Mobilne mreže četvrte generacije

Stipetić, Boris

VELEUČILIŠTE U KARLOVCU

STROJARSKI ODJEL

Stručni studij mehatronike

Boris Stipetić

.

Mobilne mreže četvrte generacije

ZAVRŠNI RAD

Karlovac, srpanj 2015.

VELEUČILIŠTE U KARLOVCU

STROJARSKI ODJEL

Stručni studij mehatronike

Boris Stipetić

.

Mobilne mreže četvrte generacije

ZAVRŠNI RAD

MENTOR: mr.sc. Vedran Vyroubal

Karlovac, srpanj 2015.

VELEUČILIŠTE U KARLOVCU

Stručni studij: **Mehatronika**

Usmjerenje:…….....Karlovac, 19.05.2015.

ZADATAK ZAVRŠNOG RADA

Student: Boris Stipetić Matični broj:0112612076

Naslov: **MOBILNE MREŽE ČETVRTE GENERACIJE**

Opis zadatka:

U završnom radu opisati arhitekturu i tehničke zahtjeve mreže četvrte generacije.

Rad treba obuhvatiti sljedeće cjeline:

1. Općeniti prikaz arhitekture LTE mreža

   princip rada; opis pristupne mreže; opis sučelja; opis evoluiranog čvora (eNodeB)
2. Opisati jezgreni dio mreže

   entitet upravljanja pokretljivošću; uslužni prilazni čvor; paketski mrežni prilazni čvor; čvor za upravljanje resursima i terećenje; poslužitelj domaćih pretplatnika
3. Opisati protokolni

   korisnička ravnina; kontrolna ravnina; osnovne razlike između TCP i SCTP
4. Opisati sigurnosne zahtjeve i mehanizme LTE mreže

   sigurnosne ravnine; koncept ključeva; autorizacija i autentifikacija; moguće napadi na LTE mrežu

Zadatak zadan:	Rok predaje rada:	Predviđen datum obrane:
19.05.2015.	20.12.2015.	Petnaest dana nakon predaje rada

Mentor: Predsjednik Ispitnog povjerenstva:

mr.sc. Vedran Vyroubal Marijan Brozović, dipl. ing.

Izjava

Izjavljujem da sam ovaj završni rad izradio samostalno, koristeći znanje stečeno tijekom studija i obavljanja stručne prakse, služeći se navedenom stručnom literaturom.

Sažetak

LTE kao mreža četvrte generacije, predstavlja prvi korak u ostvarenju ideje pokretnih komunikacija koje će se u potpunosti temeljiti na protokolu IP. Arhitektura mreže temeljene samo na komutaciji paketa poboljšana je i pojednostavljena, tako da se smanjio broj čvorova, ali je i dalje zadržana podjela na pristupnu (LTE) i jezgrenu (SAE) mrežu. Sigurnost mreže, također, treba prilagoditi novoj arhitekturi, pa su sigurnosni mehanizmi razdvojeni u više slojeva. Hijerarhija ključeva i dalje ostaje koncept po kojem se šifriraju podaci, no razvija se i svojom većom složenošću te smanjuje mogućnost neželjenog dešifriranja.

Ključne riječi: LTE, SAE, E-UTRAN, ravna arhitektura, sigurnost, IPsec, hijerarhija ključeva, autorizacija, autentifikacija

Summary

As a network of the fourth generation, LTE is the first step in the process of creating mobile communications based on the all-IP architecture. The packet switching network architecture has been improved and simplified by reducing the number of nodes, however the network has remained divided on the access network (LTE) and the core network(SAE). The network safety had to be modified to suit the new architecture. This was achieved by dividing the safety mechanisms in multiple layers. The Key hierarchy remains the method of data encryption. However the depth of the encryption has been slightly changed and it can now offer higher safety standards against unwanted data deciphering.

Key words: LTE, SAE, E-utran, flat architecture, security, IPsec, key hierarchy, authorization, authentification

Sadržaj

Sažetak 6

Summary 6

1. Uvod 8

2. Arhitektura LTE/SAE mreže 9

2.1. Pristupna mreža 9

2.1.1. OFDM 10

2.1.2. Sučelje X2 12

2.1.3. Evoluirani čvor B (eNodeB) 12

2.2. Jezgrena mreža 12

2.2.1. Entitet upravljanja pokretljivošću 13

2.2.2. Uslužni prilazni čvor 14

2.2.3. Paketski mrežni prilazni čvor 14

2.2.4. Čvor za upravljanje resursima i terećenje 15

2.2.5. Poslužitelj domaćih pretplatnika 15

2.3. Protokolni složaj 16

2.3.1. Korisnička ravnina 16

2.3.2. Kontrolna ravnina 18

2.3.3. Osnovne razlike između TCP-a i SCTP-a 18

3. Sigurnost 20

3.1. IPsec 22

3.2. Sigurnosne ravnine 23

3.3. Koncept ključeva 26

3.4. Autorizacija i Autentifikacija 28

3.5. Mogući napadi na LTE mrežu 30

3.5.1. Napad na transportnom sloju 30

3.5.2. Napad na korisničku ravninu 32

3.5.3. Napad na korisnički terminal 32

4. Zaključak 34

5. Literatura 35

6. Popis kratica 36

1. Uvod

Pokretni su uređaji već duži niz godina nešto bez čega prosječni čovjek ne može zamisliti život. Kao i svaka tehnologija, tako i ova napreduje iz dana u dan. Iako bismo pomislili da smo s 3G/3.5G mrežama bili u mogućnosti raditi sve što nam treba, pa i više, razvoj tu nije stao. S razvojem tehnologije povećat će se brzina prijenosa podataka, te je za očekivati da ćemo u skoroj budućnosti imati još veće brzine prijenosa podataka.

LTE (engl. *Long Term Evolution*) je 4G mreža koja predstavlja sljedeći korak u tehnologiji pokretne mreže. Pruža velike brzine prijenosa podataka i svrstava se u inteligentne mreže. U današnje vrijeme korisnici se služe aplikacijama koje zahtijevaju sve veće brzine prometa podataka. Korisnici, osim brzine žele kvalitetu, sigurnost i što jeftiniji promet podacima. Najznačajnija inovacija u novoj generaciji mreža, s kojom se želi postići sve ono što tržište zahtijeva, je prelazak na arhitekturu koja je u potpunosti bazirana na protokolu IP (eng. *Internet Protocol*). Takvom se arhitekturom želi doći do trenutka kada se komutacija kanala više neće koristiti u mreži, već će cjelokupna mreža biti bazirana na komutaciji paketa.

Brzine koje se postižu u LTE mreži povećane su na 100Mbit/s u silaznoj vezi i 50Mbit/s u uzlaznoj vezi. Osim arhitekture koja je poboljšana da bi se postigle veće brzine, koncept sigurnosnog mehanizma također se bazira na prethodnoj izvedbi u UMTS mreži. Kraj poboljšanja brzina, sigurnosti, kapaciteta i arhitekture ne dolazi sLTE-om. LTE ima nasljednika u mrežama, LTE-A (engl. *Long Term Evolution Advanced*), mrežu koja se temelji na LTE-u i teži novim poboljšanjima.

2. Arhitektura LTE/SAE mreže

Predstavnik četvrte generacije pokretnih mreža [1] je evoluirani paketski sustav (engl. *Evolved Packet System,* skraćeno EPS) koji čine LTE (engl. *Long Term Evolution*) i SAE (engl. *System Architecture Evolution*). Kao i u prijašnjim generacijama pokretnih mreža, EPS se sastoji od pristupnog i jezgrenog dijela, pa tako LTE predstavlja pristupni, a SAE jezgreni dio. Bitna razlika u odnosu na prijašnje generacije mreža je uvođenje takozvane ravne arhitekture (engl. *flat architecture*) čija je osnovna značajka da se i jezgrena i pristupna mreža sastoje od po jednog čvora. Jezgrena i pristupna mreža se sastoje od jednog čvora zbog toga što mreža ima kraći odziv što ima manje elemenata u svojoj strukturi. Suprotno, što je više elemenata, više puta podaci moraju biti razmijenjeni i komunikacija duže traje – što nikako nije poželjno kada je riječ o odzivu mobilnih mreža.

2.1. Pristupna mreža

Pristupni dio mreže LTE/SAE naziva se još i evoluirana UMTS zemaljska radijska pristupna mreža (engl. *Evolved UMTS Terrestrial Access Network*, skraćeno E-UTRAN). Struktura mu je bazirana na OFDM (engl. *Orthogonal Frequency Division Multiple Access*) tehnologiji za silaznu vezu i SC-FDMA (engl. *Single Carrier Frequency Division Multiple Access*) za uzlaznu vezu koju možemo smatrati poprilično jednostavnom, s obzirom da se sastoji samo od eNodeB-ova. Upravljač radijske mreže (engl. *Radio Link Controller*, skraćeno RLC), koji je u trećoj generaciji pokretnih mreža zamijenio baznu stanicu (engl. *Base Station*, skraćeno BS) iz druge generacije pokretnih mreža, u potpunosti nestaje iz E-UTRAN-a. Njegove funkcionalnosti djelomično pokrivaju neki od čvorova jezgrene mreže, ali ih se ipak većina prenosi na eNodeB koji se preko sučelja S1 spaja na jezgrenu mrežu čime postaje direktna poveznica UE (eng. *User Equipment*) s jezgrenom mrežom.

Pojednostavljenjem arhitekture pristupne mreže na samo jedan element, odnosno uvođenjem ravne arhitekture mreže, postižemo poprilično bitno smanjenje kašnjenja paketa u mreži i to na manje od 10ms, te veću brzinu odziva mreže za zahtjevnije usluge. E-UTRAN NodeB, Evoluirani Node B, eNodeB ili eNB je čvor u LTE mreži koji predstavlja evoluiranu baznu stanicu. U prijašnjim je izvedbama UTRAN-a NodeB imao minimalne funkcionalnosti i bio je kontroliran od strane RNC. Sada eNodeB nema izdvojeni element koji ga kontrolira. Upravo je eNodeB zaslužan za najjasniju razliku između UTRAN-a i E-UTRAN-a jer sada sadrži sve funkcionalnosti koje su prije bile koncentrirane u RNC-u. Povećana funkcionalnost

eNodeB-a pojednostavljuje arhitekturu i dovodi je do ”ravne arhitekture”. Kontrola je tako pomaknuta bliže radio sučelju.

