**UNIVERZITET SINGIDUNUM**
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE I MEĐUNARODNU SARADNjU

**DOKTORSKE STUDIJE**
**STUDIJSKI PROGRAM: NAPREDNI SISTEMI ZAŠTITE**

**DOKTORSKA DISERTACIJA**

# EVALUACIJA NOVOG PRISTUPA U ZAŠTITI VOIP KOMUNIKACIJA

**Mentor:**
**Prof. dr Mladen Veinović**

**Kandidat:**
**Vladimir Stanojević,master**

***Beograd,2016. godina***

Komisija za pregled i odbranu:

Mentor: prof. dr Mladen Veinović
Članovi komisije:
prof. dr Milan Milisavljević
prof. dr Petar Spalević

Datum odbrane doktorske disertacije

_____

**UNIVERZITET SINGIDUNUM**
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE I MEĐUNARODNU SARADNjU

**DOKTORSKE STUDIJE**
**STUDIJSKI PROGRAM: NAPREDNI SISTEMI ZAŠTITE**

**DOKTORSKA DISERTACIJA**

# EVALUACIJA NOVOG PRISTUPA U ZAŠTITI VOIP KOMUNIKACIJA

**Mentor:**
**Prof. dr Mladen Veinović**

**Kandidat:**
**Vladimir Stanojević,master**
**Br. Indeksa:460138/2012**

***Beograd,2016. godina***

**UNIVERSITY OF SINGIDUNUM**
**BELGRADE**
**DEPARTMENT OF POSTGRADUATE STUDIES AND INTERNATIONAL COOPERATION**

# EVALUATION OF NEW APPROACH ON PROTECTED VoIP COMMUNICATION

-DOCTORAL DISSERTATION-

**Mentor:**
**Mladen Veinović, PhD**

**Candidate:**
**Vladimir Stanojević,master**

***Belgrade, 2016.***

# SAŽETAK

U današnje vreme značaj informacije je toliko porastao u svim aspektima života, da se informacija može tretirati kao materijalno dobro i može izraziti njen vrednosni kvantitet u novcu ili ekvivaletnom dobru. U skladu sa mogućnostima skladištenja/razmene informacija korišćenjem modernih informacionih tehnologija, raste jednako proporcionalno i potreba da se ograniči pristup tim informacijama.

Poseban aspekt zaštite informacija je zaštita prenosa informacije u realnom vremenu. Kao najčešći vid ovakve komunikacije u današnje vreme srećemo razgovore korišćenjem savremenih telekomunikacionih sredstava. Vrlo rasprostranjeno sredstvo za ostvarenje ovakve komunikacije je mobilni telefon. On omogućava direktni razgovor u realnom vremenu, što je veoma bitan aspekt današnjice.

Budući da se u razgovoru razmenjuju informacije, te informacije mogu biti "od interesa" nekoj trećoj strani ili više njih, na poslovnom, državničkom ili nekom trećem planu. Isto tako stranama u razgovoru je u interesu da te informacije ne budu dostupne bilo kojoj trećoj strani. Ako izuzmemo trivijalnosti tipa da neko u neposrednoj blizini jednog od učesnika u razgovoru sluša šta taj učesnik govori drugoj strani, postoje brojni tehnički metodi (kako legalni tako i nelegalni) da se ceo razgovor (obe strane u komunikaciji) sluša, snimi i naknadno reprodukuje u cilju dobavljanja informacija razmenjenih u tom razgovoru.

Znajući ovo, određeni učesnici u razgovoru (poslovni ljudi, političari, itd) ako žele da izbegnu "odliv" informacija tokom razgovora nekoj trećoj strani moraju ili da jednostavno ne komuniciraju da daljinu tj. ne razmenjuju osetljive informacije u telefonskim razgovorima, ili da koriste raznolika tehnička rešenja za zaštitu poverljivosti razgovora.

Ta rešenja su veoma raznovrsna re[enja, počev od hardverskih, softverskih i mešanih hardversko-softverskih rešenja.

U početku to su bila striktno hardverska rešenja, dok sa razvojom hardvera opšte namene nije postao široko dostupan takav hardver u prosečnim mobilnim telefonima da se samo softverskim rešenjima može postići isti ako ne i bolje (sa aspekta performansi i kvaliteta) efekat, i svakako fleksibilnije i samim tim dugotrajno efikasnije rešenje.

U ovom radu je prikazano jedno takvo softversko rešenje koje nudi unapređenje poznatih rešenja u nekoliko aspekata.

# ABSTRACT

The importance of information nowdays increased in every aspect of life, that surely information can be treated as material goods and it's value can be expressed in money or equivalent goods. Acccording to modern abilities of storage/exchange of information ny using modern information technologies, proportional is growth of need to restrain access to particular information.

Special aspect of information security is protection of transport of information in real-time. As most common means of such real-time communication we can consider live voice communication by using modern telecomunication devices. Most common device for such purpose is cellular phone. It enables direct voice conversation in real-time, which has become an important aspect of modern living.

Considering that during such conversations informations are exchanged, thoose informations can be "information of interest" for any third party or multiple third parties, on business-, goverment- or some other-level. At the same time, parties invloved in communication have an interest to keep information revealed in communication secret from any third party. Trivialitues like someone in close physical proximity of one of participant overhear what that participant is saying aside, there are numerous technical means (both legal and illegal) to intercept, listen, store and reproduce later on the whole communication, which have for a goal to obtain information revealed in that particular conversation.

Being aware of previously said, certain participants in conversations (businessmen, politicans,etc) striving to avoid "information leaks" during conversations to any third party must either not communicate remotely (not revealing sensitive/confidental informations during telephone conversations), or use various technical solutions to keep the conversation confidental.

Such solutions are very diverse beginning with pure hardware solutions, throughout software solutions all the way to hybrid hardvware-software soluitions.

In the beginning there were strictly hardware solutions available, until with rapid development of hardware in general population devices made possible that solely software solutions became if not more, at least same as effective and quality as hardware solutions, and therefore much more flexibile/accessible, and surely long-time usable solution.

This document presents one such solution, with several improvements comparing to known such solutions.

# SADRŽAJ

# SPISAK SLIKA

# SPISAK TABELA

# I UVOD

## I.1 Predmet istraživanja

Savremene tehnologije su u zadnjoj deceniji unele revolucionarne promene u svim društvenim poljima, pa i na planu komunikacija. Nikada nije bilo lakše i dostupnije stupiti u kontakt sa nekim i razmeniti informacije. Prvo mobilna telefonija, pa smart telefoni koji omogućavaju da svako u džepu bukvalno nosi kompletan multimedijalni centar, kojim može da pristupa globalnoj mreži, informacijama i sadržajima kao i da ih generiše i postavlja na globalnu mrežu ili da ta razmena bude usko ograničena između tačno dve osobe.

Upravo ovaj drugi slučaj, gde komunikacija, odnosno sadržaj komunikacije nije javnog karaktera, već takvog da jedna ili obe strane u komunikaciji imaju interes (potrebu) da ta komunikacija bude poverljivog karaktera, tj. da njen sadržaj ne bude dostupan trećoj strani, ima posebne bezbednosne implikacije koje se moraju uzeti u obzir u eri savremene tehnike.

Naime, ta komunikacija koja se obavlja na daljinu, izložena je (celim svojim putem) direktnom presretanju jedne ili više zainteresovanih strana.

Ova okolnost je značajan i nimalo zanemarljiv rizik za npr. poslovne ljude, državnike i sl. Uopšteno gledano, privatnost komunikacije je socijalna kategorija koja se tiče i svakog pojedinca, kao i njegovo pravo.

Podrazumevano, sve mobilne komunikacije su ili potpuno otvorene (sadržaj komunikacije putuje od polazišta do odredišta kroz telekomunikacionu infrastrukturu u izvornom obliku), ili se iz gore navedenih razloga isti štiti nekim šifrovanjem.

Odabir pravog pristupa šifrovanja komunikacije je kompleksan problem, i zavisi od velikog broja faktora. Šifrovanje glasovne komunikacije u realnom vremenu ima opet svoje specifičnosti koje se moraju uzeti u obzir. Ključni aspekti ovakvog sistema zaštite koji se moraju uzeti u obzir su:

- Metode generisanja, odabira i distribuiranja ključeva šifre ili algoritma šifrovanja.
- Izbegavanje svake vrste (funkcionalnog) posrednika u prenosu zaštićenog sadržaja, jer bi samo postojanje istog bilo značajan bezbednosni rizik, tj. preferirana tačka napada.
- Odabir šifrarskog algoritma koji rezultira optimalnim balansom između nivoa sigurnosti štićenog sadržaja i performansi.

Postoje brojna istraživanja na tu temu zaštite sadržaja u VoIP sistemima, koja nude veći ili manji nivo zaštite privatnosti razgovora. Neka od tih rešenja uključuju i posebne

hardverske komponente. Međutim ta rešenja se mahom baziraju na nekom centralnom čvoru koji ima funkciju relejnog prenosnika štićenih sadržaja (sa ili bez njihovog dešifrovanja/rešifrovanja), što predstavlja idealnu polaznu tačku za napad treće strane.

Drugi problem je generisanje kvalitetnih šifarskih ključeva, i njihova bezbedna distribucija odnosno razmena.

U ovom radu je predložen jedno kompleksno i kompletno rešenje za sistem zaštićene glasovne komunikacije u realnom vremenu, korišćenjem opšteprisutnih sadržaja za šifarske ključeve, i korišćenje nekih orignalnih metoda i tehničkih rešenja da se izvrši sinhronizovanje šifarskih ključeva, njihova validacija, i ostvari kvalitetna glasovna komunikacija sa (de)šifrovanjem u realnom vremenu.

## I.2. Cilj istraživanja

U ovom radu razmatra se nov pristup u VoIP komunikaciji koji će objediniti P2P (Peer to peer) komunikaciju između dva mobilna uređaja, dakle bez posrednika čime se uklanja idealna tačka za presretanje komunikacije.

U okviru predloženog pristupa biće razmatrane i analizirane efikasnost i performanse različitih kriptozaštita, sa aspekta generisanja/razmene ključeva, kao i sam algoritam kriptozaštite u cilju određivanja one kombinacije gorenavedenih faktora koji pružaju najbolji odnos sigurnost/performanse.

Konkretno pristup se odnosi na dvosmernu glasovnu komunikaciju u realnom vremenu, i pritom je čisto softverski, dakle hardverski nezavistan.

Cilj je da se postigne zadovoljavajući stepen sigurnosti (privatnosti) sadržaja koji se transportuje, bez subjektivno uočljivog pada kvaliteta prenesenog sadržaja bilo u kvalitativnom ili kvantitativnom smislu.

Takođe u radu se predlaže korišćenje određenih opštedostupnih sadržaja na internetu kao izvor za šifarske ključeve. Ovaj predlog je utemeljen na objektivnom ispitivanju kvaliteta predloženih sadržaja za tu namenu, koje je kao i dobijeni rezultati deo ovoga rada.

Modeliranje predloženog rešenja i simulacija sa promenljivim parametrima omogućiće analizu efikasnosti i stepena sigurnosti. Posebna pažnja biće posvećena analizi stepena sigurnosti kriptoloških osnova koje se koriste za konstrukciju rešenja sa aspekta najnovijih rezultata kriptoanalitičkih istraživanja. Ovi rezultati biće prikupljeni iz radova objavljenih na poslednjim međunarodnim godišnjim kriptološkim konferencijama.

Analiza stepena sigurnosti je važan aspekt istraživanja jer ilustruje stepen proširenja koje pruža predloženo rešenje u odnosu na stepen sigurnosti postojećih rešenja.

Dodatni faktor je analiza potencijalnih „slabih tačaka“ predloženog pristupa, u kome se „izbacuje“ posrednički čvor koji bi bio polazna tačka za sve presretačke tipove napada.

U radu će biti poseban akcenat na tom aspektu, tj. razmatranju drugih „pogodnih“ tačaka napada ako takve postoje.

Postojeća literatura tretira problem zaštite privatnosti u komunikaciji uglavnom bazirano samo na inovaciji kriptografske zaštite, ali zbog prirode uspostavljanja veze kroz internet, i NAT (Network Address Translation) koji je aktivan na svim uređajima koji nemaju javnu IP adresu, te je direktno uspostavljanje veze prema takvom uređaju tehnički nemoguće, posrednik sa kojim oba uređaja uspostavljaju vezu je nezaobilazan faktor.

## I.3. Naučne hipoteze

Hipoteze koje čine osnovu ovog rada su:

1. Zaštita privatnosti (poverljivosti) razgovora je sve traženija, jer savremeni trendovi i sazrevanje svesti korisnika uslovljavaju da i njima proporcionalno raste obzir prema tome.
2. Upotreba samo kriptografskih rešenja za zaštitu sadržaja razgovora je ograničeno efikasna jer je složenost tj. sigurnost primenjenog rešenja direktno obrnuto proporcionalna performansama prenosa razgovora u realnom vremenu.
3. Eliminiše se potreba za generisanjem šifarskih ključeva, i umesto toga predlaže korišćenje određenih dostupnih sadržaja sa interneta, čiji izvor je praktično neiscrpan, a kvalitet potvrđen objektivnim testiranjem.
4. Uvođenjem nove neodređenosti, tj. ukidanjem fiksne poznate tačke koja je „centralna“ skretnica svih razgovora smanjuje se mogućnost i verovatnoća napada na tako zaštićenu komunikaciju.

Posebne hipoteze:

1. Osim striktno kriptografskog pristupa, isključenje posrednika kroz koga bi se prosleđivali zaštićeni sadržaji između krajnjih tačaka, povećava bezbednost.

2. Na internetu postoji neiscrpan izvor materijala za šifarske ključeve koji se mogu upotrebiti, a čiji kvalitet u tom smislu se može proveriti.

3. Izborom pogodnijih tehnika kriptozaštite, može se postići optimalan balans između nivoa zaštite i performansi prenosa glasa u realnom vremenu, uz simultano šifrovanje odlaznog toka i deštifrovanje dolaznog toka.

## I.5. Metode istraživanja

Složenost predmeta istraživanja zahteva primenu:

- od analitičkih osnovnih metoda: metod analize, metod apstrakcije, metod specijalizacije i metod dedukcije;
- od sintetičkih osnovnih metoda: sintezu, konkretizaciju, generalizaciju i indukciju;
- od opšte naučnih metoda: hipotetičko-deduktivnu, analitičko-deduktivnu, komparativnu, statističku i metodu modelovanja.

Primenom ovih metoda, kako pokazuju dosadašnji rezultati istraživanja, moguće je validno ostvarenje ciljeva istraživanja. Pristup istraživanju je integrativan, sintetički u tom smislu što se ni jednom metodološkom postupku ne daje isključiva prednost.

U prikupljanju podataka primeniće se: ispitivanje i metoda analize sadržaja dokumenata.

Analiza će biti ostvarena na dva nivoa :

- na nivou eksperimentalne analize realnih subjekata
- na nivou sekundarne analize rezultata ranijih istraživanja i adekvatne literature.

## I.6. Očekivani naučni i stručni doprinosi

- pregled svetskih iskustava primene VoIP protokola u sistemima mobilne telefonije,
- pregled tehnologija koje se koriste za projektovanje i implementaciju sistema za zaštitu privatnosti korisnika,
- primer korišćenja standardne metodologije i alata za softversko inženjerstvo radi proširivanja funkcionalnosti kriptozaštićene glasovne komunikacije u realnom vremenu korišćenjem standardnih smart phone uređaja.
- predlog neiscrpnog izvora jednokratnih šifarskih ključeva, i potvrda njihovog kvaliteta korišćenjem specijalizovanih softverskih alata, te analiza i prezentovanje dobijenih rezultata u pogodnom obliku za dalju obradu.
- razvoj sopstvenog sistema za dvosmernu kriptozaštitu glasa u realnom vremenu a da pritom komunikacija teče direktno između učesnika komunikacije bez posrednika.
- Merenje i analiza performansi i određivanje optimalnog balansa između kriptozaštite i performansi.

