

INTERNACIONALNI UNIVERZITET TRAVNIK

FAKULTET POLITEHNIČKIH NAUKA

ELEKTROTEHNIKA – TELEKOMUNIKACIJE

ZAVRŠNI RAD

KANALNO KODIRANJE U 4G MREŽAMA

Mentor: Doc. dr. Goran Popović

Student: Amer Delić

Travnik, august 2019.

INTERNACIONALNI UNIVERZITET TRAVNIK

FAKULTET POLITEHNIČKIH NAUKA

ELEKTROTEHNIKA – TELEKOMUNIKACIJE

ZAVRŠNI RAD

KANALNO KODIRANJE U 4G MREŽAMA

Mentor: Doc. dr. Goran Popović

Student: Amer Delić

Travnik, august 2019.

Sadržaj

1.	UVOD.....	4
1.1.	HISTORIJA RAZVOJA BEŽIČNIH MOBILNIH KOMUNIKACIJA.....	4
2.	MODEL SISTEMA	5
3.	ANALIZA OSOBINA TURBO KODOVA OSTBC SISTEMA.....	6
4.	SIMULACIJA PARAMETARA	7
5.	4G SISTEMI	9
5.1.	ARHITEKTURA LTE MREŽE	9
5.1.1.	Pristupna mreža	10
5.1.2.	Jezgrena mreža	13
5.2.	SIGURNOST	16
5.2.1.	IPsec	18
5.2.2.	Sigurnosne ravnine	19
5.2.3.	Koncept ključeva	21
5.2.4.	Autorizacija i autentifikacija.....	23
5.2.5.	Mogući napadi na LTE mrežu	25
6.	PRIMJER DEMONSTRIRANE 4G MREŽE	26
7.	KVALITETA USLUGE (QoS, Quality of Service).....	27
7.1.	Kašnjenje između krajnjih tačaka.....	27
7.2.	Kolebanje kašnjenja	27
7.3.	Gubitak paketa.....	28
7.4.	Pogreške pri prijenosu	28
8.	STRUKTURA KANALA.....	29
9.	ZAKLJUČAK	32
10.	LITERATURA	33

1. UVOD

1.1. HISTORIJA RAZVOJA BEŽIČNIH MOBILNIH KOMUNIKACIJA

Bežični mobilni komunikacijski sistemi su uvedeni početkom 1980-tih godina. Sistemi prve generacije (1G) su označeni analogno-frekvencijskom modulacijom i prvenstveno su se koristili za glasovne komunikacije.

Druga generacija bežičnih sistema (2G) se pojavila u kasnim 80-tim godinama prošlog stoljeća. Bežični sistem koji je danas u širokoj upotrebi nosi naziv 2,5G odnosno on je odskočna daska ka 3G. Dok je 2G komunikacija općenito povezana s uslugom GSM, 2.5G se obično identificira kao pokretač GPRS usluga.

3G sistemi, koji su se pojavili krajem 2002. i 2003., dizajnirani su za glasovne i stranične usluge, kao i za upotrebu interaktivnih medija poput mobline telefonije, pristupa internetu i drugih usluga. Problem sa 3G sistemima je propusni opseg koji za mobilne aplikacije iznosi 144 kbps do 2 Mbps za unutrašnje statičke aplikacije.

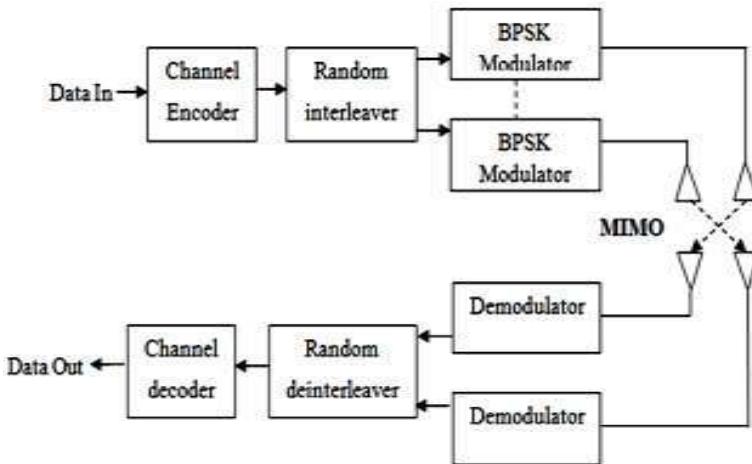
4G bežična mreža koristi OFDM multipleksiranje, ultra široki radio opseg (UWB), i milimetarsku bežičnu i pametnu antenu.

Technology	1G	2G	2.5G	3G	4G
Design Began	1970	1980	1985	1990	2000
Implementation	1984	1991	1999	2002	2010?
Service	Analog voice, synchronous data to 9.6 kbps	Digital voice, short messages	Higher capacity, packetized data	Higher capacity, broadband data up to 2 Mbps	Higher capacity, completely IP-oriented, multimedia, data to hundreds of megabits
Standards	AMPS, TACS, NMT, etc.	TDMA, CDMA, GSM, PDC	GPRS, EDGE, 1xRTT	WCDMA, CDMA2000	Single standard
Data Bandwidth	1.9 kbps	14.4 kbps	384 kbps	2 Mbps	200 Mbps
Multiplexing	FDMA	TDMA, CDMA	TDMA, CDMA	CDMA	CDMA?
Core Network	PSTN	PSTN	PSTN, packet network	Packet network	Internet

Slika 1: Historijski pregled bežičnih sistema

2. MODEL SISTEMA

Informacioni bitovi su kodirani pomoću turbo kanala i zatim mapirani digitalnom MQAM modulacijom. Mapirani podaci se ponovo kodiraju pomoću OSTBC enkodera. Tokovi nezavisnih podataka se šalju kroz OFDM modulatore koji se izvode preko IFFT i dodaju ciklički prefiks CP pa sve ovo prolazi kroz IID kanal. Prijemnik prima signale i šalje ih kroz OFDM demodulatore koji najprije odbacuju CP i izvode na N tački FFT. Izlazi OFDM demodulatora su konačno odvojeni i prošli su kroz OSTBC dekoder. Podaci se demoduliraju i onda dekodiraju koristeći logičke MAP algoritme.



Slika 2: Blok dijagram predloženog sistema

OFDM je tehnika modulacije koja se koristi da bi se pretvorio širokopojasni frekvencijski selektivni kanal u uskopojasni paralelni pljosnati feding kanal koji potiskuje intersimbolsku interferenciju (ISI). Prijemnik poslije FFT stepena, primljeni signal ispisuje kao:

$$Y(k) = H(k) \cdot X(k) + N(k)$$

gdje je:

N= broj sub-carriers

L= broj kanala

K= K-ti sub-carriers

H(k)= Rayleigh-ov koeficijent fedinga s prosječnom snagom "L" i N(0,L)

X(k)= K-ta FFT tačka prijenosnog simbola sa prosječnom snagom “P”

Y(k)= K-ta FFT tačka primljenog signala

N(k)= Gausov šum sa $\mathcal{N}(0, N\sigma^2)$.

