и користи се само у LTE мрежама.

Прва метода ECID се заснива на позиционирању на основу позиције базне станице, одговор на захтев је веома брз али са веома великом грешком. У најгорем случају као локација се добија позиција базне станице. Грешка се може смањити мерењем мрежних параметара, као што су мерење угла под којим базна станица види мобилни уређај (*AoA - Angle of Arrival*), као и времена простирања сигнала (*RTT - Round Time Trip*) анализирајући TA (*енг. Timing Advance*) параметара. Ова метода је основна и у великом броју случајева довољна за одређивање позиције, прецизност се огледа у рејону од 150 метара.



Слика 17 Функционална шема локацијских сервиса у LTE мрежама [20]

Друга метода напредне употребе GPS позиционирања уколико мобилни уређај поседује GPS пријемник и уколико је активан. Наиме поред стандардне позиције добијене од базне станице комбинује се података од глобалног позиционирања. На тај начин се доста поправља прецизност и могуће је извршити лоцирање у рејону од 10 до 50 метара.

Трећа метода користи параметре са више базних станица. Наиме користи се референтни сигнал са више суседних базних станица и упоређује се како би се добила што прецизнија позиција. На овај начин у најширем смислу користи се принцип триангулације али базиран на временским интервалима од више референтних тачака. Сигнал који се мери се зове референтни сигнал позиције PRS (*енг. Position Reference Signal*) и уведен је од Release 9 стандарда.

3.4.2 Диаметар протокол

Систем позиционирања се у великој мери базира на искоришћењу капацитета SS7 капацитета, као и протокола диаметар[8] који је наследник претходно наведеног у LTE мрежама. Ови протоколи се користе за интерконекцију различитих комуникационих мрежа и самим тим омогућавају приступ ресурсима једне мреже и из других комуникационих система. Употребом SS7 капацитета позиционирање може да се врши на глобалном нивоу до прецизности на нивоу базне станице [18].

Диаметар протокол је проширена верзија AAA (*енг. Authentication, Authorization, and Accounting*) протокола који је у основи базиран на RADIUS (*енг. Remote Authentication Dial-In User Service*) протоколу који је старији и прилично ограничен по питању проширења функционалности. Диаметар протокол се састоји из два протокола: основни диаметар

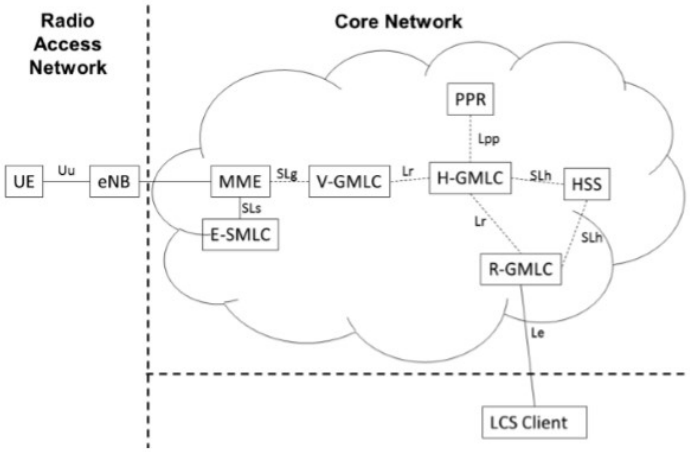
[8] Diameter Protocol

протокол и надоградње диаметра[9][16]. Основни протокол дефинише формат поруке, начин транспорта, пријаву грешака, управљање налогом и безбедносне аспекте.

Диаметар протокол контролише већину порука у језгру мреже. Поруке у оквиру протокола су дефинисане AVP (*енг. Attribute-Value Pairs*) кодовима које су дефинисане у документу *RFC3589* [19]. Сви подаци достављени овим протоколом су у облику кодова. На овај начин се размењују информације од аутентификацији корисника, омогућавање приступа, управља корисничким налозима, прослеђују поруке између различитих хијерархијских целина. Основни протокол омогућава следеће могућности:

- Достава кодова порука,
- Интерконекцију интерних целина,
- Обавештење о грешкама,
- Проширивост, додавање нових команди и кодова,
- Основне услуге неопходне за апликације као што су управљање корисничким сесијама [19].

Један од елемената који се односи на позиционирање и локацијске сервисе је дефинисан у стандарду 3GPP TS 29.173 и у њему је специфициран интерфејс између HSS и GMLC [20].



Слика 18 Логички нивои локацијских сервиса у LTE мрежама [16]

Проучавајући документ 3GPP TS 29.173 може се уочити да не постоје егзактна објашњења за све интерфејсе, односно листа није коначна. Наиме поједини интерфејси који се наводе као стандардни нису дефинисани као да се односе на диаметар протокол. Неки од њих су L_e и L_{pp} који су приказани на слици 18, а дефинитивно фигуришу у сегментима који су од интереса за локацијске сервисе. Многи од атрибута наведених интерфејса су доступни преко других интерфејса.

[9] Diameter Base Protocol and the Diameter Extensions

3.4.3 НЕДОСТАЦИ LTE ЛОКАЦИЈСКИХ СЕРВИСА

У претходном одељку је поменуто да сви интерфејси или нису дефинисани или нису дефинисани на адекватан начин. У неегзактност у дефинисању стандарда и протокола омогућава да систем буде рањив и да поседује безбедносне проблеме који могу да буду злоупотребљени. У оквиру [16] извршена је анализа појединих недостатака у оквиру локацијских сервиса. Недостаци су подељени у неколико категорија, и то:

- Одложени захтев,
- Индикатор прекорачења овлашћења,
- Компромитовани GMLC,
- Приступ уз употребу исправног захтева,
- Дуплирани и неважећи AVP кодови.

3.4.3.1 ОДЛОЖЕНИ ЗАХТЕВ

Техничка спецификација која се односи за одложени захтев захтева само једну проверу интегритета и то само приликом иницијалног захтева. Ово се дешава пошто је локација мобилног уређаја већ у мрежи и позната је. Уколико се појави захтев клијента за локацијом није легитиман он неће имати право да види податка о локацији, међутим услов за локацијом ће бити и даље испуњен јер није реализован у систему али се неће вратити оном ко је упутио захтев. На тај начин систем је само половично безбедан. Уколико нападач поседује контролу над клијентом који користи локацијске сервисе и налази се у близини мрежног чвора који је близу мобилног уређаја чију локацију жели да пресретне, може да пошаље одложени захтев и да на суседној базној станици са другог GMLC преузме податке о локацији мобилног уређаја. Овај систем је потпуно пасиван и захтева присуство мрежној инфраструктури.

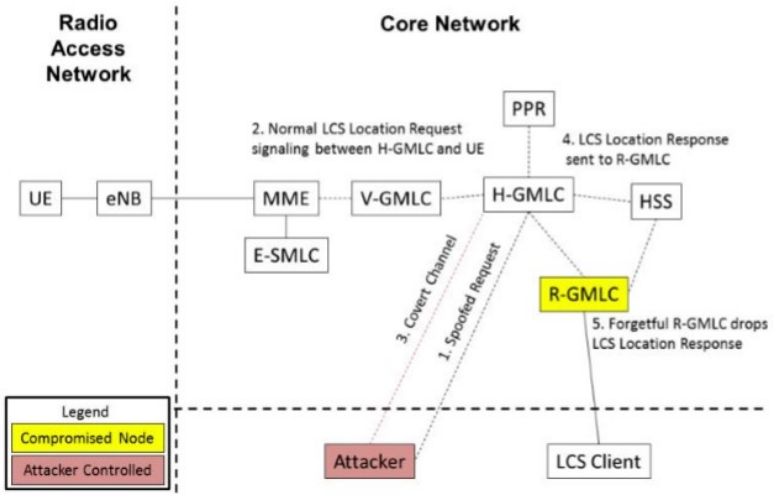
3.4.3.2 ИНДИКАТОР ПРЕКОРАЧЕЊА ОВЛАШЋЕЊА

Инплементација индикатора прекорачења овлашћења није дефинисана у спецификација. Статус који говори да ли је дошло или није дошло до прекорачења се не доставља MME. Што имплицира да аутентичност индикатора зависи од продавца и безбедности диаметар порука. Спецификације не говоре како или на који начин да валидирају ове индикаторе. Ови недостаци остављају могућности да индикатори прекорачења буду пресретнути, измењени и поново емитовани што је велики безбедносни проблем.

3.4.3.3 *Компромитовани GMLC*

Листа активних локацијских захтева је стално активна јер не постоји начин рутирања одговара сервиса ка потражиоцу захтева у систему порука које преноси диаметар протокол. Уколико нападач на неки начин компромитује GMLC може да приступи и листи захтева. Једноставно уклањањем активног захтева са листе може да учину да је GMLC селективно респонзивним. Када се одговор сервиса врати на GMLC он ће пакете да одбаци јер у систему више не види и да је постојао захетв, самим тим ни клијент неће да добије податак о локацији. Нападач може да пресретне и измени захтев клијента.

Измењени захтев може да буде прослеђен или H- GMLC или R- GMLC што је приказано на слици 19. Нападач се маскира тако што напада GMLC који је у низу после онога на који је захтев упутио легитимни клијент. На тај начин је нападач маскиран и заштићен.



Слика 19 Лажни захтев за локацијом корисника [16]

3.4.3.4 Приступ уз употребу исправног захтева

Користећи могућност да ауторизовани клијент омогући свесно или несвесно својим акредитивима да и други користе исте ресурсе могу да се злоупотребе у подаци из GMLC. Наиме уколико нападач проследи свој захтев легитимним путем у базу, одговор може да се врати и легалном клијенту и нападачу јер оба имају регуларан захетв за исти мобилни уређај.