Predlog smernica za dalji razvoj.

Rezultati rada na ovoj doktorskoj disertaciji biće objavljeni u više radova u časopisima međunarodnog značaja i saopšteni na više naučnih skupova u zemlji i inostranstvu. Pojedine ideje su već izložene na međunarodnim stručnim skupovima.

# II KOMUNIKACIONI SLOJ

## II.1. Digitalizacija i reprodukcija zvuka

Zvuk je sa aspekta fizike opseg vibracija koji ljudsko uho može da registruje. Opšteprihvaćeno je da je to frekventni opseg od 20Hz do 20kHz. Svako uho je individualno, i ne mogu svi ljudi da čuju pun spektar zvučnih vibracija u ovom opsegu.

Glas je onaj zvuk koga proizvodi čovek pri izgovoru. Izuzevši „školovane glasove“ npr. operskih pevača, glumaca i sl, u normalnoj konverzaciji frekventni opseg ljudskog glasa po empirijskim istraživanjima [1] je između 78Hz i 1108Hz.

Ovaj podatak je bitan za ispravan odabir parametara digitalizacije zvuka, konkretno frekvencije uzorkovanja (eng. sampling rate), koja treba da bude dovoljno velika da može da obuhvati svaki sadržaj predmetne digitalizacije, a opet je poželjno (sa aspekta kvantiteta transporta podataka) da ta rezolucija bude što manja, što rezultira minimalnom količinom podataka za prenos, i omogućava tečan prenos i kroz komunikacione kanale malih kapaciteta.

Kod pretvaranja kontinualnog signala (kao što je na primer glas) u diskretne signale (kao što je niz digitalnih impulsa) koristi se Teorema uzorkovanja, bazirana na Nikvistovoj teoremi koja glasi:

Da bi se očuvala struktura kontinualnog signala, potrebno je da frekvencija uzorkovanja bude dvostruko veća od maksimalne frekvencije uzorkovanog signala:

$$f_s \geq 2 \times f_{max}$$

Uzevši da je: $f_{max} \cong 2kHz$, sledi: $f_s \cong 4kHz$

Budući da je $f = \frac{1}{t}$ , sledi da je minimalni interval uzorkovanja glasa 0,00025s, tj. 250μS.

Ovu „brzinu“ uzorkovanja je lako postići sa današnjim dostupnim hardverom na prosečnim mobilnim (smart) telefonima, tako da nema potrebe za posebnim hardverskim delovima sistema za digitalizaciju glasa.

Ovako „uzorkovan“ kontinualni signal rezultira uzorcima „određene vrednosti“ (u ovom slučaju amplitude/jačine zvuka). I opseg tih vrednosti je potrebno ograničiti (kvantifikovati) u određenom opsegu. Određivanje optimalnog opsega amplitude kvantifikovanog signala je jednako bitno za kvalitet krajnjeg rezultata digitalizacije.

U A/D konverziji to se radi „svođenjem“ aktuelne vrednosti u opseg samog A/D konvertera. Tu pritom nije bitna apsolutna veličina maksimalne vrednosti, već „finoća“ tj. minimalna razlika između 2 susedne analogne veličine koje se mogu diferencirati. Ona se izražava u bit-ima, i najčešći su 8-bitni/16-bitni A/D konverteri kada se radi o konverterima

ugrađenim u kompjuterski hardver, dok se u industrijskoj elektronici sreću i neki „egzotičniji“ primerci tipa 10-bitni,12-bitni itd. U literaturi se ova osobina često naziva i „rezolucija A/D konvertera“.

Broj bitova direktno utiče na „finoću“ A/D konvertera, koja se može izraziti sledećom formulom:

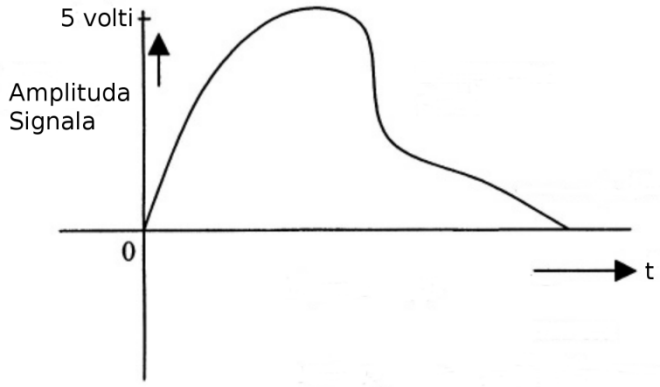
$$V_{max} = 2^r - 1$$

Gde je $V_{max}$ maksimalna kvantitativna vrednost koju A/D konverter može iskazati. Ova jako bitna osobina A/D konvertera može se ilustrovati primerom A/D konvertera koji ima 4-bitnu rezoluciju, i analogni naponski opseg 10V.

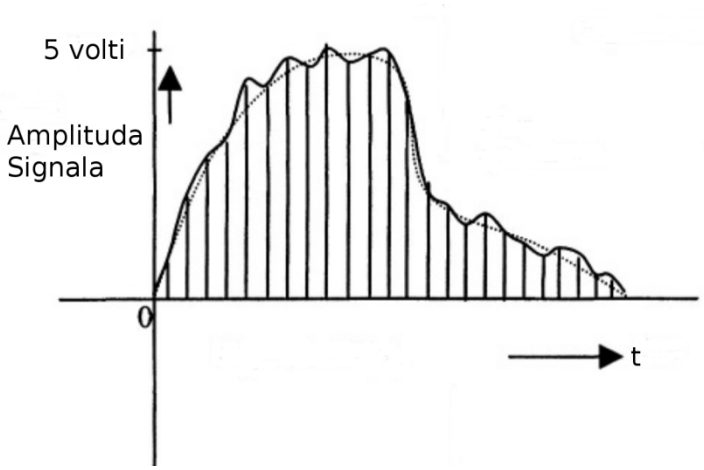
Primenivši prethodnu formulu dolazi se do vrednosti $2^4 = 16$ mogućih vrednosti (0 do $2^4 - 1$). Dakle minimalna diferencija između dva digitalna uzorka je 10V/16=0,625V.

Ili rečima, ovakav A/D konverter bi bio u mogućnosti da „detektuje“ tišinu i 15 različitih „jačina“ glasa (zvuka). U skladu sa mogućnostima aktuelnog hardvera mobilnih telefona, može se koristiti 16-bitna rezolucija A/D konverzije što dakle omogućava $2^{16}$ različitih „jačina“ glasa(zvuka), što daje veoma veliku osetljivost pri digitalizaciji i visok kvalitet pri reprodukciji tog zvuka.

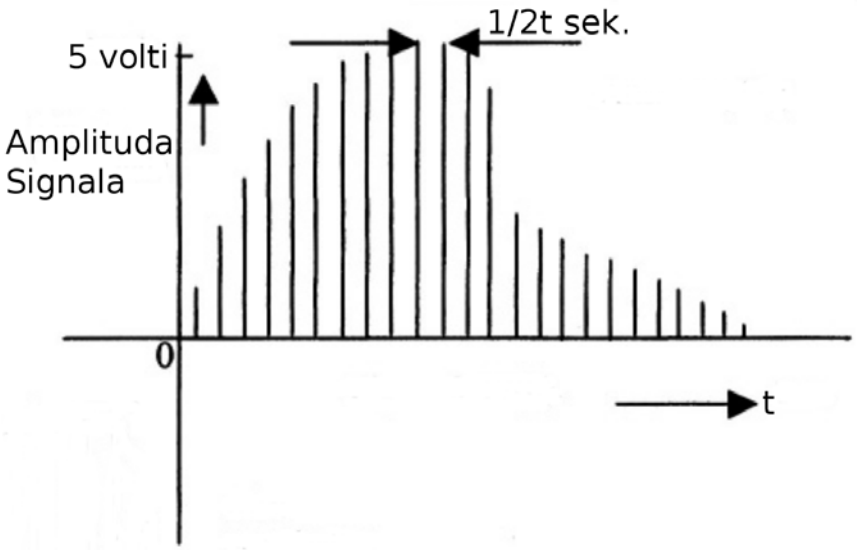
Na slikama 1-3 je prikazan proces digitalizacije u osnovnim fazama od analognog kontinualnog signala do kvantifikovanog diskretnog digitalnog signala.




slika 1. Grafik analognog signala




Slika 2. Digitalizacija analognog signala




Slika 3. Diskretno uzorkovanje digitalnog signala

Reprodukcija je obrnuti proces u kome se diskretne digitalne vrednosti signala u nizu po istovetnom redosledu u kome je zvuk digitalizovan pretvaraju ponovo u analogne vrednosti (naponske nivoe) koji se pojačavaju i reprodukuju na zvučniku uređaja.

Postoji više standarda za kvalitet zvuka. U tabeli 1. su prikazani standardni formati koji se koriste za digitalizaciju zvuka u zavisnosti od sadržaja/namene.

| Frekvencija Uzorkovanja $f_s$ [kHz] | Maksimalna frekvencija zvuka $f_{max}$ [kHz] | Primena |
|---|---|---|
| 8.000 | 3.6 | -Telefonija<br>-Diktafoni<br>Dugački razgovori se beleže u malim fajlovima |
| 11.025 | 5 | -Vrlo oskudno za muziku ali pogodno za kvalitetno skladištenje glasa |
| 22.050 | 10 | -Za skladištenje glasa gde je bitna jasnoća naročito tihih delova |
| 32.000 | 14.5 | -Za digitalizaciju muzike sa medija starije generacije kao npr. kasete |
| 44.100 | 20 | -Standardni format za muziku sa audio CD-a.<br>-Budući da beleži sve zvukove do 20kHz "pokriva" ceo čulni opseg ljudskog uha. |
| 48.000 | 21.8 | -Za digitalizaciju ultrazvučnog opsega, frekvencija uzorkovanja ide i do 96kHz u nekim primenama |

Tabela 1. Standardni formati digitalizacije zvuka

## II.2. Kapacitet transportnog kanala

Kada se zvuk digitalizuje/reprodukuje da bi se preneo nekim telekomunikacionim kanalom, kao što je to slučaj sa prenosom glasa u realnom vremenu, bitan faktor je kapacitet transportnog kanala tj. njegova propusna moć.

Kada se radi o prenosu analognog signala, propusna moć transportnog kanala (eng. bandwidth) mora biti jednaka ili veća od $f_{max}$ , jer je jedina veličina kontinualnog analognog signala njegova amplituda.

Međutim, propusna moć digitalnog transportnog kanala mora biti dovoljna da u realnom vremenu može da postigne prenos digitalizovanog zvuka. A taj digitalizovani zvuk kao kvantitativnu vrednost jednog diskretnog "uzorka" koji će biti reprodukovan po D/A konverziji sastoji se od niza od ***m*** bitova.

U skladu sa time može se izraziti minimalna potrebna propusna moć transportnog kanala digitalnog signala ( $f_{ch}$) sledećom formulom:

$$f_{ch} = 2 \times m \times f_{max}$$

Dakle, za prenos digitalnog signala potreban je m puta veći kapacitet transportnog kanala nego za istovetan analogni signal.

Za prenos zvuka u realnom vremenu kada se koristi savremena kablovska telekomunikaciona infrastruktura, bilo električna ili optička, ovo realno nije problem.

Međutim ako je transportna telekomunikaciona infrastruktura bežična, onda to nije nimalo zanemarljiv faktor i često sama propusna moć raspoloživog telekomunikacionog kanala za prenos zvuka (glasa) u realnom vremenu može da utiče znatno na kvalitet prenosa sve do nivoa (ne)mogućnosti prenosa digitalizovanog glasa delimično ili u potpunosti.

U skladu sa gore navedenim, jako je bitno optimalno odrediti parametre za digitalizaciju glasa da bi glas mogao da se nesmetano prenosi u realnom vremenu kroz raspoloživ telekomunikacioni transportni kanal.

## II.3. Projektovanje optimalnog modela digitalizacije glasa u skladu sa raspoloživim kapacitetom telekomunikacionog kanala

Da bi se osigurao zadovoljavajući kvalitet ali i kontinuitet prenosa glasa u realnom vremenu između 2 uređaja, potrebno je poći od ograničavajućih veličina. U ovom slučaju to je kapacitet transportnog kanala.

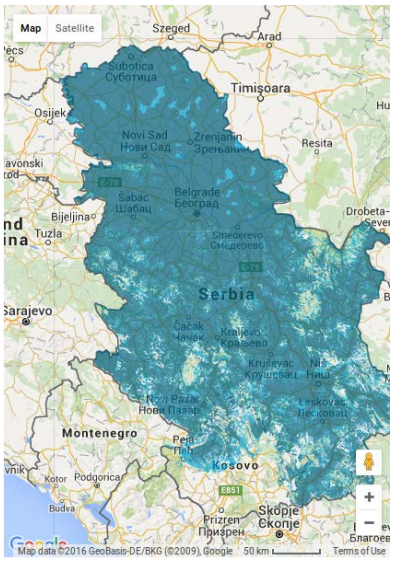
Budući da se prenos podataka obavlja između 2 mobilna uređaja, za ispravno projektovanje modela digitalizacije koji će raditi "u svim uslovima". U tabeli 2. prikazani su postojeći standardi za bežični prenos podataka kroz mrežu mobilne telefonije:

| Standard za prenos podataka | Maksimalna brzina |
|---|---|
| GPRS | 114Kbps |
| EGDE | 368Kbps |
| 3G | 3.1Mbps |
| HSDPA | 14Mbps |
| HSPA+ | 168Mbps |
| 4G/LTE | 299.6Mbps |

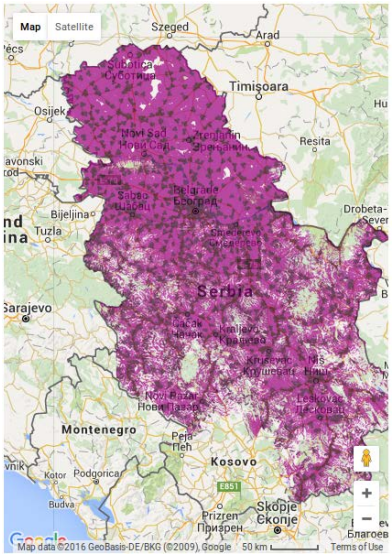
Tabela 2. Maksimalne brzine prenosa podataka po standardima mobilnih mreža

U vreme pisanja ovoga rada, po dostupnim podacima 3 najveća mobilna operatera u Srbiji, čija teritorija se može smatrati meritornom za granični uzorak donjeg praga po pokrivenosti bežičnih mreža velikih brzina, može se zaključiti da je preko 95% teritorije pokriveno sa 3G mrežom, a preko 98% teritorije sa bar EGDE signalom.[3][4][5]

Na slikama 4-9 je prikazana pokrivenost teritorije Republike Srbije sa ovim mrežama.