Onda SNR na izlazu može biti:

$$SNR_r = \frac{|H(k)|^2 \cdot P}{N \cdot \sigma^2} = L \left(\frac{P}{N \cdot \sigma^2} \right) \therefore BER = Q(\sqrt{SNR_r})$$

$$\Rightarrow BER = \frac{1}{2} \left(1 - \sqrt{\frac{SNR_r}{2 + SNR_r}} \right)$$

$$\Rightarrow BER = \frac{1}{2} \left(1 - \sqrt{\frac{\left(\frac{L}{N}\right) SNR}{2 + \left(\frac{L}{N}\right) SNR}} \right)$$

3. ANALIZA OSOBINA TURBO KODOVA OSTBC SISTEMA

1) Konvulucioni kodovi

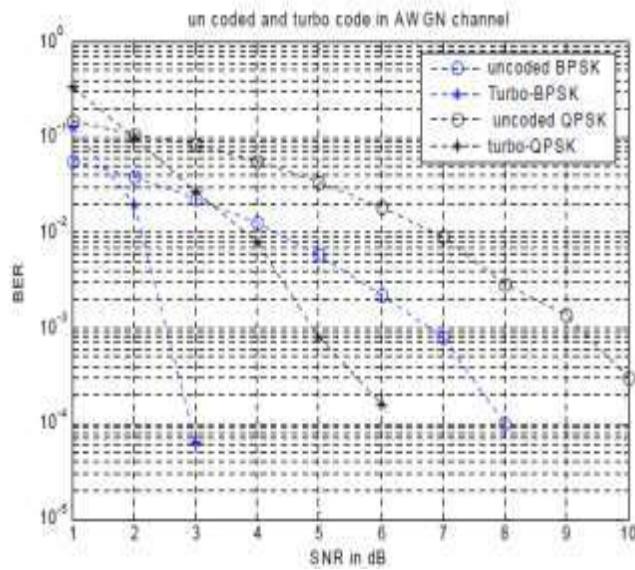
Konvulucioni kodovi pretvaraju cijeli ulazni tok u jednu kodnu riječ. Kodirani bit ne zavisi samo od trenutnog bita nego često nosi informacije i o prethodnim bitima. Dekodiranje se tradicionalno izvodi pomoću Viterbijevog algoritma. Kodovi kao što su konvulucioni kodovi imaju vise redundatnih bita da bi se mogli koristiti za ispravljanje vise grešaka. To znači da komunikacijski sistem može raditi na nižem prenosu snaga, da toleriše vise smetnji i buke i da može prenositi podatke na veće udaljenosti. Tako kodovi postaju više energetski učinkoviti.

2) Konvulucioni turbo kodovi

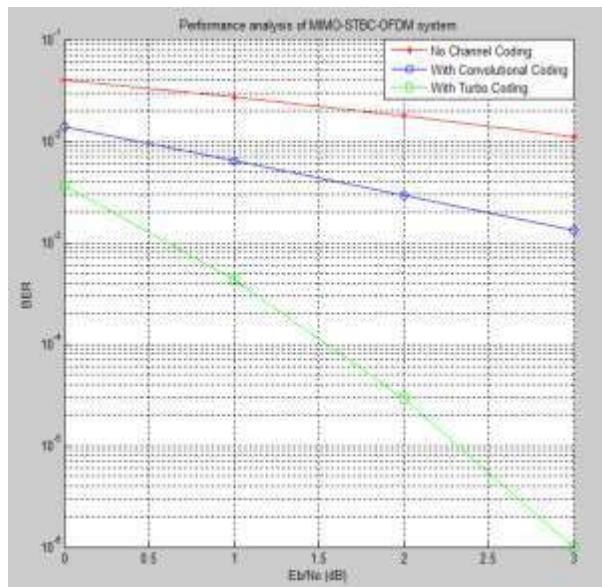
Prvi turbo kod zasnovan na konvulucionom kodiranju uveden je 1993. godine, kada je opisana shema koristeći $\frac{1}{2}$ koda preko AWGN kanala. Ovi kodovi su postizali malu vjerovatnoću greške koristeći BPSK modulaciju pri SNR-u od 0,7 dB. U novije vrijeme turbo kodovi nalaze primjenu u 4G mobilnim komunikacijama. Spajanje kodova za ispravljanje grešaka i podizanje blizu Shannon-ovog kapaciteta se naziva turbo kodiranje.

4. SIMULACIJA PARAMETARA

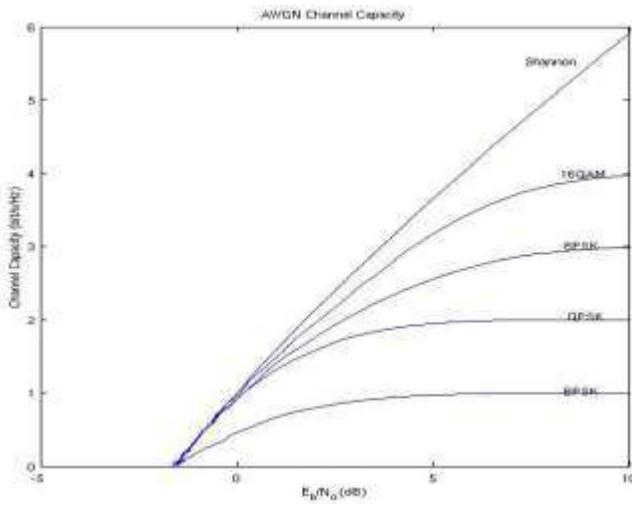
Rezultati osobina turbo kodova su opisani u nastavku. Prepostavimo da generator polinoma koristi $g_0=[1\ 0\ 1\ 1]$ i $g_1=[1\ 1\ 0\ 1]$, te da su Rayleigh-ov feding i Gauss-ov šum jednaki 0, te da je na prijemniku savršeni CSI. Za blok dužine od 40 simbola, veličina okvira od 10 blokova je 400 simbola, a veličina preklopa je 80 simbola. Spektralna efikasnost povezanog sistema je 2bps/Hz.



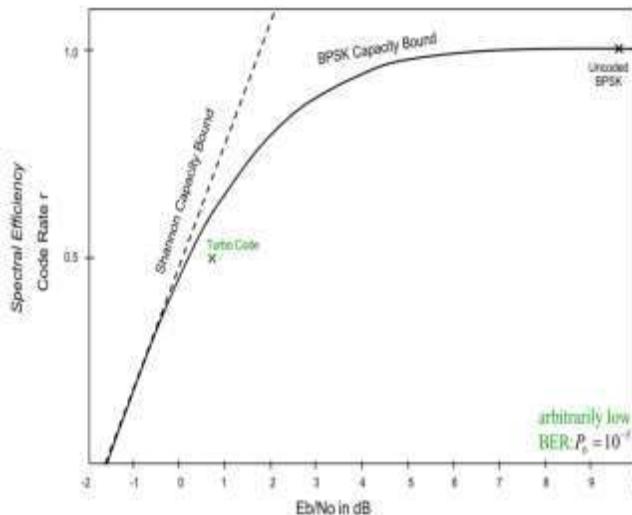
Slika 3: BER vs. SNR dijagram za nekodirani i turbo kodirani OFDM koristeći BPSK i QPSK



Slika 4: Analiza performansi MIMO-STBC-OFDM sistema s turbo kodovima



Slika 5: Spekralna efikasnosti SNR-a



Slika 6: Performanse turbo koda priblizne Shannon-ovom kapacitetu

Na slikama 3 i 4 bez kanalnog kodiranja sistem je dostigao BER na oko 10^{-2} pri 3 dB, a sa konvulacionom kodiranjem doseže BER na oko 10^{-3} pri 3 dB, a koristeći turbo kodiranje BER doseže na oko 10^{-6} također pri 3 dB. Iz rezultata simulacije se vidi da turbo kod daje najbolje performanse BER-a pri niskim SNR razinama i na taj način povećava pouzdanost u brzom prijenosu podataka po višestrukim feding kanalima.