3.4.3.5 Дуплирани и неважећи AVP кодови

Релативно отворена архитектура диаметар протокола омогућава да у истој поруци имамо два иста кода иако је то неуобичајна процедура. Не постоји процедура која проверава дупле кодове у поруци, како би се таква порука одбацила као невалидна. Постоје и кодови који су

неважећи и као такви се увек одбацују или бивају преписани са новим пољима. Ово ставља отвореном могућност да се дуплирани или неважећи кодови користе за улазак у мрежу преко скривеног канала између две базне станице. Обзиром да исте већ међусобно комуницирају и преносе поруке скривени канал би се само придодао постојећим и поруке из њега би било веома тешко филтрирати или одбацити. Те лажне поруке би се сматрале регуларним и биле реализоване у складу са захтевом.

4 БЕЗБЕДНОСНИ АСПЕКТИ И НЕДОСТАТЦИ У 4G/LTE МОБИЛНИМ КОМУНИКАЦИОМ МРЕЖАМА

4.1 Увод

Безбедносни аспекти у мобилним мрежама четврте генерације постали су прави изазов како за даваоце услуга мобилне телефоније, оператера, тако и за саме претплатнике. Дугорочна еволуција мобилних комуникација четврте генерације је у правом смислу еволуирала и у смислу безбедности. Претходно смо се борили са безбедносним изазовима које су последица еволуције архитектуре мобилних мрежа, а су LTE мрежама је поред наведене инкорпориран и интернет протокол који сам по себи има велики број безбедносних мањкавости.

У складу са наведеним у овом одељку ће бити описани безбедносни проблеми разматрани са аспекта мобилних оператера и претплатничких мобилних уређаја.

4.2 Захтеви и могућности LTE мобилних мрежа

LTE мреже су настале пре свега као последица потражње за све већим протоком података, као и потребом оператера за смањењем трошкова инфраструктуре. Иницијални захтев мреже је био 300Mbps у downlink-у и 75Mbps у uplink-у, подршка уа IPv4 и IPv6 протоколима, једноставнија структура са што мање елемената мреже, спектрална ефикасност, мало кашњење и наравно компатибилност са постојећем мрежном инфраструктуром [22]. Унапређење је резултирало да је већом профитабилношћу компанија међутим утицало је на безбедност комуникација.

LTE мобилне мреже су развијене са становишта безбедносних принципа који су важили за 3GPP и то по следећем [15]:

- Безбедан приступ мрежним ресурсима – треба да омогући кориснику безбедан приступ мрежним сервисима;
- Безбедност мрежних елемената – треба да омогући безбедност свих мрежних елемената и интермрежну комуникацију и безбедну размену података између корисника;
- Безбедност терминалних, корисничких уређаја – треба да обезбеди контролисану и безбедну комуникацију са приступном мрежном инфраструктуром,
- Апликативну безбедност – обезбеђење успостављања сигурне комуникације на апликативном нивоу мреже;

- Транспарентност и могућност конфигурације нивоа безбедности – треба да омогући кориснику могућност да се увери да безбедносни протоколи функционишу.

Наведени захтеви у погледу безбедности захтевају широк и свеобухватан спектар активности које би омогућили да буду и испуњени. Међутим колико се одмакло у реализацији истог биће анализирано у наставку.

4.3 Модел анализе

Широк појам безбедности како у реалном животу тако и у технички оријентисаним научним областима мора бити адекватно моделован да би могао да се анализира. Природно је да се једна оваква област анализира кроз саму архитектуру од самог корисника, преко мрежне инфраструктуре до екстерне мреже којој приступа.



Слика 20 Архитектура модела за анализу

Модел за анализу састоји се из четири сегмента (Слика 20):

- Мобилни уређај – UE,
- Приступна инфраструктура, E-UTRAN,
- Језгро мреже - EPC,
- Сервисна мрежа.

Анализа безбедносних аспеката биће извршена кроз наведене сегменте: мобилни уређај, приступну инфраструктуру, језгра мреже и сервисне мреже. Такође поред наведеног биће предочени могући превентивни кораци на сваком нивоу анализе.

Овај вид анализе биће више базиран на чиниоцима који су не техничке природе и више се односе на неке уопштене параметре које треба сагледати пре сагледавања безбедносних пропуста који су техничке природе.

4.4 Општи безбедносни аспекти

У оквиру наведених сегмената могу да се издвоје кључни безбедносни ризици и претње, који се преплићу у оквиру горе наведених сегмената, и то су:

- Дистрибутивна мрежа и отворена архитектура,
- Децентрализована одговорност за безбедност,
- Комплексни бизнис модел у смислу инфраструктуре и размене сервиса,
- Минимализација трошкова безбедносне заштите.

4.4.1 ДИСТРИБУТИВНА МРЕЖА И ОТВОРЕНА АРХИТЕКТУРА

LTE је својом архитектуром и инкорпорацијом пре свега IP структуре у систем довела до тога да се створи глобална комуникациона мрежа која више није самостална и није директно под надзором једног оператера. У старијим генерацијама мреже оператер је могао да контролише ниво заштите у оквиру своје мреже и на тај начин да га донекле заштити од претњи. Отворена архитектура и систем заштите је готово свуда исти као резултат тога ниво безбедности је на нижем нивоу што повећава безбедносне ризике и претње. Дистрибутивна мрежа и отворена архитектура омогућавају слабу безбедносну конфигурацију тако да нападач више не треба приступ посебним интерфејсима или ресурсима мреже да би извршио напад већ је довољно да има приступ интернету.

4.4.2 ДЕЦЕНТРАЛИЗОВАНА ОДГОВОРНОСТ ЗА БЕЗБЕДНОСТ

Оператери мобилне телефоније притиснути константно новим захтевима и немогућношћу да обезбеде сигурну средину за мобилни уређај корисника користе модел универзалне безбедности крајњих тачака комуникације (*universal end to end security level*). Овај модел безбедности нема једностран систем безбедности прописан за све даваоце услуга размене података. Овде не треба посебно разматрати LTE мрежу од остатка комуникационог света, обзиром да готово целокупан садржај комуникација може да се подведе под интернет садржај који је део велике глобалне мреже и има другачији систем заштите од традиционалне мобилне телефоније која је примарно била конципирана за пружање услуге позива и кратких SMS порука. Поред тога мобилни уређај више није обичан телефон већ уређај који има оперативни систем и велики број апликација које имају своја подешавања која корисник свесно прихвата да би могао да их користи.

На пример, апликација инсталирана тражи од корисника да дозволи приступ именику, микрофону, камери и осталим ресурсима уређаја. Уколико корисник исте одобри он свесно може да буде жртва. С тим да овај процес не може да се заштити било како од стране оператера. Оператер у случају било какве жалбе на безбедност од стране корисника може да одговори да није одговоран јер је корисника сам дозволио приступ садржајима на његовом уређају.



Слика 21 Безбедносне претње са апликативног нивоа

4.4.3 Комплексни бизнис модел у смислу инфраструктуре и размене сервиса

Оператери поред услуга крајњим корисницима омогућавају и закуп својих мрежних ресурса другим операторима. Овај модел употребе ресурса се данас веома много користи под називом национални роминг. Овај модел рада је настао пре свега као последица вишка ресурса оператера и могућности да профитира од дела инфраструктуре коју не користи пуним капацитетом. Поред наведеног ове ресурсе могу да користе и такозвани виртуални оператери који не поседују своју инфраструктуру већ је искључиво изнајмљују од других оператера. На тај начин један оператер поседује E-UTRAN док други поседује MME. Виртуални оператер користећи мрежне ресурсе другог оператера користи све расположиве сервисе и пружа услуге у своје име. У Србији су у току 2016. године поднета два захтева за покретање виртуалних оператера, *Mundio mobile* и *Globaltel* [5].

Ова врста споразума доноси нове изазове са становишта безбедности. Оператери сада деле исте ресурсе и сервисе. Ове врсте LTE аранжмана доноси са собом нове изазове да се обезбеди конзистентан систем безбедности, са становишта управљања и могућности виртуални оператера. Више мобилних оператера са различитим нивоом контроле и система безбедности а са истим мрежним ресурсима представљају претњу за крајњег корисника.

4.4.4 МИНИМАЛИЗАЦИЈА ТРОШКОВА БЕЗБЕДНОСНЕ ЗАШТИТЕ

LTE оператери су у складу са обавезама од стране међународних институција да испуне безбедносне стандарде принуђени да улажу велика финансијска средства, тако да исти труде да испуне минимуме захтева који су постављени. Постоји значајна разлика између великих мрежних оператера и мањих оператора са ограниченим ресурсима, који не успевају да испуне све безбедносне захтеве. На тај начин се ниво безбедности укупне архитектуре спушта на најнижи импленетирани ниво, смањује безбедносне прагове а самим тим и безбедност корисника.

4.4.5 ПРЕВЕНТИВНЕ МЕРЕ

Обзиром на читав спектар безбедносних ризика на највишем нивоу разматрања LTE комуникационих система потребно је издвојити неке основне превентивне мере које би делимично, уз услов да буду испуњене учиниле систем комуникације безбеднијим за крајњег корисника. Опште мере које би биле најпрактичније и функционалне би биле:

- Интероперабилност стандарда,
- Ревизија безбедносних стандарда са обавезним изменама,
- Квалитетнији уговори између оператера,
- Повећање буџета за потребе безбедности.

4.4.5.1 ИНТЕРОПЕРАБИЛНОСТ СТАНДАРДА

Архитектура мреже која је или надограђена или је досегла ниво развоја који провајдер не жели да мења. Провајдер сам дефинише које ће безбедносне стандарде користити и колико ће заштити своје кориснике. Тако да приликом интерконекције оператера наилазимо на различите стандарде и ниво безбедносне заштите. Сам корисник приликом коришћења услуга у ромингу и промене оператера неће осетити битне разлике у коришћењу уређаја. Међутим уређај ће у различитим мрежама користи различите безбедносне стандарде и сам тим бити различито заштићен.