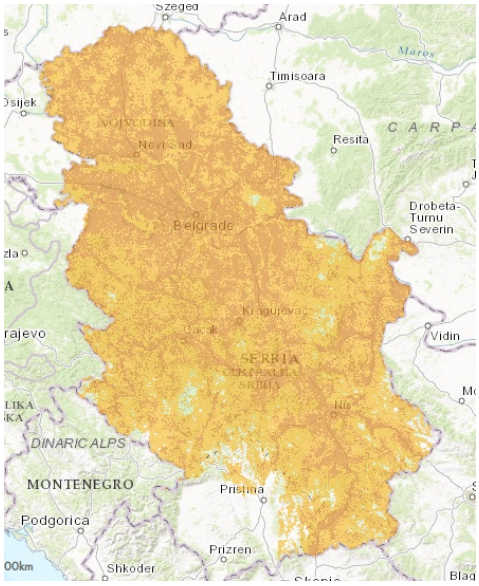

Slika 4. Telenor pokrivenost 2G mrežom



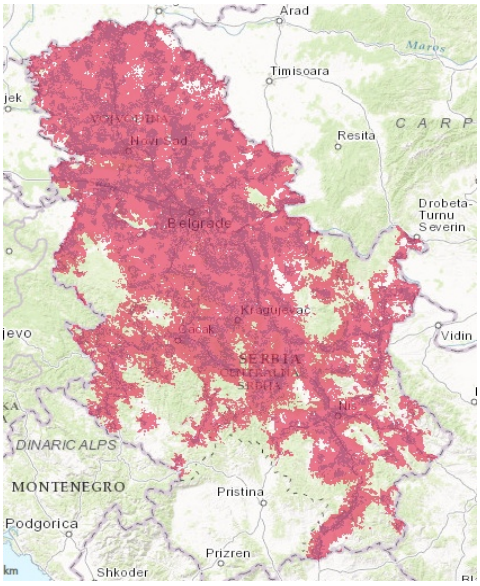

Slika 5. Telenor pokrivenost 3G mrežom


Slika 6. MTS Pokrivenost 2G mrežom


Slika 7. MTS pokrivenost 3G mrežom




Slika 8. VIP pokrivenost 2G mrežom




Slika 9. VIP pokrivenost 3G mrežom

Zaključak na osnovu raspoloživih informacija je da se „može računati“ na bežični telekomunikacioni kanal minimalne propusne moći(kapaciteta) 368Kbps.

Dalje se može sračunati maksimalni model za digitalizaciju zvuka(glasa) čiji prenos u realnom vremenu bi bio moguć kroz ovakav komunikacioni kanal. Ako bi se koristila 16-bitna rezolucija A/D konvertera (m), maksimalni broj diskretnih vrednosti (tako kvantifikovanih uzoraka) u sekundi ($f_s$) bio bi:

$$f_s = \frac{f_{ch}}{m} = \frac{376832}{16} = 23552Hz$$

A maksimalna frekvencija zvuka(glasa) ($f_{max}$)koja bi mogla biti digitalizovana u skladu sa teoremom uzorkovanja bi bila:

$$f_{max} = \frac{f_s}{2} = \frac{23552}{2} = 11776Hz$$

Budući da ugrađene rutine u softverskim bibliotekama za obradu zvuka podržavaju podrazumevano najčešće korišćene standarde digitalizacije, u skladu sa podacima iz tabele 1. bira se dakle $f_s = 22050Hz$, što omogućava $f_{max}$ =11025Hz.

Ovaj format digitalizacije će dakle omogućiti kvalitetnu reprodukciju glasa sa velikom jasnoćom kako glasnih tako i tihih zvukova(glasova), a neće prevazići kapacitet raspoloživog bežičnog transportnog kanala komunikacije.

## II.4. Empirijska provera projektovanog modela digitalizacije glasa

### II.4.1 Postavke test sistema

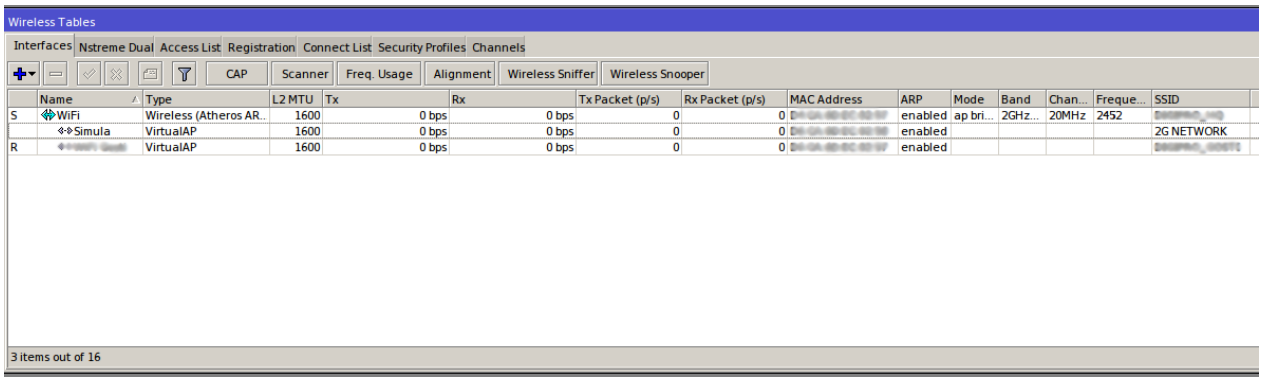
Za potrebe empirijske provere projektovanog modela, u laboratorijskim uslovima, korišćena je sledeća oprema:

1. Router MikroTik RB2011UiAS-2HnD-IN
2. Mobilni Telefon Lenovo A6000
3. PC računar

Na ruteru je pokrenut Router OS verzija 6.33.3. []Na mobilnom telefonu je Android OS verzija 5.0, a na PC računaru OS Windows 7.

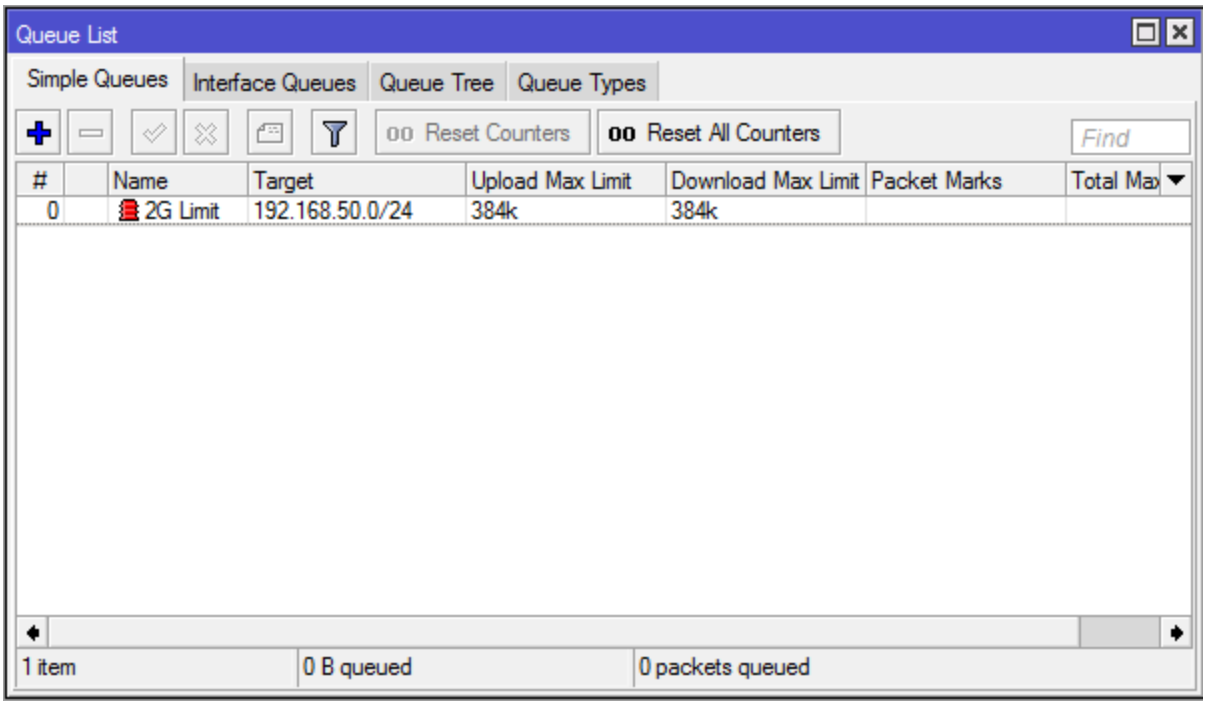
Da bi se simulirala bežična mreža transportnog kapaciteta od 368Kbps, ruter je konfigurisan na sledeći način:

1. Definisan je Virtual AP "2G NETWORK" interfejs, kako je prikazano na slici 10.




Slika 10. Virtual AP "2G NETWORK"

2. Definisan je DHCP server za interfejs "Simula", tako da je "bazen adresa" (eng. DHCP pool) u opsegu IP adresa 192.168.50/24
3. Definisano je ograničenje protoka (eng. bandwidth) korišćenjem "QUEUES" funkcije Router OS-a, na interfejsu "Simula" na 384Kbps, kako je prikazano na slici 11.




Slika 11. Ograničenje brzine protoka

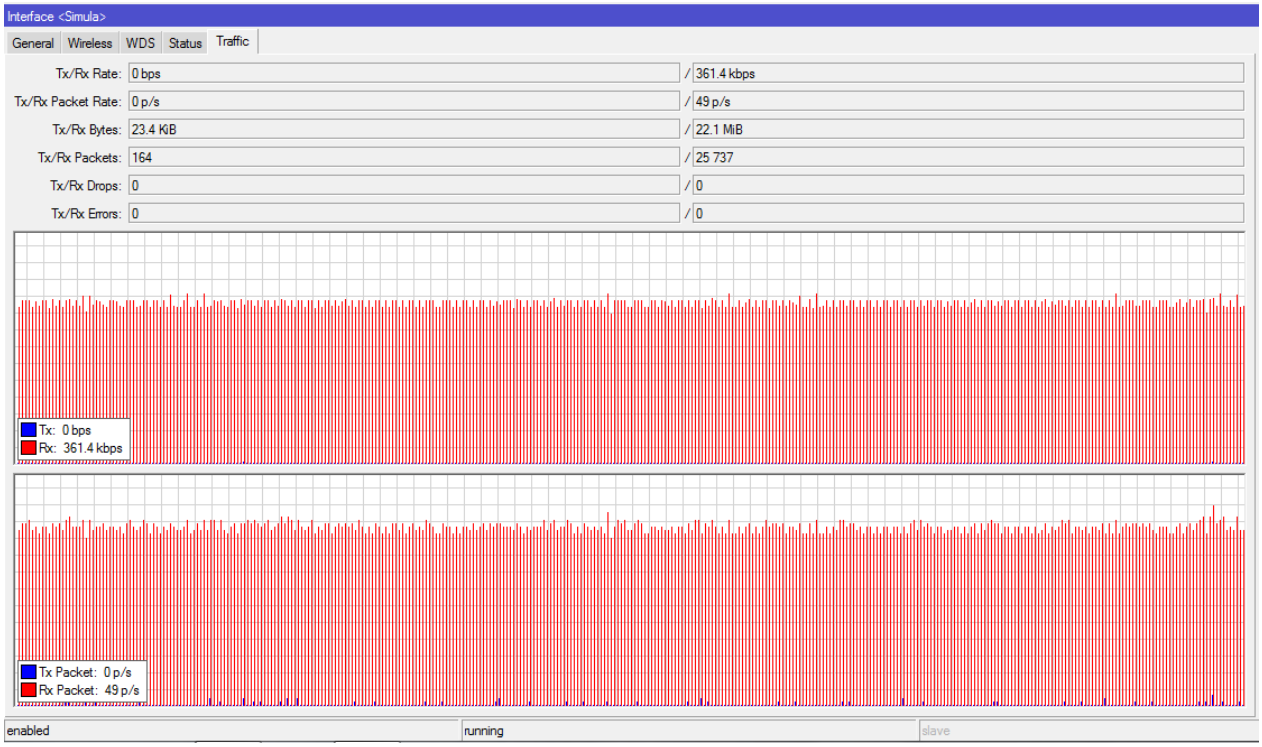
Na android uređaju je pokrenuta aplikacija koja sav zvuk koji detektuje mikrofon telefona digitalizuje sa frekvencijom uzorkovanja 22050Hz, 16-bit, i niz tako dobijenih digitalnih impulsa šalje korišćenjem UDP protokola na PC računar, port 50005.

Android uređaj je povezan direktno na predmetni ruter bežičnom konekcijom na "2G NETWORK" virtualni AP. Budući da je na ruteru definisano ograničenje protoka podataka na ovom interfejsu, aktivira se ograničenje, što se može videti po boji indikatora tog queue-a, na slici 11. koja je crvena.

Na PC računaru je pokrenuta aplikacija koja je efektivno UDP sever na portu 50005, i sve podatke koji stižu direktno prosleđuje na zvučnu karticu koja je setovana da vrši D/A konverziju u istovetnom formatu u kome je zvuk digitalizovan (22050Hz, 16bit) i reprodukuje zvuk na zvučnicima.

### II.4.2 Rezultati testova

U laboratorijskim uslovima, po gore navedenim parametrima, prenos digitalizovanog zvuka je ostvarivao efektivnu brzinu (bandwidth) 360.1Kbps, što je manje od maksimalne propusne moći 2G mobilne mreže koja je simulirana kao komunikacioni kanal, što je prikazano na slici 12.




Slika 12. Prikaz protoka podataka sa uspostavljenim ograničenjem

Ovo merenje potvrđuje da je uspostavljeno test okruženje odgovarajuće po karakteristikama realnom sistemu koji se simulira.

U ovako postavljenom simuliranom sistemu, može se konstatovati da je tako prenet zvuk na odredištu kristalno jasan, lako se mogu razaznati sve reči kao i boja glasa ne samo muški/ženski/dečiji, nego i jasno prepoznati glas poznate osobe.

Uzorak prenosa glasa u ovako postavljenom “idealnom sistemu” je priložen na pratećem CD-u, (fajl uzorak1.rsf) i može se poslušati korišćenjem priloženog namenskog programa „splayer“.