5. 4G SISTEMI

LTE (engl. *Long Term Evolution*) je 4G mreža koja predstavlja sljedeći korak u tehnologiji bežične mreže. Pruža velike brzine prijenosa podataka i svrstava se u intelligentne 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*). Takođe se arhitekturom želi doći do trenutka kada se komutacija kanala više neće koristiti u mreži, već će cijelokupna 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 s LTE-om. LTE ima nasljednika u mrežama, LTE-A (engl. *Long Term Evolution Advanced*), mrežu koja se temelji na LTE-u i teži novim poboljšanjima.

5.1. ARHITEKTURA LTE MREŽE

Predstavnik četvrte generacije bežičnih mreža je evoluirani paketski sistem (engl. *Evolved Packet System*, skraćeno EPS) koji čine LTE (engl. *Long Term Evolution*) i SAE (engl. *System Architecture Evolution*). Kao i u prijašnjim generacijama bežičnih mreža, EPS se sastoji od pristupnog i jezgrenog dijela, pa tako LTE predstavlja pristupni, a SAE jezgredni dio. Bitna razlika u odnosu na prijašnje generacije mreža je uvođenje takozvane ravne arhitekture (engl. *flat architecture*) čija je osnovna osobina 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.

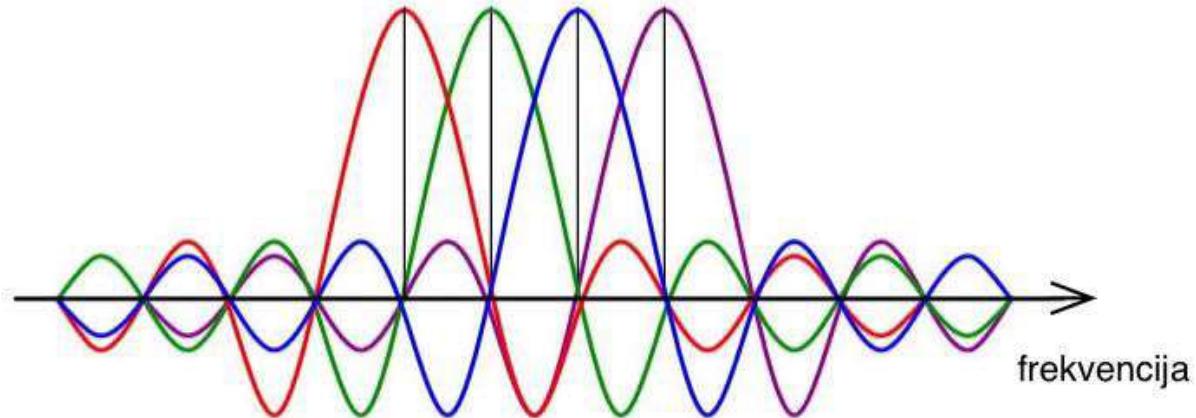
5.1.1. Pristupna mreža

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 zahtjevnejše 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 Management*, skraćeno RRM), nadzor pristupa, kontrola radio prijenosa, raspoređivanje korisničkih podataka, signalizacija i kontrola nad zračnim sučeljem, te šifriranje i sažimanje zaglavlja preko zračnog sučelja.

5.1.1.1. 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 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*) smještenih jedan blizu drugoga. Signalni su međusobno ortogonalni pa ne dolazi do njihovog međusobnog preklapanja i smetnji (slika 7). 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 subnositelja (engl. *subcarrier*).

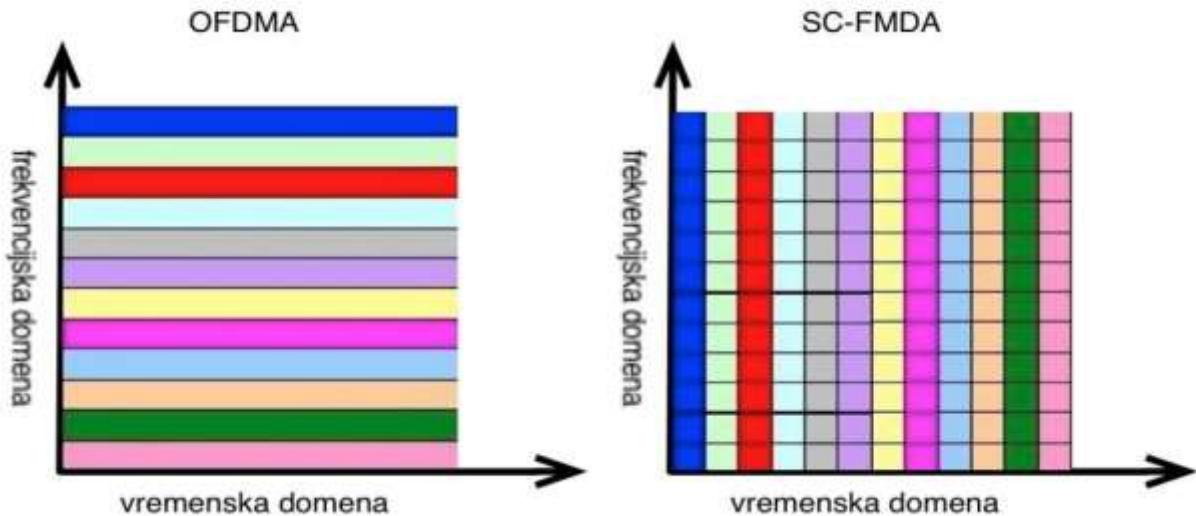
Između tih nositelja je biran odgovarajući frekvencijski razmak tako da maksimum signala svakog od subnositelja odgovara nulama svih ostalih signala. Time se dozvoljava spektralno preklapanje među nositeljima i postiže se bolja spektralna efikasnost.



Slika 7: Razmak među subnosiocima

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 subnositelje različitim korisnicima istovremeno tako da višestruki korisnici mogu istovremeno primati podatke. Kod uzlazne veze se koristi nešto drugačiji koncept: SC-FDMA (engl. *Single Carrier Frequency Division Multiple Access*). Njegovo je bitno obilježje da pojedini korisnik dobiva kontinuirani skup subnositelja 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.

Serijski slijed bitova : 



Slika 8: Kodiranje subnositelja

5.1.1.2. 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 preklapanja (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 preklapanja UE-ova.

5.1.1.3. Evoluirani čvor 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 celija. Neke od zadaća eNodeB-a su:

- Upravljanje celijama 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.

5.1.2. Jezgrena mreža

Jezgreni dio LTE/SAE mreže koji se može naći i pod nazivom EPC (eng. *Evolved Packet Core*) ili SAE (eng. *System Architecture 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).

5.1.2.1. 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 preklapanja,
- Upravljanje pokretljivošću prilikom prelaska na druge mreže,
- Odabir SGSN-a u preklapanjima 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 pronađak UE-a u stanju mirovanja.