У сладу са наведеним потребно је да се поред пружања основних услуга у смислу квалитета (брзина реакције, пропусни опсег, покривености мрежом...) потребно је да се уреди сет безбедносних стандарда који ће бити обавезни и интероперабилни, односно да корисник има задовољавајући ниво заштите у било којој мрежи.

4.4.5.2 РЕВИЗИЈА БЕЗБЕДНОСНИХ СТАНДАРДА СА ОБАВЕЗНИМ ИЗМЕНАМА

Безбедносни стандарди треба да се ревидирају периодично како еволуира систем и како напредује технологија, међутим уколико се стандарди надограђују само на нивоу необавезних предлога који никад не буду имплементирани они у пракси немају никакву применљивост. Решење проблема је креирање измена стандарда са обавезним инкорпорирањем у телекомуникациони систем. На овај начин оператери би били у обавези да спроводе нове регулативе и на тај начин унапреде систем безбедносне заштите.

4.4.5.3 КВАЛИТЕТНИЈИ УГОВОРИ ИЗМЕЂУ ОПЕРАТЕРА

Дефинисање узајамног поштовања стандарда приликом уговарања сарадње на нивоу размене капацитета мобилних оператера могао би да буде један од основних чинилаца у подизању нивоа безбедности. Наиме оператер који има одређени стандард безбедности могао би да захтева од свог партнера да или има исте или више безбедносне стандарде. Поједини оператери улажу велика финансијска средства да би њихови корисници безбедно комуницирали и не желе да се исти изложе безбедносним ризицима приликом коришћења роминга. На овај начин би велики број оператера морао да подигне своје стандарде како би био конкурентан на роминг тржишту.

4.4.5.4 ПОВЕЋАЊЕ БУЏЕТА ЗА ПОТРЕБЕ БЕЗБЕДНОСТИ

На крају ових превентивних мера долазимо и на можда најограничавајући фактор, а то су финансијска средства. Наиме питање је колико могу и колико желе да уложе у повећање безбедности. Наиме оператери су имплементирали LTE технологију како би повећали зараду коришћењем познате ИП платформе. Иако је позната да ова платформа има веома много безбедносних недостатака и да је прилично тешка за заштиту, а посебно што нуди готово неограничене могућности у размени података. У неким земљама су регулаторна тела донела одлуку да оператери треба да обезбеде и специфичну опрему за мониторинг саобраћаја и надгледање комуникација. Поред обичних корисника постоје и корпоративни корисници који не желе да улажу у систем заштите већ од пружаоца услуга захтевају одређени ниво заштите и то плаћају. Дефинитивно да су потребна унапређења на пољу безбедности која изискују велика финансијска средства која оператери тренутно не желе да уложе. Међутим у наредном периоду ће свакако морати да повећају буџет за овај издатак.

4.5 МОБИЛНИ УРЕЂАЈИ

Мобилни уређај је основ за приступ мрежи кориснику. За највећи део корисника познавање мреже на овом уређају почиње и завршава. Обзиром на велики број произвођача и стандарда ово је сигурно најнебезбеднији део система у LTE мрежама. На сам уређај и начин коришћења оператер готово да нема утицаја већ све зависи од самог корисника и предефинисаних система заштите у уређају. Најпростије речено мобилни уређај је приступна тачка (*gateway*) за различите безбедносне пропусте у мрежи. Већина напада се одвија баш у овом сегменту мреже. У овом сегменту може се издвојити неколико типова безбедносних ризика, и то:

- Физичка доступност мобилног уређаја,
- Недостатак безбедносних стандарда и контроле уређаја,
- Ризик од губитка приватних података,
- Безбедносни недостаци апликација.

4.5.1 ФИЗИЧКА ДОСТУПНОСТ МОБИЛНОГ УРЕЂАЈА

Мобилни уређаји су данас мали, компактни, преносни тако да лако могу да се изгубе и буду предмет крађе. На тај начин комплетан садржај на уређају више није безбедан, посебно уколико не постоји никакав вид заштите приступа (пин код, отисак прста, шифра...). Лице које дође у посед таквог телефона може да сазна све податке корисника, од налога за маил, социјалне мреже, банковни налог за плаћање... А колико се циљно отуђује телефон од одређеног лица а притом отмичар поседује софистицирану опрему за преснимавање података са уређаја може да приступи свим мета подацима. Међутим и поред свих безбедносних претњи и изазова обичан корисник и даље се не штити ни на који начин. Иако уређаји поседују снажне механизме заштите и енкрипције података на истом, који могу да се провале само сложеним система декрипције које могу да поседују само државне институције. Поред наведеног велики број корисника софтвер који је уграђен у телефон ослабљују (*jailbeaking, rooting, cracking...*) различитим начинима и на тај начин у ствари заобилазе или искључују безбедносне системе како би остварили неки бенифит у виду инсталирања нелегалног софтвера или фиктивног повећања перформанси уређаја. На тај начин не знајући отварају врата многим претњама којих нису ни свесни [23].

Мобилни уређај такође може да буде нападнут и са мобилне мреже или посредством уређаја који симулирајући мобилну мрежу комуницирају са уређајем.

4.5.2 НЕДОСТАТАК БЕЗБЕДНОСНИХ СТАНДАРДА И КОНТРОЛЕ УРЕЂАЈА

Производња паметних мобилних уређаја је распрострањена на целој планети код великог броја произвођача. Поред произвођача самих уређаја имамо и више различитих софтверских платформи које ти уређаји користе. Софтверске платформе у потпуности контролишу могућности мобилних уређаја. Важно је напоменути да поједини произвођачи мобилних уређаја оперативни систем који уграђују у уређај додатно мењају како би сваки модел добио неку особеност одређеног бренда. Ово је посебно заступљено на Андроид платформи оперативног система који је и најраспрострањенији. Поред распрострањености исти је и најнебезбеднији јер омогућава да апликације користе готово све ресурсе уређаја. Овде је евидентно да не постоји одређени безбедносни стандард и контрола уређаја јер данас било ко може да направи софтвер и да га објави на Play Store продавници софтвера који користе уређаји са Андроид оперативним системом. Овакви непроверени софтвери могу да имају велики број малициозних пропуста који мигу да буду злоупотребљени. Потребно је у што скоријем времену да се овај део тржишта софтвером уреди како би крајњи корисник био што безбеднији.

Велики број оператера омогућава да се небезбедни уређаји повежу на њихову мрежу и на тај начин омогућавају улазну тачку за напад. Такође велики број мобилних уређаја не поседују никакав софтвер за заштиту, односно најосновнији антивирусни програм. Мобилни оператери са непотпуно развијеном мрежом која је само надограђена са старијих генерација, лимитирана је чињеницом да не може да подржи све савремене безбедносне протоколе и на тај начин мора да спушта ниво заштите како би се мобилни уређаји могли прикључити на мрежу.

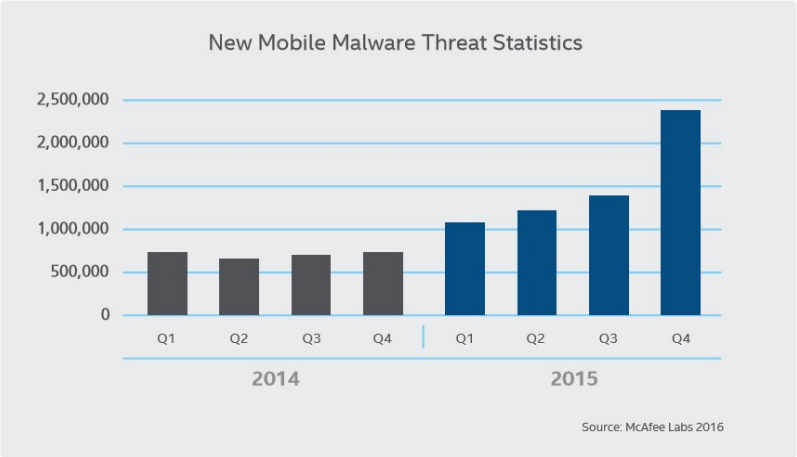
4.5.3 РИЗИК ОД ГУБИТКА ПРИВАТНИХ ПОДАТАКА

Приступ широкопојасном интернету, као и могућност трансфера велике количине података, LTE мреже чине мобилне уређаје погоднијим за нападе јер у складу са количином података које преносе највећи део истих могу и да складиште у својој меморији. Такође међутим подацима су комплетни садржаји транскрипта комуникација на друштвеним мрежама, размена порука преко Viber, WhatsApp, осталих комуникационих апликација, поред садржај на мобилним уређајима се чувају и приступни подаци за исте. Односно корисничка имена и шифре за приступ. Тако да приступ мобилном уређају омогућава и приступ свим подацима које користи и сам корисник [24].

Једном украдени подаци могу да учине корисника који је покраден жртвом манипулације, како у смислу крађе идентитета тако и злоупотребе личних података у различите противзаконите сврхе.

4.5.4 Безбедносни недостаци апликација

Обзиром да су мобилни уређаји у оквиру LTE мреже само ИП адресе, они су исто као и било који корисник ИП опсега подједнако подложни нападима и свим безбедносним ризицима. Корисници који стално инсталирају нове софтвере са било ког извора изложени су различитим вирусима, малверу, спаму, фишингу и сличним претњама које угрожавају интегритет уређаја, опсег употребе мреже самог оператера, безбедност LTE мреже и самог корисника.