Funkcije koje obavlja eNodeB su: radio prijenos do UE-a, omogućavanje potrebnih funkcionalnosti za rad RRM (engl. *Radio Resource Managment*, skraćeno RRM), nadzor pristupa, kontrola radio prijenosa, raspoređivanje korisničkih podataka, signalizacija i kontrola nad zračnim sučeljem, te šifriranje i sažimanje zaglavlja preko zračnog sučelja.

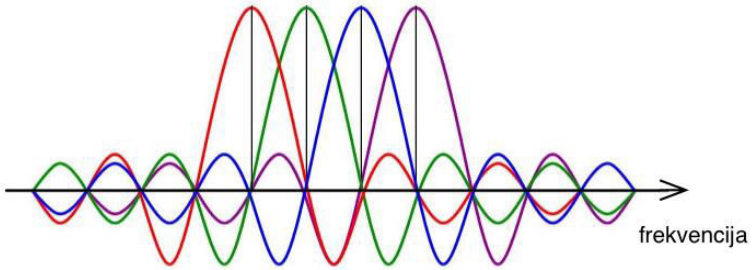
2.1.1. OFDM

Ortogonalno multipleksiranje s frekvencijskim odvajanjem (engl. *Orthogonal Frequency Division Multiplex*, skraćeno OFDM) jedna je od ključnih tehnologija LTE mreže. OFDM udovoljava zahtjevima LTE-a za fleksibilnošću spektra [2] i omogućuje ekonomičnu osnovu za šire frekvencijske pojaseve koji osiguravaju velike brzine prijenosa. Bitna razlika u širini frekvencijskog pojasa 3G mreža i LTE mreža je u tome što je kod 3G mreža širina frekvencijskog pojasa bila fiksna i iznosila 5MHz, a u LTE mreži je fleksibilna.

OFDM je tehnika modulacije koju karakterizira velik broj nositelja (engl. *carriers*[1]) smještenih jedan blizu drugoga. Signali su međusobno ortogonalni pa ne dolazi do njihovog međusobnog preklapanja i smetnji (Sl. 1). OFDM radi na principu podjele toka podataka u N paralelnih tokova. Time se smanjuje protok podataka, jer se svaki od manjih protoka prenosi preko svog podnositelja (engl. *subcarrier*[2]).

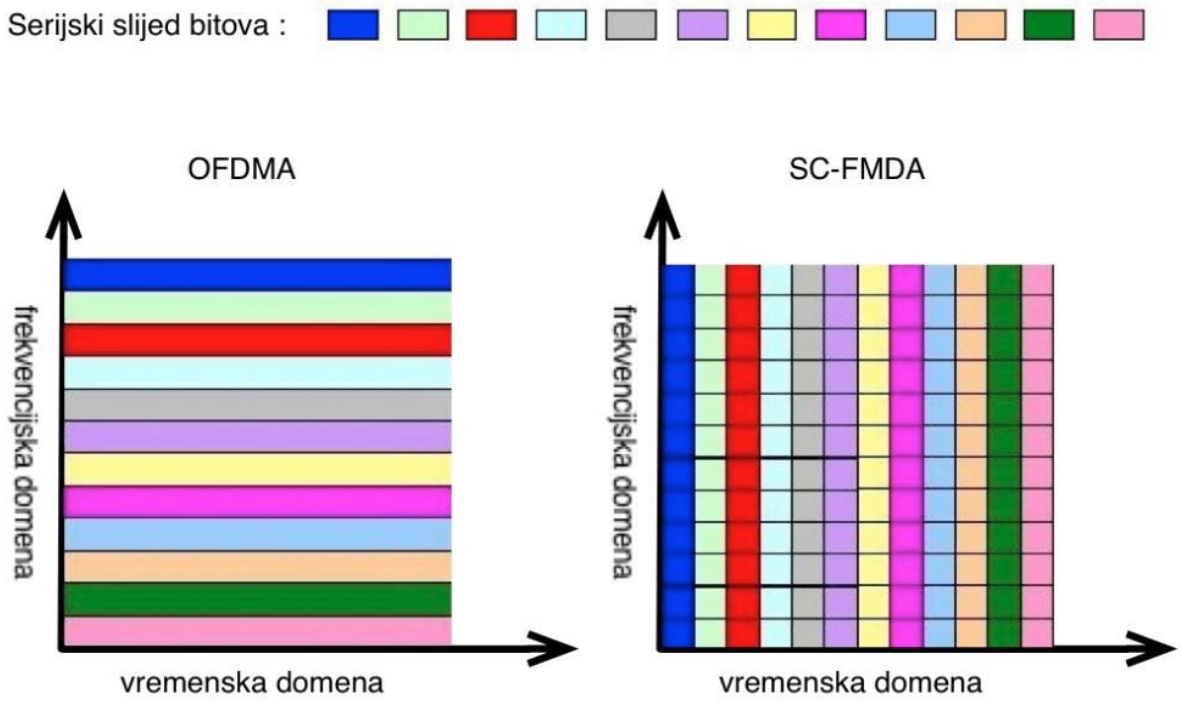
Između tih nositelja je biran odgovarajući frekvencijski razmak tako da maksimum signala svakog od podnositelja odgovara nulama svih ostalih signala. Time se dozvoljava spektralno preklapanje među nositeljima i postiže se bolja spektralna efikasnost.

[1] Nositelj je valni oblik (najčešće sinusni) moduliran s ulaznim signalom u svrhu prenošenja informacija. On je obično veće frekvencije od ulaznog signala.
[2] Podnositelj je analogni ili digitalni signal koji se prenosi radio vezom i prenosi neke dodatne informacije, kao što su glas ili podaci. Točnije, to je modulirani signal koji se modulira u drugi signal veće frekvencije i pojasne širine.



Slika 1: Razmak među podnosiocima, izvor [2]

U silaznoj vezi, tj. od eNodeB-a prema UE-u koristi se OFDMA (engl. *Orthogonal Frequency Division Multiple Access*), modificirani oblik OFDM-a koji distribuira podnositelje različitim korisnicima istovremeno tako da višestruki korisnici mogu istovremeno primati podatke. Kod uzlazne se veze koristi nešto drugačiji koncept: SC-FDMA (engl. *Single Carrier Frequency Division Multiple Access*). Njegovo je bitno obilježje da pojedini korisnik dobiva kontinuirani skup podnositelja koji zajedno djeluju kao jedan širi nositelj. SC-FDMA se uvodi zbog toga što dok radi koristi konstantnu količinu snage, smanjujući time potrošnju baterije u pokretnom uređaju.



Slika 2: Kodiranje podnositelja, izvor [2]

2.1.2. Sučelje X2

Sučelje X2 novo je sučelje definirano između eNodeB-ova. Glavna uloga sučelja X2 je smanjenje gubitaka paketa zbog pokretljivosti korisnika. Ono povezuje eNodeB s nekim od njegovih susjednih eNodeB-ova kako bi međusobno izmjenjivali signalizacijske poruke. Uobičajeno se prenosi jedan od dva tipa informacija: informacije o opterećenju (engl. *load information*) ili informacije vezane uz interferencije (engl. *interference related*) i informacije vezane uz mehanizam prekapčanja (engl. *handover-related information*). S obzirom da su sve vrste informacija koje se mogu prenositi sučeljem X2 međusobno nezavisne, moguće je imati sučelje X2 između dva eNodeB-a da bi se izmjenjivale informacije o opterećenju ili interferenciji iako se između ta dva eNodeB-a ne koristi procedura prekapčanja UE-ova.

2.1.3. Evoluirani čvor B (eNodeB)

E-UTRAN je odgovoran za sve funkcije radijske mreže, a zbog njegove već spomenute ravne arhitekture sve se te funkcije nalaze u eNodeB-ovima, od kojih svaki može upravljati s više ćelija.

Neke od zadaća eNodeB-a su:

- Upravljanje ćelijama i njihovim radijskim resursima,
- Kontrola radio pristupa,
- Kontrola pokretljivosti,
- Raspoređivanje korisnika,
- Zaštita korisničke i kontrolne razine šifriranjem,
- Upravljanje dijeljenim kanalom i kanalom slučajnog pristupa,
- Upravljanje retransmisijom,
- Usmjeravanje korisničkih podataka,
- Kompresija zaglavlja IP paketa.

2.2. Jezgrena mreža

Jezgreni dio LTE/SAE mreže koji se može naći i pod nazivom EPC (eng. *Evolved Packet Core*) ili SAE (eng. *System Arhitecture Evolution*) osigurava pristup prema ostalim podatkovnim mrežama kao što je Internet, upravlja sigurnosnim funkcijama (autentifikacija,

dodjela ključeva, ...), prati pretplatničke informacije i naplatu te kontrolira pokretljivost prema drugim pristupnim mrežama (UTRAN, WLAN, ...) i pokretljivost neaktivnih terminala.

Jezgrena se mreža sastoji od tri glavna logička čvora. U kontrolnoj ravnini (engl. *Control Plane*, skraćeno CP) nalazi se entitet upravljanja pokretljivošću (engl. *Mobility Management Entity*, skraćeno MME), dok se u korisničkoj ravnini (engl. *User Plane*, skraćeno UP) nalaze uslužni prilazni čvor (engl. *Serving Gateway*, skraćeno S-GW) i paketski mrežni prilazni čvor (engl. *Packet Data Network Gateway*, skraćeno PDN-GW). Osim navedena tri glavna logička čvora, u jezgrenom se dijelu mreže nalaze i još dva logička čvora: čvor za upravljanje resursima i terećenje (engl. *Policy Charging and Rules Function*, skraćeno PCRF) i poslužitelj domaćih pretplatnika (engl. *Home Subscriber Server*, skraćeno HSS).