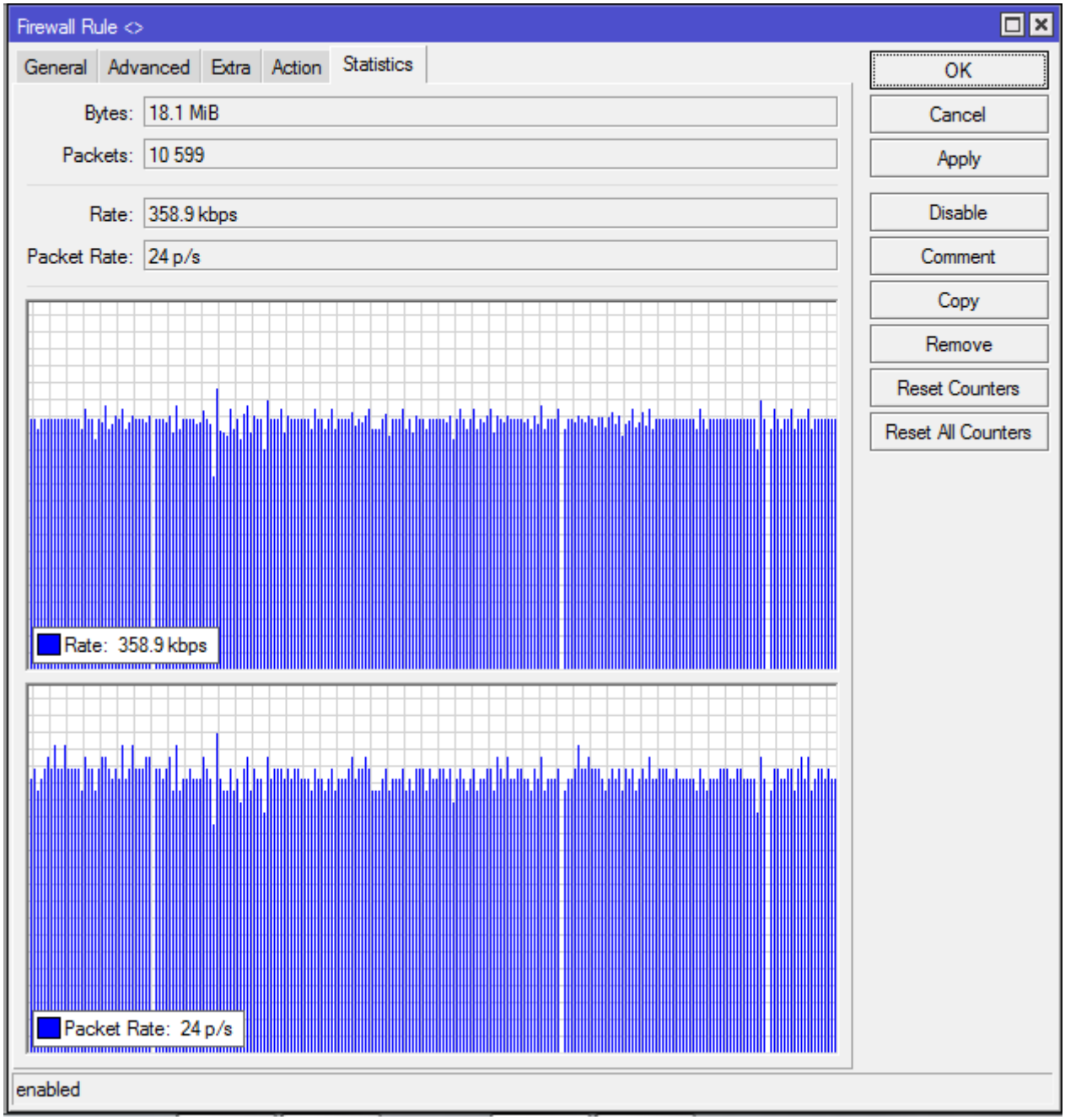
Međutim budući da u realnom svetu uslovi ne moraju da budu uvek (a često i nisu) idealni, testiran je prenos glasa u lošijim uslovima od idealnih.

Lošiji uslovi podrazumevaju da iz raznoraznih razloga koji nisu u suštini tema razmatranja ovoga rada, sav digitalizovani sadržaj zvuka (glasa) koji bude odaslat sa jednog mobilnog uređaja na drugi ne stigne na odredište.

Dalje istraživanje dakle podrazumeva da se simuliraju takvi uslovi u kojima se dešava gubitak podataka u komunikacionom kanalu, te ocena kvaliteta (razumljivosti) tako prenesenog zvuka (glasa).

Da bi se simulirao gubitak pojedinih paketa u kanalu komunikacije, potrebno je definisati određena pravila u Firewall-u rutera u testnom okruženju. Kao prva referenca uzima se idealni slučaj, tj. 100% uspešno i 0% neuspešno prosleđenih paketa.

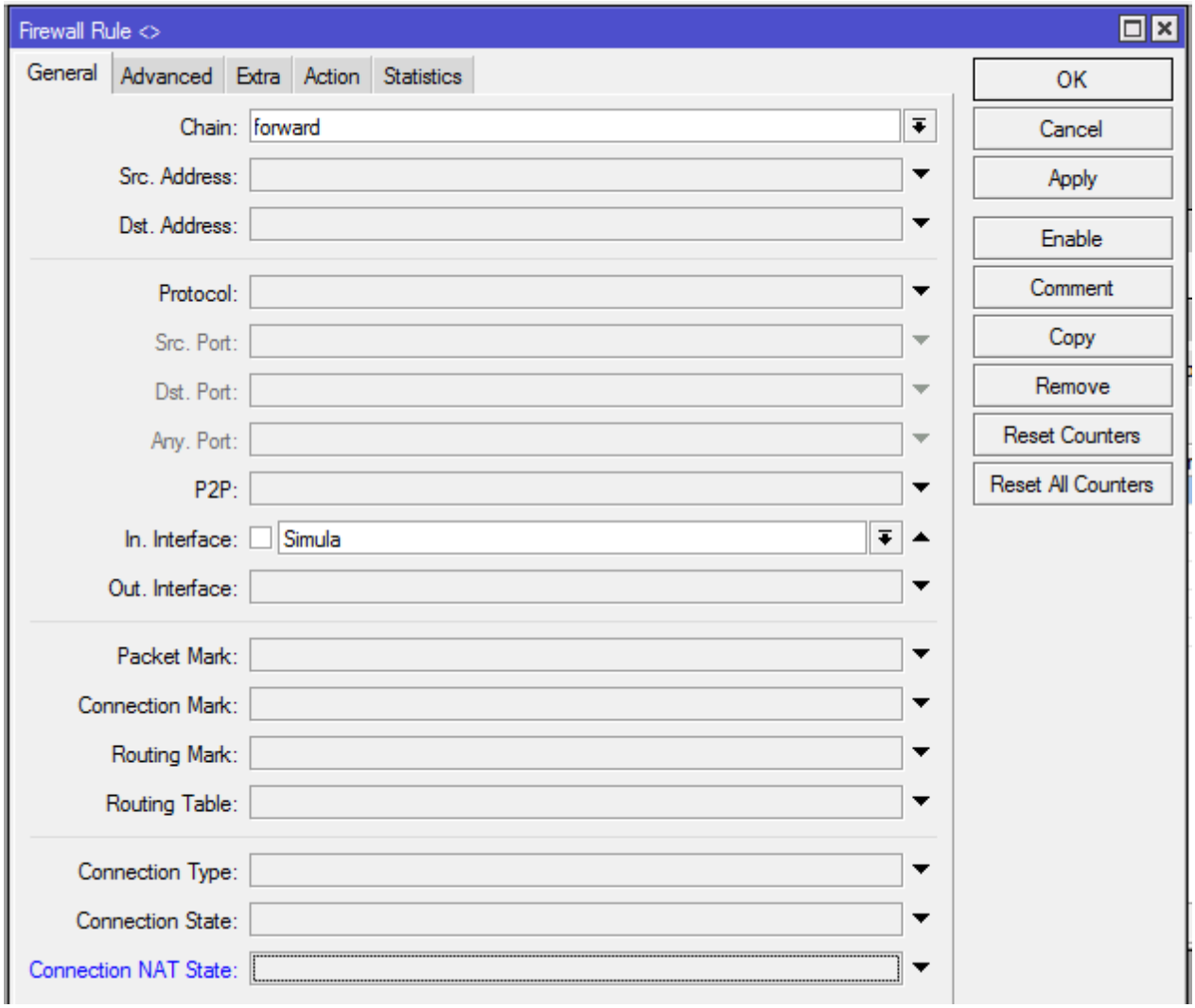
Na slici 13. je prikazan grafikon prenosa zvuka u takvim (idealnim) uslovima.



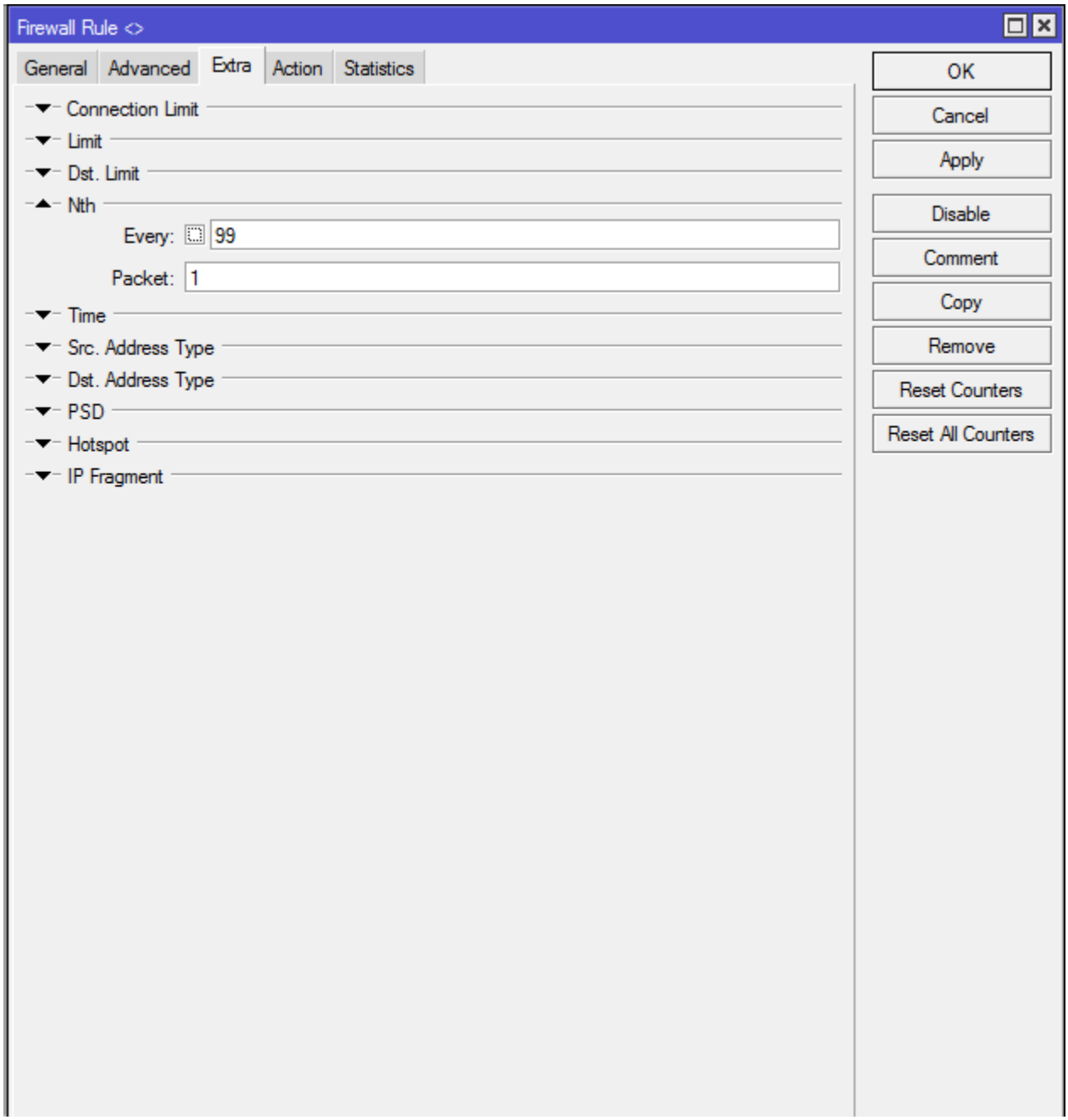

Slika 13. Prikaz prenosa podataka sa 100% uspešno prenetih paketa

Iz podataka sa slike 13. može se uočiti da je efektivna brzina prenosa (angažovani bandwidth) oko 360Kbps, i da se prenese oko 24 paketa/sek.

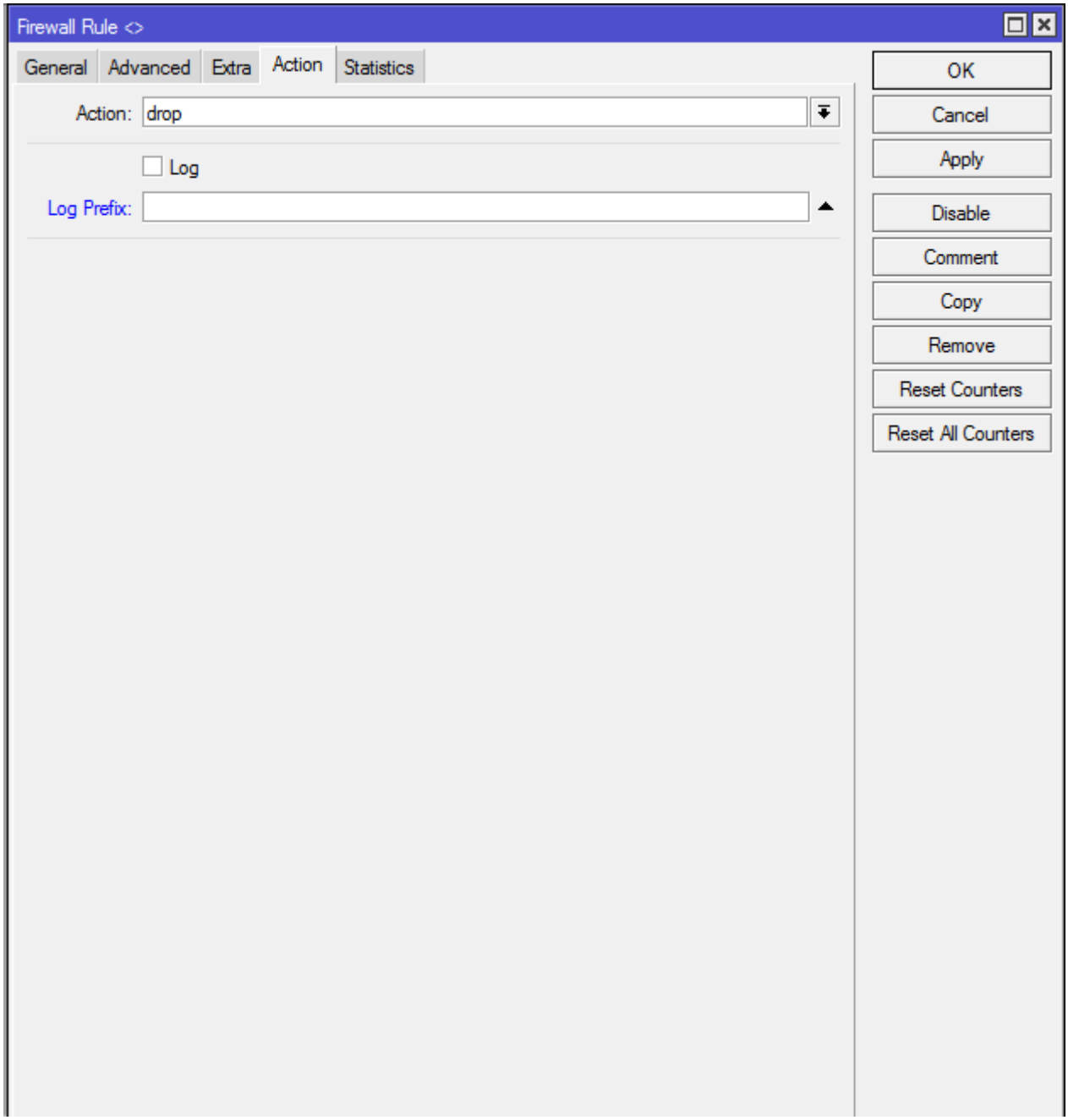
Na ruteru u testnom okruženju definisano je firewall pravilo čiji su parametri prikazani na slikama 14., 15. i 16.