Слика 22 Повећање претњи од малвера генерисаног кроз апликације мобилних уређаја

У складу са наводима компаније McAfee која с бави безбедношћу у домену информационих технологија количина малвера који се појављује у оквиру апликација се вртоглаво пење у сваком следећем кварталу а посебно између трећег и четвртог квартала 2015. године [25]. Ово је све последица развоја LTE мреже и све веће употребе мобилних уређаја као основних средстава за приступ садржајима на интернету. Овде је посебно потребно нагласити да ја у порасту коришћење мобилних апликација за вођење комерцијалних трансакција преко интернета, готово све банке омогућавају да се сви капацитети користе онлајн и на тај начин сами корисници не само да могу да буду угрожени са становишта личних података већ и могу да претрпе и финансијске губитке.

4.5.5 ПРЕВЕНТИВНЕ МЕРЕ

У складу са претходним безбедносним изазовима могуће је груписати превентивне мере у неколико категорија:

- Едукација корисника,
- Стандардизација и боља контрола квалитета произвођача мобилних уређаја и софтвера,
- Употреба антивирусних програма,
- Унапређење система аутентификације, ауторизације и енкрипције оперативног система.

4.5.5.1 ЕДУКАЦИЈА КОРИСНИКА

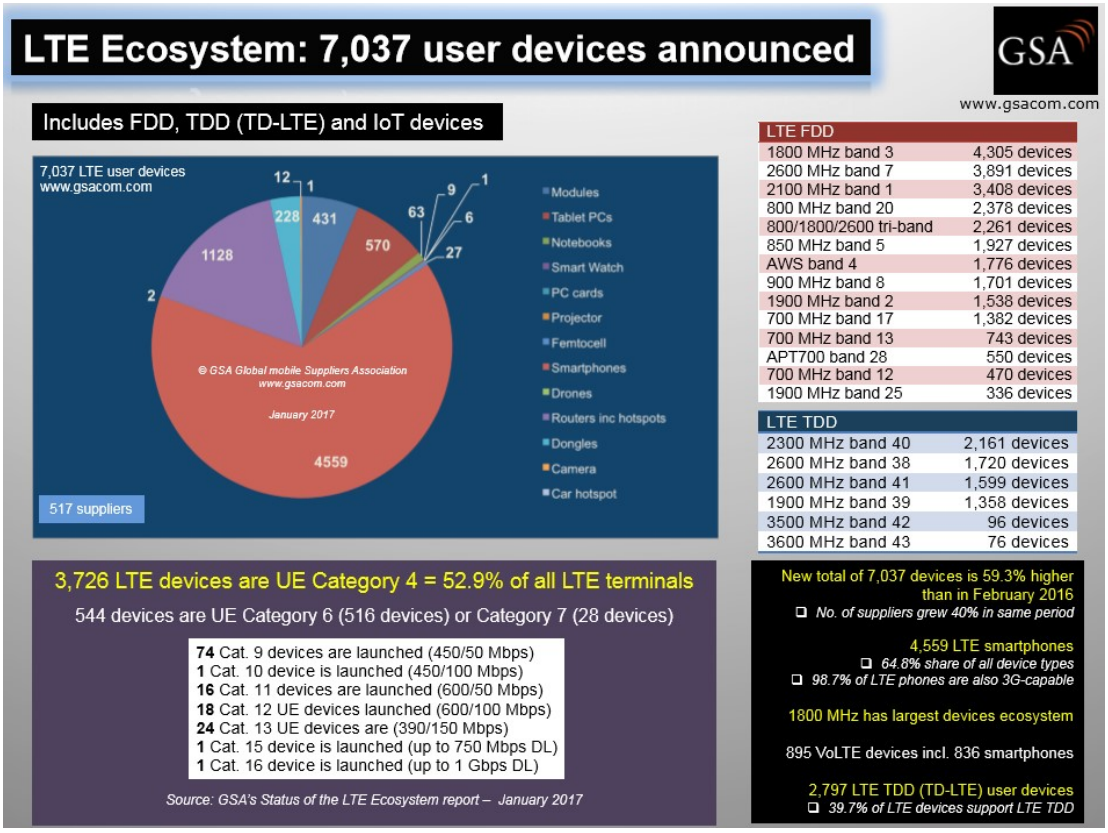
Едукација корисника је најосновнији и најефикаснији вид заштите корисника. Потребно је не само мобилни оператери и информатичко друштво да едукују кориснике већ да и они сам имају свест каквим су све ризицима изложени уколико свој уређај користе крајње непажљиво. Обзиром да продавци мобилних уређаја и мобилни оператери у жељи да што више профитирају овај сегмент потпуно занемарују. Приликом куповине уређаја или SIM картице кориснику вероватно нигде не кажу да опрезно користи свој уређај и да чува своју приватност од других. Такође регулаторна тела која би требала да се брину како о правима оператера тако би требала да брину и о правима корисника мобилних уређаја.

Један од начина да се корисник изложи ризицима је да се оператери обавежу да се омогућити сигурно коришћење својих капацитета и да обезбеде кориснику да сигурно користе пружене услуге у складу са унапред одређеним принципима. Сигурно је да би овај начин односа између корисника и оператера побољшао безбедносне аспекте али би са друге стране сигурно имао ограничавајући карактер по самог корисника. Као пример можемо навести инсталирање апликација које нису са званичних сервера већ из извора који нису сигурни[10].

[10] Third party applications – апликације које се не налазе за званичним серверима за софтверске алате (*Google Play Store, App Store, Blackbebby World, Amazon Store*)

4.5.5.2 СТАНДАРДИЗАЦИЈА И БОЉА КОНТРОЛА КВАЛИТЕТА ПРОИЗВОЂАЧА МОБИЛНИХ УРЕЂАЈА И СОФТВЕРА

Број мобилних уређаја вртоглаво расте сваким даном, на слици 23 можемо видети како се број повећава и тренутно имамо 7037 уређаја који могу да се категоришу као LTE уређаји. Видимо да је број уређаја већи за готово 60% у односу на исти период прошле године, такође је и број понуђача увећан за готово 40% што указује на веома убрзан раст тржишта.



Слика 23 LTE екосистем Јануар 2017. године[11]

Произвођачи опреме треба да заједно са мобилним операторима да установе неопходне стандарде и нивое контроле уређаја. Такође потребно је да се константно ажурира ниво стандарда који произвођачи треба да задовоље да би уређаји могли да се користе у оквиру постојећих мобилних мрежа. На тај начин штите се и произвођачи опреме, мобилни оператери и сами корисници.

[11] Статистички подаци су са вебсајта *gsacom.com – Global Mobile Suppliers Association*

4.5.5.3 УПОТРЕБА АНТИВИРУСНИХ ПРОГРАМА

Мобилни уређаји као и рачунари поседују антивирусне програме који штите софтвер и корисника од малициозних напада. На персоналним рачунарима ниво свести о коришћењу антивируса је значајно виши од корисника мобилних уређаја. У складу са извештајем IT Security Survey 2016 компаније AV Comparatives[12] [26] готово 30% корисника мобилних уређаја не користе никакав систем заштите изузев сигурносних мера које су већ имплементиране у оперативни систем. Сваки мобилни уређај би требало да има инсталиран антивирусни програм који је редовно ажуриран, ово решење је могуће једино да се у оквиру оперативног система понуди овакав софтвер као обавезан. На овај начин корисник би био заштићенији него без икакве заштите, иако и сами антивирусни програми су мета хакера који свакодневно траже пропусте како би исте злоупотребили.

4.5.5.4 УНАПРЕЂЕЊЕ СИСТЕМА АУТЕНТИФИКАЦИЈЕ, АУТОРИЗАЦИЈЕ И ЕНКРИПЦИЈЕ ОПЕРАТИВНОГ СИСТЕМА

Мобилни уређаји би требали да имају јачи систем аутентификације корисника када покушава да користи уређај, односно да се изврши верификација корисника. Данас постоји различити начини аутентификације, од пин кода, читача отиска прста, комбинације знакова на дисплеју. Међутим и поред ових метода иницијалне заштите корисници готово да не користе ни један. Што значи кад неко узме туђ уређај вероватноћа да неће успети да му приступи је равна статистичкој грешци. Корисници би свакако требали да користе овај систем заштите, јер би се на овај начин онемогућио брз и приступ подацима на уређају. Ауторизација омогућава или забрањује приступ подацима на уређају. Уређаји треба да имају подешен кориснички систем тако да одређени корисник може да приступи одређеном нивоу података. Овакав начин ће да понуди другачији вид заштите по нивоима. На крају LTE корисници треба да одабирају уређаје који омогућавају енкрипцију података као највиши вид заштите.

4.6 ПРИСТУПНА ИНФРАСТРУКТУРА

Приступна инфраструктура је комплексан део мобилних комуникација који је директно у надлежности мобилних оператера. Систем је усклађен са међународно прописаним нормама и као такав је доступан обичном кориснику. Корисник ни на који начин не може да утиче на

[12] www.av-comparatives.org

приступну инфраструктуру или да било шта мења већ само да користи ресурсе исте конекцијом са својим мобилним уређајем.

На слици 1 видимо како се одвија комуникација између мобилног уређаја и E-UTRAN приступне мреже. Као и у случају мобилних уређаја безбедносне претње можемо поделити у следеће групе:

- Физички напад,
- Лажна базна станица (eNodeB clon cell),
- Пресретање саобраћаја,
- Повреда приватности.