5.1.2.2. 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 pređe u područje drugog S-GW-a dolazi do njegove promjene, regulira uspostavu veza s korisnicima drugih mreža. SGW je lokalna anchor tačka za procedure preklapanja 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 EUTRANA-a,
- Upravljanje zahtjevima za uslugom,
- Punjenje evidencije podataka.

5.1.2.3. Paketski mrežni prilazni čvor

Paketski mrežni prilazni čvor završna je tačka 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

5.1.2.4. Čvor za upravljanje resursima i terečenje

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.

5.1.2.5. Poslužitelj domaćih pretplatnika

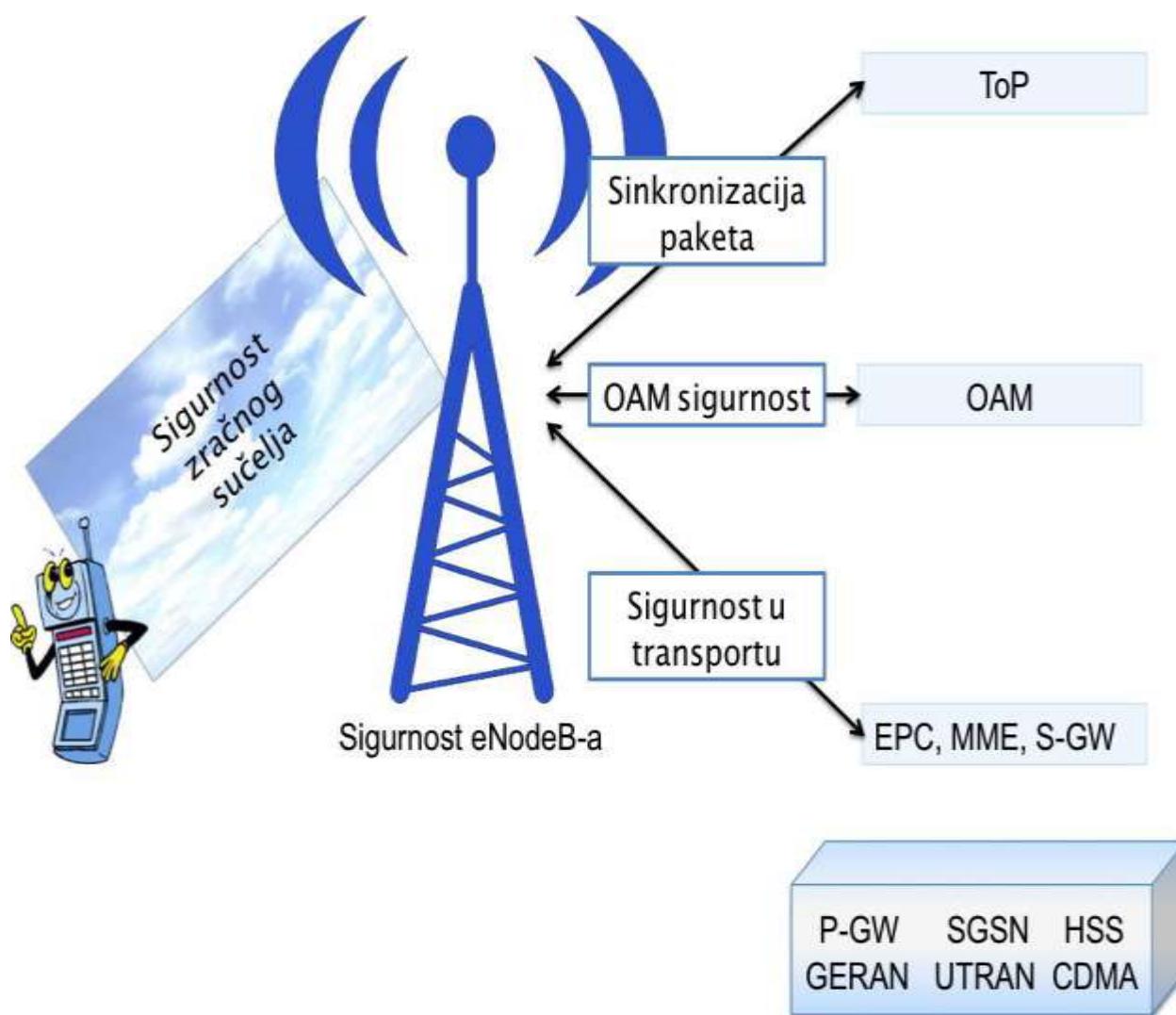
HSS entitet je odgovoran za upravljanje korisničkim profilima i vrši autentifikaciju i autorizaciju korisnika, tj. starih i novih LTE pretplatnika. Korisnički profili kojima upravlja HSS sastoje se od informacija o pretplati, sigurnosti, QoS profilima i pristupnim ograničenjima kod rominga te od fizičke 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 tačke (engl. *Access point name*, skraćeno APN) koje je oznaka dodijeljena pristupnoj tački s obzirom na standarde sistema 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. *Authentication center*, skraćeno AUC) koji generira vektore za autentifikaciju i sigurnosne šifre.

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

5.2. SIGURNOST

Cilj svih sigurnosnih zaštita je spriječavanje napada tako da vanjski napadači imaju minimalne mogućnosti za prevaru 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 sistem zaštite s imaginarnim pokušajima napada. Ako se slabosti sigurnosnog sistema na vrijeme detektiraju, proboji mogu biti ispravljeni i ažurirani u sigurnosnom sistemu. 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 sistem 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 dostupnjem 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 kako 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 cijelokupna 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 9: Različite razine sigurnosti u LTE

5.2.1. 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 sistemima, 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 prevara, dok motivacija za takve aktivnosti može biti finansijske, destruktivne pa čak i političke prirode. Moderna informacijska tehnologija kombinirana s poboljšanom pokretnom tehnologijom dovodi do novih aspekata koji mogu povećati osjetljivost na namjerne prevare. 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 sofisticirane 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 promjene podataka isključivo od ovlaštene osobe, autentičnost i verifikaciju identiteta korisnika, odnosno raspoloživost unatoč neočekivanim događajima.

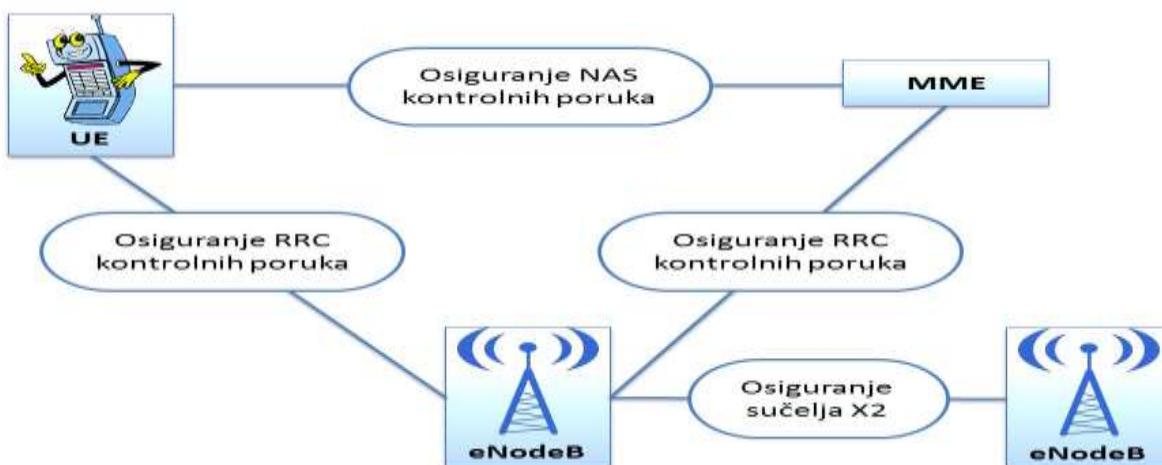
5.2.2. Sigurnosne ravnine

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 Management*) 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.