Slika 14. Setovanje firewall pravila za “gubitak paketa” 1. korak




Slika 15. Setovanje firewall pravila za “gubitak paketa” 2. korak




Slika 16. Setovanje firewall pravila za “gubitak paketa” 3. korak

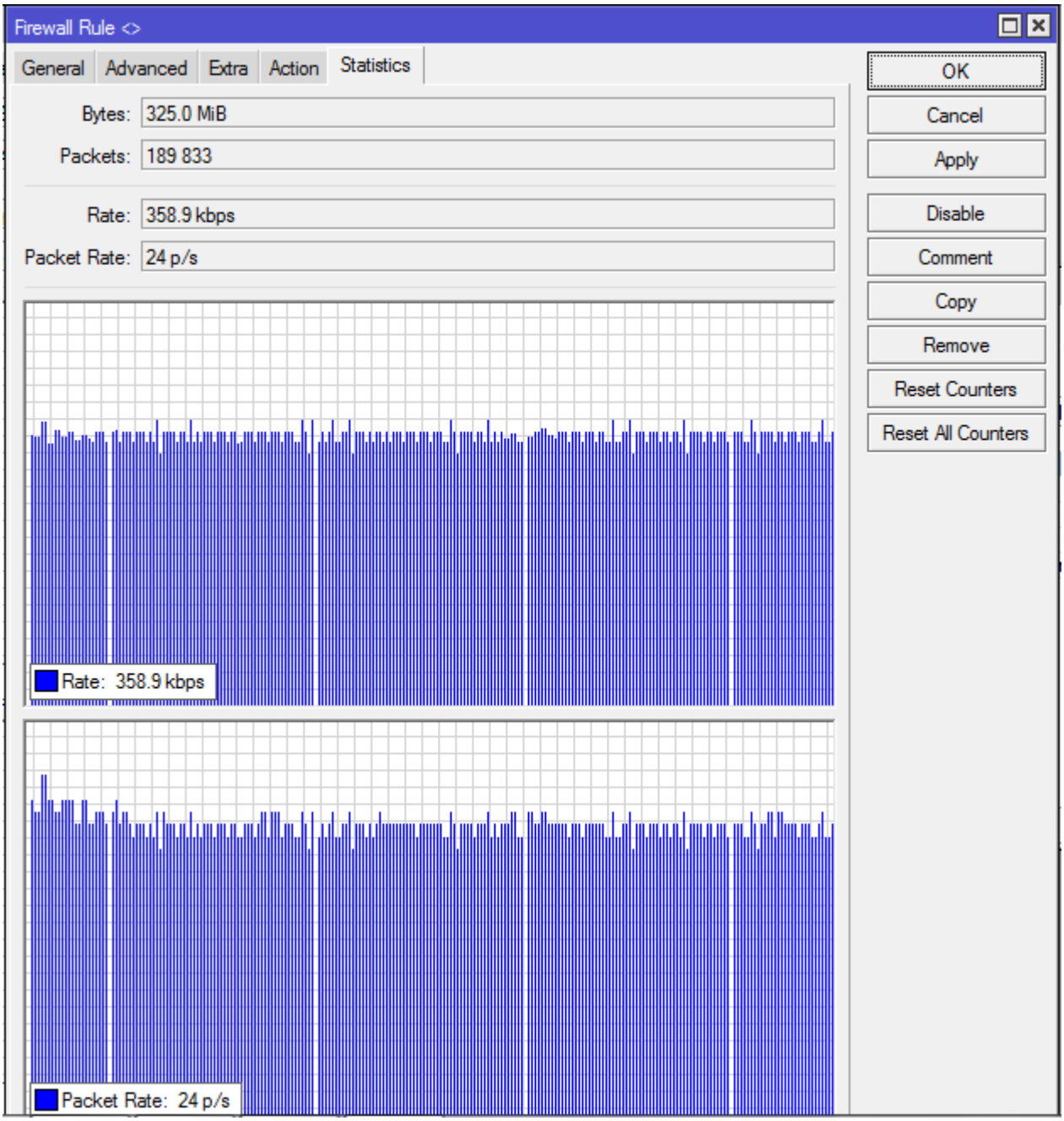
Na slici 14. može se uočiti da se pravilo odnosi na sve pakete koji stižu sa interfejsa „Simula“, tj. Virutelnog AP-a „2G Network“.

Na slici 15. U sekciji „Nth“ (n-ti po redu) pravila se definiše da se na svakih 99 paketa koji prođu jedan paket „obradi“ po ovom pravilu. Dakle 1% paketa (99+1=100) biće obrađeno po ovom pravilu.

Na slici 16. Je definisano na koji način će paketi koji ispunjavaju prethodno definisane uslove biti „obrađeni“. U konkretnom slučaju zadata akcija je „drop“ tj. Da se paket jednostavno odbaci, tj. ne isporuči na odredište.

Na ovaj način efektivno se postiže da 99% paketa stigne do odredišta, a 1% ne.

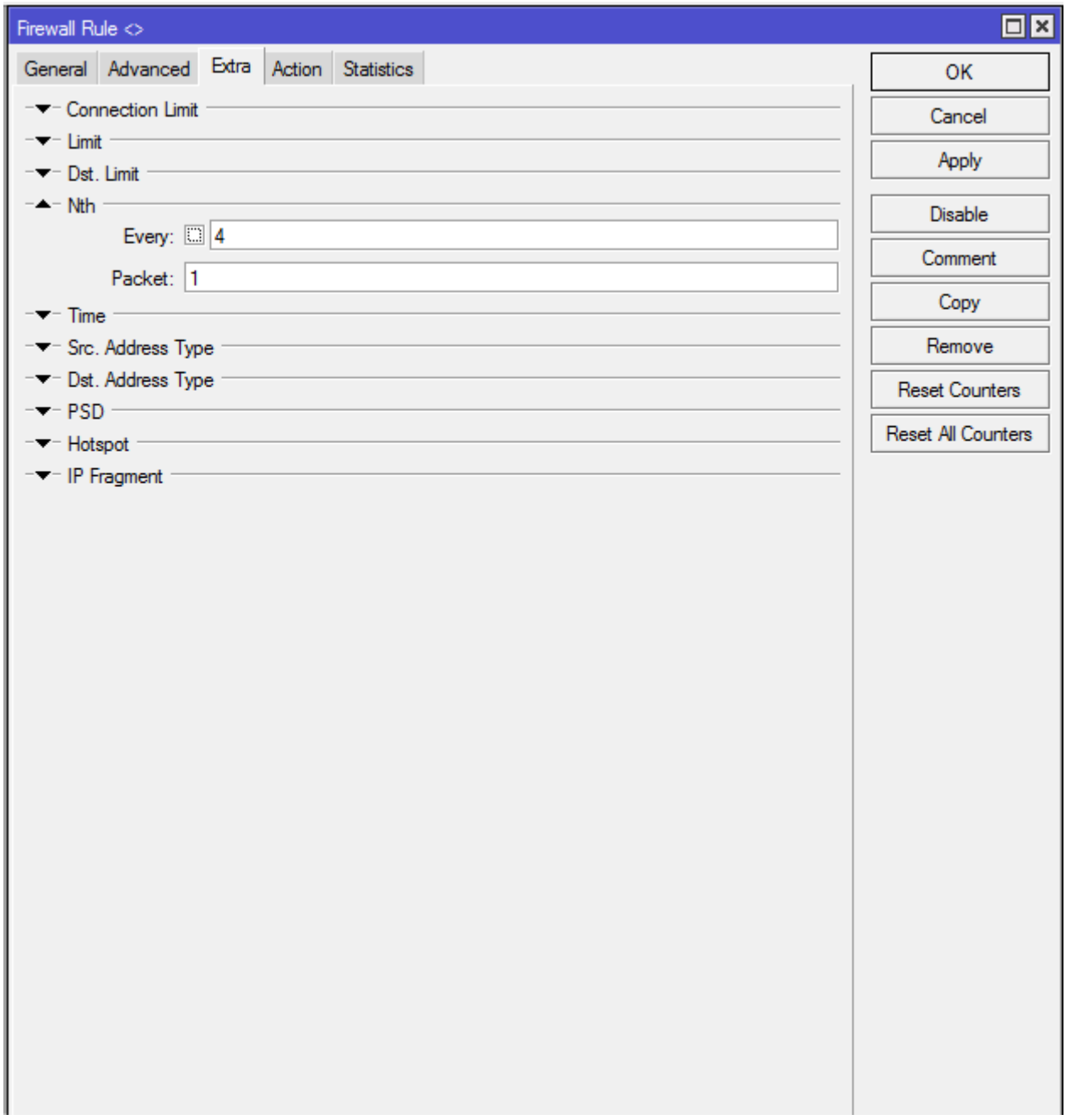
Merenja koja potvrđuju da zadato pravilo na ruteru daje tačno projektovani rezultat, su prikazana na slici 17.




Slika 17. Prikaz prenosa podataka sa 100% uspešno prenetih paketa

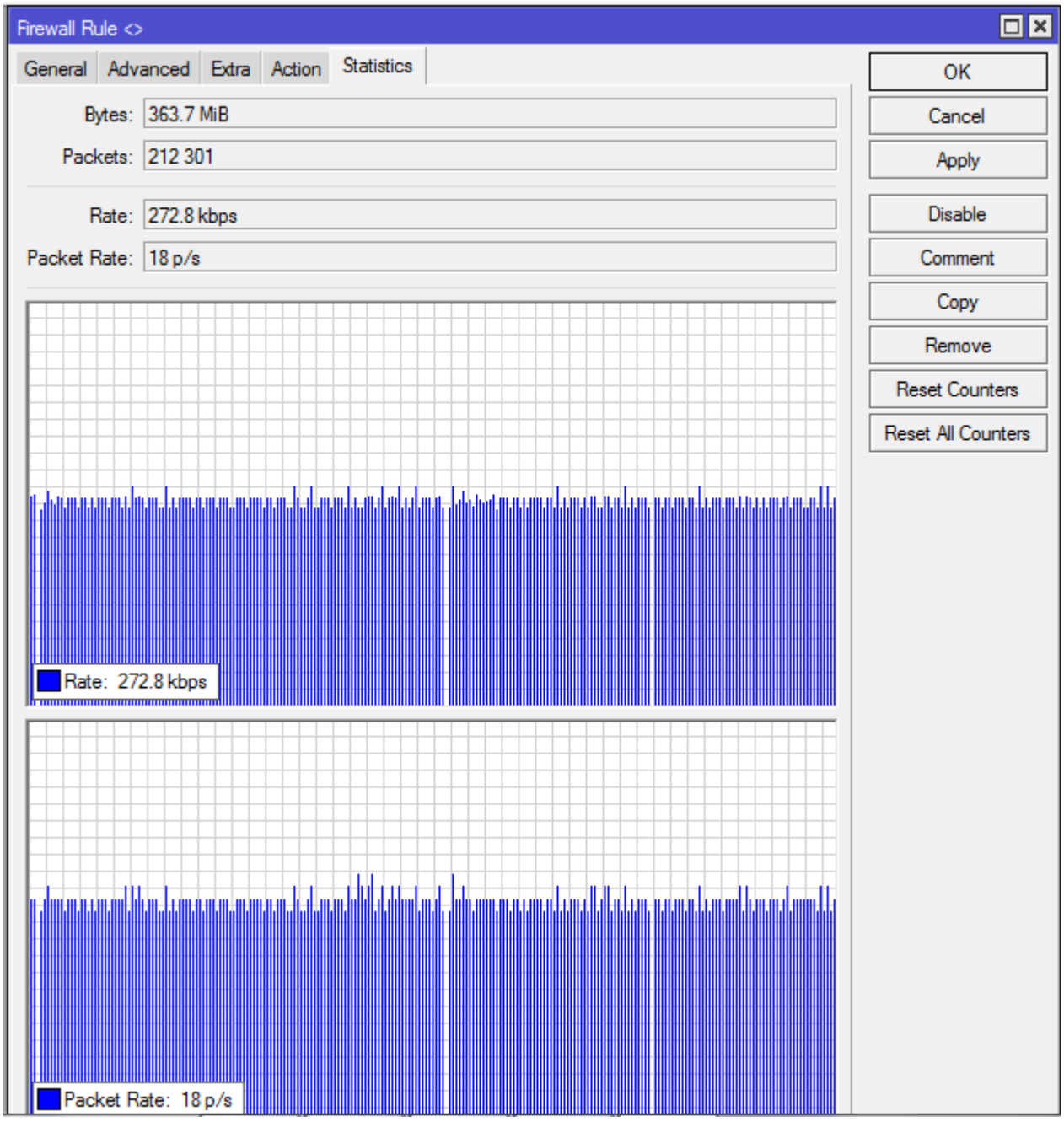
Upoređujući prosečnu vrednost angažovanog kapaciteta komunikacionog kanala pri prenosu 100% paketa (361.1Kbps) i pri prenosu 99% paketa (358.9Kbps) očigledno je da je postignut željeni efekat.

Menjajući firewall pravilo na ruteru u test okruženju, konkretno sekciju Nth pravila kao što je prikazano na slici 18. simulira se 75% uspešan prenos paketa uz 25% gubitaka.




Slika 18. Podešavanje firewall pravila za gubitak 25% paketa

Izvršena merenja pri korišćenju pravila po parametrima sa slike 18. potvrđuju da je 75% uspešnost prenosa uz 25% gubitaka. Postignuta angažovanost komunikacionog kanala je 272Kbps. Merenje ove simulacije je prikazano na slici 19.




Slika 19. Prikaz prenosa podataka sa 75% uspešno prenetih paketa

Korišćenjem gore opisanog metoda, vršene su simulacije sa različitim procentom „gubitaka“ tj. kvaliteta mobilne mreže.

