QoS u IMS-u sa aspekta govorne usluge

Opačak, Barbara

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Sveučilišni studij

QoS U IMS-u S ASPEKTA GOVORNE USLUGE

DIPLOMSKI RAD

Barbara Opačak

Osijek, 2016.

SADRŽAJ

1. UVOD

Integracija fiksno-mobilnih telekomunikacijskih i podatkovnih mreža je uvela aplikacije i multimedijske usluge u nove generacije mreža (NGN). Multimedijske usluge, kombinirajući web pregledavanje, instant poruke, VOIP, video konferencije, dijeljenje aplikacija i telefoniju postavljaju se na vrh mrežnih tehnologija. Uzroci toga su višestruki. [1]

IMS (engl. *IP multimedia subsystem*) - IP multimedijski podsustav je standardizirana mrežna arhitektura nove generacije koja je zamišljena za operatore telekomunikacijskih usluga da pruže složene usluge u mobilnim i fiksnim mrežama. IMS je arhitekturalni okvir orijentiran na pružanje trenutnih i budućih internet usluga fiksnim i mobilnim korisnicima preko višepristupne IP platforme. IMS je definiran skupinom standarda koji je napravio 3GPP (engl. *The 3rd Generation Partnership Project*) i 3GPP2. IMS omogućuje operaterima telekomunikacijskih usluga stvaranje infrastrukture usluga otvorenog tipa bazirane na IP-u što omogućuje brzi razvoj novih multimedijskih komunikacijskih usluga kombinirajući telekomunikacijske i podatkovne usluge.

U teorijskom dijelu rada obrađen je pojam IMS-a, razvoj IMS-a od njegova nastanka do danas, arhitektura, sigurnost te mehanizmi održavanja sigurnosti i kvalitete usluge IMS-a. Također je obrađen VoIP protokol, DTMF i T.38 standard. Obrađena je i kvaliteta usluge (*QoS*) kao niz specifičnih zahtjeva koje mreža mora ispuniti korisniku, a koji su potrebni kako bi se postigla potrebna funkcionalnost usluge, čimbenici koji utječu na *QoS*, parametri *QoS*-a, te *QoS* u mobilnim 2G i 3G mrežama i VoIP *QoS*.

U praktičnom dijelu rada izvedene su dvije simulacije, te obrađeni rezultati simulacija. Prva simulacija izvedena je puštanjem DTMF signala u sustavu između mreža različitih operatera telekomunikacijskih usluga, a druga simulacija izvedena je pomoću govornog signala u pozivu unutar fiskne mreže, te između fiksne i mobilne mreže. Nakon simulacija analizirani su parametri kvalitete usluge te je definiran *QoS*.

2. IMS

2.1. Razvoj IMS-a

IMS je razvijen kako bi zadovoljio potrebe razvoja mobilnih, fiksnih i IT mreža. Razvoj IMS-a je uvjetovan potrebom telekomunikacijske industrije, a naročito kako bi GSM telekomunikacijska industrija omogućila sveprisutni pristup multimedijskim uslugama [2].

IMS standarde je razvila grupa 3G.IP formirana 1999. godine. Grupa je kasnije postala dio 3GPP-a što je omogućilo bolje usklađivanje s GSM standardima koja je postala glavni korisnik.

U skladu s tim, IMS je definiran 3GPP standardima, te se njegov razvoj može pratiti u različitim verzijama (Tablica 2.1.).

Tablica 2.1. *Razvoj IMS-a i 3GPP standardi*

Verzije(RELEASE)	**Karakteristike**
Release 99 (1999)	Prvo izdanje UMTS standarda zasnovanog na tehnologiji W-CDMA. Podrška za GSM/EDGE/GPRS/WCDMA radijske pristupne mreže
R4 (2001)	Odvajanje kanalne i paketske domene u jezgrenoj mreži. Razdvajanje funkcionalnosti MSC i MGW unutar jezgrene mreže, podrška za MMS
R5 (2002)	Prvo izdanje koje uključuje IMS. Cilj je podrška uvođenju multimedijskih usluga i pristupna mreža UTRAN zasnovana na protokolu IP. Glavni signalizacijski protokol je SIP. Upravljanje kvalitetom usluge (engl. *QoS*) i napredno upravljanje uslugama i mogućnostima *charginga.* Uvođenje HSDPA.
R6 (2004)	Integracija s WLAN-om. Podrška za QoS, usluge PoC i MMS. Uvođenje MBMS, HSUPA i naprednih mogućnosti *charginga*.
R7 (2007)	Dodavanje širokopojasnog fiksnog pristupa kroz IMS. Glatko prebacivanje govornih poziva između kanalne i paketske (IMS) domene s ispoštovanim zahtjevima na kvalitetu usluge.

R8 (u tijeku)	Sve-IP mreža (engl. *AIPN - All-IP Network*). Dugoročna evolucija (engl. *Longterm evolution, LTE*), višemedijska konferencija u IMS-u.

Veliki korak korištenju IMS-a se dogodio na *Mobile World Congress*-u 2010. godine, gdje je GSMA najavio podršku za VoLTE (engl. *Voice over LTE*). Kako se sustav bazira na IMS-u, mnogi operatori su odlučili ukomponirati IMS mogućnosti unutar svojih mreža.

2.2. Arhitektura IMS-a

IMS arhitektura je relativno komplicirana što može rezultirati skupom implementacijom te potrebnim znanjem kako bi se razumjela.

Arhitektura IMS-a se sastoji od sljedećih dijelova [3], [4]:

AS (engl. *Application Server - aplikacijski server*) - pruža izvršne usluge i singalizaciju za usluge, surađuje s S-CSCF-om koristeći SIP. To omogućuje pružateljima usluge brzu integraciju i razvoj usluga dodane vrijednosti IMS infrastrukturi. Primjeri korištenih usluga su: ID pozivatelja, poziv na čekanju, proslijeđivanje poziva, blokiranje poziva, prepoznavanje malicioznih poziva, objavljanja, konferencijski pozivi, lokacijski bazirane usluge, SMS, MMS, instant poruke, VCC serveri, fiksno-mobilna konvergencija...

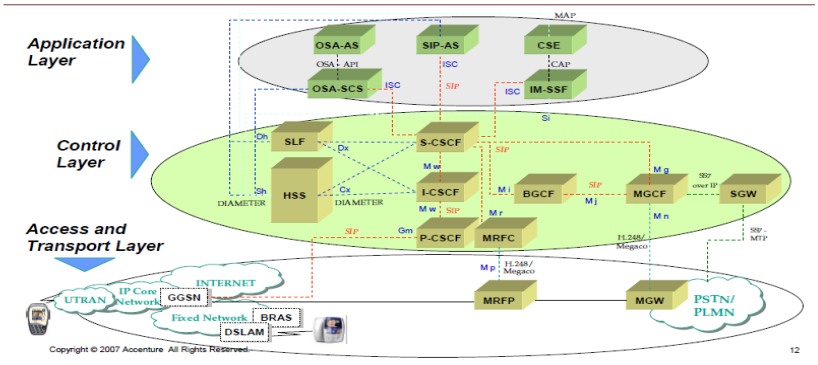
- MRF (engl. *Multimedia Resource Function*) je mrežni element čija svrha je obrada medijskih streamova poznatih kao RTP streamovi za usluge bazirane na mreži. *Media stream* obrada uključuje funkcije igranja, skupljanja DTMF znamenki, audio snimanje i reprodukcija, konferencije, prepoznavanje govora, pretvaranje teksta u govor, video obrada. Uloga MRF-a u obavljanju tih funkcija je podređena - uvijek djeluje pod izravnom kontrolom AS-a, te odgovara SRF-u (engl. *Specialized Resource Function*) inteligentne mreže.
- S-CSCF (engl. *Serving - Call State Control Function*) je *call* server s ulogom točke iz koje se usluge uključuju. S-CSCF sadrži korisnički profil koji pokazuje na koje usluge se korisnik pretplatio, te na uvjete pod kojima se usluge uključuju. S-CSCF odgovara SSF-u (engl. *Service Switching function*) inteligentne mreže. S-CSCF nadzire SIP registracije, što omgućuje vezanje korisnikove lokacije i SIP adrese. Nalazi se na putu svih signalnih poruka, te tako može provjeriti svaku poruku. S-CSCF odlučuje kojem AS-u će SIP poruka biti proslijeđena kako bi se pružila

usluga. U mreži može biti više S-CSCF-a zbog distribucije opterećenja i visoke dostupnosti.

- P-CSCF (engl. *Proxy Call Session Control Function*) - prva točka kontakta za IMS terminal. Prosljeđuje registracijske zahtjeve iz UE u I-CSCF, prosljeđuje SIP poruke S-CSCF-u kojeg administrira korisnik te prosljeđuje zahtjeve i odgovore iz UE. P-CSCF je dodjeljen IMS terminalu tijekom registracije preko DHCP-a ili u PDP kontekstu, te se ne mijenja tijekom trajanja registracije. P-CSCF se nalazi na putu svih signalnih poruka, te može provjeriti svaku poruku, autentificira korisnika i stvara IPsec sigurnosno udruženje s IMS terminalom, može kompresirati i dekompresirati SIP poruke, može se nalaziti u gostujućim i kućnim mrežama.
- I-CSCF (engl. *Interrogating Call Session Control Function*) - SIP funkcija koja se nalazi na kraju administrativne domene. Njegova adresa je objavljena u DNS-u domene kako bi ga udaljeni serveri mogli pronaći i koristiti kao točku za prosljeđivanje (npr. registriranje) SIP paketa u ovu domenu. I-CSCF ispituje HSS o lokaciji korisnika, te zatim usmjerava SIP zahtjev pripadajućem S-CSCF-u. Do standarda R6 koristio se i za sakrivanje interne mreže od vanjskog svijeta. Od standarda R7 tu funkciju je preuzeo IBCF (engl. *Interconnection Border Control Function*),
- HSS (engl. *Home Subscriber Server*) ili UPSF (engl. *User Profile Server Function*) - baza podataka svih podataka korisnika i usluge. Sadrži korisničke profile koje koristi kontrolni sloj, pretplatničke informacije koje koristi uslužni sloj, podatke za provedbu autentifikacije i autorizacije korisnika, te može sadržavati podatke o fizičkoj lokaciji korisnika. HSS također pruža funkcije HLR (engl. *Home Location Register*) i AUC (engl. *Authentication Centre*). Time korisniku omogućuje pristup paketima i domenama mreže inicijalno preko IMSI autentifikacije. Korisnički profil sastoji se od: identiteta korisnika, dodjeljenog S-CSCF imena, informacija o registraciji i roaming profila, autentifikacijih parametara, kontrolnih i uslužnih informacija.
- SLF (engl. *Subscription Locator Function*) - koristi se za pronalaženje adresa korisnika kada se koristi više HSS-a. SLF se koristi u IMS mreži kao rezolucijski mehanizam koji omogućuje I-CSCF-u, S-CSCF-u i AS-u pronalazak adrese HSS-a koji sadrži podatke o korisniku.

- BGCF (engl. *Break Out Gateway Control Function*) - IMS element koji bira mrežu u kojoj se treba pojaviti PSTN bijeg. BGCF se koristi za pozive iz IMS-a na telefon u *Circuit switched* mreži, poput PSTN ili PLMNa. BGCF prosljeđuje signale odabranoj PSTN/PLMN mrežu. Ako se bijeg dogodi u istoj mreži u kojoj je BGCF, tada BGCF odabire MGCF (engl. *Media Gateway Control Function*) koja će biti zadužena za surađivanje s PSTN-om i prosljeđuje signal MGCF-u. U drugom slučaju, prosljeđuje signal BCGF-u mreže drugog operatera. MGCF tada prima SIP signal iz BGCF i održava suradnju s PSTN mrežom.
- PSTN prolazi (engl. *Public Switched Telephony Network Gateways*) - suradnja s *Circuit Switched* (*CS*) mrežom se održava pomoću nekoliko komponenti - za signalne, media i kontrolne funkcionalnosti. SGW (engl. *Signalling Gateway*) je sučelje s signalnim zadaćama u CS-u. SGW pretvara niželojne protokole poput SCTP-a u MTP, kako bi ISUP prošao iz MGCF-a u CS mrežu. MGCF (engl. *Media Gateway Controller Function*) provodi kontrolu protokola poziva između SIP-a i ISUP-a, sučeljava SGW preko SCTP-a, kontrolira MGW resurse s H.248 sučeljem. MGW (engl. *Media Gateway*) služi za media zadaće CS mreže, konvertirajući između RTP-a i PCM-a. Također se može koristiti za media konvertiranje ukoliko korišteni kodeci ne odgovaraju.
- IM-SSF (engl. *IP Multimedia - Service Switching Function*) - čvor u IMS domeni koji osigurava suradnju između SIP kontrola sesija i inteligentne mreže tradicionalnih mreža. Ova funkcionalnost je ktirična za nove, konvergirane ponude uz nastavak usluga za korisnike visoke vrijednosti. IM-SSF također omogućuva pristup informacijama o pretplatniku dobivenih iz HSS-a koristeći MAP protokol.

Arhitektura IMS-a prikazana je na slici 2.1.

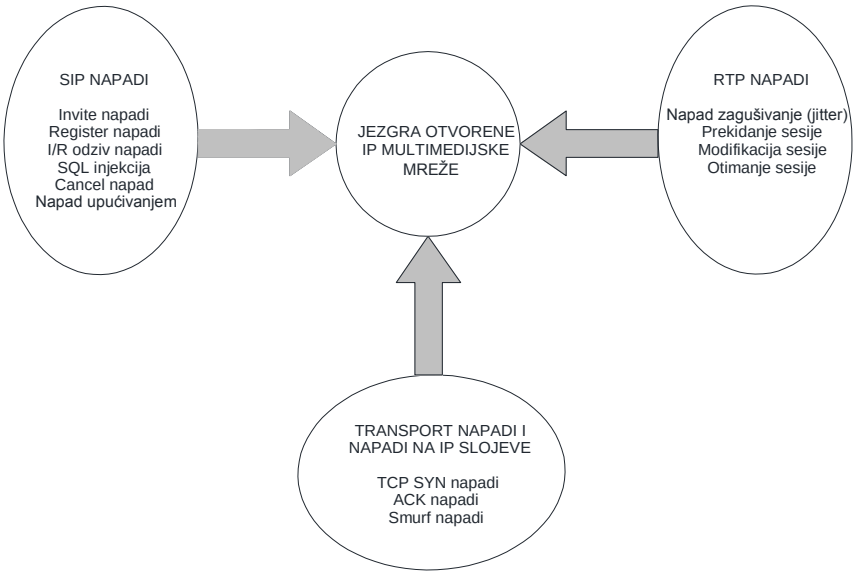


Slika 2.1. *Arhitektura IMS-a [4]*

2.3. Sigurnost IMS-a

Sigurnost IMS podsustava se definira kao sigurnost ostvarivanja veza između elemenata unutar IMS-a. Opasnosti za sigurnost IMS-a su prijetnje iz različitih domena - SIP signalni napadi, RTP media napadi, IP napadi na domene [1].