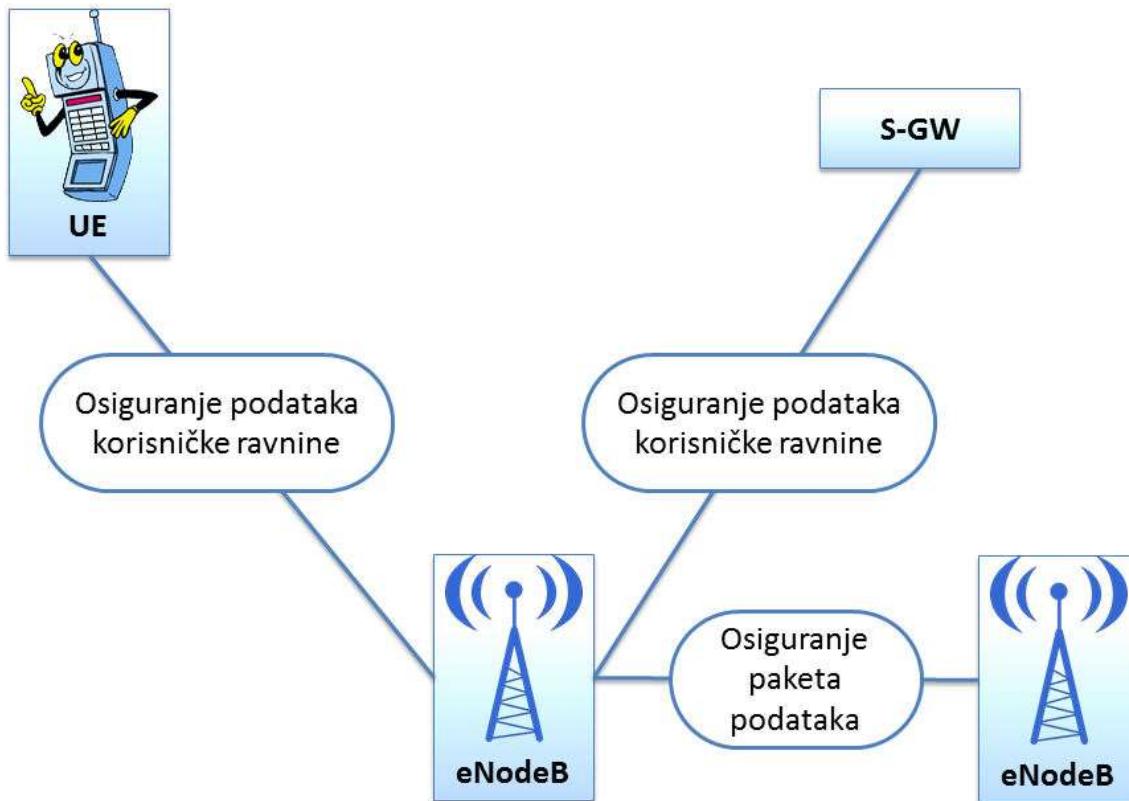
Drugačije ravnine u mreži imaju drugačije podatke te se mogu ostvariti drugačiji napadi na mreži. Zbog zaštite, sigurnosne ravnine dijele se na:

- 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 10: Sigurnost kontrolne ravnine

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 preklapanja. 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 11: Sigurnost kontrolne ravnine

Način na koji je izvedena sigurnost korisničke ravnine prikazana je slikom (Sl. 11.). 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 SGW-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 nsigurnosnu domenu.

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

5.2.3. 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 challenge 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:

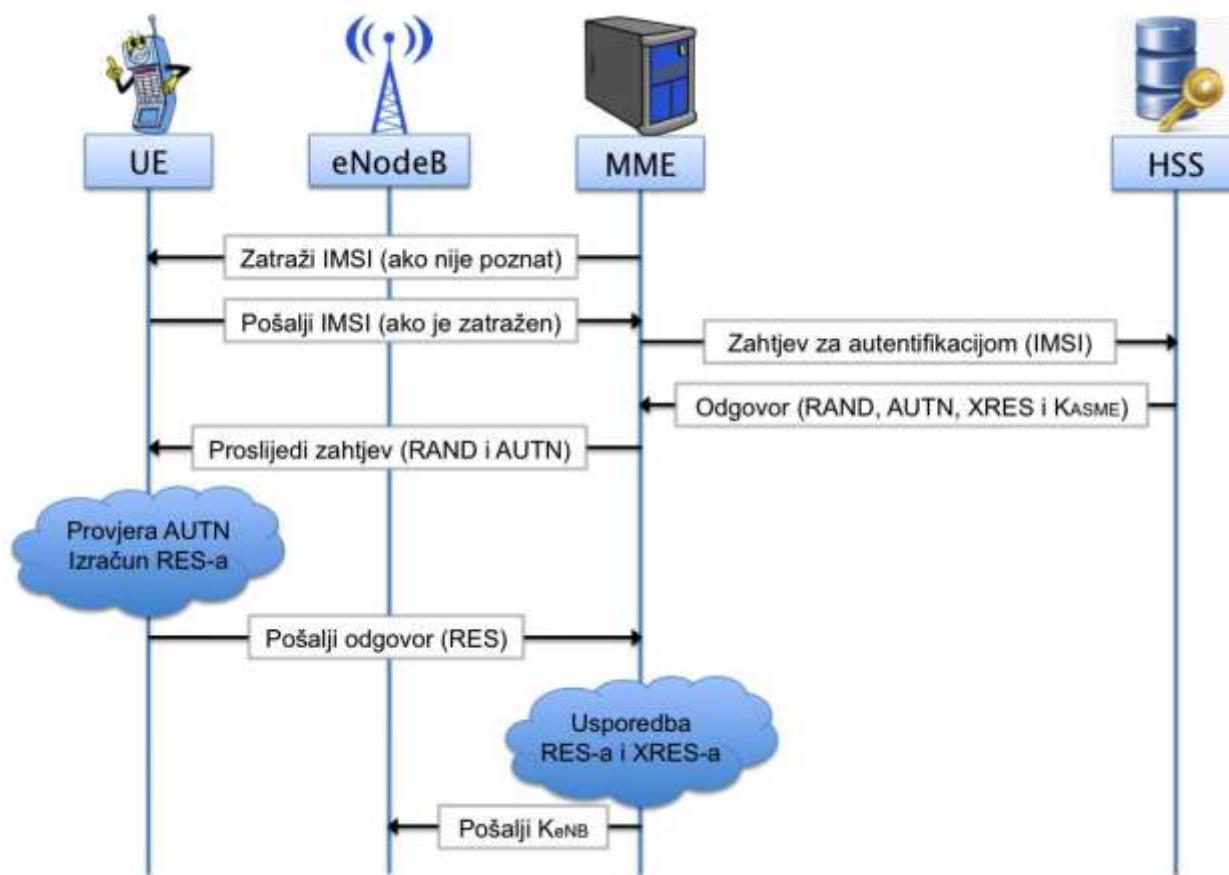
- mogućnosti bržeg preklapanja
- podjele na više dijelova zbog kojih je narušavanje sigurnosti lokalno
- povećava se složenost rukovanja sigurnosnim mehanizmima

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 $K_y = \text{KDF}(K_x, S)$ izračunava hash vrijednost od K_x i niza S , a upravo ta vrijednost postaje izvedeni ključ K_y .