U tabeli 3. su prikazani rezultati tj. ocena kvaliteta (razumljivosti) zvuka (glasa) koji je prenošen u konkretnoj simulaciji.

| Rb. | Procenat izgubljenih paketa | Efektivni kapacitet kom. Kanala | Opis kvaliteta zvuka | Ocena razumljivosti |
|---|---|---|---|---|
| 1. | 0% | 360,1Kbps | Savršeno jasan glas sa prepoznavanjem osobe čiji je glas | 5 |
| 2. | 1% | 358,9Kbps | Savršeno jasan glas sa prepoznavanjem osobe čiji je glas | 5 |
| 3. | 2% | 354,1Kbps | Savršeno jasan glas sa prepoznavanjem osobe čiji je glas | 5 |
| 4. | 5% | 330,0Kbps | Veoma jasan glas sa prepoznavanjem osobe čiji je glas, sa mikro-pauzama i mikro pucketanjem na kraju tih pauza | 4.5 |
| 5. | 10% | 315,8Kbps | Razumljiv govor, moguće jasno odrediti pol/starost govornika, ne i sa sigurnošću identifikovati osobu po glasu. Mikro pauze nešto izraženije, mikropucketanje nepromenjeno | 4 |
| 6. | 15% | 306,4Kbps | Razumljiv govor, moguće jasno odrediti pol/starost govornika, ne i sa sigurnošću identifikovati osobu po glasu. Mikro pauze nepromenjene, mikropucketanje izraženo nešto više | 3.5 |
| 7. | 20% | 287,9Kbps | Govor nije razumljiv u potpunosti, moguće odrediti pol govornika, starost ne tako lako. Teško do nemoguće identifikovati osobu po glasu. Mikropauze su postale već veoma primetne, mikropucketanje nepromenjeno. | 3 |
| 8. | 25% | 271,2Kbps | Govor delimično razumljiv, moguće odrediti pol govornika, starost sa poteškoćama. Nemoguće identifikovati osobu po glasu. Pauze (prekidi) su već značajni. Pucketanje izraženo. | 2.5 |
| | | | Govor moguće razumeti, mada uz | |

| | | | | |
|---|---|---|---|---|
| 9. | 30% | 252,0Kbps | više preslušavanja. Teško odrediti pol/starost sagovornika, mada još uvek moguće. Pauze subjektivno deluju da traju koliko i sam govor. Pucketanje izraženije. | 2 |
| 10. | 35% | 234,7Kbps | Subjektivno nema razlike od prethodnog slučaja, sem što je pucketanje neznatno izraženije. | 2 |
| 11. | 40% | 216,0Kbps | Moguće razumeti samo jako spor i jasan govor. Uz naročitu pažnju moguće odrediti pol govornika i ništa drugo. Pauze subjektivno deluju i duže od govora, pucketanje nepromenjeno. | 1,5 |
| 12. | 45% | 198,5Kbps | Moguće razumeti samo jako spor i jasan govor tek iz više preslušavanja. Uz naročitu pažnju moguće odrediti pol govornika i ništa drugo. Pauze subjektivno deluju i duže od govora, pucketanje još izraženije. | 1,5 |
| 13. | 50% | 181,2Kbps | Teško razumljiv čak i samo jako spor i jasan govor i to tek iz više preslušavanja. Teško do nemoguće odrediti čak i pol govornika. Subjektivno se doživljavaju "zalogaji" zvuka između pauza. Pucketanje nepromenjeno. | 1 |

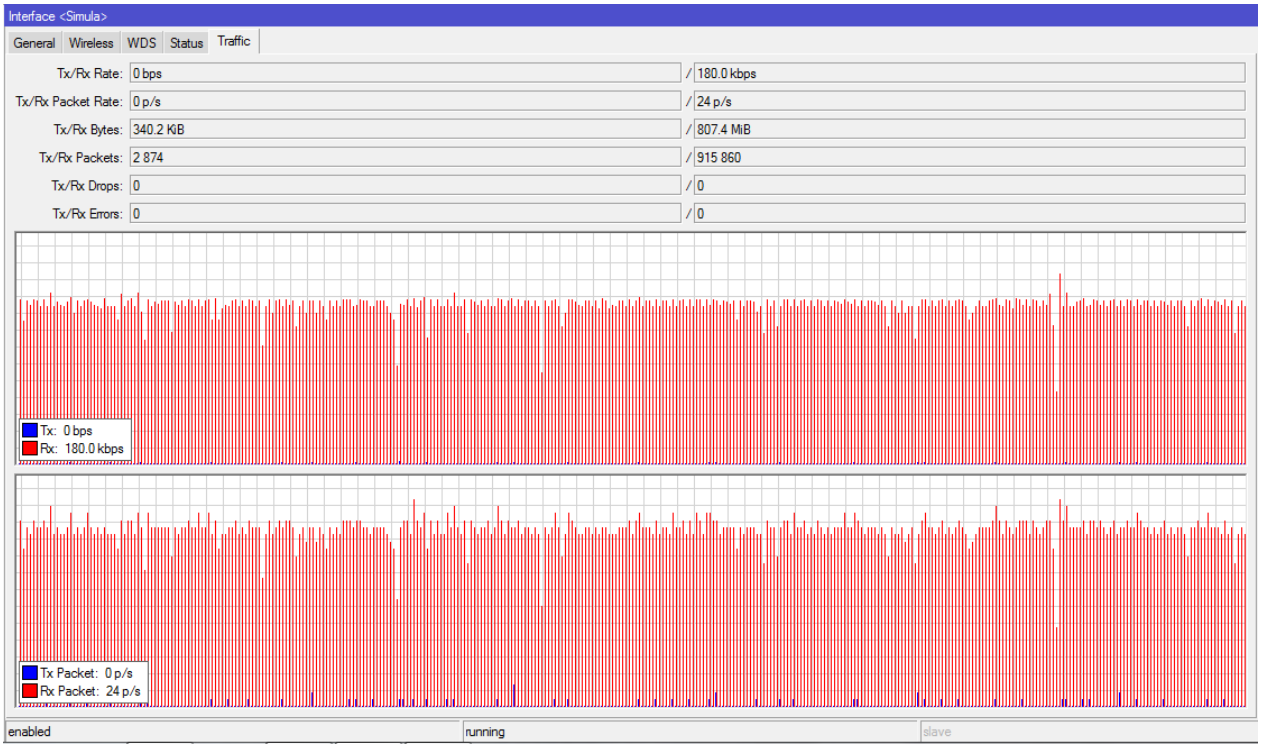
Tabela 3. Ocena kvaliteta (razumljivosti) zvuka (glasa) – prenos u simulaciji 1.

## II.5. UNAPREĐENI MODEL DIGITALIZACIJE GLASA OTPORNIJI NA NESAVRŠENOST KOMUNIKACIONOG KANALA

Kao što je rečeno u odeljku II.1. ljudski govor ne prelazi frekvenciju od 1108Hz, tako da je strogo posmatrano uzorkovanje zvuka frekvencijom od 22050Hz nepotrebno visoko. Smanjenem frekvencije uzorkovanja, smanjila bi se mogućnost uzorkovanja zvukova viših frekvencija, ali sve dok frekvencija uzorkovanja ne bi bila niža od 2216Hz, teoretski zvuk koji proizvodi ljudski glas (govor) bi trebao da bude savršeno razumljiv. Međutim, budući da se koristi Android OS kao platforma, postojeći API podržava samo određene (predefinisane) frekvencije semplovanja i to 11025Hz, 22050Hz i 44100Hz[7], eksperimentisati sa nižom frekvencijom uzorkovanja od 11025Hz nije moguće.

Koristeći istovetnu postavku opreme, sa istim pretpostavljenim komunikacionim kanalom, ali ovoga puta korišćenjem frekvencije semplovanja od 11025Hz, testiranjem u istovetnim uslovima na istovetnoj opremi može se konstatovati sledeće:

1. Angažovani kapacitet transportnog kanala u idealnim uslovima ne prelazi 180Kbps, što je tačno 50% raspoloživog kapaciteta transportnog kanala. Ovo merenje je prikazano na slici 20.



Slika 20. Prikaz angažovanog kapaciteta transportnog kanala

2. Korišćenjem iste tehnike (firewall pravila za odbacivanje svakog n-tog paketa) kao u prethodnoj simulaciji, rezultati testa prenosa ovako digitalizovanog zvuka (glasa) u ne-idealnim uslovima su prikazani u tabeli 4.

| Rb. | Procenat izgubljenih paketa | Efektivni kapacitet kom. Kanala | Opis kvaliteta zvuka | Ocena razumljivosti |
|---|---|---|---|---|
| 1. | 0% | 180,0Kbps | Savršeno jasan glas sa prepoznavanjem osobe čiji je glas | 5 |
| 2. | 1% | 178,2Kbps | Savršeno jasan glas sa prepoznavanjem osobe čiji je glas | 5 |
| 3. | 2% | 176,4Kbps | Savršeno jasan glas sa prepoznavanjem osobe čiji je glas | 5 |
| 4. | 5% | 171,0Kbps | Veoma jasan glas sa prepoznavanjem osobe čiji je glas, sa mikro-pauzama i mikro pucketanjem na kraju tih pauza | 4.5 |
| 5. | 10% | 162,0Kbps | Razumljiv govor, moguće jasno odrediti pol/starost govornika, ne i sa sigurnošću identifikovati osobu po glasu. Mikro pauze nešto izraženije, mikropucketanje nepromenjeno | 4 |
| 6. | 15% | 153,2Kbps | Razumljiv govor, moguće jasno odrediti pol/starost govornika, ne i sa sigurnošću identifikovati osobu po glasu. Mikro pauze nepromenjene, mikropucketanje izraženo nešto više | 3.5 |
| 7. | 20% | 144,5Kbps | Govor nije razumljiv u potpunosti, moguće odrediti pol govornika, starost ne tako lako. Teško do nemoguće identifikovati osobu po glasu. Mikropauze su postale već veoma primetne, mikropucketanje nepromenjeno. | 3 |
| 8. | 25% | 135,2Kbps | Govor delimično razumljiv, moguće odrediti pol govornika, starost sa poteškoćama. Nemoguće identifikovati osobu po glasu. Pauze (prekidi) su već značajni. Pucketanje | 2.5 |

| | | | | |
|---|---|---|---|---|
| | | | izraženo. | |
| 9. | 30% | 126,0Kbps | Govor moguće razumeti, mada uz više preslušavanja. Teško odrediti pol/starost sagovornika, mada još uvek moguće. Pauze subjektivno deluju da traju koliko i sam govor. Pucketanje izraženije. | 2 |
| 10. | 35% | 117,1Kbps | Subjektivno nema razlike od prethodnog slučaja, sem što je pucketanje neznatno izraženije. | 2 |
| 11. | 40% | 108,0Kbps | Moguće razumeti samo jako spor i jasan govor. Uz naročitu pažnju moguće odrediti pol govornika i ništa drugo. Pauze subjektivno deluju i duže od govora, pucketanje nepromenjeno. | 1,5 |
| 12. | 45% | 99,3Kbps | Moguće razumeti samo jako spor i jasan govor tek iz više preslušavanja. Uz naročitu pažnju moguće odrediti pol govornika i ništa drugo. Pauze subjektivno deluju i duže od govora, pucketanje još izraženije. | 1,5 |
| 13. | 50% | 90,2Kbps | Teško razumljiv čak i samo jako spor i jasan govor i to tek iz više preslušavanja. Teško do nemoguće odrediti čak i pol govornika. Subjektivno se doživljavaju "zalogaji" zvuka između pauza. Pucketanje nepromenjeno. | 1 |

Tabela 4. Ocena kvaliteta (razumljivosti) zvuka (glasa) – prenos u simulaciji 2.

Na osnovu ispitivanja može se konstatovati da je korišćenje frekvencije uzorkovanja glasa 11025Hz, ne utiče objektivno na razumljivost i kvalitet digitalizovanog zvuka, kada se radi o ljudskom glasu, ali da se pritom isti "stepen korisnosti" postiže "po duplo nižoj ceni" potrebnog kapaciteta komunikacionog kanala. U realnim uslovima korišćenja ovo znači da i tamo gde zbog kvaliteta/smetnji u mobilnoj mreži realna propusna moć komunikacionog kanala padne i do 50% neće biti primetnog gubitka kvaliteta prenetog zvuka, a tamo gde degradacija komunikacionog kanala ne prelazi 60-65% preneti zvuk biće razumljiv.

# III ŠIFROVANjE SADRŽAJA

## III.1 ŠIFARSKI SISTEMI

Pošto je sigurnost informacija naglašena potreba današnjice, sledeći sloj ili "nadogradnja" sistema za prenos glasa kroz javnu telekomunikacionu infrastrukturu je zaštita istog od neovlašćenog prisluškivanja tog sadržaja. To se postiže šifrovanjem sadržaja na uređaju sa koga digitalizovani glas polazi pre nego isti stigne do javne telekomunikacione infrastrukture, i dešifrovanjem istog na odredišnom uređaju pre reprodukcije glasa.

Kod šifrovanja se najčešće sreću dva preovlađujuća pristupa[8]:

- Šifrovanje korišćenjem algoritma šifrovanja
- Šifrovanje korišćenjem beskonačnog niza slučajnih vrednosti kao ključa šifrovanja

Prvi pristup podrazumeva da se za samo šifrovanje koristi poseban algoritam. Samim time taj algoritam je "srce" sistema zaštite i čuva se kao tajna. Ovaj pristup ima određene mane koje ograničavaju njegovu upotrebu u mnogim aspektima. Glavne mane su:

1. Nefleksibilnost: Svi korisnici sistema moraju koristiti istovetnu verziju algoritma, nije ga moguće parcijalno menjati
2. Veoma skup razvoj i verifikacija algoritma: Te algoritme pišu matematičari i kriptografi, često čitavi timovi, o to traje dugo, a zatim jednako kvalitetan tim stručnjaka mora nezavisno da verifikuje vrednost (bezbednost) algoritma.
3. Veoma ograničena upotreba u uskom krugu: Ako bilo koji korisnik sistema prestane to da bude, algoritam više "nije siguran" i ne bi smeo više da se koristi.

Drugi pristup se mnogo češće primenjuje u današnje vreme. On se bazira na ključu K šifre kojim se otvoreni sadržaj O (predmet zaštite šifrovanjem) šifrira i dobija se šifrat Š:

$$Š = f_k(O)$$

Tako dobijeni šifrat se transportuje do odredišta, i njegov sadržaj je besmislen za svakoga kome je dostupan u toku transporta a kome nije dostupan ključ. Na odredištu se šifrat dešifruje ponovo u otvoreni sadržaj tj. u izvorni oblik/značenje:

$$O = f_k(Š)$$

Sama funkcija šifrovanja $f_š$ i dešifrovanja $f_d$, korišćenjem ključa može biti istovetna i za šifrovanje i za dešifrovanje, i u tom slučaju važi:

$$f_d(f_š(O)) = O$$

Ovakvi šifarski sistemi, u literaturi, se nazivaju i simetrični šifarski sistemi.

Simetrični šifarski sistemi se primenjuju u principu na 2 načina:

1. Šifre tokova (gde se otvoreni sadržaj šifruje bit po bit ili bajt po bajt)
2. Šifre blokova (gde se otvoreni sadržaj grupiše u blokove određene dužine pa se nad njima vrši šifrovanje –blokovski šifarski sistemi)

Takođe u određenim slučajevima se koristi istovetna funkcija za šifrovanje i dešifrovanje korišćenjem ključa $f_k$, ali se koriste različiti ključevi za šifrovanje ($k_1$) i dešifrovanje ($k_2$). U tom slučaju važi:

$$Š = f_{k1}(O)$$
i
$$O = f_{k2}(Š)$$
te
$$O = f_{k2}(f_{k1}(O))$$

Ovakvi šifarski sistemi, u literaturi, se nazivaju asimetrični šifarski sistemi.

Kod asimetričnih šifarskih sistema sa ključevima, mora postojati određena funkcionalna relacija (najčešće matematička) između ključeva kojim se šifruje/dešifruje sadržaj. Karakterističan primer ovakvih šifarskih sistema je šifarski sistem sa javnim i privatnim ključem. Kod ovog sistema, javni ključ (koji se tako naziva jer on ne mora da se krije kao tajna) se koristi za šifrovanje sadržaja (a upotrebom javnog ključa nije moguće dešifrovati sadržaj), a privatni ključ (koji se mora kriti kao tajna) se koristi sa dešifrovanje sadržaja. Ovaj sistem je naročito značajan zbog toga što rešava problem bezbedne razmene ključeva (u ovom slučaju javnog ključa).

Pri korišćenju ovog pristupa sam algoritam tj. funkcija šifrovanja/dešifrovanja nije tajna koja se štiti. Na taj način moguća je masovna produkcija uređaja/alata koji podržavaju ovakvo šifrovanje, bez ugrožavanja bezbednosti samih štićenih podataka. Kao tajna se čuva i štiti sam ključ/ključevi (de)šifrovanja.

Za potrebe realizacije ovog projekta, odabran je najprostiji, ali nikako neefikasan algoritam šifrovanja XOR-ovanja originalnog sadržaja izuzetno dugačkim ključem.