Sigurnosni izazovi IMS-a su DoS napadi, opasnosti iz *open-based* IP infrastrukture, SIP signalni i media napadi, te su prikazani na slici 2.2.



Slika 2.2. *Opasnosti za sigurnost IMS-a [1]*

Denial-of-service **(DoS) napadi** - zagušuju radio signale zahtjevima za autentifikaciju P-CSCF-u i ostalim uređajima, npr. slanjem mnogo zahtjeva s krivim adresama što opterećuje IMS, te time korisnik ne može dobiti uslugu.

Spoofing **napadi (napadi zavaravanja)** - maliciozni čvor se skriva u mreži i ometa promet, te ga kvari porukama. Ti čvorovi tada postaju pouzdani čvorovi u IMS-u.

Man-in-the-middle **napadi (čovjek-u-sredini napadi)** - hakeri traže propuste i prekidaju proces autentifikacije i zaštite integriteta kako bi dobili usluge IMS-a besplatno.

Impersonizacija - impersoniziranje servera uzrokuje pogrešno usmjeravanje poruka. Postojeći autentifikacijski sustav ne može razlikovati uljeza i legitimnog korisnika što daje besplatan pristup IMS uslugama. Tako žrtva plaća za napadačevo korištenje usluga.

Prisluškivanje - hakeri dobivaju informacije o sesijama ako su poruke poslane u čistom tekstu, te tako mogu lako napraviti napad na temelju informacija iz sesije

Napad pogađanjem zaporke - iako haker ne može slomiti IMS-ov proces autentifikacije, može napraviti napad pogađanjem zaporke kako bi iskoristio legitimne račune korisnika. Haker šalje napade slanjem mnogo zahtjeva za registraciju P-CSCF-u te dobiva 401-neautorizirane poruke iz IMS jezgre. Napadač može dobiti 200 OK odgovora u uspješnom napadu.

SQL injekcija - *message-tamper* tip napada - SIP poruke pružaju priliku za takav tip napada. Ova vrsta napada ne cilja samo na modifikaciju podataka, već uzrokuje zabranu pristupa kolapsom usluga baze podataka. Utilizacija Web sučelja čini IMS ranjivijim ovoj vrsti napada.

Prekid medijske sesije - BYE zahtjev se koristi za prekidanje uspostavljene sesije. Napadač šalje lažnu BYE poruku, koja je proslijeđena iz P-CSCF-a u UE1. UE1 pretpostavlja da poruka dolazi iz UE2. Stoga UE1 zaustavlja RTP tok dok UE2 i dalje šalje RTP pakete UE1 jer nema informaciju o prekidu veze. Za ostvarenje ovog napada, napadač mora znati sve parametre sesije. To se može postići proučavanjem mreže ili korištenjem *man-in-the-middle* napada za umetanje BYE zahtjeva u sesiju.

***CANCEL* napad** - CANCEL naredba prekida zahtjev koji je u tijeku. Napadač može utilizirati CANCEL metodu kako bi prekinuo INVITE zahtjev od strane legitimnog korisnika. Napadač šalje lažnu CANCEL poruku P-CSCF-u prije nego je generiran odgovor za INVITE zahtjev. P-CSCF pretpostavlja da poruka dolazi od strane legitimnog korisnika. IMS jezgra prihvaća CANCEL poruku i zaustavlja procesuiranje INVITE zahtjeva. CANCEL naredba se može koristiti za prekidanje samo INVITE zahtjeva.

Re-INVITE napad - INVITE naredba uspotavlja sesiju između dva korisnička uređaja. Uloga re-INVITE poruke je modificiranje informacija aktualne sefije promjenom adresa, portova, dodavanjem *media stream-a*, brisanjem *media-stream-a*... Napadač može napraviti DoS napad slanjem krivotvorene re-INVITE poruke kako bi modificirao sesiju.

Odbijanje - korisnik ili mreža odbijaju radnje koje se odvijaju.

Maskiranje - napadač obmanjuje sustav da je autorizirani korisnik kako bi dobio povjerljive informacije i usluge.

IP multimedia services identity module* (*ISIM*) *cloning - kloniranje identifikacijskog modula IP multimedijske usluge - ovaj proces mijenja identitet jednog člana članom istog tipa. ISIM se može klonirati izvodom tajnog ključa (K) i interancionalnog identiteta mobilnog pretplatnika (engl. *IMSI - international mobile subscriber identity*) iz jednog ISIM-a, te prebacivanjem u drugi ISIM koristeći drug etehnike napada.

2.4. Mehanizmi održavanja sigurnosti IMS-a

Cilj mehanizama održavanja sigurnosti IMS-a je osigurati privatnost korisnika i zaštitu mreže od zloupotrebe. Radi održavanja sigurnosti IMS-a koriste se sljedeći mehanizmi:

Povjerljivost korisnika- pruža povjerljivost identiteta korsnika, lokacije korisnika i nemogućnost praćenja korisnika. Stoga se korisniku dodjeljuje privremeni identitet kako se trajni identitet korisnika ne bi mogao otkriti radio pristupom. Također, korisnikovi podaci i signali koji mogu otkriti korisnikov identitet su kodirani.

Autentifikacija subjekta - temelji se na autentifikaciji korisnika i mreže, te se primjenjuje pri uspostavi veze između korisnika i mreže. Koristi se autentifikacijski mehanizam koristeći autentifikacijski vektor od strane korisnika mreže, te lokalni autentifikacijski mehanizam.

Povjerljivost podataka - osigurava povjerljivost korisnikovih podataka i signalnih podataka. Postiže se šifriranim algoritmima i ključevima.

Integritet podataka - osigurava integritet podataka i izvornu autentifikaciju signalnih podataka, a postiže se integritetnim algoritmima i integritetnim ključevima.

Dostupnost mreže i usluga - osigurava dostupnost mreže i usluga cijelo vrijeme svim korisnicima. Kako bi se osigurala dostupnost, mrežu je potrebno zaštititi od DoS i DDos napada.

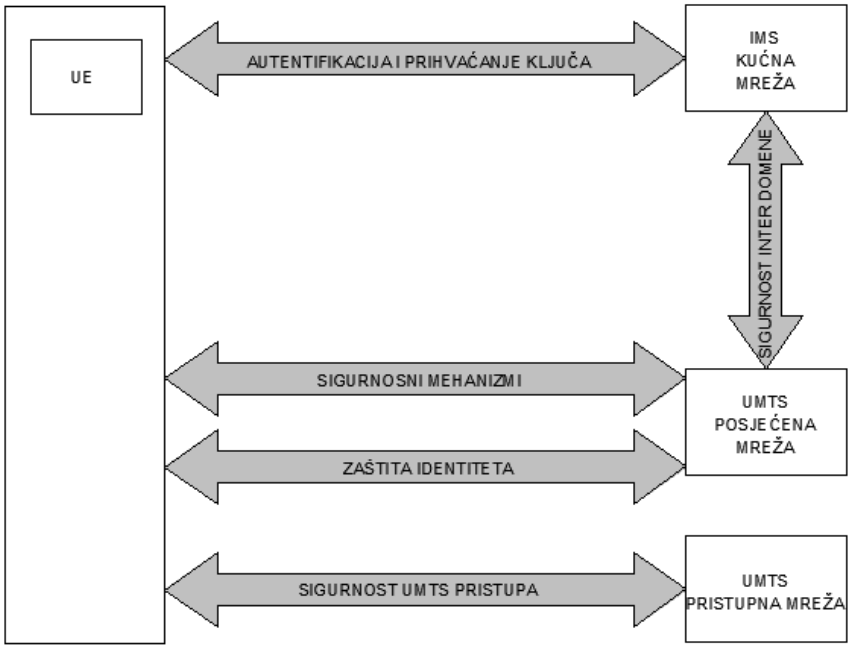
Kontrola prevara - štiti vrijedne stvari i dodatne usluge od nelegitimnih korisnika i hakera osiguravajući AS - aplikacijski server. 3GPP i 3GPP2 su standardizirali IMS sigurnost u svojim različitim izdanjima:

- rani standardi u 3GPP izdanju 5 pružaju ograničenu funkcionalnost sigurnosti, te im je cilj zaštititi rani razvoj IMS-a. Ovi standardi pružaju autentifikaciju pretplatnika za pristup uslugama i povjerljivost identiteta korisnika na radio sučelju, te šifriranje na radio sučelju.

- potpuno rješenje IMS sigurnosti je standardizirano u 3GPP izdanju 6. Ovo izdanje sadrži punu funkcionalnost sigurnosti - napravljeno je na temelju ranijih sigurnosnih rješenja s ciljem da ih se popravi. Pruža nova sigurnosna svojstva i nove usluge za zaštitu mreža i terminala s zaštitom podataka. Sastoji se od mrežne domene sigurnosti i sigurnosnog pristupa koji definiraju SIP sigurnost u *hop-by-hop* načinu. *End-to-end* sigurnost nije podržana. Shema sigurnosti IMS-a prikazana je na slici 2.3.

Sigurnost IMS-a sastoji se od sljedećih mehanizama:

- autentifikacija i prihvat ključa između IM pretplatnika i kućne mreže
- sigurnosni mehanizam potvrde između IM klijenta i posjećene mreže
- zaštita integriteta i povjerljivost
- sigurnost mrežne domene između različitih domena
- postojeća GPRS/UMTS sigurnost pristupa



Slika 2.3. *Shema sigurnosti IMS-a*

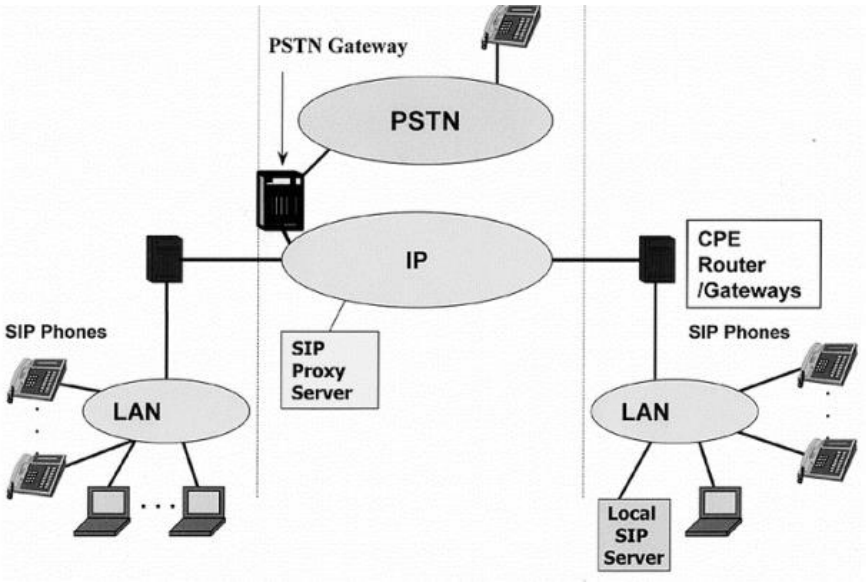
Sigurnosni mehanizmi IMS-a su određeni sljedećim sigurnosnim udruženjima (engl. *security association* - SA)

- SA1 - pruža obostranu autentifikaciju korisnika i mreže (Sl. 2.4.). HSS je odgovoran za generiranje ključeva i *challenge-a*, a zatim šalje autentifikaciju pretplatnika S-CSCF-u.
- SA2 - pruža sigurnu vezu i sigurnosno udruženje između UE i P-CSCF
- SA3 - pruža sigurnost unutar mrežne domene. HSS trajno sprema podatke pretplatnika i usluge.
- SA4 - pruža sigurnost između različitih mreža za SIP čvorove, primjenjuje se samo kada je P-CSCF u gostujućuj mreži (npr. kada je korisnik u *roamingu*).
- SA5 - pruža sigurnost interno u mreži između SIP čvorova, te se primjenjuje kada je P-CSCF u kućnoj mreži. IMS štiti sav IP promet u jezgri mreže koristeći NDS/IP, što pruća povjerljivost, integritet podataka, autentifikaciju i antiponavljačku zaštitu prometa.
- SA6 - osigurava povjerljivost i integritet podataka HTTP prometa.
- SA7 - štiti korisnika i njegove podatke na pristupnim mrežama (UMTS, GSM, GPRS, WLAN, DSL, VoIP).

2.5. VoIP

VoIP (engl. *Voice over Internet Protocol*) je glasovna komunikacija koja koristi IP (engl. *Internet Protocol*) za prijenos komunikacije za razliku od tradicionalne telefonije PSTN (enlg. *Public Switched Telephone Networks*) koja koristi kružni sklop. VoIP tehnologija radi tako da se informacije digitalno prenose u jednom ili više paketa. Paketi imaju svoj cilj, te ondje mogu dolaziti različitim putevima [5].

VoIP zahtjeva više protokola za signaliziranje poziva, uspostavu poziva, transport govora kroz mrežu, kvalitetno preusmjeravanje, rezervaciju resursa, naplatu usluge te upravljanje mreže prema QoS.



Slika 2.4. *Dijagram IP telefonskog sustava spojenog na IP mrežu [5]*

Slika 2.4. prikazuje dijagram IP telefonskog sustava spojenog na IP mrežu. IP telefoni su spojeni preko LAN-a, te se pozivi mogu uspostaviti lokalno preko LAN-a. IP telefoni sadrže kodeke za kodiranje i dekodiranje govora, te paketiziranje i depaketiziranje kodiranog govora u IP pakete. Pozivi između različitih mjesta se mogu uspotaviti preko širokopojasne IP mreže. Proxy serveri odrađuju IP registraciju telefeona i koordiniraju signalizaciju poziva. Također je moguće i spajanje na PSTN preko VoIP *gateway-a* [5].