2.2.1. Entitet upravljanja pokretljivošću

Entitet upravljanja pokretljivošću ili skraćeno MME temeljni je čvor jezgrene mreže i namijenjen je za signalizaciju porukama koje se izmjenjuju preko kontrolne ravnine između UE-a i ostalih čvorova jezgrene mreže, kao što je npr. HSS. To se odvija preko NAS protokola (engl. *Non Access Stratum protocols*, skraćeno NAS protocols). MME je nadležan i za čvorove pristupnog dijela mreže. Sadrži kontrolne funkcije slične kontrolnoj SGSN (eng. *Serving Gateway Support Node*) ravnini.

MME upravlja sljedećim funkcijama:

- NAS signalizacija,
- Sigurnost NAS signalizacije,
- Kontrola sigurnosti u pristupnom sloju (engl. *Access Stratum*, skraćeno AS),
- Odabir PDN-GW i S-GW elemenata,
- Odabir drugih MME-ova prilikom prekapčanja,
- Upravljanje pokretljivošću prilikom prelaska na druge mreže,
- Odabir SGSN-a u prekapčanjima između LTE i 3GPP 2G/3G pristupnih mreža,
- Upravljanje popisima praćenih područja (engl. *Tracking Area*, skraćeno TA),
- Domaći i međunarodni roming,
- Autentifikacija korisnika,
- Uspostava i upravljanje nositeljima (engl. *bearers*),
- Upravljanje retransmisijom UE-a i ostalim funkcijama vezanim za pronalazak UE-a u stanju mirovanja.

2.2.2. Uslužni prilazni čvor

Uslužni prilazni čvor ili S-GW osigurava povezanost UE-a i PDN-GW-a preko korisničke ravnine. S-GW tunelira podatke prema P-GW i prati kretanje korisničkog terminala između eNodeB-ova pristupne mreže, tj. ukoliko korisnik prijeđe u područje drugog S-GW-a dolazi do njegove promjene. Regulira uspostavu veza s korisnicima drugih mreža. S-GW je lokalna anchor točka za procedure prekapčanja između eNodeB-ova i za pokretljivost između 3GPP mreža.

Funkcionalnosti koje posjeduje su:

- Slanje i prosljeđivanje podatkovnih paketa,
- Zakonsko presretanje poziva (engl. *Lawful interception*, skraćeno LI),
- Označavanje paketa na transportnoj razini za uzlaznu i silaznu vezu,
- Upravljanje privremenom pohranom (engl. *buffering*) paketa u stanju mirovanja E-UTRANA-a,
- Upravljanje zahtjevima za uslugom,
- Punjenje evidencije podataka.

2.2.3. Paketski mrežni prilazni čvor

Paketski mrežni prilazni čvor završna je točka podatkovnog sučelja prema PDN-u. Kao i S-GW osigurava vezu između UE-a i SAE-GW-a preko korisničke ravnine. Sučeljem je povezan na S-GW s jedne strane i na PDN s druge strane. Obavlja i zadatke GGSN-a (engl. GPRS *Gateway Support Node*). Za razliku od S-GW-a koji se mijenja s promjenom lokacije korisnika, PDN-GW ostaje isti sve dok je korisnik mrežno priključen.

Uključuje sljedeće funkcionalnosti:

- Alokacija IP adrese korisničkog terminala,
- Filtriranje i inspekcija paketa,
- Zakonsko presretanje poziva,
- Označavanje paketa na transportnom sloju u silaznoj vezi,
- Service level charging u ulaznoj i silaznoj mreži,
- *Online* naplata

2.2.4. Čvor za upravljanje resursima i terećenje

PCRF (engl. *Policy Charging and Rules Function*) je odgovoran za donošenje odluka oko upravljanja resursima i za kontrolu naplate na temelju protoka podataka kroz PDN-GW. Osigurava autorizaciju kvalitete usluge (engl. *Quality of Service*, skraćeno QoS) koja odlučuje kako će se tretirati određeni tok podataka koji će biti u skladu s korisnikovim pretplatničkim profilom. Informacije o pretplati korisnika za pojedinu uslugu mogu sadržavati npr. maksimalnu klasu QoS ili maksimalnu moguću brzinu, a PCRF ih može koristiti kao osnovu za donošenje odluka o naplati. Funkcionalnosti koje posjeduje naslijedio je od UMTS logičkih čvorova: PDF (engl. *Policy Decision Function*) i CRF (engl. *Charging Rules Function*).

PCRF osigurava nadzor mreže. Od mrežnog elementa AF (engl. *Application Function*) prima informacije o sjednici i mediju koje prije spremanja može provjeriti i odlučiti jesu li pouzdane. PCRF obavještava AF o događajima na prometnoj (engl. *traffic*) ravnini.

2.2.5. Poslužitelj domaćih pretplatnika

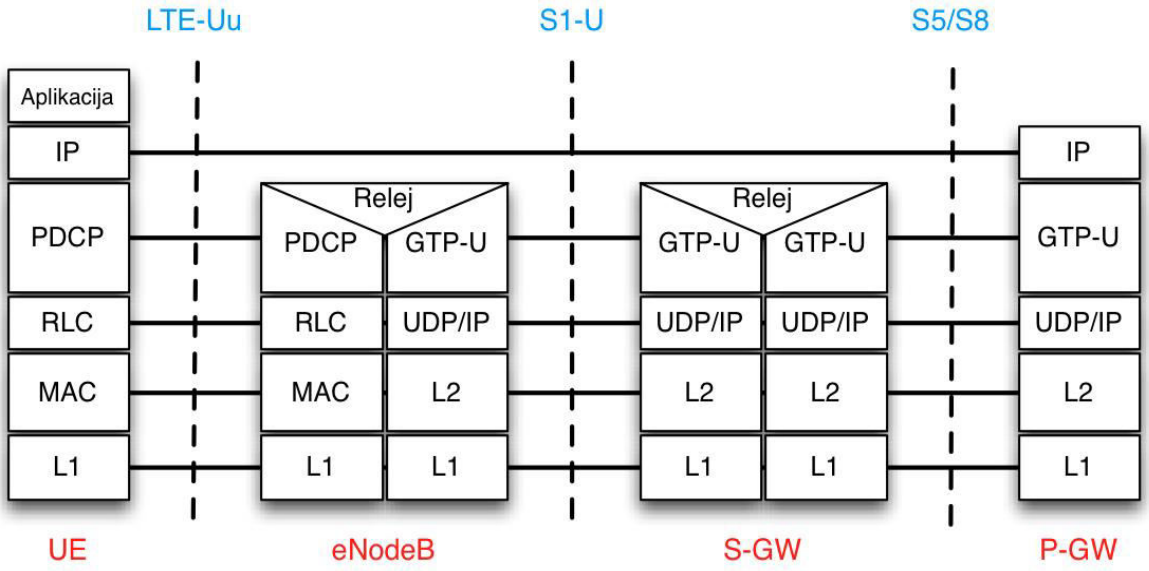
HSS entitet je odgovoran za upravljanje korisničkim profilima i vrši autentifikaciju i autorizaciju korisnika, tj. starih i novih LTE pretplatnika. Korisnički profili kojima upravlja HSS sastoje se od informacija o pretplati, sigurnosti, QoS profilima i pristupnim ograničenjima kod rominga te od fizičke lokacije na kojoj se korisnik trenutno nalazi. Sadrži informacije o PDN-ovima na koje se korisnik može spojiti, i to ili u obliku imena pristupne točke (engl. *Access point name*, skraćeno APN) koje je oznaka dodijeljena pristupnoj točki s obzirom na standarde sustava imenovanja domena (engl. *Domain Name System*, skraćeno DNS) kako bi je opisala PDN-u ili kao PDN adresa koja ukazuje na pretplatničku IP adresu. HSS posjeduje i dinamičke informacije, kao što je identitet MME-a na koji je korisnik trenutno spojen ili registriran. Može imati integriran i centar za autentifikaciju (engl. *Authentification center, skraćeno* AUC) koji generira vektore za autentifikaciju i sigurnosne šifre.

Kad MME primi zahtjev od UE-a kako bi započeo prikapčanje na mrežu, MME šalje zahtjev za provjeru autentičnosti podataka na AUC / HSS. Nakon izvođenja algoritama za generiranje random vrijednosti, AUC ih kombinira u autentični vektor (AV = rand || XRES || CK || IK || AUTN) i šalje ga na MME s odgovorom autentifikaciju podataka.

2.3. Protokolni složaj

LTE protokolni složaj između različitih elemenata je podijeljen na korisničku i kontrolnu ravninu. Protokoli su slični onima korištenima u UMTS mreži. Možemo ih podijeliti u tri sloja koji se djelomično poklapaju s ISO OSI (engl. *International Organization for Standardization Open System Interconnection*) strukturom slojeva. Prvi sloj LTE/SAE-a je srodan fizičkoj realizaciji sučelja, dakle tu svrstavamo radio sučelje i optičke kablove. Drugi sloj je srodan razini podatkovne poveznice i pristupnoj razini, a treći se odnosi na protokole pristupnog sloja. U LTE/SAE mreži aplikacijska razina je uključena u treći sloj.

2.3.1. Korisnička ravnina



Slika 3: Protokoli koji obavljaju zadaće E-UTRAN-a na korisničkoj ravnini

- Sloj 1 (engl. *Layer* 1, skraćeno L1) ili fizički sloj osigurava sredstva i osnovne funkcionalnosti za prijenos bitova preko radio sučelja silaznom ili uzlaznom vezom. Radio sučelje se bazira na dvije odvojene tehnike pristupa: OFDMA za silaznu vezu i SC-FDMA za uzlaznu vezu. Za prijenos podataka i signalizaciju definiran je i set LTE kanala. Kanali su pojednostavljeni u usporedbi s 3G verzijama, te su uklonjeni namjenski ili tzv. *dedicated* kanali. LTE fizički kanali dinamički se povezuju na trenutno dostupne resurse, tj. antene i fizičke blok resurse uz pomoć raspoređivača (engl. *scheduler*). Fizički sloj preko kanala za prijenos upravlja prijenosom podataka k višim slojevima LTE/SAE. Također se brine o prilagođavanju veze, kontroli snage, pretraživanju stanica, početku

sinkronizacije i prekapčanju. Pomoću kanalnog kodiranja i modulacije osigurava zaštitu podataka od grešaka u kanalu.