- K_x je nadređeni ključ, ključ koje se u hijerarhiji nalazi na višoj poziciji.
- K_y 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 izведен iz CK i IK tijekom AKA procesa, a nalazi se u HSS-u i UE-u.
- KeNB – Ključ eNodeB-a za preklapanje. Ključ izведен u eNodeB-u i UE-u tijekom preklapanja.
- 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 izведен iz eNodeB-a i UE-a.
- KRRCenc – Ključ za kodiranje podataka koji se šalju pomoću protokola RRC.

5.2.4. 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 potvrđan pristup se korisniku treba dodijeliti. Tek nakon što je klijent autenticiran, 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 12: Proces autentifikacije kod LTE-a

Na slici 12. 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 potvrđio 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, 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 imenom, a odnosi se na situaciju prilikom koje se mobilna stanica kreće na granicu između dviju ćelija koje su pokrivenе mrežom s različitim baznim stanicama. Problem koji se javlja je kako odrediti na koju će se baznu stanicu mobilna stanica spojiti. Rješenje je dopustiti mobilnoj stanci 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.

5.2.5. 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 absolutno zaštiti mrežu. Zaštita za skoro sve dijelove mreže već postoji, no uvjek se javljaju novi napadi. Najčešće vrste napada su:

- 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 poluotvorena. Takve poluotvorene konekcije spremaju se u memoriju, te do isteka određenog vremena poslužitelj pokušava iznova poslati SYN/ACK pakete.

- Napad na korisničku ravninu

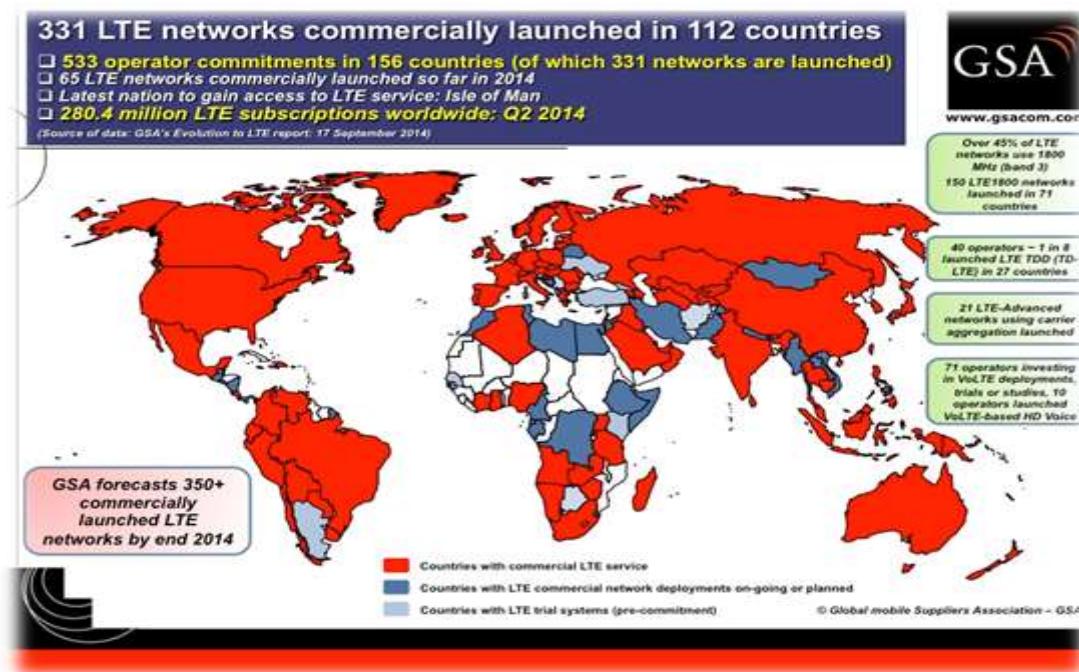
Primjer napada: Dva eNodeB čvora moraju razmijeniti korisničke podatke u obliku podatkovnih paketa. Napadač prislушкиje vezu kojom se šalju podaci između dva čvora eNodeB kako bi saznao korisničke podatke. Komunikacija između dva eNodeB čvora u korisničkoj ravnini zaštićena je protokolom IPsec. Protokol 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.

- 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. 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 komplikirano, 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.

6. PRIMJER DEMONSTRIRANE 4G MREŽE

Azija predstavlja najdinamičnije područje kad je reč o razvoju telekomunikacionih mreža četvrte generacije. To, između ostalog, potvrđuju aktivnosti japanske kompanije NTT DoCoMo, giganta iz oblasti telekomunikacija. Početkom marta prošle godine, on je ponudio interesovanje javnosti demonstracijom nove telekomunikacione mreže četvrte generacije. Demonstracija je priređena u istraživačkom i razvojnom centru kompanije lociranom nedaleko od Tokija. Centar se nalazi u tehnološkom parku u kome radi više od 40 istraživačkih organizacija mnogih poznatih svetskih kompanija. NTT DoCoMo svoja istraživanja obavlja sa oko 1.200 zaposlenih i u saradnji sa partnerskim kompanijama (Intel, Texas Instruments, Cisco Systems, HP, Ericsson, Nokia, Fujitsu). U istraživački centar ulaže oko 130 milijardi jena godišnje (oko 1.1 milijardu dolara). Mnogi komentari o najnovijim aktivnostima te kompanije bili su skeptični, s obzirom na to da kompanija još uvek ima problema sa mrežom prethodne, treće generacije. NTT DoCoMo trenutno ima oko dva miliona korisnika 3G usluga i oko 40 miliona korisnika 2G servisa. Bez obzira na sve komentare i probleme, kompanija je pristupila razvoju nove ultrabrzre 4G mreže. Ona se zaista može nazvati ultrabrzom, jer će se prenos podataka obavljati brzinom od 50 Mb/s (upload), odnosno 100M/s (download). To je oko 260 puta brže od prenosa podataka u 3G mreži (384Kb/s). Tako velika brzina će bez problema omogućiti prenos različitih audio i video sadržaja.



Slika 13: Zemlje u kojima je komercijalno predstavljena LTE tehnologija

7. KVALITETA USLUGE (QoS, Quality of Service)

Osiguranje kvalitete usluge (QoS) za prijenos vremenski osjetljivih (real-time) informacija od velike je važnosti za daljni razvoj i širenje područja upotrebe IP mreža. Kvalitatan prijenos vremenski osjetljivih informacija bio je donedavno ostvariv samo u mrežama s komutacijom kanala (Circuit Switching), gdje se za prijenos koristi zasebna komunikacijska linija, ili u spojno orijentiranim mrežama s komutiranjem paketa, gdje se za prijenos vremenski osjetljivih informacija koristi zaseban virtualni krug sa strogo definiranim parametrima kvalitete usluge. Najvažniji parametri koji određuju kvalitetu prijenosa vremenski osjetljivih informacija su kašnjenje između krajnjih tačaka (end-to-end delay), kolebanje tog kašnjenja, mjera gubitka paketa i mjera pogrešaka pri prijenosu.