4.6.1 Физички напад

Повећани захтеви за доступношћу LTE капацитета на територијалном нивоу, а посебно у густо насељеним областима и урбаним зонама где се налази велики број корисника доводи то тога да мрежна инфраструктура бива физички доступна. Пример можемо да узмемо савремени тржни центар, који је свакодневно препун посетилаца који желе да користе напредне LTE функције. Да би оператери омогућили ове услуге врши се уградња терминалне опреме која се огледа у фемто базним станицама (*femtocell*) и кућним мини базним станицама (*Home eNodeB - HeNodeB*). Оваква опрема је доста јефтинија од регуларних базних станица. Огледа се у смањеним капацитетима, слабијом покривеношћу, али и слабијим безбедносним систем. Обзиром да ове углавном нису физички заштићене омогућавају несметан приступ и конекцију на исту са одговарајућом опремо, а самим тим и приступу мрежи.

4.6.2 Лажна базна станица

Лажне базне станице имају различите намене, од прикупљања идентификационих података до пресретања садржаја. Лажне базне станице се користе са клонирају постојеће базне станице и да на тај начин комуницирају са мобилним уређајима. Једна од варијанте употребе је и IMSI Catcher . Проблем није уколико ове уређаје користе владине агенције које за то имају дозволу од релевантних државних институција. Међутим обзиром на доступност технологија и бесплатних софтверских решења, уз познавање технологије могуће је направити један такав уређај са основним функционалностима[27].



Слика 24 LTE IMSI catcher[13] - лабораторијски модел

На слици 24 приказан је један модел IMSI Catcher-a који је у ствари лабораторијски модел који може да се користи у малим просторијама, обзиром да има малу снагу, али апсолутно функционално задовољава по питању прикупљања идентификационих података и лоцирање мобилних уређаја у домету.

4.6.3 ПРЕСРЕТАЊЕ САОБРАЋАЈА

Пресретање саобраћаја је један од најтежих изазова за нападача у LTE мрежама, међутим уколико успе да искористи одређене недостатке у мрежи може на известан начин да декриптује податке корисника. Пресретање саобраћаја може да се реализује: прислушкивањем, преусмеравањем корисника, MitM напад и DoS (*енг. Denial-of-Service*) напади. Једна од мана која је позната и добар је пример како се може пресрести саобраћај је ситуација када се идентификација мобилног уређаја пренесе без енкрипције, као слободан текст у оквиру иницијалне приступне процедуре [28] [29]. Ова мањкавост омогућава да пресретач прати мобилни уређај или да изврши напад MitM користећи ИМСИ број корисника, што је претходно већ појашњено.

[13] Преузето са https://arstechnica.com/security/2015/10/low-cost-imsi-catcher-for-4glte-networks-track-phones-precise-locations/

4.6.4 ПОВРЕДА ПРИВАТНОСТИ

Повреда приватности је писана у [30] и огледа се у принципу да нападач може вишеструко искористи процедуру упита мобилног уређаја за идентификационим подацима (*paging procedure*) да лоцира мобилни уређај. Наиме нападач прозва мобилни уређај шаљући захтеве за ИМСИ или TMSI више пута. Затим добијене резултате корелише са претходним и на тај начин идентификује корисника на датој локацији и има могућност да га лоцира. На овај начин може да се лоцира корисник, али не и да се пресретне саобраћај. За пресретање саобраћаја потребно је да се саобраћај прво пресретне а затим декриптује, што је за мобилне мреже 4. генерације за сада тешко изводљиво али не и немогуће.

4.6.5 ПРЕВЕНТИВНЕ МЕРЕ

Превенција напада на нивоу приступне инфраструктуре огледа се у следећим поступцима:

- Физичка заштита опреме,
- Надзор мреже, (IPS (*енг. Intrusion prevention systems*) monitoring),
- Ауторизација, аутентификација и енкрипција,
- Унапређење безбедности архитектуре.

4.6.5.1 ФИЗИЧКА ЗАШТИТА ОПРЕМЕ

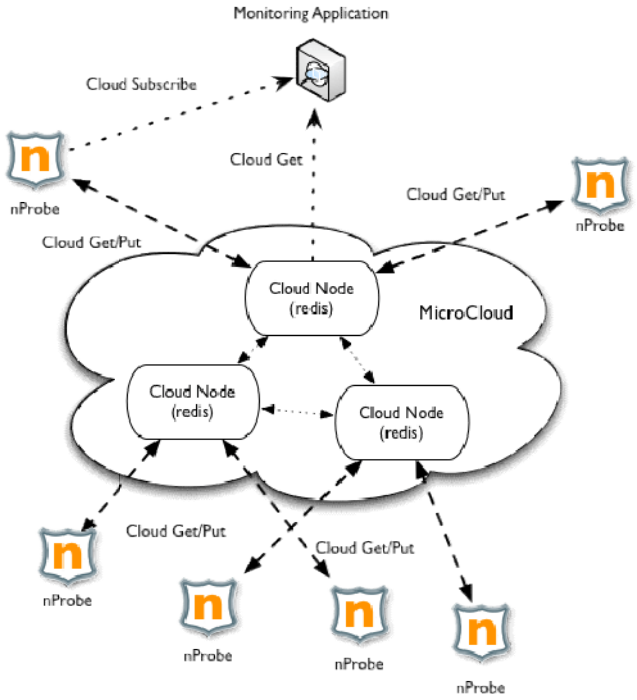
Мобилни оператери би требали да обезбеде да њихова мрежна опрема буде физички недоступна за конекцију од стране нежељених субјеката. Овде се посебно мисли на мале базне станице које се инсталирају унутар објеката. Уколико се било ком кориснику омогући да физички приступи мрежној опреми треба се постарати да на уређајима постоје дефинисане листе корисника који могу да се ауторизују на уређају. То је најосновнији вид заштите али и ин је довољан да се лице које покуша неовлашћено да приступи уређају успори у намери.

4.6.5.2 НАДЗОР МРЕЖЕ

Превенција злоупотребе бежичних мрежа, односно системи који се користе за заштиту могу функционално да се употребе и у случају лажних базних станица у LTE мрежама. Наравно системе треба прилагодити специфичној функцији. Оператери у свом систему заштите треба константно да мониторишу стање инфраструктуре, на начин да систем сам алармира аномалије у мрежи као и појаву чинилаца који нису саставни део система. Надзор

мреже не треба да буде само у обавези оператера већ и регулаторних тела за телекомуникације, као више инстанце.

За надзор мреже са техничког становишта користе се посебни хардверски уређаји. Можемо га разматрати као IDS (*енг. Intrusion Detection System*) и IPS надзор. Да ли су потребна ова система? Уколико узмемо у обзир први систем који детектује упад у мрежу, аларм са истог нам говори да је до упада дошло и да је потребно одмах реаговати како би се што више смањила штета. Треба узети у обзир да један овакав систем ће сигурно генерисати велики број аларма дневно и потребно је ипак да човек мониторише систем, како би могао да раздвоји шта је лажно а шта стварно. Други систем је везан за превенцију. Уколико желимо квалитетан ниво заштите потребно је да користим оба система. Овакви системи су у понуди водећих светских произвођача мрежне опреме и система за безбедност (Cisco, McAfee, Fortinet, Sourcefire, IBM, TippingPoint, Juniper) [31].



Слика 25 Методика надзора мреже коришћењем сонди[14]

Систем је конципиран тако што се на више места у мрежи постављају сонде које мониторишу систем. За мониторинг се користи GTP (*енг. GPRS Tunnelnig Protocol*) протокол. Циљ је да се мониторише саобраћај у мобилним мрежама свих генерација. Протокол функционише у два одвојена сегмента, односно посебна протокола. Први је GTP-U који се користи за мониторинг саобраћаја који је транспортован кроз мрежу (пошта, претраживање,

[14] Ппреузето са http://www.ntop.org/nprobe/monitoring-mobile-networks-2g-3g-and-lte-using-nprobe/

игрице...). Други је протокол GTP-C који се користи да прати сигнализацију ка језгру мреже. Мониторише пријављивање и одјављивање корисника са мреже (мониторише идентификационе параметре IMSI, APN (*енг. Access Point Name*)). Комплетан прикупљени садржај се чува у базама података и може да се користи за накнадну анализу[32].

4.6.5.3 АУТОРИЗАЦИЈА, АУТЕНТИФИКАЦИЈА И ЕНКРИПЦИЈА

Иницијална спецификација безбедносних процедура за 3GPP која је важећа и за LTE мобилне мреже је дата у документу TC 33.203 [32]. Документ дефинише механизме аутентификације, као и обезбеђење саобраћаја између језгра мреже и мобилног уређаја. Јака енкрипција и аутентификација мобилног уређаја у фази приступања мрежи обезбеђују да исти буду безбедни од лажних базних станица и разних врста напада.

Адаптивни кључеви – PKI (*енг. Public Key Infrastructure*) који уз кључ који се налази на самој SIM картици уређаја омогућавају да мобилни уређај енкриптује садржај који пласира ка базној станици. Као пример можемо узети енкрипцију ИСМИ идентификатора. Енкрипцију би требало имплементирати између мобилног уређаја и базне станице на начин да се осујети напад, на пример када нападач потражује од мобилног уређаја идентификационе податке или локацију[30].

4.6.5.4 УНАПРЕЂЕЊЕ БЕЗБЕДНОСТИ АРХИТЕКТУРЕ

Пораст корисника LTE мрежа, као и количина података која се транспортује кроз мрежу расте експоненцијално. Мобилни оператери су суочени да са све већом потражњом капацитета обезбеде да QoS буде на што вишем нивоу. Овде се посебно издвајају безбедносни аспекти који треба да обезбеде потребан ниво сигурности а да не наруше QoS. Савремена решења као и развојни пројекти да се изврши предикција потребних капацитета мреже и да се у складу са истим пројектује и имплементира.