- MAC (engl. *Medium Access Control*) protokol najniži je protokol na drugom sloju korisničke ravnine. Osnovna funkcionalnost MAC protokola upravljanje je kanalima za prijenos (uz pomoć kojih komunicira s fizičkim slojem), a preko logičkih kanala komunicira s višim slojevima. MAC multipleksira podatke iz logičkog kanala kako bi se mogli prenijeti kanalom za prijenos, te ih demultipleksira na prijamu ovisno o razini prvenstva logičkih kanala. MAC uključuje funkcionalnost HARQ (engl. *Hybrid Automatic Retransmission on reQuest*), te se brine o rješavanju sudara i identificira korisnički uređaj. Entitet upravljanja pokretljivošću (engl. *Mobility Management Entity*, skraćeno MME) je glavni logički čvor jezgrene mreže u kontrolnoj ravnini. MME je zadužen za signalizacijske poruke koje se šalju između UE-a i čvorova jezgrene mreže. Funkcionalnosti MME-a su slične funkcionalnostima SGSN-a, a i sam MME je najčešće fizički izveden unutar SGSN čvorova. MME ima više funkcionalnosti: omogućuje da se UE registrira ili odjavi s mreže, pozivanje korisnika te sudjelovanje u prikapćanju poziva, te prati korisnike koji su u mirovanju na razini područja praćenja (engl. *Tracking Area*, skraćeno TA). Funkcionalnost koja je najvažnija za sigurnost korisnika je sudjelovanje MME-a u autentifikaciji i autorizaciji te provjera korisnika.
- RLC (engl. *Radio Link Control*) se nalazi odmah iznad MAC protokola na drugom sloju korisničke ravnine te komunicira s njim kanalima za prijenos. Prenosi PDU (engl. *Protocol Data Unit*) iz PDCP (engl. *Packet Data Convergence Protocol*). S PDCP-om komunicira preko pristupne točke SAP (eng. *Security Access Point*). RLC se koristi za formatiranje i prijenos podataka između korisničkog uređaja i eNodeB-a. Vrši mapiranje na logičke kanale i obavlja segmentaciju, kao i slijednu isporuku višim slojevima i retransmisije. RLC može pružiti korekciju ARQ (engl. *Automatic Repeat Query*) grešaka, segmentaciju PDU-ova, duplikaciju detekcije i sl. Omogućuje tri stanja za prijenos podataka: potvrđeno stanje AM za prijenos podataka u realnom vremenu, nepotvrđeno stanje UM za usluge u nerealnom vremenu i transparentno stanje TM za slanje sistemskih informacija.
- PDCP (engl. *Packet Data Convergence Protocol*) protokolu RRC pruža uslugu prijenosa njegovih podataka za šifriranje i zaštitu, protokolu IP pruža uslugu prijenosa IP paketa. Svaki radijski nositelj (engl. *radio bearer, skraćeno RB*) uvijek koristi PDCP. Protokol PDCP upravlja ROCH (engl. *Robust Header Compression*) kompresijom zaglavlja, upravlja i funkcijama šifriranja i dešifriranja.

Osim navedenih protokola, na korisničkoj se ravnini susrećemo i s dobro poznatim protokolima TCP/IP i UDP.

2.3.2. Kontrolna ravnina

Osim protokola MAC, RLC, PDCP i fizičkog sloja koji su prisutni na korisničkoj ravnini, na kontrolnoj se pojavljuju još tri protokola:

- RRC (engl. *Radio Resources Control*) protokol je koji se nalazi u eNodeB-u. Donosi odluke o prekapčanju ovisno o veličini susjednih stanica poslanih od strane korisničkog uređaja, prenosi sistemske informacije, kontrolira učestalost izvještaja mjerenja od strane UE-a (npr. informacije o kvaliteti kanala). Osim toga, vrši prijenos UE formacija od izvornog do ciljnog eNodeB-a za vrijeme prekapčanja. RRC je odgovoran za postavljanje i održavanje radijskih nosilaca. Brine se i o emitiranim informacijama sustava vezanim uz AS, te prijenosu NAS poruka, straničenju, uspostavljanju RRC veze, upravljanju sigurnosnim ključevima, pokretljivosti, ...
- NAS (engl. *Non-Access Stratum*) je protokol između korisničkog uređaja i MME-a. Smješten je iznad protokola RRC koji omogućava poruku nositelja za NAS prijenos. Najvažniji zadaci NAS protokola su autentifikacija, kontrola sigurnosti te upravljanje EPS nositeljima.
- SCTP (engl. *Stream Control Transmission*) je svoju funkcionalnost naslijedio od protokola TCP. Osigurava pouzdanu isporuku signalizacijskih poruka.

2.3.3. Osnovne razlike između TCP-a i SCTP-a[3]

SCTP se razlikuje od TCP-a u dvije ključne karakteristike:

- **višestruki domaćin (multihoming):** za čvor u mreži kaže se da je višestruki domaćin ako poseduje više IP adresa, tj. ako postoji više transportnih adresa (kombinacija IP adresa i SCTP porta) koje predstavljaju odredišnu adresu podataka koji se šalju tom čvoru. Protokoli višeg nivoa biraju jednu od ovih odredišnih adresa kao primarnu za slanje svojih podataka. U slučaju kvara na mreži, kada primarna postane nedostupna,

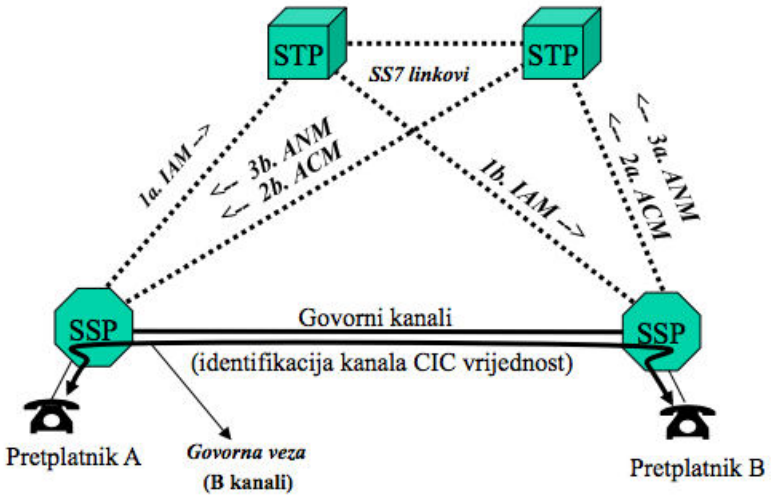
[3] Preuzeto sa web portala – https://wordpress.org/, znanstveni članak (blog) profesorice Aleksandre Jerinić

podaci se usmjeravaju na alternativne odredišne adrese. TCP, za razliku od SCTP-a ne podržava multihoming;

- **višestruki tokovi (multistreaming):** karakteristika SCTP-a je mogućnost razdvajanja i poruka višestrukim SCTP tokovima podataka. Ovi tokovi omogućavaju nezavisnu isporuku u pravilnom redoslijedu. Prednost višestrukih tokova je ta da ukoliko dođe do gubitka paketa u jednom toku, onda taj gubitak ne utječe na prijenos paketa na drugim tokovima. Prednost korištenja višestrukih tokova možemo pokazati na primjeru ISUP protokola. ISUP –(eng. *ISDN User Part*) podržava uspostavu i raskid veza između krajnjih točaka za osnovnitelefonski poziv. Postupno će ga zamijeniti BISUP. BISUP (eng. *Broadband ISDN User Part*) je ATM protokol za podršku usluga poput:

    - HDTV (eng. *High Definition Television*),
    - višejezična TV, videokonferencije, …

  Poruke se odašilju različitim putevima za isti poziv koje se potom usmjeravaju tako da se provodi automatska raspodjela opterećenja signalizacijskih linkova. Tok poruka kroz signalizacijsku mrežu koristi osnovni poziv do uspostave veze.



Slika 4: Ilustracija višestrukih tokova

Pozivajući pretplatnik u izvorišnom SSP (eng. *Security Service Provider*) čvoru podiže (off-hook) i bira broj.

1.a) Izvorišni SSP odašilje ISUP poruku IAM (eng. *Integrated Assessment Model*) i rezervira zadani kapacitet kanala. (IAM sadrži OPC (eng. *Open Platform*

Communications), DPC (eng. *Deferred Procedure Call*), CIC (eng. *Carrier Identification Code*), birani broj, CPID (eng. *Communication Planning and Information Design*) i ime pozivajućeg/opcija).

1.b) IAM se usmjarava kroz pripadni STP od strane izvorišnog SSP.

Odredišni SSP provjerava birani broj i tablicu usmjeravanja, te potvrđuje da je pozvani pretplatnik pripravan za oglašavanje.

2.a) Odredišni SSP šalje ACM prema izvorišnom SSP preko pripadnog STP i time potvrđuje da je zatraženi kanal rezerviran.

2.b) STP usmjerava ACM prema izvorišnom SSP na kojeg je priključen pozivajući pretplatnik.

3.a) Pozvani B podiže MTK (off-hook). Odredišni SSP zaustavlja oglašavanje i upućuje ANM prema izvorišnom SSP.

3.b) STP usmjerava ANM prema izvorišnom SSP koji verificira vezu s rezerviranim kanalom. Uključuje se naplata.

Ukoliko za prjenos ISUP signalizacijskih paketa koristimo TCP tada svi paketi koriste jedan tok. Tako u slučaju greške na jednom paketu svi ostali paketi moraju čekati njegovu ispravnu poruku što dovodi do nedopustivog kašnjenja. SCTP koristi za svaki poziv poseban tok i tada greške na jednom toku ne utječu na ostale tokove.