2.5.1. Signalizacija poziva

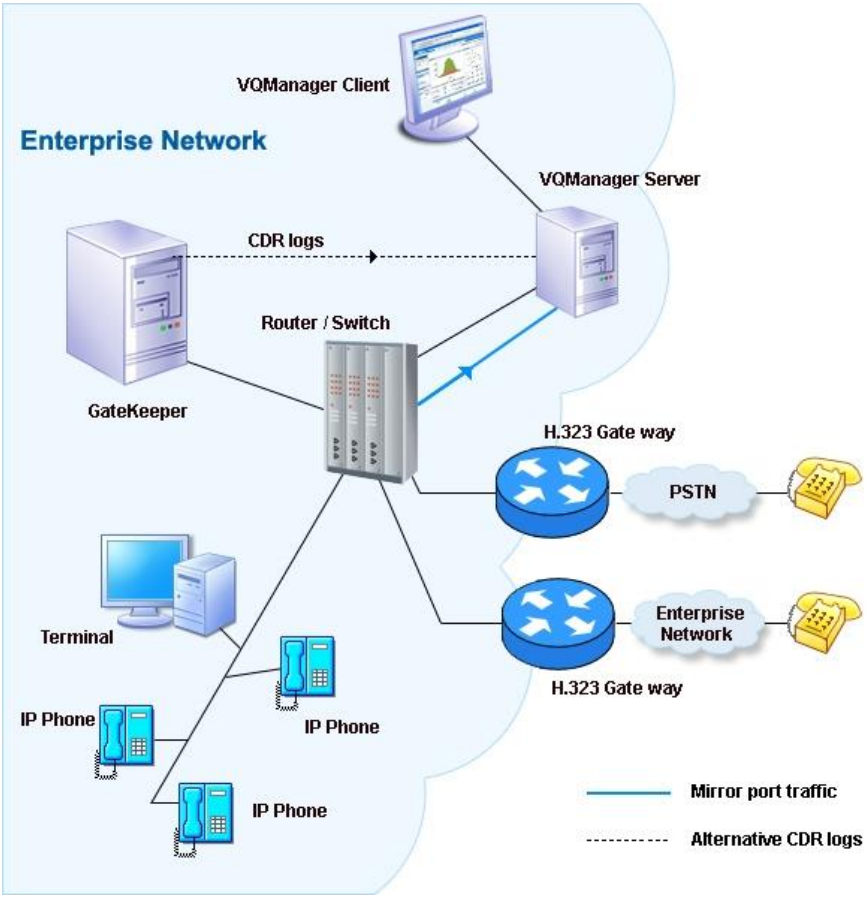
Kada se VoIP koristi za sinkronizirane glasovne ili multimedijalne komunikacije između dvije ili više strana, tada koristi signalizaciju koja kreira i upravlja pozivom.

Signalizacije internet telefonije odnosi se na nekoliko funkcija: prijevod imena i korisnikove lokacije uključuje mapiranje između imena različitih nivoa apstrakcije, značajka pregovaranje omogućuje grupi krajnjih sustava dogovor o razmjeni medija i njihovih parametara poput kodiranja, upravljanje sudionicima poziva za mogućnost uključivanja i isključivanja dodatnih sudionika iz poziva, značajku izmjena koja omogućuje prilagodbu kompozicije medijske sesije tijekom poziva.

Signalizacijski VoIP protokoli su sljedeći:

- H.323
- SIP (engl. *Session Initiation Protocol*)
- MGCP (engl. *Media Gateway Control Protocol*)
- Megaco/H.248

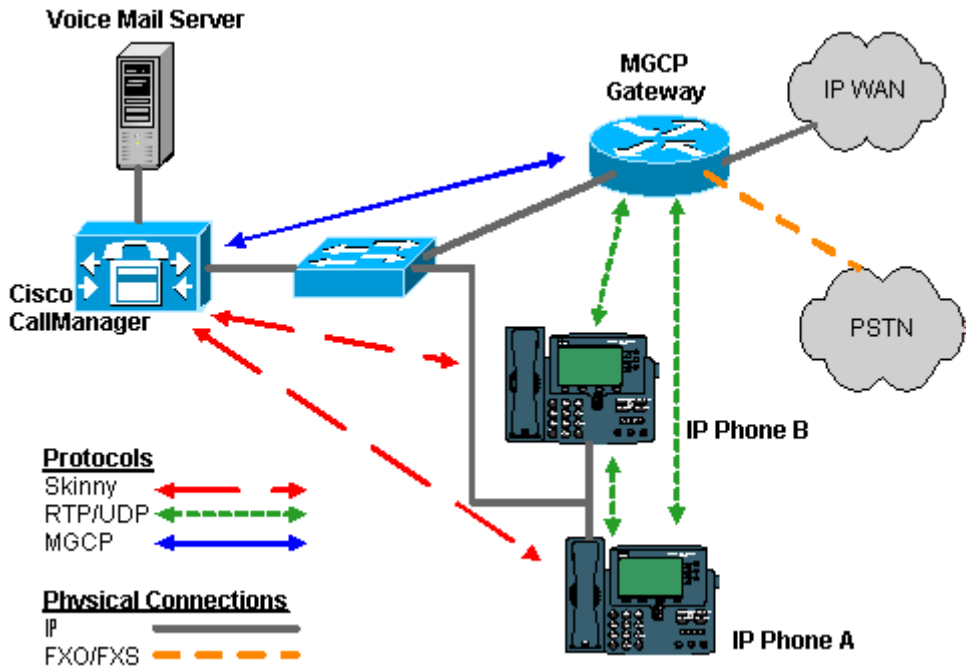
H.323 protokol je jedan od protokola za uspostavu poziva koji se najduže koriste. Standardiziran je od strane Međunarodne unije za telekomunikacije (ITU). Koristi se kao zajednički protokol na glasovnim pristupnicima kako bi spojio VoIP mrežu sa PSTN mrežom. H.323 koristi TCP za komunikaciju. Uspostavljanje poziva ovim protokolom zahtjeva mnogo *back-and-forth* TCP tokova.



Slika 2.5. *Protokol H.323 u funkciji [6]*

Media Gateway Control Protocol **(MGCP)** se najčešće koristi kako bi poslužitelj poziva kontrolirao vezu glasovnog pristupnika s PSTN-om. Od drugih protokola za uspostavu poziva razlikuje se po tome što kod njega krajnje točke, ili telefoni, ne koriste MCPG da bi kontrolirali telefonski poziv.

MGCP koristi UDP port 2427 port za slanje poruka između pristupnika i poslužitelja poziva. Kako poslužitelj poziva kontrolira pristupnik, većina obavještajnih informacija se nalazi tamo.



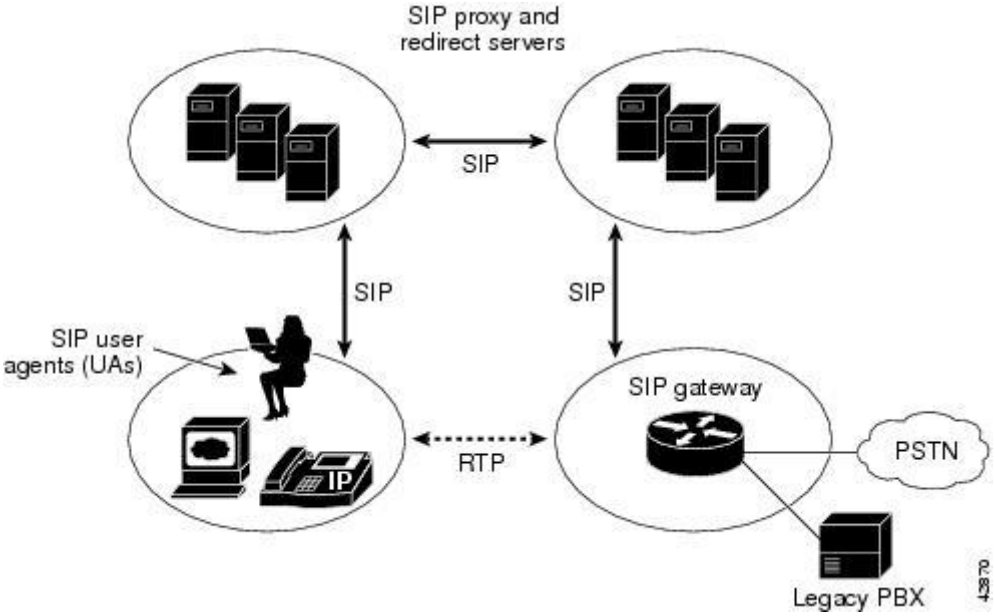
Slika 2.6. *Protokol MGCP u funkciji [5]*

Session Initation Protocol **(SIP)** je signalizacijski protokol koji se koristi za uspostavu, modifikaciju i raskidanje multimedijskih sesija u IP mrežama [7]. Razvijen je od strane IETF-a, a prihvatila su ga i ostala značajna međunarodna standardizacijska tijela kao glavni protkol u višemedijskim domenama 3G mobilnih sustava. SIP je baziran na HTTP transakcijskom modelu zahtjeva i odgovora. SIP protokol se može koristiti za uspostavljanje bilo kojeg tipa sesije. Kako podržava i IPv4 i IPv6, područje primjene je bitno prošireno te je olakšana migracija IP mreža prema IPv6.

SIP protokol se sastoji od četiri sloja:

- sintaksa i kodiranje koje koristi ABNF pravila
- transportni sloj - definira kako korisnik šalje zahtjeve i prima odgovore putem mreže
- transakcijski sloj - upravlja retransmisijama aplikacijskog sloja, povezivanjem odgovora i zahtjeva, te istekom vremena aplikacijskog sloja
- sloj korisnika transakcije - kada korisnik transakcije šalje zahtjev, potrebno je kreirati klijent transakciju te joj proslijediti zahtjev s IP adresom na koju treba poslati zahtjev.

Značajke SIP protokola su određivanje lokacije, mogućnosti i dostupnosti korisnika, te uspostava i upravljanje višemedijskim sesijama. Slika 2.7. prikazuje logičke komponente i način rada SIP-a.



Slika 2.7. *Logičke komponente SIP-a [7]*

2.5.2. Prijenos

Za razliku od većine internet aplikacija koje za komunikaciju koriste TCP/IP protokol, VoIP koristi kombinaciju RTP-a i UDP-a preko IP. UDP pruža nepouzdanu izravnu uslugu dostave koristeći IP za prijenos poruka između točaka na internetu. RTP, u suradnji s UDP-om, pruža *end-to-end* mrežne prijenosne funkcije za aplikacije koje prenose *real-time*

podatke, poput audia i videa, preko unicast i multikastih mrežnih usluga. RTP ne čuva resurse i ne garantira *QoS*. Protokol RTCP omogućuje praćenje linka, ali većina VoIP aplikacija nudi kontinuirani stream RTP/UDP/IP paketa bez obzira na gubitak ili kašnjenje paketa do primatelja.

2.5.3. Kašnjenje

Kašnjenje uključuje kašnjenje zbog procesuiranja kodeka, te zbog širenja. Prema ITU-T standardima G.114, preporučena su sljedeća kašnjenja u jednom smjeru:

- 0 to 150 ms: prihvatljivo za većinu aplikacija
- 150 to 400 ms: prihvatljivo za internacionalne veze
- > 400 ms: neprihvatljivo za opće planirane mrežne namjene, u izuzetnim slučajevima se može prekoračiti

Kolebanje kašnjenja (engl. *jitter*) je također važno. Primateljev telefon mora kompenzirati kolebanje s *bufferom*, što uzrokuje kašnjenje ranijih paketa i manje kašnjenje kod kasnijih paketa kako bi zvuk bio pravilan. Svi paketi koji stignu kasnije od duljine *buffera* se odbacuju. Kako je potreban što manji gubitak paketa, kašnjenje *buffera* se postavlja na maksimalnu vrijednost koja se može očekivati. To kašnjenje *buffera* mora se uzeti u obzir u ukupno *end-to-end* kašenjenje koje slušatelj doživljava pri razgovoru koristeći paket telefoniju.

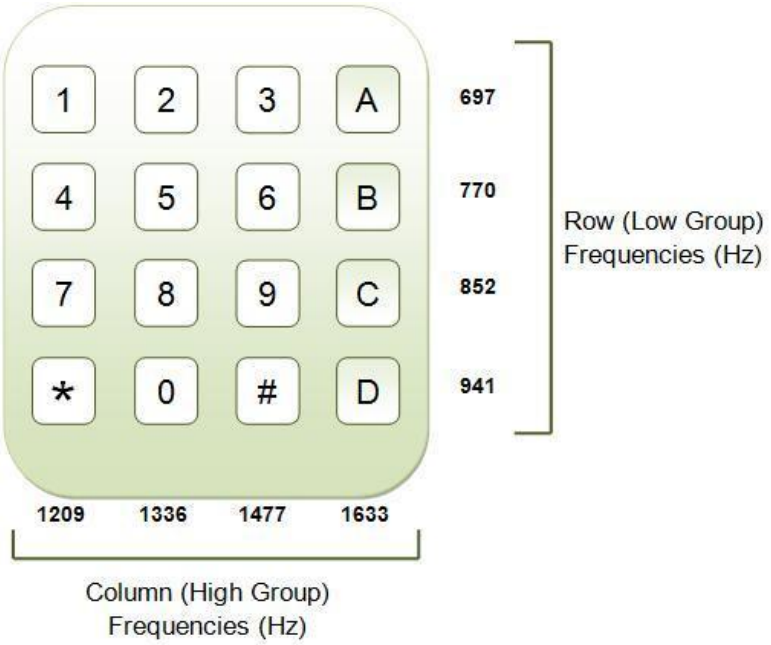
2.6. DTMF (engl. *dual tone multi frequency*)

DTMF (engl. *dual tone multi frequency*) - dvotonski prijenos podataka - signal telefonskoj kompaniji koji se stvara kada se na običnom telefonu pritisnu tipka. Svaka tipka koja se pritisne na telefonu stvara dva tona specifične frekvencije. Kako glas ne bi imitirao te tonove, jedan ton se stvara iz grupe tonova visoke frekvencije i jedan ton iz grupe tonova niske frekvencije. Tonovi su prikazani u tablici 2.2., te na slici 2.8.

Tablica 2.2. *DTMF znamenke*

Znamenka	Niska frekvencija	Visoka frekvencija		Znamenka	Niska frekvencija	Visoka frekvencija
1	697	1209 Hz		**9**	852	1477
2	697	1336		**0**	941	1336
3	697	1477		*	941	1209
4	770	1209		#	941	1477
5	770	1336		**A**	697	1633
6	770	1477		**B**	770	1633
7	852	1209		**C**	852	1633
8	852	1336		**D**	941	1633

Signali A,B,C i D su rijetki u telefonskim mrežama, te se koriste za kontrolu mreže.