4.7 ЈЕЗГРО МРЕЖЕ (EVOLVED PACKET CORE (EPC))

Језгро мреже је есенцијалан део и у њему су обједињени сви чиниоци мреже. ЕПЦ је задужен за аутентификацију корисника, приступну ауторизацију, управљање корисничким налозима (*AAA - user authentication, access authorisation and accounting*), ИП алокацију, трансфер сигнализације, потрошњу, QoS и безбедност [32]. У овом одељку ће посебно бити разматрана безбедност језгра мреже. Безбедносни изазови језгра мреже као и транспортног слоја се огледају у следећим категоријама:

- Неауторизовани приступ,

- DoS и DDoS (*енг. Distributed Denial of Service*) напади,
- Злоупотреба ИП адресе претплатника.

4.7.1 НЕАУТОРИЗОВАНИ ПРИСТУП

Неауторизовани приступ је један од проблема који се посебно јавља у сегменту пружања услуга роминга. Наиме мобилни оператери морају да деле своју аутентификацију са другим операторима приликом коришћења роминга, а посредник је сам мобилни уређај који се конектује на интернет посредством роминг провајдера. Не знајући какав систем заштите користи конектовани мобилни уређај мобилни оператер мора да обезбеди трансфер података и поред тога је и одговоран за безбедност наведеног корисника у мрежи. Ово је велики изазов за сваког мобилног оператера јер нажалост стандарди заштите нису на истом нивоу код сваког оператера. На тај начин може да се омогући неовлашћен приступ самом језгру мреже. Уколико заштитни протоколи у виду IPsec (*енг. Internet Protocol Security*), IKE (*енг. Internet Key Exchange*), D-H (*енг. Diffie–Hellman key exchange*), EAP (*енг. Extensible Authentication Protocol*), ESP (*енг. Encapsulating Security Payload*) нису имплементирани контрола саобраћаја не постоји а самим тим ни заштита језгра мреже [7].

4.7.2 DOS И DDOS НАПАДИ

Као што је објашњено у претходним поглављима миграција СС7 у дијаметар доста оператера није сигурно да ће ова миграција донети значајан напредак у безбедности, односно безбедносним пропустима у мобилним мрежама. Наши мобилни уређаји нису имуни на DoS нападе као ни било који уређај који своје ресурсе повлачи из ИП базираних структура. У складу са [33] можемо да DoS нападе у LTE мрежама групишемо у следеће категорије:

- DoS напади преко локацијског захтева, CLR (*енг. Cancel Location Request*) – локални претплатнички сервис (HSS) захтева од MME да обрише корисника са мреже,
- DoS напади преко захтева за упис новог претплатника, IDR (*енг. Insert Subscriber Data Request*) – HSS доставља захтев за MME да упише новог корисника и да му проследи податке о статусу и локацији,
- DoS напад преко захтева за тренутном локацијом, ULR (*енг. Update Location Request*) – MME од HSS захтев да му проследи тренутну локацију уколико је претплатник променио исту. Претплатник током овог захтева може да буде искључен са мреже али без већих последица. У најгорем случају мораће да рестартује мобилни уређај.

Сличан приступ је и кад су у питању DDoS напади.

4.7.3 Злоупотреба ИП адресе претплатника

Једна од особина LTE мрежа која је нужно прихваћена због широкопојасног карактера је и IP протокол који је са собом донео недостатке и безбедносне ризике који су одавно познати. Преузимање IP адресе, спуфинг, инсталација нежељених пакета преко мреже, све су то сада проблеми и LTE мрежа. Хаковање уређаја и крађа као и инсталирање малициозних садржаја како би се експлоатисали приватни подаци у циљу злоупотребе су сада реалност. Нападач може да искористи претплатника тако да му изазове трошкове, такође у случају да иста IP адреса се промени и додели другом претплатнику злоупотреба може да се настави [34].

4.7.4 Превентивне мере

Превентивне мере које би унапредиле систем заштите језгра мреже су делимично сличне као и у случају приступне мреже. У складу са претходним детаљима из анализе превентивне мере је могуће категорисати по следећем:

- Имплементација безбедније архитектуре,
- Унапређење енкрипције,
- Надзор мреже.

4.7.4.1 Имплементација безбедније архитектуре

Обзиром на препоруке за 3GPP које су наведене у [32] потребно је да се у архитектуру имплементирају IPsec као обавезни и саставни део мреже. Унапређење архитектуре искључиво зависи од мобилног оператера, финансијских могућности, али о од регулаторних тела која могу да својим уредбама утичу на брзину и начин имплементације. IPsec би требало да се налазе и у сегменту контроле мрежних контролних протокола и сегмента саобраћаја који остварује претплатник. Још један ефикасан систем заштите може да се реализује имплементацијом VPN (*енг. Virtual Private Network*) и VLAN (*енг. Virtual Local Area Network*) мрежа [35]. Препорука је да се у наредном периоду користи VPN за безбедан трансфер података у језгро. За ову намену можемо користити посебне издвојене VLAN мреже. На овај начин саобраћај се може изоловати у одређене зоне мреже које су дефинисане самим VLAN мрежама. Тако да уколико и дође до нарушавања безбедности оно се завршава у одређеном сегменту мреже и не шити се даље [35]. На овај начин могући нападач се доводи у слепу

улицу и поступак упада мора да понавља изнова. Имплементација ове методологије мрежу чини безбеднијом али и доста комплекснијом.

4.7.4.2 Унапређење енкрипције

Као и у претходном случају у складу са [32] дате су препоруке за начин и врсте енкрипције које је потребно имплементирати. Врсте енкрипције које су претходно наведене потребно је само да се имплементирају у систем и да се активно користи. На овај начин нападач чак и да приступи мрежи или пресретне саобраћај добиће само огроман материјал за декрипцију. А то захтева време, ресурсе и новац, резултат је увек неизвесан. Овде може да се наведе пример квалитетне енкрипције коју користи компанија Apple на својим уређајима. Наиме у случају када су покушали да декриптују мобилни телефон Iphone уложили су огромне ресурсе и новац и на крају је дискутабилно да ли је било успешно. Ово је и одличан пример како произвођач својом политиком штити корисника своје опреме од одавања личних података[15].

4.7.4.3 Надзор мреже

Константан надзор мреже на свом нивоима је од круцијалног значаја за безбедност. Наиме и поред све опреме која ради углавном аутономно, нападачи су увек и на неки нови начин домишљати да системе заштите или заобиђу или заварају. У овом сегменту човек је кључни играч и са једне и са друге стране. Правовремено уочавање неправилности је од изузетног значаја за правовремено реаговање и спречавања нежељених последица. Безбедност не зависи само од једног оператера већ и од суседних зато је потребно да сви заједно подигну ниво надзора.

Језгро мреже треба да се штити од удара на било који саставни елемент. Управљање саобраћајем треба да обезбеди правилно оптерећење елемената језгра. За пример можемо узети DoS напада који се на овај начин може готово неутралисати без последица по функционалност система.

4.8 Сервисна мрежа

Сервисна мреже или једноставније приступна мрежа је крајњи циљ корисника који користи LTE капацитете. Углавном је тај садржај везан за интернет и сервисе које пружа

[15] Информација преузета са а https://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/

претплатнику. IP мултимедијални подсистем - IMS је начин да се мултимедијални садржаји доставе претплатнику. Безбедносни менаџмент је у овом случају подједнако важан као и QoS. Не треба заборавити да се поред мултимедијалног садржаја кроз приступну мрежу одвијају и операције које су везане за трансфер новца, плаћање, трансфер личних података и других осетљивих података. У складу са наведеним могу се издвоји следећи безбедносни ризици:

- Неовлашћени приступ,
- Злоупотреба сервиса, крађа услуга,
- Неовлашћени надзор, преузимање сесија.

4.8.1 НЕОВЛАШЋЕНИ ПРИСТУП

Архитектура ИМС је отворена и дистрибуциона, као таква креирана је од великог броја тачака које морају бити осигуране. Размена ИП адресе између различитих провајдера, који нуде различите сервисе и услуге, претплатника доводи у ситуацију да стално осцилује између зона са различитим нивоом заштите. Овакав приступ чини језгро ИМС рањивим. Велика количина података би требало да има заштиту у виду механизама који ће омогућити сигуран приступ кориснику. Зоне са различитим заштитом су сегменти који омогућавају да се изврши неовлашћен приступ подацима претплатника у зони када је најмање заштићен или уопште није заштићен. Систем заштите функционише на систему најслабије карике, кад она буде пробијена цео систем је пробијен и угрожен.

4.8.2 ЗЛОУПОТРЕБА СЕРВИСА, КРАЂА УСЛУГА

Злоупотреба сервиса и крађа услуга представљају директан губитак за мобилне операторе. У овом случају претплатник је тај који омогућава злоупотребу јер му је на неки начин онемогућено да има приступ садржајима који немају обични претплатници. Злоупотреба се може вршити само са мобилних уређаја који имају наведене привилегије. Један од начина је да се услуге не тарифирају и на тај начин нападач користи услуге мобилног оператера које он нигде не региструје изузев у заузетости ресурса. Наиме технички се ова злоупотреба спроводи употребом функције за контролу сесије, CSCF (*енг. Call Session Control Function*). Када мобилни уређај неће да се дисконектује са језгра IMS након захтева CSCF, што узрокује да CSCF престаје да обрачунава саобраћај а претплатник остаје и даље повезан на IP сервис и неовлашћено га користи [36].

4.8.3 НЕОВЛАШЋЕНИ НАДЗОР, ПРЕУЗИМАЊЕ СЕСИЈА

Неовлашћени надзор отпочиње када нападач неовлашћено надзире SIP сесију између два корисника. Без заштите SIP конекција једноставно може да се надзире употребом *Wireshark* софтвера који може да снима размену података у SIP сесији. Нападач у истом сценарију може у одређеном тренутку да преузме конекцију и инсталира малициозни софтвер на неки од уређаја. Такође може да прикупља саобраћај, утиче на квалитет размене података [36].