3. Sigurnost

Cilj svih sigurnosnih zaštita je spriječavanje napada tako da vanjski napadači imaju minimalne mogućnosti za prijevaru ili bilo kakvu zloupotrebu koja podliježe kaznenom ili prekršajnom zakonu. U svakom je trenutku važno zaštititi privatnost korisnika i osigurati stabilni rad pružatelja usluga. Sigurnosni sustav LTE-a razvija tehnologije s ciljem saznavanja trenutnih i budućih metoda za napade na mrežu kao i njihove utjecaje na tehničke i uslužne dijelove mreže. Napadi mogu usporiti ili u gorem slučaju paralizirati velik dio mreže i prouzrokovati smanjenje dostupnosti usluga, što kao rezultat ima gubitak prihoda i smanjenja broja korisnika. Razvoj aktualnih sigurnosnih procesa ima više aspekata.

Prvi korak u planiranju osiguranja mreže je identificirati sigurnosne prijetnje. Različite faze razvoja dovode do različitih rizika koje LTE/SAE sustav treba identificirati. To dovodi do liste sigurnosnih potreba i do specifikacije sigurnosne arhitekture. Sljedeći korak je uzeti u obzir prijetnje sa softverske razine, dakle treba osiguravati *kod* što je više moguće tijekom kodiranja i razvoja softvera. Na kraju, podrazumijeva se da je potrebno testirati sustav zaštite s imaginarnim pokušajima napada. Ako se slabosti sigurnosnog sustava na vrijeme detektiraju, proboji mogu biti ispravljeni i ažurirani u sigurnosnom sustavu.

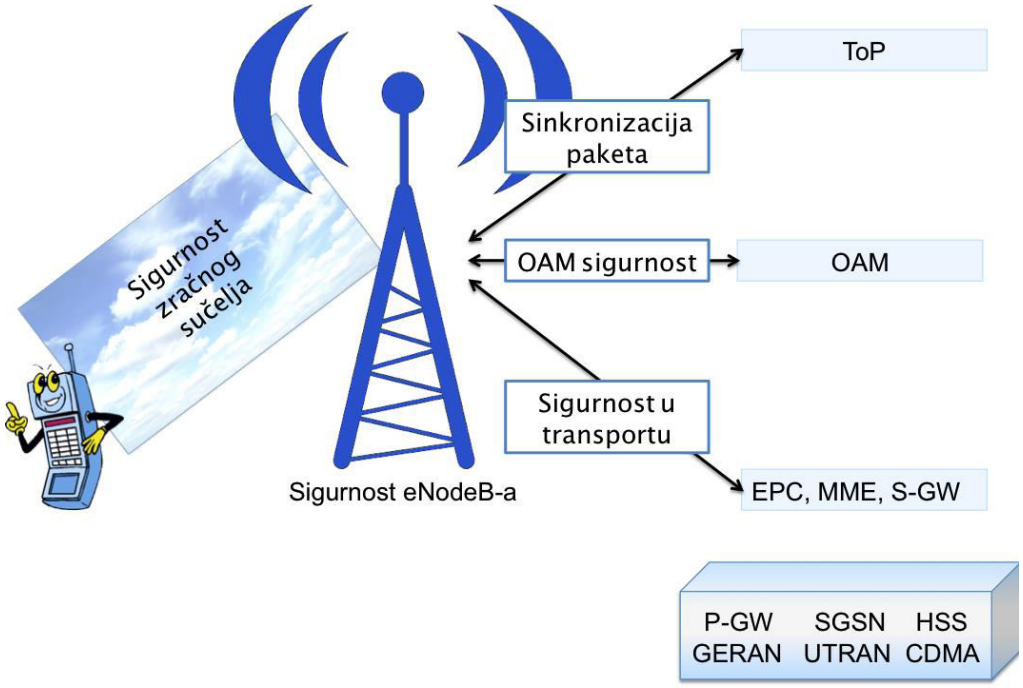
LTE/SAE mreža se bazira na IP-u, što znači da je slaba na iste napade kao i bilo koja druga mreža koja se temelji na komutaciji paketa. Glavni je cilj LTE/SAE mrežnih operatora reducirati mogućnosti za zloupotrebu mreže, a LTE sustav osigurava povjerljivost i integritet za signalizaciju između od UE-a do MME-a. Zaštita povjerljivosti temelji se na šifriranju signalnih poruka. Zaštita integriteta osigurava da se poruka tijekom prijenosa ne promjeni. Sav LTE promet je osiguran korištenjem PDCP-a (engl. *Packet Data Convergence Protocol*) u radijskom sučelju. U kontrolnoj ravnini PDCP osigurava oboje – kodiranje i zaštitu integriteta za RRC signalne poruke koje se šalju kroz PDCP pakete. U korisničkoj ravnini, PDCP izvodi kodiranje korisničkih podataka bez zaštite integriteta.

LTE/SAE arhitektura ima specijalne karakteristike koje bi trebalo uzeti u obzir prilikom planiranja sigurnosti. Bazirana je na ravnoj arhitekturi, što znači da sav radio pristup završava u eNodeB-u. Nadalje, protokol IP je također vidljiv u eNodeB-u. Izazovi vezni uz sigurnost sve su veći kako se poboljšava arhitektura mreže. Na primjer, eNodeB je moguće staviti na lokacije koje su dostupnije, a samim time što su na lokacijski dostupnijem mjestu postaju dostupnije i neovlaštenim upadanjima u mrežu.

LTE/SAE mreža surađuje i s prethodnim izdanjima mreža koje mogu biti potencijalne otvorene rupe u sigurnosti, premda se ne moraju isti problemi javljati u starijim izvedbama mreža.

Uspoređujući mrežu temeljenu samo na IP tehnologiji i mrežu s prethodnim 2G/3G principima sigurnosti, može se primijetiti kao LTE zahtijeva proširenje autentifikacije i broja ključeva u cilju sprječavanja napada koji se javljaju u modernim IT mrežama. To znači da je hijerarhija ključeva, kao i cjelokupna sigurnost, složenija nego prije. Također, to znači da eNodeB ima dodatne funkcionalnosti vezane uz sigurnost u odnosu na prethodne funkcionalnosti baznih stanica u 2G ili 3G mreži.

Zbog kompleksnosti napada na mreže, sigurnosni lanac LTE-a obuhvaća različite razine zaštite od napada, kao što je prikazano slikom.



Slika 5: Različite razine sigurnosti u LTE-u, izvor [3]

3.1. IPsec

Mobilni operateri moraju zaštiti korisničke podatke pokretnih uređaja od prisluškivanja, kopiranja podataka, krađe identiteta i ostalih načina neautoriziranog korištenja računa korisnika. U GSM i UMTS sustavima, provjera autentičnosti i kodiranje podataka

odvija se između korisničkog uređaja i RNC-a. Već u nekim izvedbama UMTS-a postoje čvorovi NodeB koji omogućuju zaštitu pomoću IPsec-a (engl. *Internet Protocol Security*).

LTE/SAE mijenja temelje pokretne komunikacije jer se potpuno temelji na IP okolini, što za sobom, povlači mogućnost rasta prijevara, dok motivacija za takve aktivnosti može biti financijske, destruktivne pa čak i političke prirode.

Moderna informacijska tehnologija kombinirana s poboljšanom pokretnom tehnologijom dovodi do novih aspekta koji mogu povećati osjetljivost na namjerne prijevare.

Na primjer, oprema bazne stanice je tradicionalno izrazito fizički zaštićena. Radio i transportna oprema su bili zaštićeni prilikom konstruiranja tako da je pristup bio omogućen samo autoriziranim osobama. U budućnosti se može očekivati da bi se takav tip opreme mogao nalaziti na javnim mjestima ili čak i u kućanstvima.

S druge strane, metode za napade uključuju napredne alate koje je sve jednostavnije nabaviti preko interneta. Takve aktivnosti uključuju sve sofisticiranije napade.

Za LTE kao standardizirano rješenje sigurnosti koristi se IPsec (engl. *Internet Protokol security*) zajedno sa PKI (engl. *Public Key Infrastructure*). PKI se primjenjuje za provjeru mrežnih elemenata i autorizaciju prilikom pristupa mreži, dok IPsec osigurava integritet i povjerljivost prilikom transporta na kontrolnoj i korisničkoj ravnini. IPsec je protokol koji obuhvaća mehanizme za zaštitu prometa kriptiranjem i/ili autentifikacijom IP paketa. IPsec osigurava tajnost, mogućnost promijene podataka isključivo od ovlaštene osobe, autentičnost i verifikaciju identiteta korisnika, odnosno raspoloživost unatoč neočekivanim događajima.

3.2. Sigurnosne ravnine

Kada se govori o sigurnosti cijele mreže uočava se kako je potrebno za svaki dio mreže posebno razraditi na koji način mrežu treba zaštiti i koje se vrste napada mogu dogoditi. Jedinstvena zaštita za sve dijelove mreže ne može se postići jer svaki dio mreže ima svoje posebne funkcionalnosti. Zato treba uzeti u obzir više različitih sigurnosnih stavki koje se trebaju povezati i osigurati od napada cjelokupnu LTE/SAE mrežu. Neke od sigurnosnih stavki su:

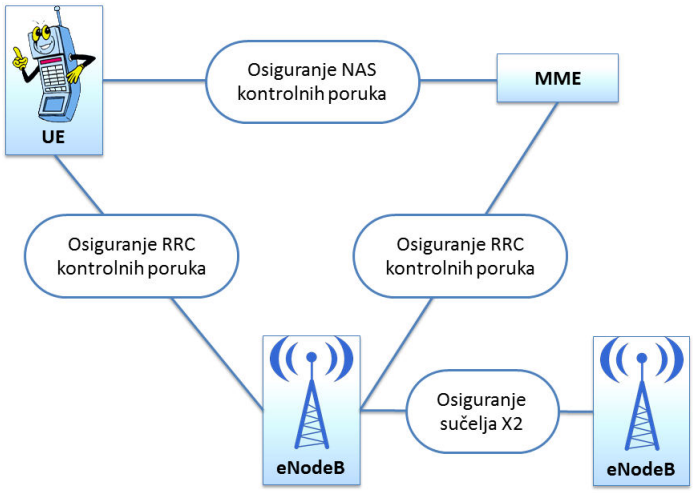
- Sigurnost u zračnom sučelju (engl. *U-plane* i *C-plane security*) uključuje korištenje algoritma za šifriranje koje se koristi za sigurnost korisničke ravnine

i sigurnost kontrolne ravnine te pristupne točke za sigurnosnu signalizaciju (uključujući distribuciju ključeva).