XOR funkcija iz Bulove algebre ima tablicu istinitosti prikazanu u tabeli 5.:

| A | B | A xor B |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Tabela 5. XOR operacija Bulove algebre

XOR operacija ima jedinstveno bitno svojstvo da je potpuno reverzibilna. Dakle ako je:

$$C = A\ xor\ B$$

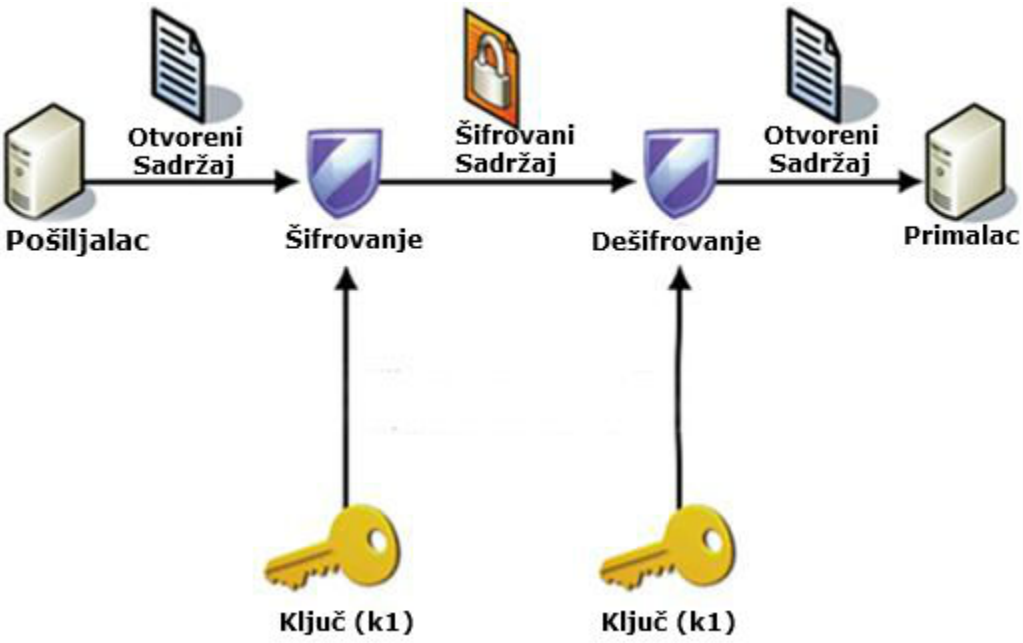
onda važi da je:

$$C\ xor\ B = A$$

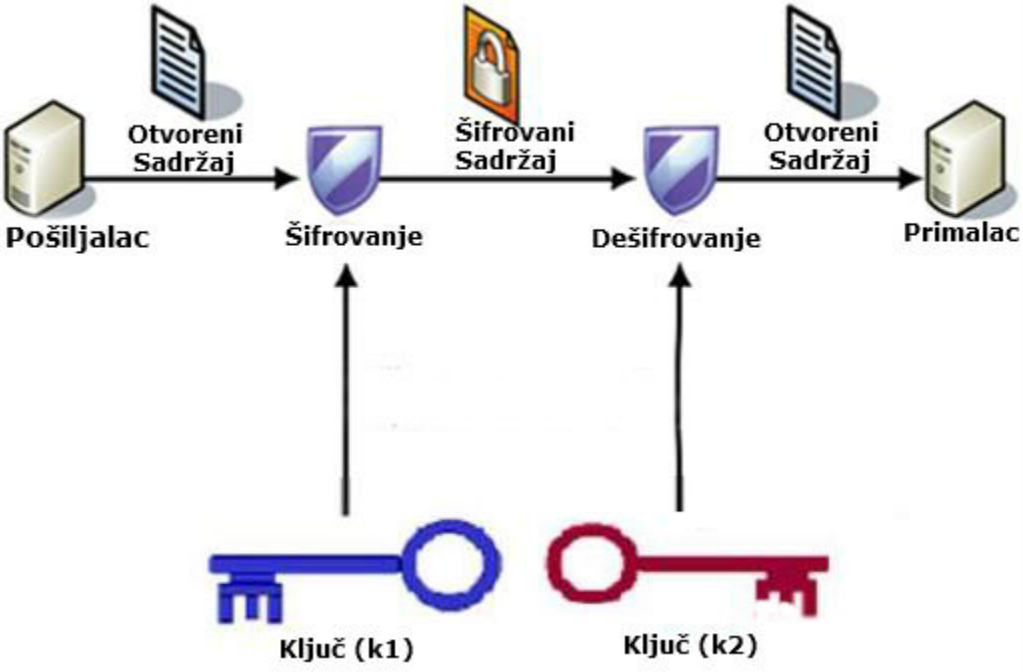
Osim ovog bitnog svojstva zbog koga se XOR operacija koristi masovno u šifarskim algoritmima raznih vrsta, ona je standardna mašinska operacija ugrađena u sve modern računarske procesore, što je čini izuzetno brzom za izvršenje i "neopterećujućom" za hardver. Tako se procesorska snaga značajno štedi i može se koristiti za druge potrebe, ili se upotrebljivost ovakvog šifarskog sistema može proširiti i na značajno skromnije hardverske uređaje.

Ovako štićeni podaci su onoliko sigurni koliko je kvalitetan ključ koji se koristi, što je lako kvantitativno proveriti, a neuporedivo jeftinije i brže generisati nove po potrebi nego razvijati/menjati sam algoritam (de)šifrovanja.

Na slikama 21. i 22. su prikazane blok šeme šifarskih sistema sa korišćenjem istovetnog i različitih ključeva za (de)šifrovanje.




Slika 21. Blok šema šifarskog sistema sa simetričnim ključem




Slika 22. Blok šema šifarskog sistema sa asimetričnim ključem

U praksi kroz istoriju koristile su se mnoge metode koje možemo grupisati po osnovnoj funkcionalnosti u supstitucione šifarske sisteme i transpozicione šifarske sisteme.

Supstitucioni šifarski sistemi podrazumevaju da se pojedine strukturne celine podataka (npr. znakovi tj. slova ako se radi o tekstu) zamenjuju drugom (ali uvek istom po pravilu algoritma koji se koristi) celinom iste (prosta i polialfabetska supstituciona šifra), ili čak različite strukture (homofonična i poligramska supstituciona šifra).

Ovakvi algoritmi mogu se predstaviti sa „supstitucionim tabelama“ koje su dvokolonske i gde u prvoj koloni stoji izvorna strukturna celina (npr. slovo), a u drugoj koloni svakog reda stoji „zamenska struktura“ tj. onaj simbol (slovo) ili više njih koji će zameniti polazni pojam (slovo).

Kod kreiranja ovakvog šifarskog sistema postoje 2 pristupa:

1. Određivanje nekog pravila po kome se polazno slovo zamenjuje drugim.
2. Kreiranje proizvoljne „supstitucione tabele“.

Istorijski je poznata „Cezarova šifra“ koja se može uzeti kao klasičan primer supstitucionog šifarskog sistema. Po tom sistemu svako slovo se menja sa slovom koje je „3 mesta dalje“ od slova koje se šifruje, odnosno kada se dešifruje, svako slovo šifrata se menja slovom koje je „3 mesta pre“ od konkretnog slova šifrata (gledano po pozicijama pojedinih slova u abecedi).

Nešto modernija verzija (samo po vremenu upotrebe, ali nimalo naprednija) proste supstitucione šifre je i ROT13 algoritam, po kome se slova pri šifrovanju/dešifrovanju „pomeraju“ za 13 mesta udesno/ulevo, po redosledu abecede. Broj 13. nije slučajno odabran za ovu namenu. Naime, Engleska abeceda ima 26 znakova (slova) (A-Z). Tako da za bilo koje slovo iz Engleske abecede važi da ako se ono „pomeri“ u bilo koju stranu za 13 mesta pa se ponovo pomeri za 13 mesta u istom smeru, krajnji rezultat će biti istovetni polazni znak (slovo).

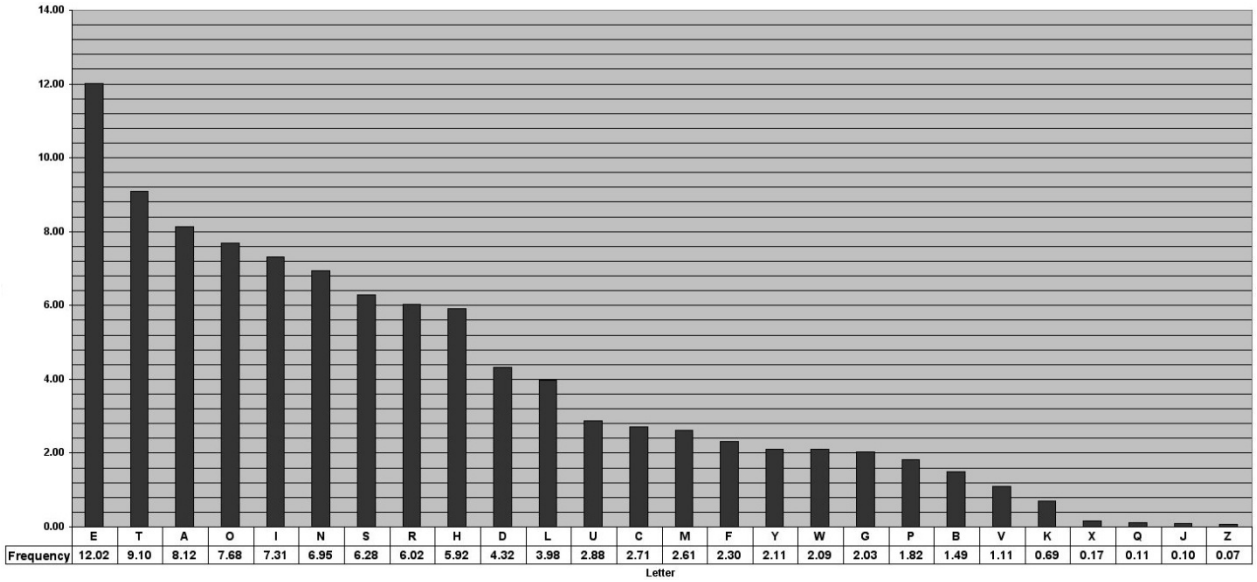
Prosti supstitucioni šifarski sistemi su veoma niskog nivoa zaštite, jer ih je moguće i „ručno“ dešifrovati jer tako šifrovan tekst „ne krije osnovne frekvencije slova otvorenog teksta“.

Prebrojavajući broj ponavljanja određenog znaka (slova) u šifratu, sa velikom verovatnoćom se može tvrditi da znak koji se ponavlja najveći broj puta predstavlja slovo „e“ u otvorenom tekstu. Zatim slovo „t“, pa slovo „a“ itd.

U tabeli 5. [9] je prikazana učestanost slova abecede u Engleskom jeziku. Isti podatak je dat ilustrativno na slici 23. [9]

| Slovo | Frekv. učestanosti | Slovo | Frekv. učestanosti |
|---|---|---|---|
| E | 12.02% | M | 2.61% |
| T | 9.10% | F | 2.30% |
| A | 8.12% | Y | 2.11% |
| O | 7.68% | W | 2.09% |
| I | 7.31% | G | 2.03% |
| N | 6.95% | P | 1.82% |
| S | 6.28% | B | 1.49% |
| R | 6.02% | V | 1.11% |
| H | 5.92% | K | 0.69% |
| D | 4.32% | X | 0.17% |
| L | 3.98% | Q | 0.11% |
| U | 2.88% | J | 0.10% |
| C | 2.71% | Z | 0.07% |

Tabela 6. Učestalost slova abecede u Engleskom jeziku




Slika 23.Statistika učestalosti pojedinih slova u abecedi

Koristeći samo ovaj podatak, svako bi mogao da dešifruje ovako šifrovan tekst[10]. Postoje i brojni računarski algoritmi pisani specijalno za ovu namenu[11]

Polialfabetske supstitucione šifre koriste više ključeva, tj. koriste skup od više supstitucionih alfabeta, gde se konkretni alfabet za supstituciju menja sukcesivno po „istrošenju“ celog pojedinačnog alfabeta. Ako za primer uzmemo da se ključ sastoji od 10 jednoslovnih alfabeta, onda se prvo slovo otvorenog teksta menja slovom prvog šifarskog

alfabeta, drugo drugim i tako do destog slova. Tako će svako 11. slovo biti ponovo šifrovano sa prvim slovom ključa, drugo sa drugim, itd. Tu se uvodi pojam „ciklusa“ šifre, i on je direktno proporcionalan dužini ključa. Logično, što je ključ duži, to je šifarski sistem „jači“.

Posebna vrsta ovakvog šifarskog sistema je „tekući ključ“ (eng. „running key chiper“), u literaturi poznat i kao „knjiga“, gde je dužina ključa jednaka tekstu koji se šifruje.

Ipak, i ovakve šifre su veoma niske sigurnosti, jer se mogu dešifrovati, čak i ručno, bez upotrebe računara.[12]

Transpozicioni šifarski sistemi podrazumevaju da elementi otvorenog teksta ne menjaju vrednost, već samo poziciju. Raspon varijacija je ogroman, počevši od jednostavne stubične transpozicione šifre do naprednih varijanti npr. rotor mašina, čiji najpoznatiji predstavnik je Nemačka mašina „Enigma“ koja je korišćena za vreme II svetskog rata.

Međutim upotreba iole efikasnijeg transpozicionog šifarskog sistema za (de)šifrovanje glasa u realnom vremenu, gde prenos kako je već prikazano ide „u paketima“ je veoma ograničena, jer bi transpoziciono šifrovanje moglo da se primeni samo u okviru paketa, i algoritam bi morao da bude jednostavan/monolitan, bez mogućnosti efikasnog „nadovezivanja“ zbog realne mogućnosti da neki paketi ne budu isporučeni, te se time „lanac kida“, i samim tim se narušava „sekvenca“ i onemogućava primena takvog algoritma transpozicioniranja koji bi se „prostirao na više paketa“. U suprotnom primenom obične sirove snage (eng. brute force) nad pojedinačnim paketima koji su veoma male dužine dešifrovanje bi bilo moguće čak i u realnom vremenu.

Obzirom na prethodno izneto, za šifrovanje glasa u realnom vremenu jedini racionalan izbor je supstitucijski šifarski sistem. On može biti „pojačan“ nekim transpozicionim šifarskim sistemom na nivou pojedinačnih paketa, ali u osnovi mora biti supstitucija.

U literaturi[13] se pominje kao idealni šifarski sistem, sistem „Sveske za jednokratnu upotrebu“. Autori ovog sistema su major Joseph Muborgne i Gilbert Vernam.

„Srce“ ovakvog šifarskog sistema je knjiga/sveska ispunjena velikim slučajnim nizom slova bez ponavljanja. Pri šifrovanju se otvoreni sadržaj tj. svako njegovo pojedinačno slovo šifruje sa pojedinačnim slovom iz te sveske. U originalnom rešenju šifrovanje se vrši tako što se pozicija (abecedna) svakog slova iz otvorenog teksta sabira sa pozicijom (abecednom) odgovarajućeg (po redu) slova iz sveske. Dobijeni broj se deli sa brojem 26 (broj slova u abecedi) i ostatak deljenja je rezultirajući šifrat.

Primalac šifrovane poruke mora posedovati istovetnu svesku (sa istovetnim sadržajem), i koristi je za dešifrovanje primljene poruke.

Bitan aspekt ovog sistema je pravilo da se deo slučajnog niza iz sveske koji je jednom upotrebljen za šifrovanje/dešifrovanje nekog sadržaja koristi samo taj jedan put i nikada više.

Od presudne važnosti kod korišćenja ovog šifarskog sistema je kvalitet „slučajnog niza“ koji ispunjava svesku ključa. Ovo naročito postaje značajan problem jer dužina ključa za svaku „poruku“ mora biti jednaka dužini same poruke, pošto za potrebe šifrovanja glasovne komunikacije treba obezbediti kvalitetne jednokratne slučajne nizove za ključ dužine više megabajta ili čak gigabajta.