4.8.4 ПРЕВЕНТИВНЕ МЕРЕ

Превенција упада из сервисне мреже, огледа се директно у повећању безбедносних протокола, које можемо поделити на следећи начин:

- Гранична безбедност,
- Укључење безбедносних протокола,
- Јача аутентификација,
- Имплементација безбедносних *gateway-a.*

4.8.4.1 ГРАНИЧНА БЕЗБЕДНОСТ

Сваки сегмент IMS треба да има свој систем заштите, односно свака засебна мрежа треба да буде ограничена на свој ниво заштите, да би се заштитила од неовлашћеног упада из других мрежа. На пример корисници роминг услуга приступају IMS садржаја, односно интернету преко приступне тачке која није безбедна са гледишта провајдера услуга. Тај гранични део треба да буде обезбеђен. Мобилни оператери треба да инвестирају у сигурну архитектуру која садржи *firewall* системе, системе за филтрирање пакета, праћење транслације адреса, VPN и енкрипцију приликом размене података са другим мрежама.

4.8.4.2 УКЉУЧЕЊЕ БЕЗБЕДНОСНИХ ПРОТОКОЛА

Безбедносни протоколи омогућавају безбедност на различитим слојевима мреже, као што је SSL (*енг. Secure Socket Layer*), TLS (*енг. Transport Socket Layer*) и DTLS (*енг. Datagram Transport Socket Layer*). Прикривени надзор садржаја може бити елиминисан енкрипцијом садржаја SIP сигнализације. Мобилни оператери морају да пројектују мрежу тако да омогући све услуге а да притом има имплементирање све безбедносне протоколе. Ово протоколи омогућавају сигурну везу између мобилног уређаја и IMS сервиса.

4.8.4.3 ЈАЧА АУТЕНТИФИКАЦИЈА

Мобилни оператери треба да уведу јачи вид аутентификације између мобилног уређаја и IMS сервиса, као и сигурних *gateway-a* да обезбеди безбедну размену података између претплатника и IMS мреже. Мрежа треба да буде конфигурисана тако са се мобилни уређај пре конекције са ISM сервисом рутира на одговарајући SEG (*енг.Secure Gateway*) и да добије потврду да је IPsec функционалан за пренос података. IPsec омогућава интегритет, безбедности и веродостојност података који су оригинално заштићени одређеним механизмом аутентификације.

4.8.4.4 *ИМПЛЕМЕНТАЦИЈА БЕЗБЕДНОСНИХ* GATEWAY-A

Пошто је једна од основних намена IMS-a да креира јединствену платформу за многобројне провајдере, управљање безбедносним параметрима излази из домена традиционалних *firewall* и рутер платформи. Вишеструке активне платформе захтевају различите нивое QoS, корисничка права, енкрипцију и аутентификацију. Мобилни оператери би требало да унапређују скалабилну безбедносни инфраструктуру и безбедносне *gateway* да би превазишли комплексност комуникација у LTE мрежама.

ЗАКЉУЧАК

Овај мастер рад је пре свега ретроспектива безбедносних изазова који вребају не само у LTE мрежама већ и у мрежама претходних генерација. Технологија пресретања мобилних комуникација и безбедносних ризика који су последица IP утицаја, као и сублимација метода, техника, препорука и механизама заштите корисника мрежа четврте генерације обезбеђује да се читалац овог рада информише и едукује о ризицима којима се излаже током комуникације мобилни уређајем.

Обезбеђење безбедних комуникација је једно од основних начела заштите интегритета претплатника. Добро познавање основних постулата архитектуре мобилне и метода заштите комуникација представља основу за развој техника за пресретање саобраћаја корисницима који за то имају одобрене акредитиве од стране надлежних државних институција. С друге стране познавање безбедносних пропуста у мрежи омогућава нам да правовремено и превентивно делујемо на примену средстава за пресретање од стране лица која их злоупотребљавају. Технике пресретања су одавно превазишле основну намену да се идентификује и лоцира претплатник. Технике као што су активација микрофона, GPS система, преузимање контроле над мобилним уређајем, преузимање садржаја како са уређаја тако и са канала комуникације су напредне функције уређаја за пресретање. Све ове технолошке могућности нам говоре да више ништа не може да буде сакривено или заштићено уколико се користи прави технолошки приступ и уколико претплатник свој мобилни уређај користи без активних система заштите и пре свега савесно.

Анализом безбедносних аспеката мобилних мрежа четврте генерације може се закључити да су безбедносни ризици вишеструки. Сви учесници процеса комуникације треба да на свом нивоу обезбеде да се поштују основни постулати сигурне комуникације. Први и основни чинилац безбедне комуникације су регулаторна тела и институције који се баве креирањем нових и унапређењем постојећих стандарда. Следећи у низу су произвођачи инфраструктуре и мобилних уређаја који треба да имплементирају стандарде и препоруке регулаторних тела. Мобилни оператери као носиоци пружања услуга треба да имплементирају све стандарде који могу да учине комуникацију безбедном и да усвајају препоруке надлежних институција без обзира на трошкове, јер само претплатник који је безбедан у коришћењу услуга је задовољан претплатник. На крају корисник мобилног уређаја мора да буде едукован и свестан да свакодневно излазе своју приватност на милост и немилост различитим претњама које вребају у комуникационом екосистему. Држава преко

регулаторних тела и својим инструментима треба да уложи средства и едукацију корисника, промовише и обезбеди безбедне телекомуникационе услуге.

Ера у којој живимо учинила је да виска технологија буде доступна готово свима, сигурно да обичан корисник не може да направи уређај за пресретање мобилних комуникација. Израда једног оваквог уређаја и са минималним могућностима захтева познавање више различитих технологија, од мобилних телекомуникација, напредног програмирања, система заштите и система простирања сигнала. Истраживањем доступности хардвера и софтверских садржаја на интернету, који су јавно доступни и отворени за даљи развој и унапређења, може се закључити да уређај за пресретање мобилних комуникација са основним функционалностима може израдити група лица која добро познаје наведене области, без потребе за специјализованим технолошким капацитетима. Што имплицира да такав један уређај уколико ји под контролом државних институција може да се злоупотреби и проузрокује нарушавање безбедности корисника савремених мобилних уређаја.

Мобилне комуникације четврте генерације су свакако саставни део наше стварности и у будућности ће повећати своје капацитете кроз 5Г мобилну мрежу. Могућности свакако треба користити, али увек треба да се поштују основна начела безбедне употребе мобилних уређаја.

Мастер рад представља један виши ниво познавања технолошких достигнућа LTE мрежа и свакако је основа за даљи наставак истраживања безбедносних ризика и генерисања нових препорука и механизама заштите.

ЛИТЕРАТУРА

[1] E. Dalham, S. P. (2014). *4G: LTE/LTE-Advanced for Mobile Broadband.* Oxford: Elsevier.

[2] G.R.Sambaskar,.A.D.Raut. A *technical paper on mobile computing (3rd generation)*. *International Journal of Research In Science & Engineering , 1* (1).

[3] M.R. Bhalla, A.V. Bhalla. (2010). Generations of Mobile Wireless Technology: A Survey. *International Journal of Computer Applications (0975 – 8887) , 5*.

[4] (2009). *3GPP TR 33.821 V8.0.0.* Valbonne: 3GPP.

[5] (2016). *Pregled tržišta elektronskih komunikacija u Republici Srbiji.* Beograd: RATEL.

[6] (2016). *Pokrivenost signalom mobilne telefonije u Srbiji* . Београд: РАТЕЛ.

[7] Ali-Yahiya, T. (2011). *Understanding LTE and its Performance.* Springer Science+Business Media.

[8] (2009). *3GPP TR 23.830 V9.0.0.* Valbonne - FRANCE : 3GPP.

[9] M. Veinović, M. Ćajić, B. Brkić. (2012). *Tehnike i metode napada na komunikacioni kanal pri prenosu podataka u mobilnoj telefoniji* . Beograd: Univerzitet Singidunum.

[10] (2007). *ETSI TS 102 656 V1.1.1 (2007-11) - Lawful Interception (LI); Retained Data.* France: ETSI.

[11] M. Solanki, S. Salehi, and A. Esmailpou . (2013). *LTE Security: Encryption Algorithm Enhancements* . Norwitch: ASEE Northeast Section Conference .

[12] Ooi, J. (2015). IMSI Catchers and Mobile Security . *School of Engineering and Applied Science University of Pennsylvania* .

[13] (2013). *LTE Security I: LTE Security Concept and LTE Authentication.* Netmanias.

[14] G. Orhanou, S. El-Hajji. (2013). The New LTE Cryptographic Algorithms EEA3 and EIA3. *Applied Mathematics & Information Sciences , Appl. Math. Inf. Sci. 7, No. 6, 2385-2390 (2013)*.

[15] (2008). *3rd Generation Partnership Project, "TS 33.401: System Arhitecture Evolution (SAE); Seuority arhitecture. Network, ver. 8.1.1, releise 8".* 3GPP.

[16] M. Hofer, J. McEachen, M. Tummala. (2014). Vulnerability Analysis of LTE Location Services. *System Sciences (HICSS), 47th Hawaii International Conference , 10.1109/HICSS.2014.635* .

[17] (2012). *An overview of LTE positioning.* Sunnyvale: Spirent.

[18] (2004). *3GPP TS 29.002 V3.20.0* . 3GPP.

[19] *Diameter Base Protocol*. (2003, September). Retrieved May 11., 2017., from https://tools.ietf.org: https://tools.ietf.org/html/rfc3588

[20] (2014). *ETSI TS 129 173 V12.2.0* . 3GPP.