Slika 2.8. *DTMF znamenke [8]*

2.7. G.711 standard

G.711 kodek je ITU standard visoke brzine (64 kbps), te se smatra materinjim jezikom moderne mreže digitalne telefonije [9].

Iako je formalno standardiziran 1988. godine, izumljen je i uveden od strane tvrtke Bell Systems još u 70-im godinama prošlog stoljeća. T1 prenositelj koristio je 8-bitnu PCM (engl. *Pulse Code Modulation*) shemu kodiranja s brzinom od 8000 uzoraka u sekundi. To je omogućilo maksimalnu širinu raspona zvuka od 4000 Hz. T1 prenositelj prenosi 24 digitalna PCM kanala multipleksirana zajedno dok poboljšani europski E1 standard prenosi 30 kanal.

Postoj dva zakona na kojima se temelji G.711 standard:

- A-zakon
- μ-zakon

μ-zakon je autohton T1 standardu korištenom u Sjevernoj Americi i Japanu. A-zakon je autohton E1 standardu korištenom u ostatku svijeta. Razlika između ova dva zakona je u načinu uzorkovanja analogno signala. U oba programa signali se uzorkuju logaritamiskim načinom. A-zakon predviđa viši dinamički raspon za razliku od μ-zakona. Rezultat toga je "jasniji" zvuk zbog manjeg zagušenja uzoraka.

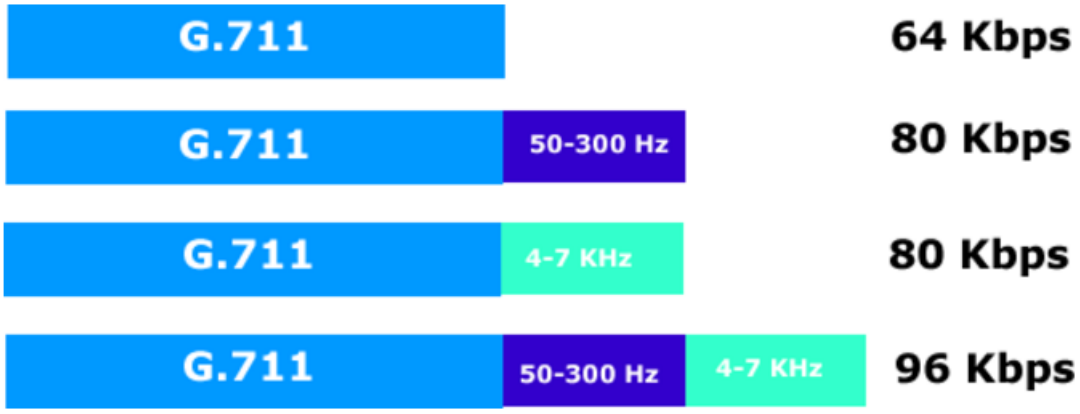
Korištenje G.711 u VoIP-u daje najbolju kvalitetu zvuka jer taj standard koriste i PSTN mreže i ISDN linije, te stoga zvuk zvuči kao i kod običnog ili ISDN telefona. Također, G.711 ima najmanje kašnjenje budući da praktički i nema potrebe za *buffering*-om.

Nedostatak standarda je što treba veći pojas od ostalih kodeka (do 84 kbps) koristeći UDP i IP). Usprkos tome, s obzirom na trend povećanja širokopojasne propusnosti, to i ne predstavlja veliki problem, te je stoga G.711 standard podržan od strane većine VoIP pružatelja.

G711.1 kodek odobren od strane ITU-T u ožujku 2008. godine. Izrađen je na temelju kodeka G.711 s ciljem lagane interoperabilnosti sa starom G.711 infrastrukturom [10].

G.711.1 sadrži dva dodatna sloja. Prvi sloj poboljšava kvalitetu G.711 na niskim frekvencijama uključujući raspon 50-300 Hz, koji se obično ne prenose s G.711. Drugi sloj kodira visoke vrekvencije do 7 kHz koristeći različite proširene slojeve.

G.711.1 zahtjeva brzine prijenosa od 80 do 96 kbps ovisno o korištenju jednog ili dva produžena sloja. Na slici se nalazi prikaz osnovnih brzina i dodatnih karakteristika G.711.1 slojeva.



Slika 2.9. *Slojevi G.711.1 kodeka [10]*

2.7.1. Usporedba G.711, G.723 i G.729 kodeka

G.723 kodek je ITU standard koji koristi ADPCM metodu i pruža dobru kvalitetu zvuka pri brzini od 24 do 40 kbps. Koristi se većinom za DCME (engl. *Digital Circuit Multiplication equipment*) aplikacije. G.723.1 kodek je kodek koji kompresira zvuk u okvirima od 30ms [11].

G.729 kodek prenosi zvuk vrlo efikasno na brzini od 32 kbps za razliku od 87 kbps (G.711), ali je u prijenosu ljudski glas sintetiziran vokoderom (koder govornog signala) [12]. Vokoder koristi generator tona, generator zvuka, te filter koji oblikuje zvuk kao što kod ljudi to rade grlo, usta, jezik, usne i nosnice. Kao rezultat, vokoder proizvod razumljiv govor, ali zvuk zvuči kao govor robota. Kako je to neprihvatljivo u današnjoj komunikaciji, G.729 koristi uzorke stvarnog govora kako bi podesio postavke vokodera, uspoređujući stvarni zvuk sa sintetiziranim zvukom. Rezultat svega je slična kvaliteta zvuka kao i kod standarda G.711, ali koristeći skoro trećinu brzine. Kako je za procesuiranje potrebno mnogo ciklusa, neki VoIP uređaji limitiraju broj *stream*-ova. Nedostatak G.729 kodeka je u faks podatkovnom prijenosu i prijenosu tonova jer je G.729 napravljen za prijevod zvuka, a ne podataka.

U tablici 2.3. se nalazi usporedba bitnih karakteristika G.711, G.723 i G.729 kodeka [11].

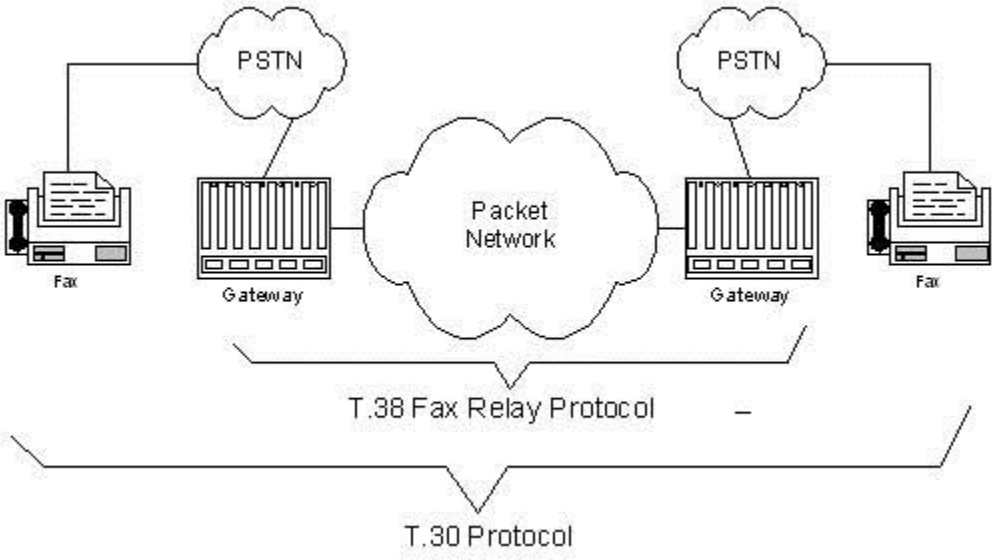
Tablica 2.3. *Usporedba G.711, G.723 i G.729 kodeka*

	G.711	**G.723**	**G.729**
Frekvencija (Hz)	300-3400	300-3400	300-3400
Brzina prijenosa (kbps)	64, 80 ili 96	24/40	8
Prednosti	Precizan prijenos zvuka Vrlo mali troškovi procesuiranja	Visoka kompresija - usporedno tome visoka kvaliteta zvuka Omogućuje simultano kodiranje i dekodiranje u *software-u* (na brzim računalima) Puno efikasniji u videokonferencijama/telefoniji nego POTS (engl. plain ordinary telephone service)	Malo kašnjenje za kompresiju zvučnih podataka (10 ms) Mala brzina (oko 8 kbps) - razlog korištenja u VoIP aplikacijama
Nedostaci	Slaba efikasnost mreže Koristi više od 64 kbps, što zahtijeva 128 kbps u svakom smjeru za komunikaciju	Zahtjeva veliku snagu procesora Nije prikladan za glazbene i zvučne efekte Manja kvaliteta od mnogo drugih kodeka s istom brzinom podataka	Potrebna licenca za korištenje Smanjenje kvalitete zvuka marginalno

Tablica 2.3. prikazuje kako svi kodeci rade u istom rasponu frekvencija, ali imaju različite brzine prijenosa podataka. Iako manje potrebne brzine prijenosa daju prednost kodecima G.723 i posebno G.729 u odnosu na G.711, potreba za jačom snagom procesora kod G.729 i potrebna licenca za G.729 protokol može biti nedostatak pri korištenju. Iz toga, ovisno o potrebi, svaki protokol može biti najkorisniji za određenu upotrebu.

2.8. T.38 standard

T.38 je ITU standard za slanje FAX-a kroz IP mreže u real-time modu (stvarnom vremenu). FAX poruke se šalju kao UDP ili TCP/IP paketi.



Slika 2.10. *Način rada T.38 protokola [13]*

Slika 2.10. prikazuje način rada T.38 portokola. Dva faksa komuniciraju koristeći T.30 faks protokol. Interkonekcija PSTN s IP paketima zahtjeva "*gateway*" između PSTN i IP mreža. PSTN-IP *gateway*-i podržavaju TDM glas na PSTN strani te VoIP i FoIP na paket strani.

Za glasovne sesije, *gateway* će uzeti glasovne pakete na IP strani akumulirati nekoliko paketa da osigura tok TDM podataka te ih prenijeti dalje duž TDM-a do mjesta gdje će biti pohranjene.

Faks podaci se prenose modemima, kojima gubitak paketa uzrokuje kreiranje krivih jedne ili više linija slike ili u najgorem slučaju prekid faks sesije. Stoga se koristi T.38 kako bi prevario terminal da misli da direktno komunicira s drugim T.30 terminalom. Također će T.38 ispraviti mrežna kašnjenja s tzv. tehnikama lažiranja pošiljatelja (engl. *spoofing techniques*), te izgubljenih paketa i paketa koji kasne s *buffer*-menadžment tehnikama.

Spoofing tehnike se odnose na logičku implementaciju u T.38 koja modificira naredbe protokola i odgovore na TDM strane kako bi zadržale mrežna kašnjenja na IP u svrhu toga

da ne dođe do prekida transakcije. To se postiže ispunjavanjem linija slike ili namjernim ponovnim slanjem poruka kako bi se ostvarilo mrežno kašnjenje između faks terminala.

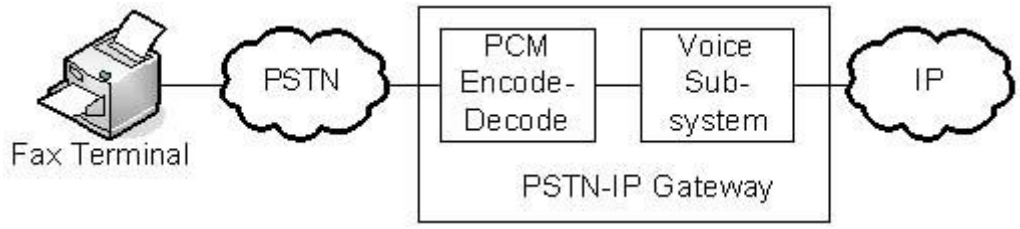
Mreže koje nemaju gubitak paketa ili preveliko kašnjenje mogu ostvariti prihvatljive faks performanse bez T.38 protokola ako su PCM satovi u svim *gateway*-ima visoke preciznosti. T.38 uklanja efekt da PCM satovi nisu sinkronizirani, te uz to i smanjuje potrebnu mrežnu propusnost 10 puta, te ispravlja gubitak paketa i kašnjenje.

2.8.1. Propusnost

T.38 *gateway* se sastoji od dva osnovna elementa: faks modema i T.38 podsustava. Faks modemi moduliraju i demoduliraju PCM uzorke analognih podataka, pretvarajući analogni signal u binarnu translaciju i obrnuto. PSTN mreža uzorkuje analogni signal glasovnog ili modemskog signala 8000 puta u sekundi, te ga kodira kao 8-*bit data byte*-ove, što znači 64000 *bit/s* prijenos podataka u jednom smjeru. Stoga za obostranu komunikaciju modemska transakcija troši 128000 *bita* mrežne propusnosti.

Tipični modem u faks terminalu prebacuje podatke brzinom 14400 *bit/s*. Ako se analogni podaci prvo prebacuju u digitalni oblik, potrebno je samo 14400 *bita* plus nekoliko *byte*-ova za mrežu. Kako je T.30 *half-duplex* protokol, mreža je potrebna za samo jedan smjer u tom trenutku.

2.8.2. Sinkronizacija PCM sata



Slika 2.11. *Sinkronizacija PCM sata [13]*

Slika 2.11. prikazuje sustav u kojem postoji jedan PCM sat u faks teminalu i jedan u gateway modemu koji se koristi za aktiviranje uzorkovanja analogne linije 8000 puta u sekundi. Ovi satovi su obično prilično precizni, ali u nekim jeftinim terminal adapterima znaju biti prilično neprecizni. Ako terminal šalje podatke u *gateway*, a sat u *gateway*-u je prespor, *bufferi* će se u *gatewayu* preopteretiti i prekinuti transakciju. Kako je razlika

obično mala, ovi problemi se javljaju u dugim, detaljiziranim faks porukama što daje više vremena satovima za uzrokovanje preopterećenja *buffera* u *gatewayu.* što je isto kao i gubitak ili dupliciranje paketa.

2.8.3. Gubitak paketa

T.38 pruža pogodnosti eliminacije efekta gubitka paketa redundancijom podataka. Kada je paket poslan, jedan, dva ili više prethodno poslanih podataka se ponavljaju. To povećava potrebnu propusnost mreže (i dalje puno manje nego bez korištenja T.38), ali omogućuje primajućem *gateway*-u rekonstrukciju reda kompletnog paketa čak i ako postoji velik gubitak paketa.