- Sigurnost u transportu uključuje algoritam za šifriranje i zaštitu integriteta tijekom transporta podataka i transportne sigurnosne signale (uključujući distribuciju ključeva).
- CM (engl. *Certificate Managment*) sadrži definiciju javnog ključa i ključa za upravljanje.
- OAM (engl. *Operations, Administration, Maintenance*) brine o sigurnosti upravljačke ravnine (engl. *M-plane security*).
- ToP (engl. *Timing over Packer*) osigurava sinkronizaciju sigurnosne ravnine pomoću paketa za frekvenciju i vremenske sinkronizacije.
- Intra LTE i Inter System Mobility osiguravaju sigurnost prekapčanja.

Drugačije ravnine u mreži imaju drugačije podatke te se mogu ostvariti drugačiji napadi na mreži. Zbog zaštite, sigurnosne ravnine dijele se na:

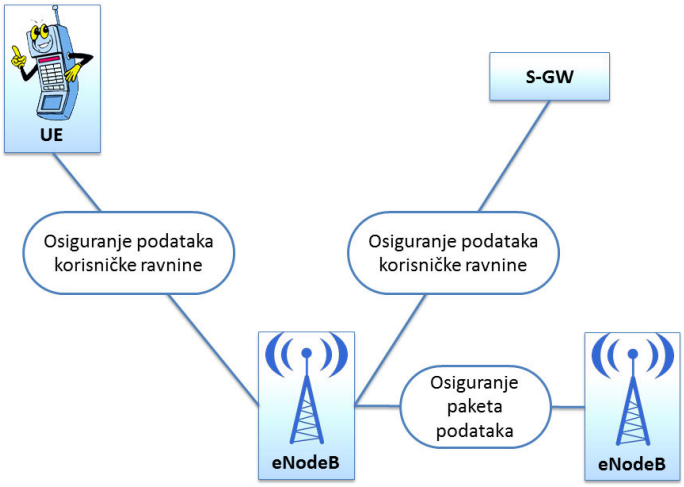
- Sigurnost korisničke ravnine (engl. *U-plane security*)
- Sigurnost kontrolne ravnine (engl. *C-plane security*)
- Sigurnost upravljačke ravnine (engl. *M-plane security*)
- Sigurnost sinkronizacijske ravnine (engl. *S-plane security*)



Slika 6: Sigurnost kontrolne ravnine, izvor [3]

Sigurnost kontrolne ravnine prikazana je slikom (Sl. 5). Protokol NAS brine o autentifikaciji i autorizaciji, sigurnosti te mobilnosti. Podaci koje on šalje između UE-a i

MME-a moraju biti zaštićeni te im mora biti osiguran integritet. RRC se nalazi ispod NAS-a i mora osigurati integritet podataka. RRC šalje sistemske informacije i brine o prijenosu poruka do protokola NAS, pa se njegovi podaci šifriraju. Šifriranje RRC signalizacijskih poruka se događa između UE-a i eNodeB-a, pa ponovno između eNodeB-a i MME-a. RRC sudjeluje i u procesu prebacivanja podataka od jednog eNodeB-a do drugog za vrijeme 5 prekapčanja. Kako bi proces prebacivanja bio u potpunosti zaštićen mora se zaštiti i sučelje X2. To je sučelje koje definira vezu između dva eNodeB-a, a fizički je najčešće izvedeno od optičkih vlakna.



Slika 7: Sigurnost kontrolne ravnine, izvor [3]

Način na koji je izvedena sigurnost korisničke ravnine prikazana je slikom (Sl. 6). Korisnički se podaci šalju putem UE – eNodeB – S-GW. Zaštita korisničkih podataka osigurava se šifriranjem podataka, a za šifriranje podataka od UE-a do eNodeB-a brine se protokol PDCP. Jedna od funkcija protokola PDCP je osiguravanje sigurnosti podataka koji se šalju preko zračnog sučelja. PDCP šifrira i dešifrira podatke korisničke ravnine, osigurava njihov integritet iako sama korisnička ravnina nema mogućnost osiguranja integriteta podataka te koristi slijedni broj kako bi detektirao ponovljene poruke. Nadalje, korisnički podaci šalju se protokolom IP, odnosno njegovom verzijom IPsec koja je poboljšana u pogledu sigurnosti podataka. Upravo IPsec šifrira podatke koji se šalju između eNodeB-a i S-GW-a, ali ne i one koji se šalju između eNodeB-ova. U fizičkom pogledu eNodeB ima u sebi integriranu funkciju za IPsec, pa se za eNodeB kao sam čvor može reći da predstavlja malu sigurnosnu domenu.

Podaci koji se moraju zaštiti u upravljačkoj ravnini šalju se između eNodeB-a i EMS-a ili NMS-a. NSM (engl. *Network Managment System*) se koristi za praćenje rada mreže. Pojedine elemente u mreži posebno nadzire sustav EMS (engl. *Element Managment System*). Zadaci upravljačke ravnine su:

- promatranje uređaja,
- stanja u kojem su uređaji i problemi oko samih uređaja u mreži,
- omogućavanje pravovremenih obavijesti o utjecaju određenih akcija na cjelokupnu mrežu,
- identificiranje problema i pružanje mogućih rješenja

Sigurnost sinkronizacijske ravnine može a i ne mora u sebi imati šifriranje sinkronizacijskih paketa, a integritet paketa koji se šalju između eNodeB-a i ToP-a osigurava IPsec.

3.3. Koncept ključeva

IMSI (engl. *International Mobile Subscriber Identity*) je jedinstveni broj koji identificira korisnika. Obično je duljina broja 15 znamenki, ali može biti i kraći. Sastoji se od oznake zemlje, oznake mreže operatora te oznake pokretnih korisnika. IMSI je pohranjen u SIM kartici, a koristi se kao ključ za dohvaćanje podataka o korisniku iz baze podataka o svim korisnicima - HSS-a. IMSI se što rjeđe moguće šalje kroz mrežu da bi se zaštitili podaci korisnika, a umjesto njega se onda koristi privremeni TMSI (engl. *Temporary Mobile Subcriber Identity*).

MSISDN (engl. *Mobile Subscriber ISDN Number*) je broj koji se nalazi u SIM kartici, a jedinstveno odgovara telefonskom broju jednog korisnika. Sastoji se od 15 znamenki koje pokazuju pozivni broj zemlje, mrežnog operatora i korisnika.

IMEI (engl. *International Mobile Equipment Identity*) je broj koji identificira sam pokretni uređaj, a ne SIM karticu unutar njega.

AKA (engl. *Authentication and Key Agreement*) je postupak koji opisuje autentifikaciju između korisnika i mreže. AKA postupak se sastoji od mehanizma zahtjev-odgovor koji se temelji na zajedničkom ključu koji je pohranjen na SIM kartici terminala i u središtu za provjeru autentičnosti AUC (engl. *Authentication Center*). AUC je dio HSS-a u LTE mreži. Zajednički ključ koristi se kao ulazni parametar u algoritme koji izračunavaju ostale ključeve koji služe za zaštitu integriteta (engl. *Integrity Key*, skraćeno IK) ili zaštitu

povjerljivosti (engl. *Confidentiality Key*, skraćeno CK). Za izračunavanje vektora koji predstavlja odgovor na zahtjev za autentifikaciju koriste se još: RAND (engl. *Random challange number*) i AUTN (engl. *Autentification token*), te se u konačnici uspoređuju dobiveni odgovori na poslane zahtjeve od UE-a i HSS-a: RES (engl. *Response*) i XRES (engl. *Expected Response*).

Hijerarhija ključeva izvedena je tako da je sama hijerarhija produbljena u odnosu na hijerarhiju ključeva u UMTS mreži.

Dublja hijerarhija ključeva je bolje zbog:

- mogućnosti bržeg prekapčanja
- podjele na više dijelova zbog kojih je narušavanje sigurnosti lokalno
- povećava se složenost rukovanja sigurnosnim mehanizmima

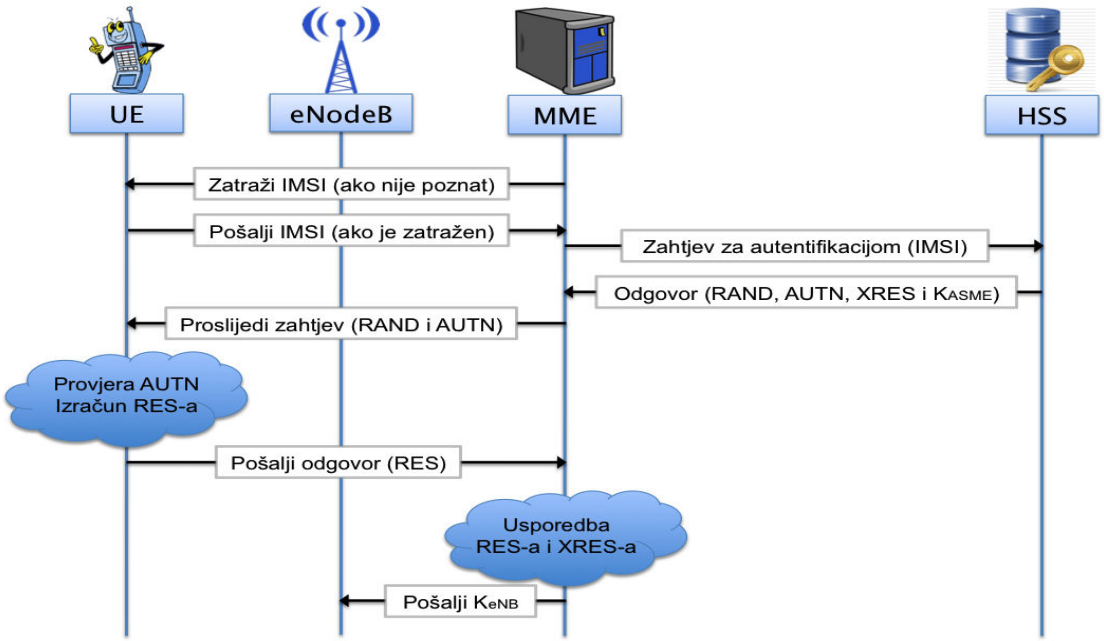
Ključ K (engl. *Key*) uvijek postoji. Svi ostali ključevi su izvedeni. Postoje funkcije po kojima se ključevi izvode – KDF (engl. *Key Derivation Function*). To je šifriranje ključeva pomoću hash funkcije (engl. *Hash Function*). Formula Ky=KDF(Kx,S) izračunava hash vrijednost od Kx i niza S, a upravo ta vrijednost postaje izvedeni ključ Ky.