7.1. Kašnjenje između krajnjih tačaka

Prilikom prijenosa video ili audio signala, kašnjenje između prijemnika i predajnika u velikoj mjeri utječe na kvalitetu reprodukcije signala. Razne studije su pokazale da su kašnjenja audio signala veća od 100 – 150 ms primjetna i neugodna za ljudsko uho. Kod interaktivnih videokonferencija, slika i zvuk moraju biti sinhronizirani na prijemnoj strani, pa slijedi da ukupno kašnjenje video signala između krajnjih tačaka također ne smije biti veće od 100 – 150 ms. Veća kašnjenja video paketa također uzrokuju lošiju kvalitetu reprodukciju slike poput trzanja i “zamrzavanja” slike, ili prividno usporenog gibanja objekata. Najveći doprinos kašnjenju između krajnjih tačaka u pravilu daje samo procesiranje video signala (kapturiranje, komprimiranje). Ono izravno zavisi o korištenom formatu, koderu i parametrima slike. Ova kašnjenja mogu biti i nekoliko stotina ms, ali su ona predvidiva i približno konstantna, pa se u nekim slučajevima mogu tolerirati veća kašnjenja, uz uvjet zadržavanja malog kolebanja kašnjenja i osiguranja sinkronizacije predajnika i prijemnika, te audio i video signala.

7.2. Kolebanje kašnjenja

Kolebanje kašnjenja je kritičan parametar pri prijenosu vremenski osjetljivih informacija. Kašnjenja predvidivog i približno stalnog iznosa mogu se kompenzirati vremenskom sinhronizacijom elemenata na putu signala, ali i veća i nepredvidiva kolebanja kašnjenja mogu predstavljati veliki problem pri reprodukciji slike.

Kolebanje kašnjenja je razlika kašnjenja između dva susjedna paketa. Najveći doprinos kolebanju kašnjenja unosi proces raspoređivanja i prosljeđivanja paketa na mrežnim čvorovima. To se posebno odnosi na slučaj zagušenja na mreži i uređajima, tako da ovo kolebanje značajno zavisi i o vanjskim parametrima, poput ukupnog opterećenja mreže. Iznosi kolebanja kašnjenja trebali bi biti što manji, a prihvatljivim se mogu smatrati kolebanja do iznosa oko 1 ms.

7.3. Gubitak paketa

Izgubljeni paketi su normalna pojava u mrežama. Do gubitaka paketa može doći zbog preopterecenja linka, precestih kolizija na LAN-u ili pak zbog fizickog oštecenja medija. TCP protokol ima ugraden mehanizam kojim posredstvom retransmisija može popraviti ovakve slucajeve. Kako se za prijenos govora koristi nepouzdani UDP, o izgubljenim paketima mora brinuti aplikacija. Ukoliko je postotak izgubljenih paketa mali, reda 1%, nisu potrebne nikakve akcije, jer svaki paket nosi 20 ms pa gubitak govornog signala u tom trajanju jedva je primjetljiv. Gubitak paketa do 10% oštijek se da ispraviti na prijemnoj strani, preko toga smatra se da je veza neupotrebljiva za prijenos govora. Problem izgubljenih paketa rješava se u sklopu codeca. Postoji više razlicitih algoritama za ublažavanje efekta izgubljenih paketa, a neki od njih su:

- ignorirati izgubljene pakete ako je rijec o malim postotcima,
- kod vecih postotaka možemo ponoviti prethodno primljeni paket, što u vecini slucajeva može zadovoljiti, ali je daleko od dobrog rješenja,
- izgubljene pakete možemo interpolirati nekom od prediktorskih metoda.

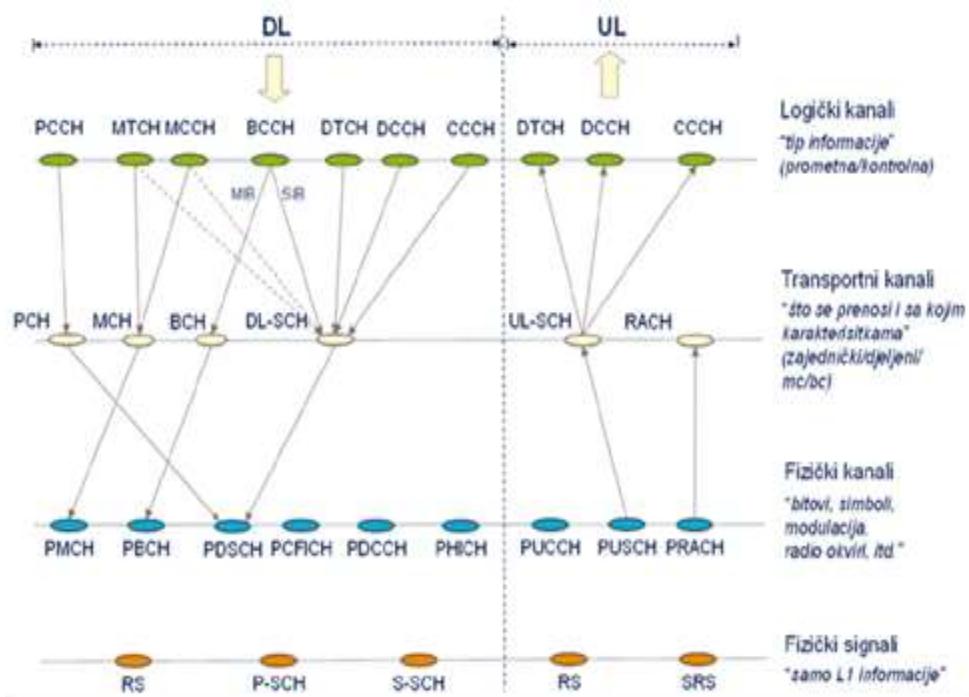
Prediktor se “navikava” na visinu i boju glasa u toku normalne konverzacije a u slučaju gubitka paketa pokušava predvidjeti kakav je sadržaj nosio taj paket.

7.4. Pogreške pri prijenosu

Utjecaj pogrešaka pri prijenosu video paketa između krajnjih tačaka također utječe na kvalitetu reprodukcije slike. Ovaj je utjecaj čak i manje izražen nego kod prijenosa podatkovnih paketa, jer jedan pogrešno primljeni bit ili paket predstavlja tek mali dio ukupne informacije o slici. Ipak, veliki broj pogrešno primljenih paketa može prouzročiti degradaciju kvalitete slike. Parametri kojima se iskazuje stepen pogrešaka pri prijenosu signala su mjera pogrešaka bitova (BER – Bit Error Rate) i mjera pogrešaka paketa (PER – Packet Error Rate).

8. STRUKTURA KANALA

LTE tehnologija koristi četiri nivoa kanala za prenos podataka i različitih informacija. Svaki od ovih nivoa obavlja posebne zadatke uz pomoć više vrsta kanala što je prikazano na slici 14.