3. *QoS* (engl. *Quality of service* - kvaliteta usluge)

QoS se u telekomunikacijskim mrežama definira kao niz specifičnih zahtjeva koje mreža mora ispuniti korisniku, a koji su potrebni kako bi se postigla potrebna funkcionalnost aplikacije (usluge). Korisnici određuju potrebne zahtjeve u obliku *QoS* parametara. Kvaliteta usluge može biti ključna na poslovnom tržištu. *QoS* parametri su nužni za indikaciju kvalitete usluge ili proizvoda, te su važan čimbenik u određivanju usluge između različitih pružatelja usluga. Ako su cijene usluga slične, kvaliteta postaje ključni čimbenik za korisnike [14].

Čimbenici koji uzrokuju degradaciju *QoS* su sljedeći:

- zagušenje - uzrokovano prekomjernim prometom (engl. *bottleneck* - usko grlo)
- kašnjenje - uzrokovano lošim svojstvima mrežne opreme pri velikim opterećenjima, te udaljenošću i retransmisijom izgubljenih paketa
- djeljeni komunikacijski kanali - karakteriziraju ih kolizije i velika kašnjenja
- mreže s ograničenom propusnošću s lošim upravljanjem kapacitetom

3.1. *QoS* parametri

Kako bi se pružila i održala *QoS*, upravljanje resursima mora voditi računa o sljedećim parametrima:

- dostupnost resursa

- kontrola resursa

- *QoS* zahtjevi aplikacija

QoS parametre je potrebno nadzirati i relocirati resurse u skladu s anomalijama u sustavu. Aplikacijski sloj osigurava potrebne *QoS* parametre prije rezervacije resursa. Ako su zahtjevi postignuti, sesija započinje. Ukoliko dođe do promjene stanja (degradacije *QoS*-a), te upravljanje resursima ne može kompenzirati nedostatke, aplikacija se može prilagoditi novoj razini *QoS* ili degradirati na smanjeni nivo usluge. Mjerenje *QoS* se temelji na sljedećim parametrima: kašnjenje, kolebanje kašnjenja, gubitak paketa, propusnost...

Kašnjenje - neizostavni parametar u komunikacijama budući da su krajnje točke udaljene i informacijama treba vremena da dođu do krajnje točke. Kašnjenje može narasti ako su paketi u dugačkom redu u mreži (zagušenje) ili prolaze kroz manje direktnu rutu zbog izbjegavanja zagušenja. Kašnjenje se može mjeriti jednosmjerno (ukupno vrijeme od izvora do krajnje točke) ili kružno (vrijeme od izvora do krajnje točke plus vrijeme od krajnje točke natrag do izvora). Kružno kašnjenje se češće koristi budući da se može mjeriti iz jedne točke koristeći naredbu "*Ping*". Također, kružno kašnjenje je relativno točan način izračuna kašnjenja jer isključuje vrijeme koje odredišni sustav provodi procesuirajući paket. Naredba "*Ping*" ne provodi procesuiranje paketa. Ona samo šalje signal nazad kada zaprimi paket. Ako je potrebno preciznije mjerenje kašnjenja, potrebno je mjerenje u obje točke u mreži. Konačan rezultat je minimalno vrijeme kašnjenja potrebno u toj vezi za slanje paketa iz izvora u odredište.

Kolebanje kašnjenja (engl. *jitter*) - varijacija kašnjenja, te se prikazuje kao varijabilna transimisija kašnjenja paketa kroz mrežu. Pojava kolebanja se događa zbog internih redova u *routerima* (zagušenje prometa), promjene ruta... Ovaj parametar ozbiljno utječe na kvalitetu audio i video streaminga. Kako bi se kontroliralo kolebanje, potrebno je prikupiti pakete i držati ih dovoljno dugo dok najsporiji paket ne stigne na vrijeme, te ih poslagati u potrebnom redu za reprodukciju. Video i *audio streaming webstranice* poput *Youtube*-a koriste ublaživače (engl. *buffer*) za smanjenje kolebanja. Pri pokretanju videa ili audio snimke, započinje "*buffering*" prije *streaminga*. Iako to uzrokuje dodatno kašnjenje, potrebno je u slučaju aplikacija osjetljivih na kolebanje.

Gubitak paketa - događa se kada jedan ili više paketa podataka koji se prenose preko interneta ili mreže ne dostignu odredište. Bežićne i IP mreže ne mogu garantirati da će paketi biti uopće dostavljeni, te neće uspjeti dostaviti neke pakete ako paketi stignu kada su *bufferi* puni. Gubitak paketa može biti uzrokovan i drugim faktorima poput degradacije signala, visokog opterećenja mreže, odbacivanjem oštećenih podataka. Bežićne mreže imaju veću vjerojatnost gubitka podataka zbog interferencija s drugim mrežama, preprekama poput zgrada i okoliša. Transportni protokoli poput TCP-a (engl. *Transfer Control Protocol*) mogu kontrolirati dostavu paketa dobivajući potvrde o primitku od strane primatelja paketa. Ako se paket izgubi tijekom prijenosa, TCP automatski ponovno šalje segmente koji nisu potvrđeni na štetu smanjenja ukupne propusnosti veze.

Propusnost - količina podataka koju mreža šalje ili prima, ili količina podataka procesuirana u određenom vremenu. Mjerna jedinica je bit po sekundi (*bit/s* ili *bps*). Propusnost može biti manja od ulazne količine zbog gubitaka i kašnjenja u sustava. Mjerenje propusnosti prikazuje brzinu kojom korisnik može skinuti neku informaciju s pojedinih servera, ali se ne mora odnositi na skidanje određenog sadržaja. Postoji mnogo faktora koji utječu na brzinu skidanja: opterećenje servera kojemu korisnik pristupa, udaljenost servera od mjerenog sustava (u smislu mrežnih routera), brzina računala, broj programa pokrenutih na računalu, konfiguracija mreže.

U tablici se nalaze neki zahtjevi *QoS*-a za najčešće korištene aplikacije na internetu.

Tablica 3.1. *Zahtjevi QoS-a za najčešće korištene aplikacije na internetu*

APLIKACIJA	**QoS ZAHTJEVI**		
	Kašnjenje	**Jitter**	**Gubitak paketa**
VoIP	Malo	mali	srednje
Videokonferencija	Malo	mali	srednje
Audio/video streaming	Srednje	srednje	srednje
Poslovni podaci	Srednje	varijabilno	malo
e-mail	Veliko	veliko	malo
Prijenos podataka	Veliko	veliko	malo

SLA (engl. *Service Level Agreement* - Ugovor o kvaliteti usluge) - ugovor između korisnika i mrežnog operatera. SLA definira točno značenje parametara, što se događa u slučaju nepoštivanja odredbi ugovora. Neki operateri izdaju SLA za sve vrste korisničkog odnosa (rijedak slučaj), a većinom se to čini samo za velike korisnike koji znaju što odredbe ugovora zaista znače.

Postoje tri vrste SLA:

- Korisnički SLA - opisuje usluge koje dobiva korisnika. To je ugovor između korisnika i operatera napisan u uvjetima koje korisnik može razumjeti
- SLA pružatelja usluge - opisuje kako će se različiti zahtjevi ispuniti za resurse i usluge koje pruža treća strana. Obično nastaje iz ugovora između pružatelja usluge i operatera

- Interni SLA - fokusira se na resurse i ima ulogu upravljanja setom usluga i komponentama usluge koji su definirani jednim od dva prethodno navedena SLA. To je ugovor između organizacijskih funkcija između operaterskih poslova.

3.2. QoS u 2G i 3G mrežama

QoS u mobilnim mrežama se definirao kao sposobnost pružanja zadovoljavajuće usluge koja obuhvaća kvalitetu zvuka, jačinu signala, malu vjerojatnost blokiranja i prekida poziva, visoke podatkovne brzine za multimedijske i podatkovne aplikacije...

QoS parametri u mobilnim mrežama su sljedeći:

- propusnost
- kašnjenje
- postotak izgubljenih paketa
- postotak paketa s greškom
- pouzdanost

U 1G i 2G mrežama poput GSM i CDMA postoji samo jedan parametar QoS-a, a to je zvuk. Za razliku od navedenih mreža, u 3G mrežama potrebno je ostvariti QoS za zvuk, te za podatke. Kako su glasovne usluge još uvijek primarne usluge, prednost se daje QoS zvuka.

Najveća razlika između 2G i 3G mreže je u brzini prijenosa podataka. Brzina prijenosa podataka u 2G mreži je manja od 50000 bit/s dok za 3G mrežu ta brzina može biti i preko 4 miliona bit/s.

3G tehnologija pruža visok nivo sigurnosti u usporedbi s 2G tehnologije jer 3G mreže dopuštaju provjeru validacije tijekom komunikacije s drugim uređajima.

Ostvarivanje poziva je jednako lako na 2G i 3G mrežama, te ne postoji primjetna razlika osim što 3G mreža omogućuje i uspostavu video poziva. Prijenos tekstualnih poruka i slika moguć je na obje mreže, ali 2G mreže imaju podatkovni limit i malu brzinu prijenosa podataka. [15]

3.3. *QoS VoIP*-a

Kvaliteta usluge VoIP-a mjeri se pomoću tri mehanizma [16]:

- IntServ
- DiffServ
- RSVP

IntServ (engl. *Integrated Services*) je protokol za pružanje *QoS* na internetu. Razvio ga je IETF. IntServ je razvijen za pružanje jednoznačnog, *end-to-end QoS* za niz paketa koji imaju isti izvor i odredište. IntServ radi dopuštajući domaćinu da zatraži po protoku *end-to-end* resurse duž puta podataka. Tada mreža pruža *feedback* domaćinu može li asistirati u tome zahtjevu. Primarni fokus u razvoju IntServa čine tri kontrolne funkcije:

- Klasifiikacija paketa
- Raspoređivanje
- Kontrola pristupa

Kontrolni mehanizmi definiraju mnoge esencijalne principe na kojima se temelji IP bazirana *QoS*.

IntServ dopušta fleksibilnost u smislu klasifikacije paketa, ali nakon klasifikacije paketi imaju jednak tretman. Taj proces se obrađuje planerom paketa koji administrira prosljeđivanje paketa korištenjem redova, timera i drugih mehanizama.

Kontrola ulaza je odluka o dostupnosti resursa. Nužna je za stvaranje sigurnosti da će novi putevi održavati *QoS* bez utjecaja na postojeće puteve u mreži. Kako bi se ispunili uvjeti, potreban je zahtjev za prikladne resurse jer ako resursi nisu dostupni, zahtjev se može odbiti. Unutar IntServ, aplikacije utiliziraju signalni protokol za komunikaciju s mrežom o svojim *QoS* zahtjevima. Signalni protokol je odgovoran i za instalaciju i uspostavljanje *QoS* kontrole u mreže. To pruža sposobnosti koje mreža treba kako bi iskomunicirala upravljačke informacije s aplikacijom. Postoji više višestrukih signalnih protokola koje je razvio IETF, a najpoznatiji je RSVP (engl. *Resource Reservation Protocol*). IntServ developeri razvili su kontrolne i signale mehanizme za QoS, te QoS usluge: kontrolirano opterećenje i garantirane usluge (jedine dvije usluge koje je definirao IETF). IETF-ove odredbe određuju mehanizme koje mreža mora podržavati kako bi pružala *QoS*. Usluga

kontroliranog opterećenja je usluga namjenjena velikoj količini paketa koje treba dostaviti s minimalnim kašnjenjem (zvuk i slika koji nisu u stvarnom vremenu). Ova usluga je razvijena za pružanje najbolje usluge u neopterećenim i slabo opterećenim mrežama. Garantirana usluga kontrolira maksimalni red kašnjenja kako bi osigurala da paketi stižu u predodređenom vremenu (video i interaktivni glas, daljinska kontrola, financijske transakcije, aplikacije osjetljive na kašnjenje.)

RSVP je signalni protokol za identifikaciju komunikacija između pošiljatelja i primatelja. Radi s mrežnim osnovama za QoS tokove. RVSP poruke se koriste za međusobnu komunikaciju između korisnika. RSVP protokol se može koristiti zajedno s IntServ-om. Ako se koriste u kombinaciji, svaka RSVP poruka identificira resurse koje su zahtjevane od mreže koristeći IntServ ograničenja. RSVP se može koristi i u kombinaciji s MLPS-om, te u tom slučaju služi za prenošenje oznaka veza i točnih informacija o prosljeđivanju. RSVP je *receiver-based* protokol. *Receiver-based* protokoli su usluge koje zahtjeva primatelj, odgovaranje na poruke dobivene od pošiljatelja. Kako bi se započela RSVP sesija, pošiljatelj šalje PATH poruku kako bi locirao put kroz mrežu za podatke. U skladu s *QoS*, primatelj šalje RESV (engl. *reservation-request* - rezervacija-zahtjev) poruku s podacima o mogućoj podršci za pojedinu klasu sustava. Rezervacijske poruka putuju mrežom obrnutim putem dok ih ne dobije pošiljatelj. RSVP pokušava napraviti rezervaciju resursa u svakoj mrežnoj komponenti u kojoj će proći tok aplikacije. U skladu s QoS zahtjevima, RSVP-*enabled routeri* i ostale mrežne komponente moraju uspostaviti "stanje" za individualne RSVP tokove. RSVP stvara privremeno, "meko" stanje na svim RSVP uređajima između pošiljateljskih i primateljskih čvorova. RSVP šalje i isprekidane poruke za osvježenje stanja. Stanje se briše ako nema *refresh* poruka u određenom vremenskom periodu.

Prednosti korištenja "mekog" stanja su mogućnost RSVP-a prilagodbi promjenama u mreži, te to što RSVP može prilagoditi put provjerom i osvježenjem stanja između primatelja i pošiljatelja kao odgovor na promjene prosljeđivanja.

Nedostaci RSVP-a su visoki troškovi, ograničeno proširenje, izračun rezervacija po putu, resursi memorije u svakom routeru, veliki obujam poruka za razmjenu.

DiffServ je QoS mehanizam koji omogućuje mrežnom prometu razbijanje u male tokove za prikladno obilježavanje. Tokovi se obilježavaju kako bi ih uređaju na putu u mreži mogli identificirati i pružiti odgovarajući tretman.

Funkcije DiffServ-a se dijele u dva dijela: rubne funkcije i funkcije u mrežnoj jezgri. Rubne funkcije su kompleksnije funkcije koje nadziru domaćini ili routeri. Manje kompleksne funkcije nadziru uređaju u unutarnjoj mreži. DiffServ poziva upravitelje mrežom da odrede propusnost ili kašnjenje potrebne za klasu ili klase mreža. Upravitelji mrežom moraju konfigurirati rutere kak obi se prilagodi zahtjevu.