- Kx je nadređeni ključ, ključ koje se u hijerarhiji nalazi na višoj poziciji.
- Ky je izvedeni ključ
- S je niz znakova koji je najčešće slučajan, ali može unutar niza sadržavati i informacije u kojim slučajevima će ključ vrijediti.
- K – glavni ključ za GSM, UMTS, EPS. Tajni ključ koji je pohranjen u SIM-u i AuC-u.
- CK, IK – Ključevi za šifriranje i integritet. Par ključeva koji se dobiva u AuC-u tijekom procesa AKA.
- KASME – Ključ od MME-a. Ključ koji je izveden iz CK i IK tijekom AKA procesa, a nalazi se u HSS-u i UE-u.
- KeNB – Ključ eNodeB-a za prekapčanje. Ključ izveden u eNodeB-u i UE-u tijekom prekapčanja.
- KNASint – Ključ koji osigurava integritet za NAS signalizaciju.

- KNASenc – Ključ za kodiranje NAS signalizacije.
- KUPenc – Ključ za kodiranje koji se koristi da bi zaštitio podatke korisničke ravnine.
- KRRCint – Ključ koji osigurava integritet za RRC signalizaciju izveden iz eNodeB-a i UE-a.
- KRRCenc – Ključ za kodiranje podataka koji se šalju pomoću protokola RRC.

3.4. Autorizacija i Autentifikacija

Autentifikacija i autorizacija dva su slična pojma, no oni nisu sinonimi. Autentifikacija je proces provjere identiteta, odnosno osobnih podataka korisnika tijekom pokušaja spajanja na mrežu. U procesu autentifikacije šalju se šifrirani podaci od klijenta prema serveru kako bi se mogla uspostaviti komunikacija sa mrežom. Autorizacija je provjera da li se pokušaj spajanja treba dozvoliti i ako je odgovor potvrdan pristup se korisniku treba dodijeliti. Tek nakon što je klijent autentificiran, pokreće se proces autorizacije, odnosno korisniku se dozvoljava ili zabranjuje pristup. Autorizacija se može dogoditi samo nakon uspješne autentifikacije. Proces autentifikacije i proces autorizacije moraju biti uspješni da bi se korisnik mogao uspješno spojiti na mrežu.



Slika 8: Proces autentifikacije kod LTE-a

Na 7. slici prikazuje se postupak autentifikacije, gdje na početku MME (eng. *Mobility Management Entity*, skraćeno MME) pokreće proceduru na način da šalje IMSI (eng. *International Mobile Subscriber Identity*), zajedno s identitetom poslužiteljske mreže (SN ID, engl. *Serveing Network Identity*) do HSS (eng. *Home Subscriber Server*) od domaće mreže. U slučaju da MME-u nije poznat kod IMSI, u trenutku prije slanja podataka do HSS-a, MME će zatražiti IMSI od UE-a. UE poslati će IMSI do MME-a preko zračnog sučelja u tekstualnom obliku, ali ta procedura slanja IMSI-ja se događa samo u posebnim situacijama kada ni na koji način nije moguće saznati IMSI. Kao rezultat na zahtjev za autorizacijom MME od HSS-a prima vektor koji sadrži: RAND (engl. *Random challange number*), AUTN (engl. *Autentification token*), XRES (engl. *Expected Response*) i KASME (eng. *key of MME*). Nakon što MME primi vektor koji u sebi sadrži RAND i AUTN, on šalje RAND i AUTN do UE-a. Tada UE procesira primljene informacije kako bi potvrdio da se na ispravnoj mreži događa proces autentifikacije, te na temelju svog ključa izračunava odgovor – RES i šalje ga natrag prema MME-u. HSS i UE koriste jednak algoritam prilikom izračunavanja odgovora koji šalju MME-u. MME u konačnici ima obadva dogovora RES i XRES, te ako su oni jednaki, autentifikacija se završava uspješno. U konačnici se izračunava KeNB (eng. *Key for eNODE*) koji eNodeB-u javlja da je autentifikacija uspješno obavljena i da treba osigurati zračno sučelje za slanje signalizacijskih i podatkovnih poruka.

Sučelje X2 ima još jednu bitnu funkciju [4], a to je prijenos starijih informacija o UE-u (engl. *Historical UE information*). Na primjer, informacije o zadnjih nekoliko ćelija u kojima se UE nalazio ili informacije koliko je vremena UE proveo u kojoj od ćelija, šalju se iz izvorišnog u ciljni eNodeB kako bi se odredilo pojavljuje li se ”ping-pong” učinak.

Ping-pong efekt je opisan već samim svojim imenom, a odnosi se na situaciju prilikom koje se mobilna stanica kreće na granicu između dviju ćelija koje su pokrivene mrežom s različitih baznih stanica. Problem koji se javlja je kako odrediti na koju će se baznu stanicu mobilna stanica spojiti. Rješenje je dopustiti mobilnoj stanici da nastavi komunicirati s baznom stanicom s kojom je trenutno spojena do trenutka kada jačina signala nove bazne stanice ne prijeđe vrijednost jačine signala stare bazne stanice.

Ping-pong primopredaja (HO) u LTE je jedan od najvažnijih problema koji smanjuju performanse mreže. Utjecaj ping-pong u mrežama se i dalje istražuje i pokušava optimizirati. HO algoritam pamti stari put između izvora ENB i SGW (eng. *Serving Gateway*) / MME tijekom izvođenja ping-pong efekta i odgađanja završetka HO-a. Simulacijski rezultati takvih algoritma pokazali su da se stopa ping-pong predaje može smanjiti, a time se i povećala

kvaliteta mreže. Rezultati ukazuju na to da se optimalna vrijednost vremena treba pažljivo izabrati, kako bi se smanjila vjerojatnost ping-pong HO i istovremeno zadržalo neprekidanje poziva na najnižim razinama.

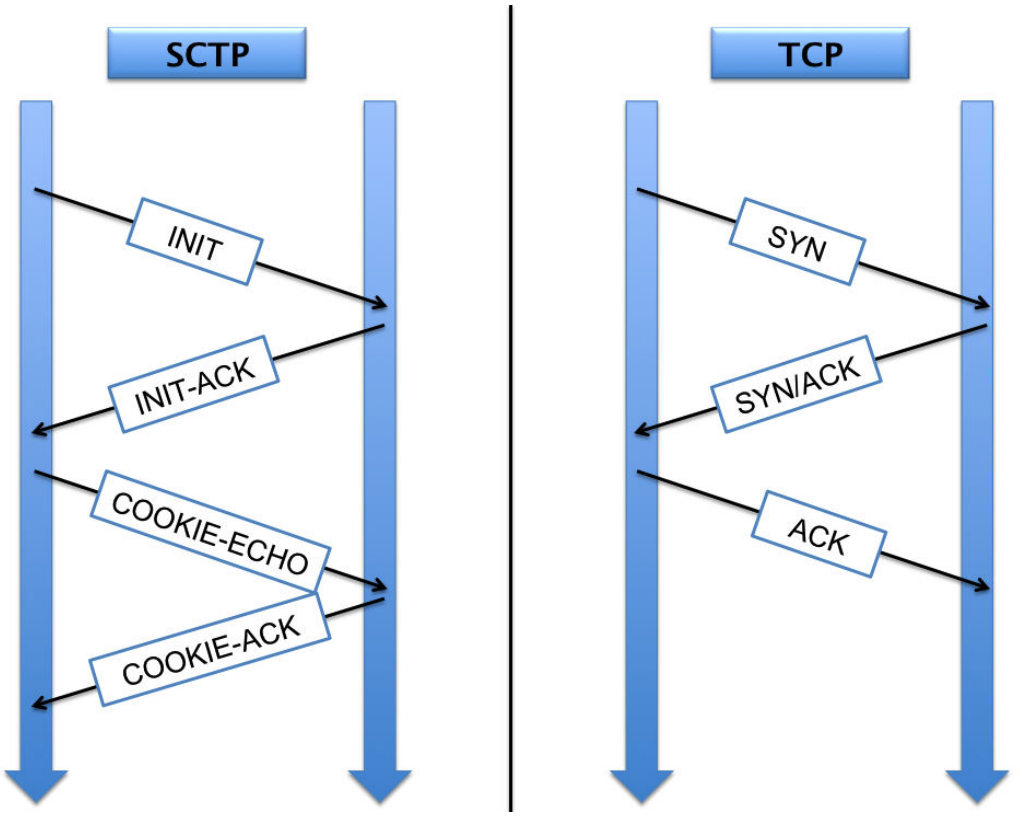
3.5. Mogući napadi na LTE mrežu

Napadom na mrežu može se smatrati bilo kakvo djelovanje na mrežu zbog kojeg mreža ne može raditi neometano. Napadi mogu biti namjerni, slučajni, planirani, izvršavani zbog profita, osvete, zadovoljstva itd. Napadi mogu utjecati na bilo koji dio mreže i zbog toga sustav zaštite mora pokrivati cijelu mrežu. Nemoguće je predvidjeti sve vrste napada, pa je tako nemoguće apsolutno zaštiti mrežu. Zaštita za skoro sve dijelove mreže već postoji, no uvijek se javljaju novi napadi. U nastavku su opisane tri vrste napada za koje će se sigurnosni mehanizmi pobrinuti te ih spriječiti.