Slika 14: Mapiranje kanala

Logički kanali služe za opis tipa podataka koji se prenose, a mogu biti kontrolni ili prometni. Kontrolnim kanalima se prenose informacije vezane za kontrolnu ravan, dok se prometnim kanalima prenose informacije korisničke ravni.

Logički kanali koji su podržani u LTE tehnologiji su:

- odašiljački kontrolni kanal (eng. BCCH – *Broadcast Control Channel*) čija je uloga slanje sistemskih kontrolnih informacija u silaznoj vezi;
- kontrolni kanal za upravljanje radio pozivima (eng. PCCH – *Paging Control Channel*) koji služi za prenos radio poziva u silaznoj vezi, a koristi se onda kada mreža ne zna tačnu lokaciju mobilne stanice;
- zajednički kontrolni kanal (eng. CCCH – *Common Control Channel*) kojim se dvosumno razmenjuju kontrolne informacije između mreže i korisničkih uređaja. Najčešće se upotrebljava od strane mobilnih stаница koje nemaju RRC konekciju sa mrežom i mobilne stанице koje koriste zajedničke transportne kanale kad pristupaju novoj ćeliji nakon rezbora ćelije;
- prideljeni kontrolni kanal (eng. DCCH – *Dedicated Control Channel*) se koristi u oba smera za slanje kontrolnih informacija između mreže i mobilne stанице, a uspostavlja se kroz postupak RRC uspostave konekcije;
- kontrolni kanal za grupno odašiljanje (eng. MCCH – *Multicast Control Channel*) služi za prenos MBMS¹ raspoređivanja i kontrolnih informacija prema mobilnim stanicama koje koriste ove servise;
- prideljeni prometni kanal (eng. DTCH – *Dedicated Traffic Channel*) se dodeljuje samo jednoj mobilnoj stanci i služi za prenos korisničkih informacija u oba smera;
- prometni kanal za grupno odašiljanje (eng. MTCH – *Multicast Traffic Channel*) je kanal kojim se prenose prometni podaci prema mobilnim stanicama koje koriste MBMS.

Navedeni logički kanali se dalje mapiraju na transportne, čiji je broj sveden na minimum kako bi se izbeglo kašnjenje usled velikog broja promena tipa kanala. U transportne kanale spadaju:

- odašiljački kanal (eng. BCH – *Broadcast Channel*) kojim se u silaznoj vezi prenose specifične informacije prema svim mobilnim stanicama na području jedne ćelije. Ovaj kanal ne podržava upravljanje dijagramom zračenja;
- deljeni kanal u silaznoj vezi (eng. DL-SCH – *Downlink Shared Channel*) je kanal čiji su resursi podeljeni između korisnika u silaznoj vezi. Podržava adaptaciju veze izmenama modulacije, kodiranja ili odašiljačke snage, kao i diskontinuirani prijem (eng. DRX – *Discontinuous Reception*). Ima mogućnost upravljanja dijagramom zračenja,
- pozivni kanal (eng. PCH – *Paging Channel*) se šalje u celoj ćeliji i podržava diskontinuirani prijem;
- kanal za grupno odašiljanje (eng. MCH – *Multicast Channel*) predstavlja MBMS transportni kanal koji se odašilje na području cele ćelije i pri tome podržava MBMS odašiljanje sa više ćelija (eng. MBSFN – *MBMS Single Frequency Network*);

- dijeljeni kanal u uzlaznoj vezi (eng. UL-SCH – *Uplink Shared Channel*) je kanal čiji se resursi dele između korisnika na uzlaznoj vezi. Adaptacija veze je moguća uz pomoć izmena modulacije, kodiranja ili odašiljačke snage, a takođe je moguće i upravljanje dijagramom zračenja;
- kanal za slučajni pristup (eng. RACH – *Random Access Channel*) se koristi u uzlaznoj vezi za ostvarivanje vremenske sinhronizacije kao i za slanje informacija pomoću kojih se pribavljaju odobrenja za slanje podataka. Najčešće se više korisničkih uređaja nadmeće za korištenje ovog kanala.

MAC sloj prosleđuje podatke za slanje fizičkom sloju u vidu transportnih blokova, a osim fizičkih kanala na koje se mapiraju odgovarajući transportni kanali postoje i fizički kanali za prenos informacija ka ili sa MAC sloja gde spadaju:

- fizički kontrolni kanal u silaznoj vezi – PDCCH koji služi za kontrolnu signalizaciju (za kontrolu snage, raspoređivanje u silaznoj vezi i odobravanje raspoređivanja u uzlaznoj vezi);
- fizički kontrolni kanal u uzlaznoj vezi – PUCCH takođe ima ulogu u kontrolnoj signalizaciji (zahtevi za raspoređivanjem u uzlaznoj vezi, CQI, ACK/NACK);
- kanal indikatora kontrolnog formata (PCFICH – eng. *Physical Control Format Indicator Channel*) definiše format PDCCH na silaznoj vezi;
- kanal HARQ indikatora (eng. PHICH – *Physical Hybrid ARQ Indicator Channel*) služi za prenos HARQ informacije (ACK/NACK) u silaznoj vezi.

Pored fizičkih kanala postoje i fizički signali koji podržavaju funkcije fizičkog sloja ali ne prenose nikakvu informaciju sa MAC sloja. U fizičke signale spadaju:

- referentni signali (eng. RS – *Reference Signals*) koji služe za merenja i koherentnu detekciju u silaznoj i uzlaznoj vezi;
- sinhronizacijski signali (eng. P-SCH i S-SCH – *Primary and Secondary Synchronization signals*) koji imaju ulogu u silaznoj vezi pri izboru ćelije tako što definišu sinhronizaciju na okvire i detektuju identitet ćelije;
- referentni signal za ispitivanje (eng. SRS – *Sounding Reference Signal*) koji služe za merenja pri raspoređivanju u uzlaznoj vezi.

9. 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.

10. LITERATURA

- 1) Filip Lemić: Algoritmi raspodjele potkanala, bitova i snage u višekorisničkim OFDMA sustavima, diplomski rad, FER Zagreb, 2013.
- 2) Man Young Rhee: “Wireless mobile internet security”, 2nd edition, Wiley, UK, 2013.
- 3) Muškardin Marin, Falan Sandro: 3GPP Long Term Evolution i ns-3 LENA, znanstveni članak
- 4) Penttinen, Jyrki T.J. : ”The LTE/SAE Deployment Handbook”, Wiley, UK, 2012.
- 5) O. Edfors, M. Sandell, J.-J. van de Beek, S. K. Wilson, and P. O. Börjesson, “OFDM channel estimation by singular value decomposition,” IEEE Trans. Commun., vol. 46, pp. 931–939, July 1998.
- 6) William E. Ryan, Shu Lin: “Channel Codes: Classical and Modern“, Cambridge Univeristy Press, 2009
- 7) <http://ieeexplore.ieee.org/Xplore/home.jsp>, datum pristupa: 9.8.2019.
- 8) <https://www3.nd.edu/~mhaenggi/NET/wireless/4G/>, datum pristupa: 9.8.2019.
- 9) https://www.fer.unizg.hr/_download/repository/PrZv_10_2018.pdf, datum pristupa 12.8.2019.