DiffServ sadrži i polje za pomoć pri obilježavanju paketa, DS polje. Informacije koje su prikupljene u DS polju se nalaze u obliku DSCP-ova (engl. *DiffServ Code Point*). DSCP definira tretman paketa tijekom prijenosa u mreži. Rubni uređaji (domaćini i routeri na rubu mreže) imaju ulogu obrade klasficikacije i DSCP-a. Rubni uređaji su odgovori za prikljupljanje pojedinih tokova i njihovo kombiniranje u makrotokove, te oblikovanje i odbacivanje prometa kako bi odgovarao profilu.

Nakon što se promet uskladi, krajnja točka će ga propisno obilježiti i otkriti DiffServ dijelu mreže. Paketi se obilježavaju pravilnim raspoređivanjem paketa koje provode *routeri* na svakom "skoku" duž puta. Ta se funkcija naziva *PHB* (engl. *Per Hop Behavior* -ponašanje po skoku)

PHB prepoznaje kako paket treba teritrati na svakog skoku. Trenutno postoje tri standardizirana PHB-a:

- zadani PHB - prosljeđivanje s najboljim učinkom
- ubrzano prosljeđivanje - garantira da svaki DiffServ čvor stvara malo kašnjenje, *jitter* i gubitak. Također omogućuje i ulazak određenog prometa u mrežu.
- osigurano prosljeđivanje - pruža manje mogućnosti u odnosu na ubrzano prosljeđivanje, te nadzire resurse na temelju četiri klase prometa

4. PRAKTIČNI DIO

U praktičnom dijelu rada obrađeni su zvukovni zapisi u različitim uvjetima, kako bi se prikazao utjecaj određenih parametara na QoS.

Praktični dio diplomskog rada sastoji se od dviju simulacija prijenosa određenog tipa signala kroz mrežu baziranu na SIP protokolu. Simulacije su izvedene pomoću programskog paketa GNS3 (*Graphics Network Simulator*) koji omogućava emulaciju različitih kompleksnih mreža. Ovaj je programski paket odabran zbog mogućnosti simulacije stvarnih elemenata mreže u virtulanom okruženju.

U obje simulacije korišteni su signali s kodekom G.711, koji je najrasprostranjeniji i najupotrebljivaniji kodek u govornim uslugama. Usporedbu signala s različitim kodecima nismo obradili iz tehničkih razloga, a nismo bili niti u mogućnosti napraviti analizu signala s drugim kodecima u programskom paketu *Wireshark,* koji smo koristili.

4.1. DTMF signal u sustavu mreža različitih operatera telekomunikacijskih usluga

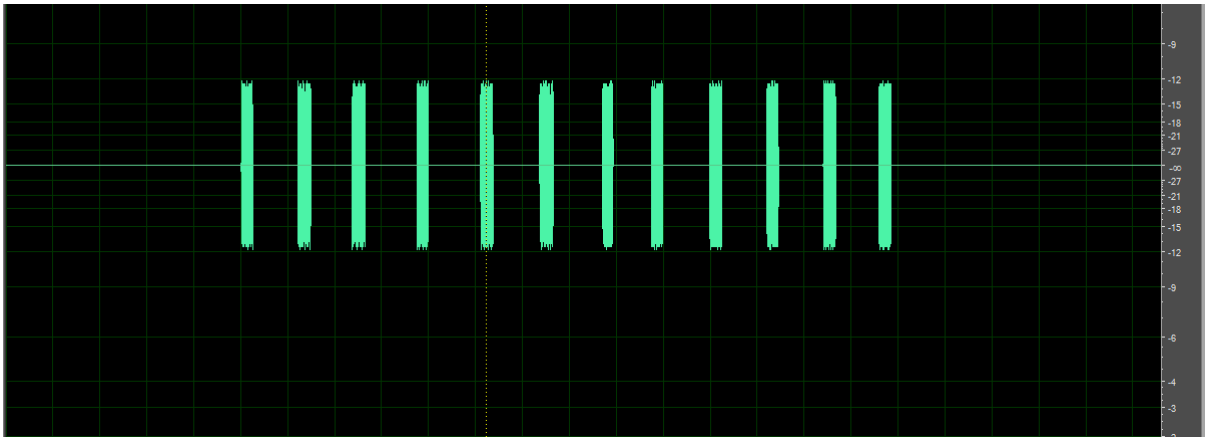
Svrha prve simulacije je utvrditi što se događa s DTMF signalom kada prolazi kroz sustav mreža različitih operatera s podešenim različitim parametrima, one su u daljnjem tekstu označene redom M1, M2, M3.

Dobiveni rezultati registrirali su se na definiranom mirror portu za SIP i RTP protokole. Veza je uspostavljena po G.711 kodeku i koristi se DTMF *in-band* metoda za slanje znamenki. Sva tri poziva su završila na istoj terminalnoj opremi i snimani su pod istim uvjetima.

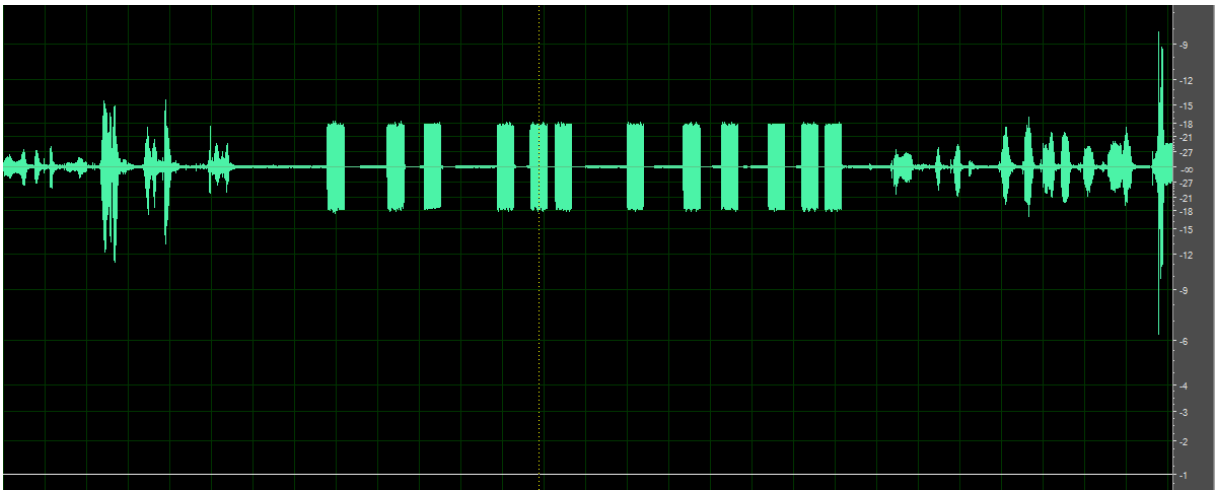
Osim dobivenih rezultata prikazanih na vremenskim grafovima korišten je i programski paket *Wireshark.*

Analizom mjerenja određene DTMF znamenke dobiveni su sljedeći grafovi prikazani u vremenskoj domeni na slikama 4.1., 4.2. i 4.3.

Slika 4.1. Signal prikazan u vremenskoj domeni na izlazu iz mreže operatera M1



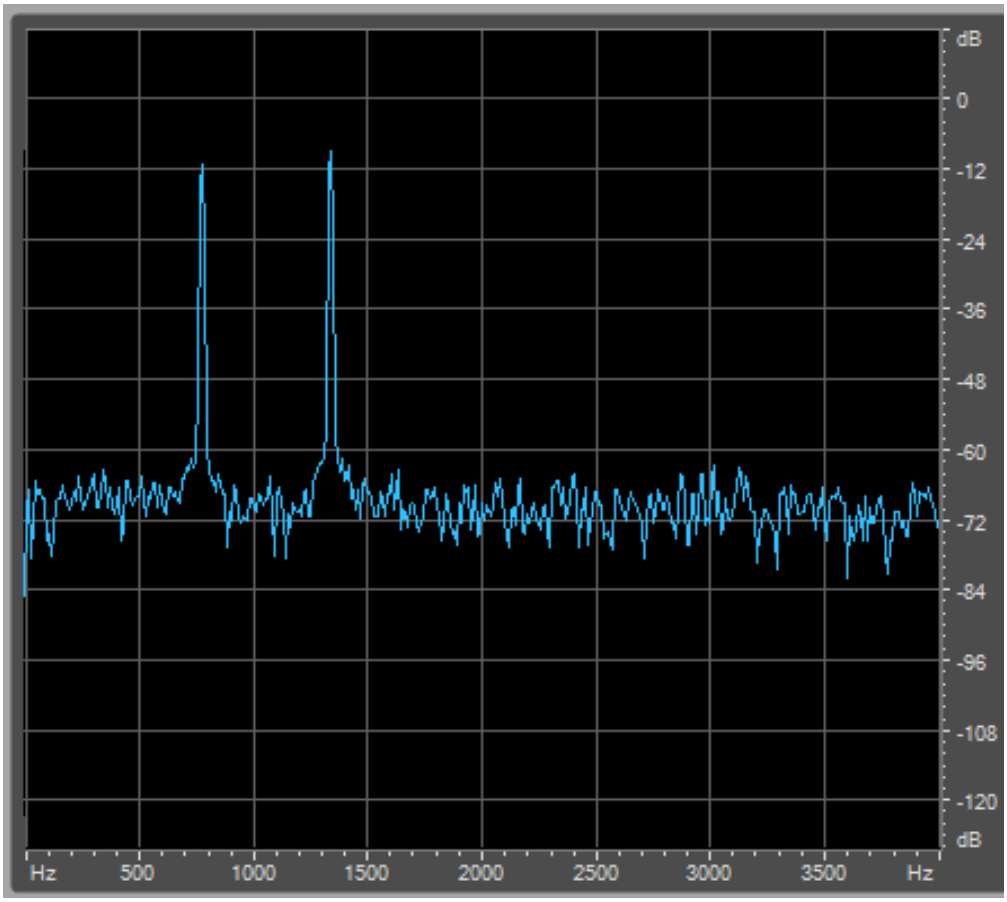
Slika 4.2. Signal prikazan u vremenskoj domeni na izlazu iz mreže operatera M2



Slika 4.3. Signal prikazan u vremenskoj domeni na izlazu iz mreže operatera M3

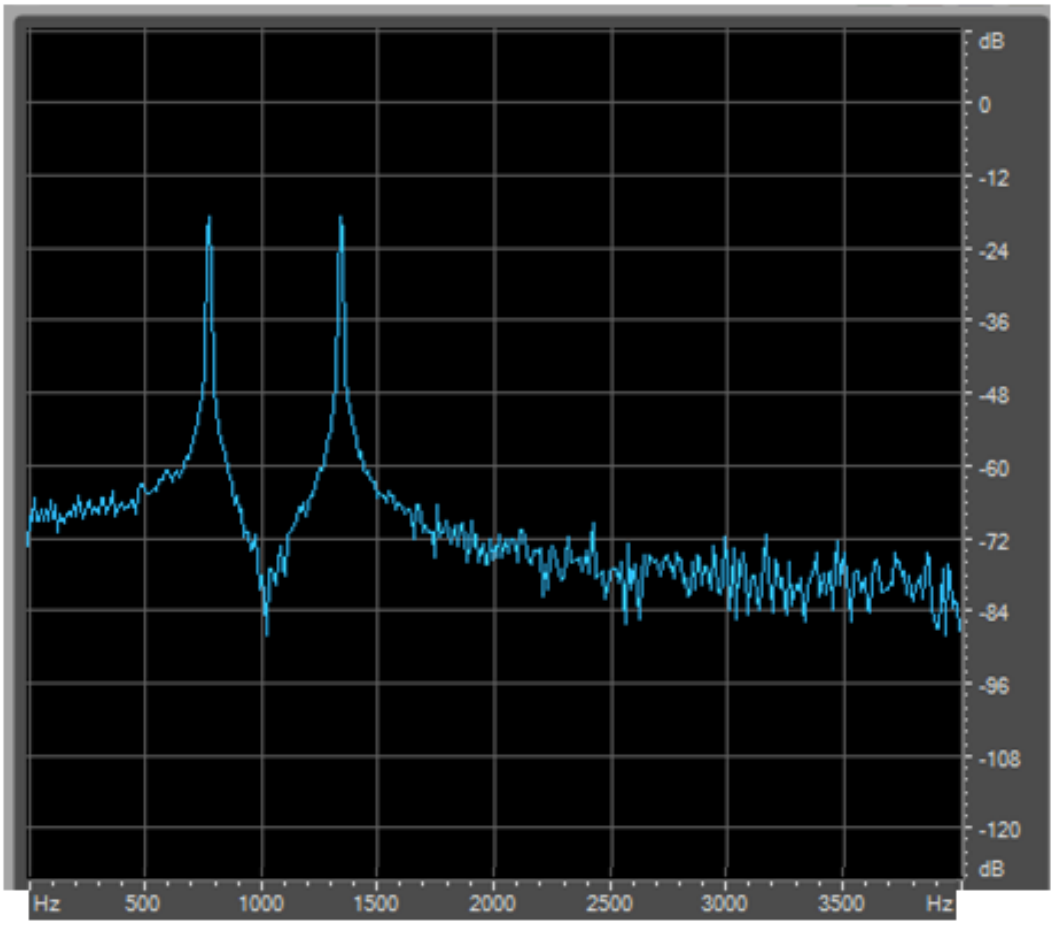
Na svakom od navedenih grafova može se vidjeti 12 DTMF znamenki koje su prošle kroz simulator.

Prebacivanjem grafova iz vremenske u frekvencijsku domenu i promatranjem točno određene DTMF znamenke 5 dobiveni su sljedeći grafovi.