3.5.1. Napad na transportnom sloju

Primjer napada: Napadač želi zakrčiti mrežu na transportnom sloju slanjem višestrukih sinkronizacijskih poruka.

Glavni protokoli transportnoj sloja su UDP i SCTP. SYN napad (engl. *SYN flood attack*) je napad koji se zasniva na slanju sinkronizacijskih paketa prema poslužitelju, koji odgovara sa SYN/ACK (eng. *Acknowledgement*) paketima prema klijentu. Klijent u takavom napadu ne odgovara poslužitelju s ACK paketom te ostavlja konekcije poluotvorenima. Takve poluotvorene konekcije spremaju se u memoriju, te do isteka određenog vremena poslužitelj pokušava iznova poslati SYN/ACK pakete. Problem se događa zbog velikog broja poluotvorenih konekcija koje usporavaju otvaranje novih konekcija ili ih uopće ne otvaraju, a može doći čak i do rušenja poslužiteljske aplikacije zbog zauzeća memorije.



Slika 9: Usporedba protokola SCTP i TCP, izvor [3]

Rješenje takvog problema u 4G mrežama pronađeno je u protokolu SCTP (engl. *Stream Control Transmission Protocol*) koji ima mogućnost otkrivanje SYN napada, nakon ćega se napad zaustavi. SCTP je ime za protokol u transportnom sloju mreža baziranih na protokolu IP i ima sličnu funkcionalnost kao protokoli TCP (engl. *Transmission Control Protocol*) i UDP (engl. *User Datagram Protocol*). Jedna od razlika u odnosu na TCP i UDP je što SCTP ima zaštitni mehanizam od SYN napada koji se zove princip četverostrukog rukovanja (engl. *4 way handshake*). Princip četverostrukog rukovanja je uspoređen s principom kojeg koristi TCP. SCTP radi tako da kada poslužitelj primi zahtjev za vezom ne zauzima resurse u memoriji nego u odgovoru šalje cookie zaštitni parametar. Tek nakon što primi klijentov odgovor s istim zaštitnim parametrom, poslužitelj zauzima resurse u memoriji potrebne za uspostavu veze i natrag šalje potvrdu za zadnju primljenu poruku.

Razvojem Interneta, osobnih računala i računalnih mreža raste mogućnost sigurnosnih prijetnji, ranjivosti i štetnih napada. Hakeri, virusi, osvetoljubivi zaposlenici i čak ljudska pogreška neke su od opasnosti na mreži. Internet je nedvojbeno postao najveća mreža javnih podataka, uključujući i olakšanu osobnu i poslovnu komunikaciju.

Pristupni napadi provode se nakon što se otkriju ranjivosti u mrežnim prostorima, kao što je autentifikacijski servis i FTP (eng. *File Transport Protocol*) s ciljem da pronađu

korisnički račun e-pošte, bazu podataka i ostale povjerljive informacije. DoS (eng. *Denial of Service*) napadi sprječavaju pristup dijelovima ili cijelim računalnim sistemima. Oni obično šalju veliku količinu nekontroliranih podataka na uređaj koji je spojen na mrežu neke tvrtke ili Internet, blokirajući tako protok ispravnog prometa. Štoviše, takav napad može prerasti u DDoS (engl. *Distributed Denial of Service*) u kojem napadač kompromitira više uređaja ili korisničkih stanica.

3.5.2. Napad na korisničku ravninu

Primjer napada: Dva eNodeB čvora moraju razmijeniti korisničke podatke u obliku podatkovnih paketa. Napadač prisluškuje vezu kojom se šalju podaci između dva čvora eNodeB kako bi saznao korisničke podatke.

Komunikacija između dva eNodeB čvora u korisničkoj ravnini zaštićena je protokolom IPsec. Protokol IPsec zajedno s protokolom IKE (engl. *Internet Key Exchange*) šifrirat će podatke, tako da napadač može snimiti samo šifrirane podatke koje neće biti u mogućnosti dešifrirati jer će mu ključ šifriranja ostati nepoznat. IKE je protokol koji rješava problem razmjene dijeljenih ključeva kroz nesigurnu mrežu pomoću IKE daemona. Rad protokola IKE opisujemo na slijedeći način:

1. Pošiljatelj šalje IPsec paket i aktivira se njegov IKE
2. Pošiljateljev daemon aktivira daemona od primatelja kako bi se mogli razmijeniti dijeljeni ključevi.
3. Daemoni razmjenjuju ključeve i dogovaraju se oko algoritma za šifriranje.
4. Daemoni se vraćaju mirovati, a otvara se IPsec tunel i šalju se podaci.

3.5.3. Napad na korisnički terminal

Primjer napada: Napadač želi klonirati korisnički račun i prijaviti se na mrežu kao osoba koja već postoji u mreži te koristiti usluge mreže na tuđi račun.

Slika 10: LTE SIM kartica [5]

Svaki korisnik da bi mogao biti spojen na mrežu mora imati SIM broj, IMSI broj i nepromjenjiv ključ K koji se sastoji od 128 bitova. SIM kartica na kojoj se nalaze ovi tajni podaci zapravo je najuspješnija pametna kartica (engl. *Smart card*) u povijesti. Svoju popularnost temelji na činjenici da su podaci na njoj jako sigurni. Vrlo je komplicirano, bez autorizacije, sa SIM kartice saznati koji podaci se nalaze na njoj. SIM kartica zaštićena je čak i u fizičkom aspektu tako da ni pod mikroskopom ne odaje svoje podatke. No kako niti jedna tehnologija nije u potpunosti sigurna, sa SIM kartice se ipak nekada mogu ukrasti podaci. Ako se ukrade sa SIM kartice nepromjenjivi ključ K, moguće je klonirati korisnika. Proces autentifikacije korisnika u mreži odvija se postupkom zahtjeva i odgovora koji se baziraju upravo na šifiriranju s ključem. Kada se klonirani terminal spoji na mrežu, on može koristiti usluge kao bilo koji drugi korisnik. No, takve napade je lako uočiti jer ih primjećuje sama mreža koja u tom trenutku zapazi da se jedan korisnik nalazi na više lokacija. U takvim situacijama isključuju se iz mreže i korisnik kojem je ukraden identitet i klonirani korisnik.

4. Zaključak

Prelaskom s 3G mreže na 4G mreže postignut je veliki napredak u razvoju pokretnih komunikacija uzimajući u obzir izvedbu cjelokupne mreže. Poboljšanja 4G mreže najvidljivija su korisnicima u obliku povećanja brzine za prijenos podataka. Korisnici s 4G mrežnom tehnologijom imaju mogućnost korištenja pametnih pokretnih uređaja sa svim njihovim mogućnostima i aplikacijama koje mogu koristiti u realnom vremenu. No, brzina nije jedina prednost 4G mreža. Prelazak na arhitekturu koja se u cijelosti bazira na protokolu IP, za sigurnost mreže znači uvođenje novih, poboljšanih razina zaštite od vanjskih napada. Koliko god se 4G mreža činila sigurnom, upravo je sigurnost glavna prepreka za uvođenje LTE-a jer je opseg napada jako velik, a tehnologija zaštite kompleksna i skupa. Problem koji se javlja vezan uz sigurnost je rast broja novih napada s porastom novih tehnologija, za razliku od vremena razvoja 2G i 3G mreža kada je taj broj bio vrlo malen. Sigurnost 4G mreže će se razvijati i unaprjeđivati usporedno s razvojem same mreže. LTE, kao predstavnik 4G mreža koje ne koriste više komutaciju kanala, sigurno će imati veliku ulogu u budućnosti pokretnih komunikacija.

5. Literatura

[1] Penttinen, Jyrki T.J. : ”The LTE/SAE Deployment Handbook”, Wiley, UK, 2012.

[2] Filip Lemić: Algoritmi raspodjele potkanala, bitova i snage u višekorisničkim OFDMA sustavima, diplomski rad, FER Zagreb, 2013.

[3]Muškardin Marin, Falan Sandro: 3GPP Long Term Evolution i ns-3 LENA, znanstveni članak, dostupno na: http://ieeexplore.ieee.org/Xplore/home.jsp

[4] Alcatel, Lucent: ”The LTE Network Architecture”, s Interneta: http://lte.alcatel-lucent.com/locale/en_us/downloads/Alcatel-Lucent_LTE_Transport_WhitePaper.pdf

[5] JEŽIĆ, G: Regulatorni aspekti mreža i usluga, zavodska skripta, FER Zagreb, 2014.

6. Popis kratica

3G	3rd Generation (Cellular Systems)
4G	4th Generation (Cellular Systems)
ACK	Acknowledgement
AKA	Authentiction and Key Agreement
AUC	Authentification Centre
AUTN	Authentification Token
BS	Base Station
CK	Confidentality Key
CM	Certificate Managment
DL	downlink
EMS	Element Managment System
eNodeB	Evolved Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
GGSN	GPRS Gateway Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Comunications
GTP	GPRS Tunneling Protocol
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
IK	Integrity Key
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Sucriber Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
K	Key

KDF	Key Derivation Function
LTE	Long Term Evolution
MAC	Medium Access Control
MIMO	Multiple Input Multiple Output
MME	Mobility Management Entity
MSISDN	Mobile Sucriber ISDN Number
NAS	Non-access Stratum
NSM	Network Managment System
OAM	Operation, Administration, Maintenance
OFDM	Orthogonal Frequency-Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiple Access
PDCP	Packet Data Convergence Protocol
PDU	Packet Data Units
PDN-GW	Packet Data Network Gateway
PKI	Public Key Infrastructure
RAND	Random Number
RES	Response
RLC	Radio Link Control
RNC	Radio Network Controller
RRC	Radio Resource Control
RRM	Radio Resource Management
SAE	System Architecture Evolution
SC-FDMA	Single Carrier Frequency Division Multiple Access
SCTP	Stream Control Transmission Protocol
SGSN	Serving Gateway Support Node
S-GW	Serving Gateway
TA	Tracking Area
TCP	Transmission Control Protocol
TMSI	Temporary IMSI
ToP	Timing over Packer
UDP	User Datagram Protocol

UP	uplink
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UTRAN	Universal Terrestrial Radio Access Network
XRES	Expected Response