[21] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi and J-P. Seifert. (2016). Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. *ISBN 1-891562-41-X.* san Diego: NDSS.

[22] M. Rajković, Lj. Marković, M. Arsekić-Kraković, M. Janković . (2014). Pregled tehnologija mobilnog širokopojasnog pristupa i konvergencija ka all-ip bežičnim mrežama. *PosTel* .

[23] H.J. Wang, W. Zhu, C. Guo. Smart Phone Attack and Defence.

[24] (2013). *Deloitte Technology, Media and Telecommunication Predictions 2013.* Deloitte.

[25] (2016). *Mobile Threat Report What's on the Horizon for 2016.* McAfee.

[26] (2016). *IT Security Survey 2016.* AV comparatives.

[27] G. Escudero-Andreu, R. C.-W. Phan and D. J. Parish. (2012). Analysis and Design of Security for Next Generation 4G Cellular Networks. PgNET .

[28] D.. Perez, J. Pico. (2011). *A practical attack against GPRS/EDGE/UMTS/HSPA mobile data.* Washington DC: Taddong BlackHat DC 2011 Briefings .

[29] C.-E. Vintilă, V.-V. Patriciu, I. Bica. (2011). Security Analysis of LTE Access Network. *ISBN:978-1-61208-113-7*.

[30] M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon, R. Borgaonka. (2012). New Privacy Issues in Mobile Telephony: Fix and Verification.

[31] *Monitoring Mobile Networks (2G, 3G, and LTE) using nProbe*. (2013). Retrieved April 15, 2017, from http://www.ntop.org: http://www.ntop.org/nprobe/monitoring-mobile-networks-2g-3g-and-lte-using

[32] (2008). *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services (Release 7).* ITU.

[33] Sheridan, K. (2016, 11 7). *4G Cellular Networks At Risk Of DoS Attacks*. Retrieved 05 03, 2017, from www.darkreading.com: http://www.darkreading.com/mobile/4g-cellular-networks-at-risk-of-dos-attacks/d/d-id/1327422

[34] Dong W. Kang, Joo H. Oh, Chae T. Im, Wan S. Yi and Yoo J. Won. (2013). A Practical Attack on Mobile Data Network Using IP Spoofing.

[35] Miguel Angel Alvarez, Frederic Jounay, Tamas Major, Paolo Volpato. (2011). *LTE backhauling deployment scenarios.* NMG.

[36] E. Belmekki, N. Bouaouda, B.Raouyane, M. Bellafkih. (2013). IP multimedia subsystem: security evaluation. *51* (1992-8645).

СПИСАК СЛИКА

Слика 1 Еволуција мобилних комуникационих система..... 9
Слика 2 Ћелијска структура мреже [1]..... 11
Слика 3 Спецификација захтева за LTE мреже у издањима 3GPP [1]..... 13
Слика 4 Могућности мобилних мрежа 4. генерације..... 14
Слика 5 Приказ раста броја LTE уређаја..... 15
Слика 6 Анализа броја претплатника у оквиру LTE мрежа као и предикција раста корисника за 2020. годину..... 15
Слика 7 Упоредни приказ покривености територије Р. Србије сигналом LTE мобилне телефоније [6]..... 17
Слика 8 LTE референтни модел [7]..... 19
Слика 9 Функционална шема LTE архитектуре мреже..... 19
Слика 10 Комуникациони протоколи по нивоима..... 21
Слика 11 VoLTE секвенца успостављања позива..... 23
Слика 12 Приступна инфраструктура..... 26
Слика 13 Концепт заштите у LTE мрежама [13]..... 29
Слика 14 Централизовани систем надзора комуникација..... 32
Слика 15 Принцип пасивног надзора мобилних комуникација..... 34
Слика 16 Принцип активног надзора мобилних комуникација..... 35
Слика 17 Функционална шема локацијских сервиса у LTE мрежама [20]..... 39
Слика 18 Логички нивои локацијских сервиса у LTE мрежама [16]..... 40
Слика 19 Лажни захтев за локацијом корисника [16]..... 42
Слика 20 Архитектура модела за анализу..... 45
Слика 21 Безбедносне претње са апликативног нивоа..... 47
Слика 22 Повећање претњи од малвера генерисаног кроз апликације мобилних уређаја 52
Слика 23 LTE екосистем Јануар 2017. године..... 54
Слика 24 LTE IMSI catcher - лабораторијски модел..... 57
Слика 25 Методика надзора мреже коришћењем сонди..... 59

СПИСАК ТАБЕЛА

Табела 1 Преглед основних карактеристика мобилних комуникационих мрежа 10
Табела 2 Техничке карактеристике базних станица [1] 26
Табела 3 Алгоритми енкрипције [15] 31
Табела 4 LTE безбедносни кључеви [13] 32

СПИСАК СКРАЋЕНИЦА

3G - Third Generation
3GPP - 3rd Generation Partnership Project
AAA - Authentication, Authorization, and Accounting
A-GNSS - Assisted Global Navigation Satellite System
AoA - Angle of Arrival
APN - Access Point Name
AS - Access Stratum
ASME - Access Security Management Entity
ATM - Asynchronous Transfer Mode
AuC - Authentication Center
AUTN - Authentication Token
AVP - Attribute-Value Pairs
BSC - Base Station Controller
CDMA - Code Division Multiple Access
CK - Cipher Key
CLR - Cancel Location Request
CRF - Charging Rules Function
CS - Circuit switching
CSCF - Call Session Control Function
DDoS - Distributed Denial of Service
D-H - Diffie -Hellman key exchange
DL - Down Link
DoS - Denial-of-Service
DTLS - Datagram Transport Socket Layer
E2E IP - End To End IP)
EAP - Extensible Authentication Protocol
ECID - Enhanced Cell ID
EDGE - Enhanced Data for GSM Evolution
EEA - EPS Encryption Algorithms
EIA - EPS Integrity Algorithms
eNB - e Node B
EPC - Evoluated Packet Core
EPS - Evaluated Packet System
EPS AKA (енг. EPS Authentication and Key Agreement)
ESP - Encapsulating Security Payload
E-UTRA - Evolved UMTS Terrestrial Radio Access
E-UTRAN - Evolved UMTS Terrestrial Radio Access Network
FCC - Federal Communication Commission
FDD - Frequency Division Duplex
GEA - GPRS encryption algorithm
GMLC - Gateway Mobile Location Centre
GPRS (енг. General Packet Radio Services
GSM - Global System for Mobile Communications
GTP - GPRS Tunnelnig Protocol
HARQ - Hybrid Automatic Repeat-reQuest
HeNB - Home eNodeB
HLR - Home Location Register
HSDPA - High Speed Download Packet Access

HSPA - High Speed Packet Access
HSS - Home subscriber server
HSUPA - High Speed Upload Packet Access
IDR - Insert Subscriber Data Request
IDS - Intrusion Detection System
IK - Integrity Key
IKE - Internet Key Exchange
IMEI - International Mobile Equipment Identity
IMS - IP Multimedia Subsystem
IMSI - International Mobile Phone Subscriber
IMT-Advanced - International Mobile Telecommunications-Advanced
IP - Internet Protocol
IPS - Intrusion prevention systems
IPsec - Internet Protocol Security
LAC - Local Area Code
LAN - Local Area Network
LBS - Location Based Services
LCS - Location Services
LPP - LTE Positioning Protocol
LTE - Long Term Evolution
MAC - Media Access Control
MCC - Mobile Country Code
MIMO - Multiple Input Multiple Out
MitM - Man in the Middle
MME - Mobility Management Entity
MNC - Mobile Network Code
MSC-a - Mobile Switching Center
MSIN - Mobile Subscriber Identification Number
MSISDN - Mobile Subscriber Integrated Services Digital Network
NAS - Non-access stratum
OFDMA - Ortogonal Frequency Division Multiple Access
OTDOA - Observed Tome Differencial of Arrival
PCRF - Policy and Charging Rules Function
PDCP - Packet Data Convergence Protocol
PDF - Policy Decision Function
PDN - Public Data Network
PDN GW - Public Data Network Gateway
PDU - Protocol Data Unit
PKI - Public Key Infrastructure
PPR - Privacy Profile Register
PRS - Position Reference Signal
PS - Packet switching
PSTN - Public Switched Telephone Network
QAM - Quadrature Amplitude Modulation
QoS - Quality of Service
RADIUS - Remote Authentication Dial-In User Service
RAND - RANDom number
RAT - Radio Access Technology
RLC - Radio Link Control
RRC - Radio Resourse Control
RSRP - Reference Signal Received Power
RTP - Realtime Transfer Protocol

RTT - Round Time Trip
SAE - System Architecture Evolution
S-CSCF - Serving - Call Session Control Function
SCTP - Stream Control Transmission Protocol
SEG - Secure Gateway
SGW - Signaling Gateway
SIM - Subscriber Identity Module
SIP - Session Initiation Protocol
SMS - Short Message Service
SQN - Sequence Number
SRES - Signed Response
SS7 - Signaling System 7
SSL - Secure Socket Layer
SUPL - Secure User Plane Location
TA - Timing Advance
TAC - Tracking Area Code
TDD - Time Division Duplex
TDMA - Time Division Multiple Access
TLS - Transport Socket Layer
TMSI - Temporary Mobile Subscryber Identity
UE - Eser Equipment
UL - Up Link
ULR - Update Location Request
UMTS - Universal Mobile Telecommunications System
VLAN - Virtual Local Area Network
VLR - Visitor Location Register
VoIP - Voice over IP
VoLTE - Voice over LTE
VPN - Virtual Private Network
WCDMA - Wideband Code Division Multiple Access
WiFi - Wireless Fidelity
WiMAX - Worldwide Interoperability for Microwave Access
WWAN - Wireless Wide Area Network
XRES - Expected Response