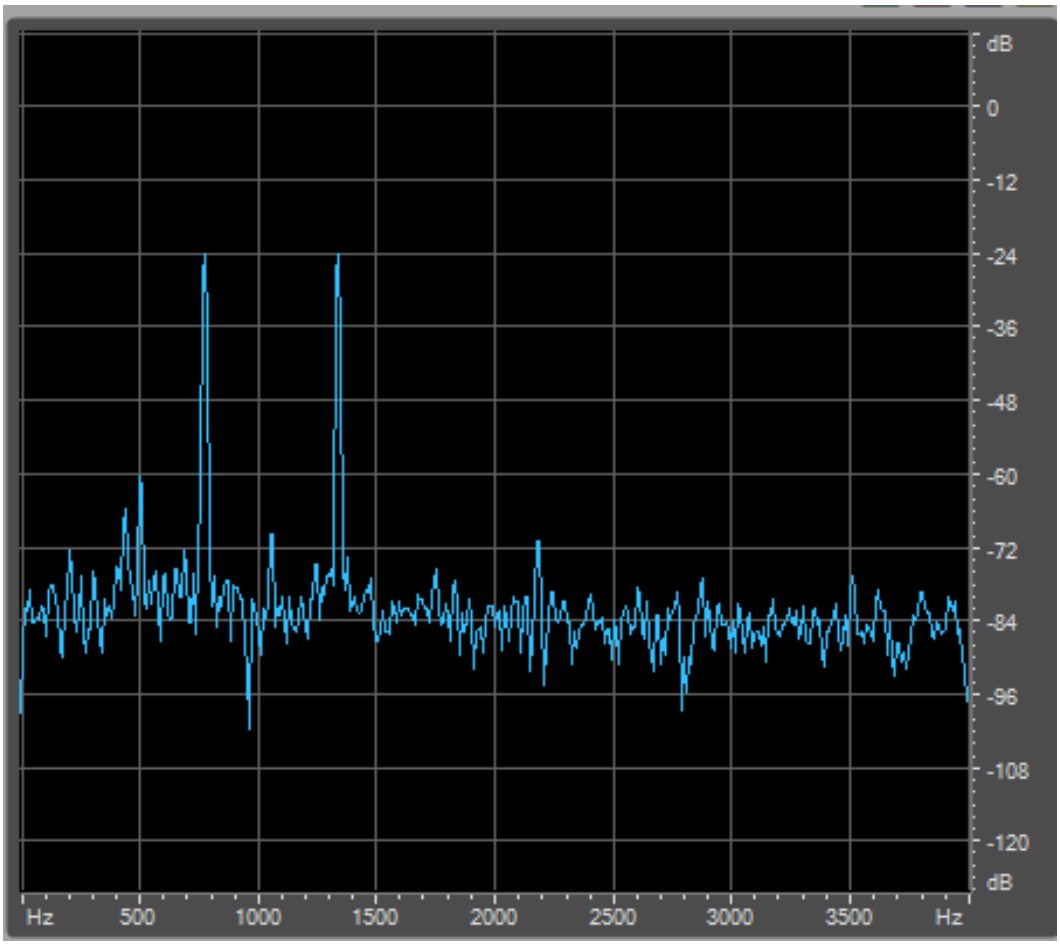


Slika 4.4. Signal prikazan u frekvencijskoj domeni na izlazu iz mreže operatera M1

Na slici 4.4. je prikazan spektar frekvencija DTMF znamenke 5. Iz grafa se može očitati kako se ukupni signal znamenke 5 sastoji od frekvencija dvaju superponiranih signala frekvencija 1336 Hz i 770Hz (Slika 2.8.). Na slikama 4.5. i 4.6. su također prikazane spektralne komponente DTMF znamenke 5 kada je prošla kroz mrežu operatera M2, odnosno M3.



Slika 4.5. Signal prikazan u frekvencijskoj domeni na izlazu iz mreže operatera M2



Slika 4.6. Signal prikazan u frekvencijskoj domeni na izlazu iz mreže operatera M3

Tablica 4.1. Očitane vrijednosti snage signala i šuma sa slika 4.4., 4.5, 4.6.

	Oznaka mreže		
	Operater M1	Operater M2	Operater M3
Snaga signala [dB]	-10	-18	-24
Snaga šuma [dB]	-62	-61	-60
SNR [dB]	52	43	36

Vrijednost SNR u tablici 4.1. dobivena je pomoću sljedeće formule:

$$\text{SNR} = \text{Snaga signala} - \text{Snaga šuma [dB]} \tag{4-1}$$

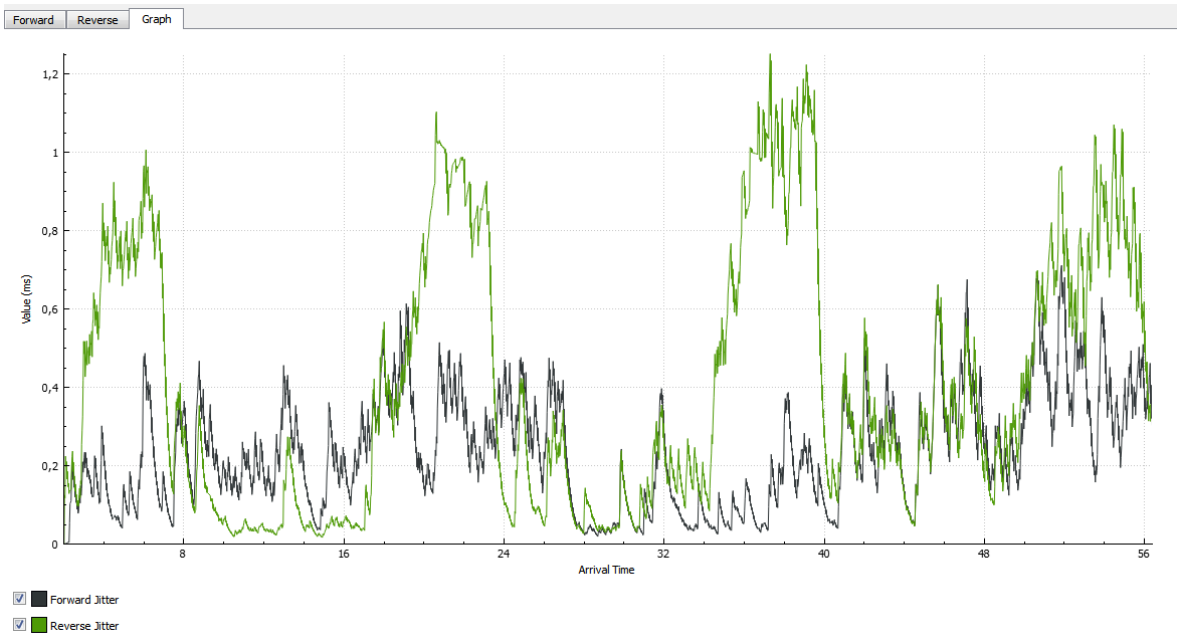
Na grafovima u frekvencijskoj domeni se može vidjeti kako u trećem testiranju dolazi do smanjenja omjera signal-šum što može dovesti do nemogućnosti razlučivanja frekvencije izlaznog signala.

Za ista tri signala pomoću programa *Wireshark* izvršena su preslušavanja dobivenih signala nakon kojeg se moglo zaključiti da u trećem testiranju dolazi do distorzije signala odnosno pojave šuma koji se može detektirati ljudskim sluhom.

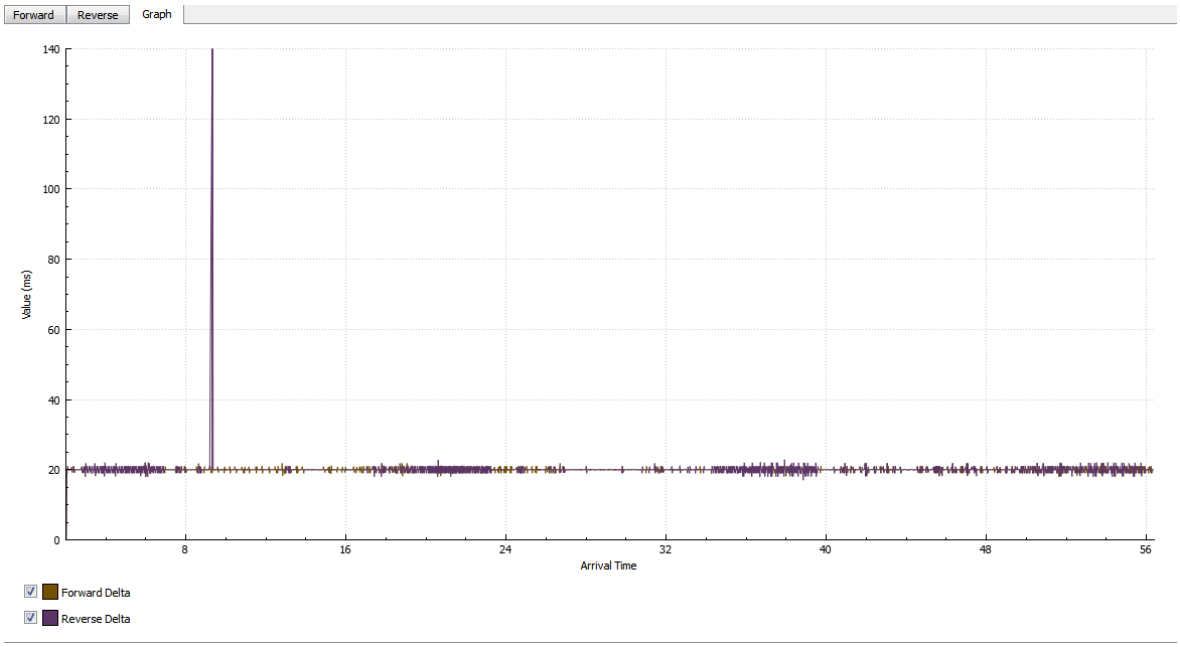
4.2. Govorni signal u pozivu unutar fiksne, te između fiksne i mobilne mreže

Svrha druge simulacije je utvrditi što se događa sa signalom kada je upućen poziv iz fiksne u fiksnu mrežu te kada je poziv upućen iz fiksne u mobilnu mrežu.

Analizom oba govorna signala u programskom paketu *Wiresharku* dobiveni su sljedeći grafovi i statistički podaci poslanih i primljenih paketa.



Slika 4.7. Grafički prikaz kolebanja koje opisuje kvalitetu signala unutar fiksne mreže

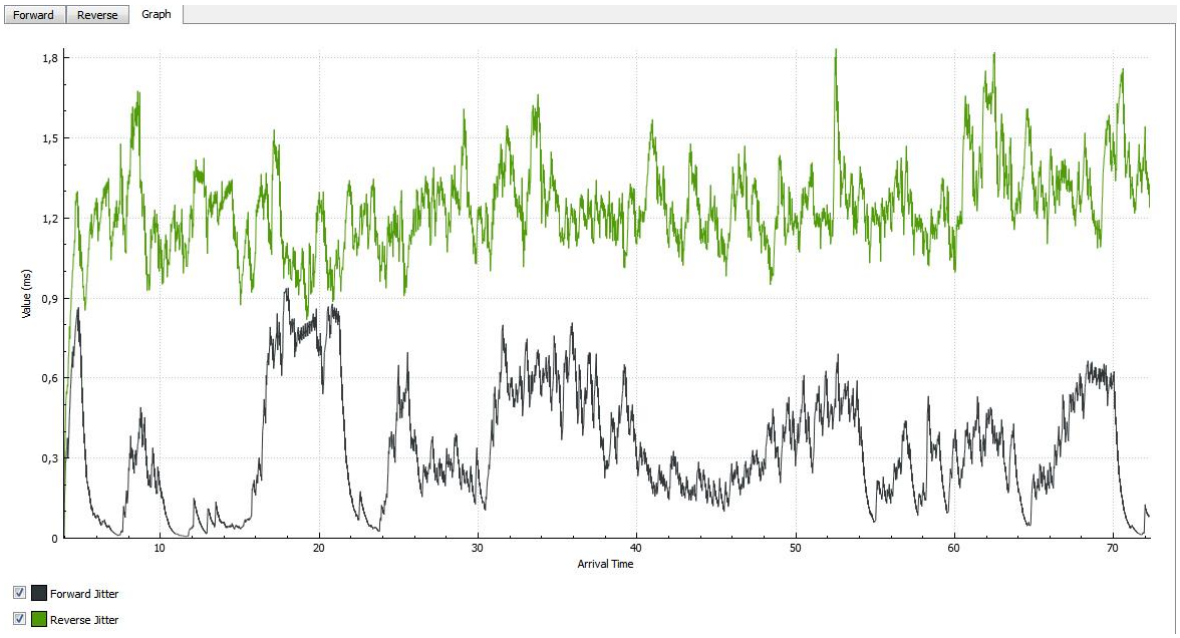


Slika 4.8. Grafički prikaz kašnjenja koje opisuje kvalitetu signala unutar fiksne mreže

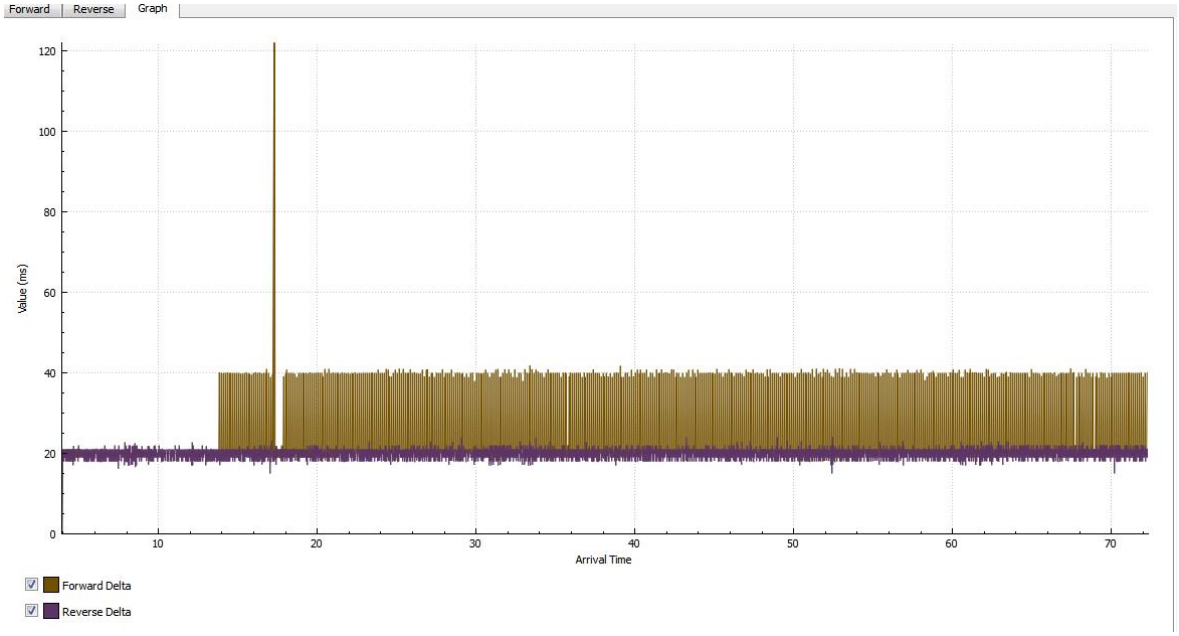
Forward		Reverse	
SSRC	0x83fd9c4a	**SSRC**	0x83fd9c4a
Max Delta	22.00 ms @ 527	**Max Delta**	140.01 ms @ 921
Max Jitter	0.71 ms	**Max Jitter**	1.25 ms
Mean Jitter	0.24 ms	**Mean Jitter**	0.41 ms
Max Skew	-1.85 ms	**Max Skew**	2.19 ms
RTP Packets	2721	**RTP Packets**	2709
Expected	2721	**Expected**	2709
Lost	0 (0.00 %)	**Lost**	0 (0.00 %)
Seq Errs	0	**Seq Errs**	0
Duration	54.40 s	**Duration**	54.28 s
Clock Drift	-5 ms	**Clock Drift**	-5 ms
Freq Drift	7999 Hz (-0.01 %)	**Freq Drift**	7999 Hz (-0.01 %)

Slika 4.9. Statistički parametri koji opisuju kvalitetu signala unutar fiksne mreže

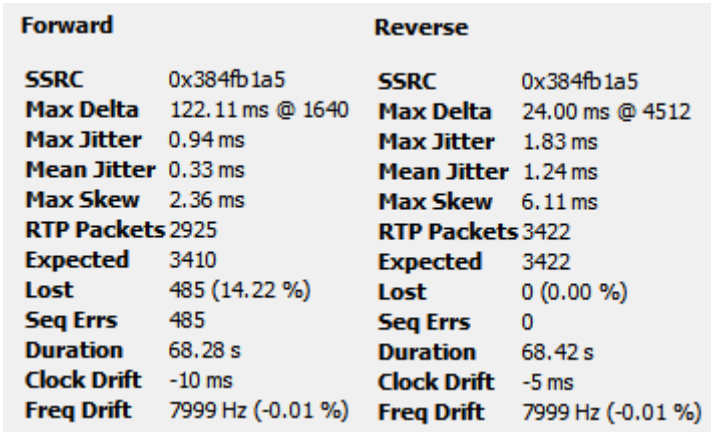
Slike 4.7., 4.8. i 4.9. nam prikazuju kako u pozivu koji je bio upućen unutar fiksne mreže nije došlo do gubitaka paketa te da su svi parametri koji opisuju kvalitetu usluge zadovoljavajući. Preslušavanjem snimke govora i ljudskim sluhom moguće je potvrditi da su rezultati dobiveni grafičkom i statističkom analizom zadovoljavajući.



Slika 4.10. Grafički prikaz kolebanja koje opisuje kvalitetu signala između fiksne i mobilne mreže



Slika 4.11. Grafički prikaz kašnjenja koje opisuje kvalitetu signala između fiksne i mobilne mreže



Forward		Reverse	
SSRC	0x384fb1a5	**SSRC**	0x384fb1a5
Max Delta	122.11 ms @ 1640	**Max Delta**	24.00 ms @ 4512
Max Jitter	0.94 ms	**Max Jitter**	1.83 ms
Mean Jitter	0.33 ms	**Mean Jitter**	1.24 ms
Max Skew	2.36 ms	**Max Skew**	6.11 ms
RTP Packets	2925	**RTP Packets**	3422
Expected	3410	**Expected**	3422
Lost	485 (14.22 %)	**Lost**	0 (0.00 %)
Seq Errs	485	**Seq Errs**	0
Duration	68.28 s	**Duration**	68.42 s
Clock Drift	-10 ms	**Clock Drift**	-5 ms
Freq Drift	7999 Hz (-0.01 %)	**Freq Drift**	7999 Hz (-0.01 %)

Slika 4.12. Statistički parametri koji opisuju kvalitetu signala između fiksne i mobilne mreže

Slike 4.10.,4.11. i 4.12. koje govore o kvaliteti signala između fiksne i mobilne mreže prikazuju kako je za razliku od slika 4.7., 4.8., 4.9. koje govore o kvaliteti signala unutar fiksne mreže, došlo do jačeg narušavanja kvalitete signala. Iz statističke analize se vidi kako pri prijenosu signala iz mobilne u fiksnu mrežu dolazi do gubitaka paketa. Osim gubitaka paketa koji su vrlo izraženi (14,22%) narušeni su i ostali parametri koji opisuju kvalitetu signala kao što su kašnjenje i kolebanje. Preslušavanjem snimke govora i ljudskim sluhom moguće je utvrditi kako je kvaliteta usluge loša te kako su statistički i grafički podaci točni.

5. ZAKLJUČAK

Razvoj tehnologije u posljednjih dvadeset godina doveo je do mnogo promjena i inovacija u svijetu komunikacije. Računala, tableti i pametni telefoni postali su sastavni dio naše svakodnevice, a želja korisnika za novim, jeftinijim sadržajima i inovacijama natjerala je davatelje usluge na brži napredak i proširenje svojih usluga.

Velike promjene dogodile su se i u području govorne usluge. Iako je klasična telefonija vrlo pouzdana i široke dostupnosti, cijena te vrste komunikacije je skupa, pogotovo s udaljenim osobama. Pojava IMS-a je omogućila razvoj novih multimedijskih komunikacijskih usluga kombinirajući telekomunijacijske i podatkovne usluge. Omogućeno je znatno jeftinije telefoniranje i komunikacija u bilo koje krajeve svijeta.

Uz cijenu, u govornim uslugama je vrlo bitna i kvaliteta usluge QoS. QoS je ključni čimbenik korisniku bez obzira na cijenu usluge, te je stoga bitna što kvalitetnija usluga. Čimbenici koji mogu utjecati na kvalitetu usluge su zagušenja uzrokovana prekomjernim prometom, kašnjenja u mreži što usporava i otežava komunikaciju, dijeljeni komunikacijski resursi, mreže operatera s ograničenom propusnošću i lošim upravljanjem kapacitetom. Zato pružatelji usluga moraju voditi računa o parametrima QoS-a koji su i sami analizirani na različitim signalima u radu: kašnjenju, *jitteru* (kolebanju kašnjenja), gubitku paketa, propusnosti mreže. Ovisno o načinu komunikacije, QoS zahtjevi se mijenjaju pa su tako stroži za VoIP komunikaciju u odnosu na audio/video i podatkovni prijenos. Bitni čimbenik je i sigurnost samog sustava. Svakim danom poboljšava se sigurnost IMS sustava što dovodi i do povećanja korištenja i širenja usluga baziranih na IMS-u.

Kako su se kroz povijest s vremenom razvijale nove tehnologije, nije isključeno da će i u budućnosti s razvojem tehnologije doći do novih usluga, koje će zasigurno biti potrebno popratiti s još nestandardiziranim kvalitetama usluge koje će se s vremenom razviti.

6. SAŽETAK

IMS (engl. *IP multimedia subsystem*) - IP multimedijski podsustav - je standardizirana mrežna arhitektura nove generacije koja je zamišljena za operatere telekomunikacijskih usluga da pruže složene usluge u mobilnim i fiksnim mrežama. IMS je arhitekturalni okvir orijentiran na pružanje trenutnih i budućih internet usluga fiksnim i mobilnim korisnicima preko višepristupne IP platforme. IMS je definiran skupinom standarda koji je napravio 3GPP (engl. *The 3rd Generation Partnership Project*) i 3GPP2. IMS omogućuje operaterima telekomunikacijskih usluga stvaranje infrastrukture usluga otvorenog tipa bazirane na IP-u što omogućuje brzi razvoj novih multimedijskih komunikacijskih usluga kombinirajući telekomunikacijske i podatkovne usluge.

QoS se u telekomunikacijskim mrežama definira kao niz specifičnih zahtjeva koje mreža mora ispuniti korisniku, a koji su potrebni kako bi se postigla potrebna funkcionalnost aplikacije (usluge). Korisnici određuju potrebne zahtjeve u obliku *QoS* parametara. Kvaliteta usluge može biti ključna na poslovnom tržištu. *QoS* parametri su nužni za indikaciju kvalitete usluge ili proizvoda, te su važan čimbenik u određivanju usluge između različitih pružatelja usluga. Ako su cijene usluga slične, kvaliteta postaje ključni čimbenik za korisnike.

Čimbenici koji uzrokuju degradaciju *QoS* su sljedeći: zagušenje (engl. *bottleneck* - usko grlo), kašnjenje, djeljeni komunikacijski kanali i mreže s ograničenom propusnošću s lošim upravljanjem kapacitetom

Kako bi se pružila i održala *QoS*, upravljanje resursima mora voditi računa o sljedećim parametrima: dostupnost resursa, kontrola resursa, *QoS* zahtjevi aplikacija

Ključne riječi: IMS - IP multimedijski podsustav, 3GPP, sigurnost IMS-a, VoIP, DTMF - dvotonski prijenos podataka, DTMF znamenke, G.711, G.711.1, G.723, G.729, T.38 standard, ITU, PCM sat, QoS - kvaliteta usluge, QoS parametri

ABSTRACT

IMS - IP multimedia subsystem - is a standardized network architecture of a new generation which is designed for operators of telecommunications services to provide complex services to mobile and fixed networks. IMS is an architectural framework focused on providing current and future Internet services fixed and mobile users through multi-access IP platform. IMS is defined by a group of standards created by 3GPP (The 3rd Generation Partnership Project) and 3GPP2. IMS enables operators of telecommunications services creation of service infrastructure based on open IP, enabling a fast development of new multimedia communications services combining telecommunications and data services.

QoS in telecommunications networks is defined as a set of specific requirements that the network has to fulfil, and which are required to achieve the required functionality of the application (service). Users define the necessary requirements in the form of QoS parameters. The quality of service can be a key to the business market. QoS parameters are necessary to indicate the quality of services or products, and are an important factor in determining the services between different providers. If the prices of similar quality becomes a key factor for the users.

The factors that cause degradation of QoS are: congestion, delay, shared communication channels and networks with limited bandwidth with poor management capacity

To provide and maintain QoS, resource management must take into account the following parameters: resource availability, resource control and QoS application requirements.

Keywords:

IMS - IP multimedia subsystem, 3GPP, IMS security, VoIP, DTMF - dual tone multi frequency, G.711, G.711.1, G.723, G.729, T.38 standard, ITU, PCM clock, QoS - Quality of Service, QoS parameters

7. LITERATURA

[1] S. A. Ahson, M. Ilyas, **Ip Multimedia Subsystem (IMS) Handbook,** CRC Press, 2009.

[2] http://www.radio-electronics.com/info/telecommunications_networks/ims-ip-multimedia-subsystem/tutorial-basics.php , pristup ostvaren 15.06.2016

[3] S. Znaty, J. Dauphin Efort, **IP Multimedia Subsystem: Principles and Architecture, http://www.efort.com/**

[4] **IMS architecture overview**, An overview of IMS architecture and related Accenture experience, Universita Federico II - Napoli, 27.04.2007

[5] C. Vaishnav, **Voice over Internet Protocol (VoIP): The Dynamics of Technology and Regulation**, Massachusetts Institute of Technology, 2006

[6] http://presentsoftware.blogspot.hr/2010/10/h323.html , pristup ostvaren 20.09.2016.

[7] N. Biondić, M. Vukušić-Vasiljevski, L. Medak, V. Bolt, V. Vrlika, **Protokol za pokretanje sesija**, Ericcson Nikola Tesla; Revija 18(2005)

[8] http://www.engineersgarage.com/tutorials/dtmf-dual-tone-multiple-frequency, pristup ostvaren 15.06.2016

[9] http://www.voip-info.org/wiki/view/ITU+G.711 , pristup ostvaren 20.09.2016.

[10] http://www.en.voipforo.com/codec/new-codecs-g7111-g7291.php , pristup ostvaren 20.09.2016.

[11] https://speechcodecs.wordpress.com/ , pristup ostvaren 20.09.2016.

[12] http://www.voip.com/blog/2008/05/g729-versus-g711.html , pristup ostvaren 20.09.2016.

[13] https://en.wikipedia.org/wiki/T.38 , pristup ostvaren 20.09.2016.

[14] F. Carvalho de Gouveia, T. Magedanz, **Telecommunication systems and technologies - Vol. II - Quality of Service in Telecommunication Networks**, Encyclopedia of Life Support Systems (EOLSS)

[15] http://www.engineersgarage.com/contribution/difference-between-2g-and-3g-technology , pristup ostvaren 20.09.2016

[16] K. Gonia, **Latency and QoS for Voice over IP**, SANS Institute InfoSec Reading Room , Copyright SANS Institute. 2004.

8. ŽIVOTOPIS

Barbara Opačak rođena je 23. kolovoza 1990. godine u Osijeku, gdje je pohađala osnovnu školu i opću gimnaziju. Nakon toga 2009. upisala je sveučilišni preddiplomski studij računarstva na Elektrotehničkom fakultetu u Osijeku. Na drugoj godini se prebacuje na sveučilišni preddiplomski studij elektrotehnike, smjer Komunikacije i informatika. Tijekom studija aktivno zagovara uključivanje mladih u društvo. Godine 2009. izabrana je u Studentski zbor Elektrotehničkog fakulteta gdje postaje potpredsjednica i članica Fakultetskog vijeća. Po završetku Sveučilišnog preddiplomskog studija, 2012. upisuje sveučilišni diplomski studij elektrotehnike, smjer Komunikacije i informatiku. Iste godine izabrana je u novi saziv Studentskog zbora i postaje predsjednica Studentskog zbora Elektrotehničkog fakulteta te Studentskog zbora Sveučilišta J.J.Strossmayera u Osijeku. Također, postaje članica Senata Sveučilišta J.J. Strossmayera te Hrvatskog studentskog zbora. Godine 2013. stažira u Bruxellesu u Uredu hrvatskog zastupnika u Europskom Parlamentu Davora Ive Stiera. Godine 2014. postaje potpredsjednica Studentskog zbora Sveučilišta J.J.Strossmayera u Osijeku, pravobraniteljica Hrvatskog studentskog zbora te je izabrana u novi saziv Savjeta mladih Grada Osijeka. Organizirala je razne manifestacije, međunarodna putovanja, radionice, predavanja i tribine koji su za cilj imali unaprijediti studentski standard i standard mladih u gradu Osijeku. Za svoje izvannastavne aktivnosti 2015. godine na svečanoj sjednici Fakultetskog vijeća dobiva Priznanje Elektrotehničkog fakulteta u Osijeku za doprinos ugledu Fakulteta i Sveučilišta.