## III.2. KLjUČEVI ZA ŠIFARSKI SISTEM

Kao što je navedeno u prethodnom odeljku, problem kvaliteta ključa za šifarski sistem je od suštinske važnosti.

Praktično ključevi mogu da se obezbede samo na dva načina:

1. Generisanjem ključeva
2. Korišćenjem postojećih ključeva

Prvi metod ma koliko privlačno delovao je prilično teško ostvariv u praksi za konkretnu primenu šifrovanja glasa u realnim uslovima. Problemi su sledeći:

1. Potreba za kvalitetnim algoritmom –generatorom slučajnih brojeva. Ovako nešto striktno gledano ne postoji. Postoje računarski algoritmi koji su u suštini generatori pseudo-slučajnih nizova.
2. Korišćenje kvalitetnih algoritama za generisanje pseudo-slučajnih nizova iziskuje angažovanje značajnih hardverskih resursa, što sa skorašnjim razvojem tehnologije gubi na značaju, ali mora se imati u vidu.
3. Praktično je nemoguće ako se koristi iole kvalitetan algoritam,takav da se ključevi generišu u realnom vremenu, jer nije moguće postići takvu „sinhronizaciju“ ključeva da se i kod pošiljaoca i primaoca istovremeno generišu istovetni nizovi pseudo-slučajnih brojeva. Tu prestaje priča o bilo kakvoj slučajnosti.
4. Poseban problem bi bio distribucija ovako generisanog ključa bez ozbiljnog kompromitovanja celog šifarskog sistema, i povrh svega problem sa dodatnim opterećenjem transportnog kanala.

Imajući sve ovo u vidu, jedina racionalna opcija za šifrovanje glasa u realnom vremenu je korišćenje postojećih ključeva. Međutim i ova opcija ima svoje probleme:

1. Zbog enormne veličine jednokratnog ključa (za svaki pojedinačni razgovor), realan je problem skladišni kapacitet u mobilnim uređajima.
2. Distribucija ključeva tolike veličine je takođe veoma neefikasna „na daljinu“ plus predstavlja rizik od presretanja ključa od treće strane i upotrebe istog za dešifrovanje buduće komunikacije.

Ovi problemi su ipak rešivi primenom pristupa (ne)skladištenja ključeva kako je prezentovano u nastavku.

### III.2.1 ODABIR PODESNOG MATERIJALA ZA KLjUČEVE

Umesto problematičnog generisanja ključeva, efikasnije i racionalnije je koristiti već dostupne dugačke nizove slučajnih brojeva.

Veoma je širok dijapazon dostupnih takvih "materijala". Glavna karakteristika koja se traži je da su nizovi brojeva statistički slučajni sa što dužom serijom bez ponavljanja kako pojedinačnog broja, tako (što je još značajnije) i nizova od 2, 3,....n brojeva, gde se verovatnoća ponavljanja sekvence od n brojeva treba da bude u takvoj relaciji da što je broj n veći, da je broj ponavljanja sekvence dužine n brojeva teži nuli.

Takva karakteristika može se pronaći kod svih vrsta kompresovanih sadržaja, jer je upravo osnovna funkcija kompresionih algoritama da se uočavaju ponavljanja naročito sekvenci (što dužih to bolje) i beleže po principu tzv. "klizajućeg rečnika" (eng. sliding dictionary), čime kompresovani sadržaj rezultira virtuelno nizom podataka bez ponavljanja. Sami kompresioni algoritmi nisu predmet ovog rada, samo se ova karakteristika kompresovanog sadržaja koristi kao polazna premisa da su kompresovani sadržaji pogodni za izvor dugačkih sekvenci slučajnih brojeva sa minimalnom redudansom.

Više o samim kompresionim algoritmima može se pročitati u literaturi [14][15][16].

Pri odabiru konkretnog materijala koji bi se koristio kao ključ po principu "beležnice za jednokratnu upotrebu", potrebno je da isti ispunjava sledeće kriterijume:

1. Da bude dostupan u realnom vremenu obema stranama u komunikaciji
2. Da ispunjava kvalitativne statističke kriterijume da se može smatrati dovoljno kvalitetnim nizom slučajnih brojeva.

Bilo koji sadržaj javno dostupan na internetu ispunjava prvi kriterijum.

Ispunjenje drugog kriterijuma, međutim mora se detaljnije ispitati pre donošenja suda o (ne)pogodnosti određene vrste dostupnih kompresovanih materijala. U ovom radu ispitani su sledeći tipovi kompresovanih sadržaja, datih u tabeli 6.

| Rb. | Naziv |
|---|---|
| 1. | GIF slike |
| 2. | JPEG slike |
| 3. | PNG slike |
| 4. | MP3 audio fajlovi |
| 5. | Video fajovi kompresovani raznim varijantama MPEG kompresije |

Tabela 7. Formati ispitivanih kompresovanih sadržaja

Razlog zbog koga se posebno ispituju tri različita kompresovana formata slike je taj što su neki od njih bez gubitaka (eng. loseless), a neki sa gubicima, koji za rezultat imaju određene trajne gubitke originalnog sadržaja i nemogućnost 100% tačne reprodukcije originalnog sadržaja dekompresijom kompresovanog sadržaja, što može skalabilno da se određuje prilikom inicijalne kompresije originalnog sadržaja, tako da gubitak ne utiče na subjektivni vizuelni doživljaj posmatrača slike, ili utiče u određenoj meri, a pritom daje proporcionalno značajno veći stepen kompresije.

Da li i koliko to utiče na kvalitet tako kompresovane slike za upotrebu ključa za šifrovanje, je interesantno pitanje sa aspekta odabira pogodnog materijala za tu namenu.

Pošto je dužina niza bitan faktor, biće razmatrane slike visoke rezolucije slikane sa digitalnim foto aparatom, preuzete u sirovom (eng. raw) formatu sa foto aparata, pa zatim kompresovane navedenim algoritmima i onda baterijom specijalizovanih statističkih testova ocenjivati njihovu podobnost za šifarske ključeve kao duge nizove slučajnih brojeva.

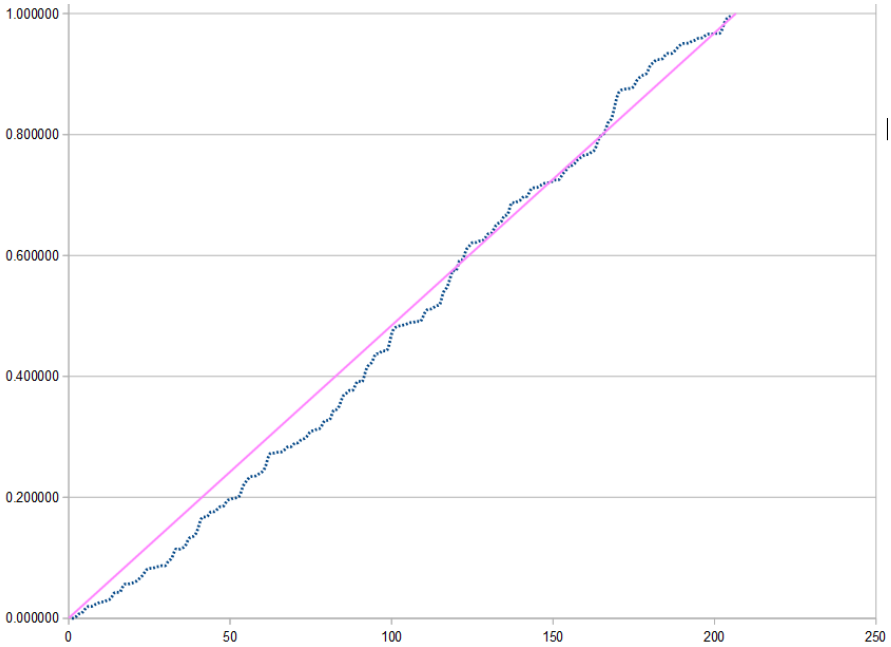
Da bi rezultat bio što merodavniji, koristiće se u ovom testu slike različitih sadržaja: pejsaži, portreti, predmeti, u kolor i crno beloj tehnici.

Za ispitivanje vrednosti pojedinih fajlova, po kriterijumu kvaliteta dugačkog niza slučajnih brojeva, koristiće se alat dieharder[17]. On je unapređena verzija (sadrži bateriju od ukupno 114 statističkih testova) originalnog alata diehard[18] koga je kreirao George Marsaglia na FSU (Florida State University) 1995. godine.

U interpretaciji kvaliteta “stvarne slučajnosti” dugačkog niza koriste se p-vrednosti koje su direktna interpolacija ispitivanog niza po određenom statističkom testu nasuprot “nulte hipoteze”[19].

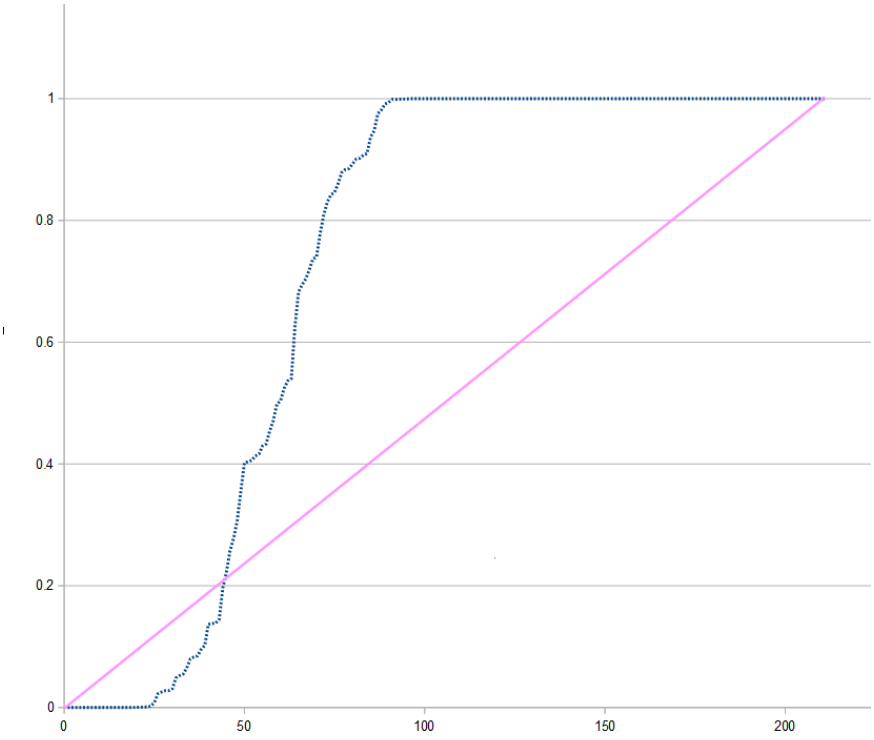
U stvarnosti, dobijene p-vrednosti se sortiraju pa se na osnovu njih može dobiti „grafik raspodele slučajnosti“. On vizuelno prikazuje nivo „savršenosti slučajne raspodele u dugačkom nizu vrednosti“.

Na slici 24. je prikazan rezultat ispitivanja niza dobijenog merenjem raspada radioaktivnog izotopa, što se može smatrati prirodno slučajnom sekvencom. Na grafiku prava dijagonalna linija predstavlja liniju „idealne slučajne raspodele“, a tačkasta kriva prikazuje dobijene p-vrednosti[20].




Slika 24. Grafik primera idealne slučajne raspodele

Nasuprot tome, na slici 25. dat je grafikon p-vrednosti dobijenih ispitivanjem klasične rand() funkcije u C jeziku[20].




Slika 25. Grafik slučajne raspodele rand funkcije u C jeziku

Očigledno je da rand() funkcija iz standardne biblioteke C jezika daje veoma loš rezultat kada se duži niz tako dobijenih vrednosti propusti kroz ovu bateriju testova, sa aspektta ocene “prave slučajnosti niza vrednosti”.

Ova dva primera mogu se uzeti kao „kontrolni uzorci“, tj. reference za ispitivanja pojedinih predloženih formata.

### III.2.2 SLIKE KAO IZVOR KLJUČEVA

Testiran je uzorak od 9 slika, svaka je snimljena u odgovarajući format koji je ispitivan, u kolor i crno-beloj verziji. Ukupan uzorak dakle iznosi 54 slike.

Svaka od slika je na priloženom CD-u u folderu “uzorci materijala za ključeve”, podfolder slike, pa u odgovarajućim podfolderima nazvanim po ekstenzijama fajlova tj. formata koji su ispitivani. Dobijeni rezultati ispitivanja su prikazani u folderu rezultati u obliku .xslx fajlova sa odgovarajućim nazivima.

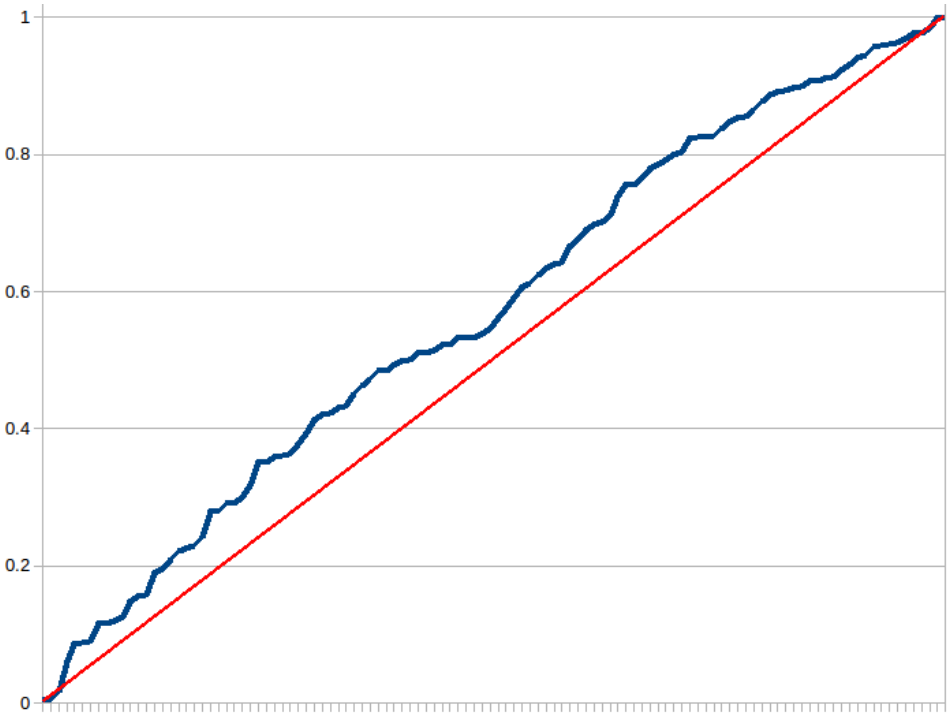
Spisak baterije testova koje dieharder softver izvodi nad sadržajem predmetnih datoteka je sledeći:

1. diehard_birthdays
2. diehard_operm5
3. diehard_rank_32x32
4. diehard_rank_6x8
5. diehard_bitstream
6. diehard_opso
7. diehard_oqso
8. diehard_dna
9. diehard_count_1s_str
10. diehard_count_1s_byt
11. diehard_parking_lot
12. diehard_2dsphere
13. diehard_3dsphere
14. diehard_squeeze
15. diehard_sums
16. diehard_runs
17. diehard_craps
18. marsaglia_tsang_gcd
19. sts_monobit
20. sts_runs
21. rgb_bitdist

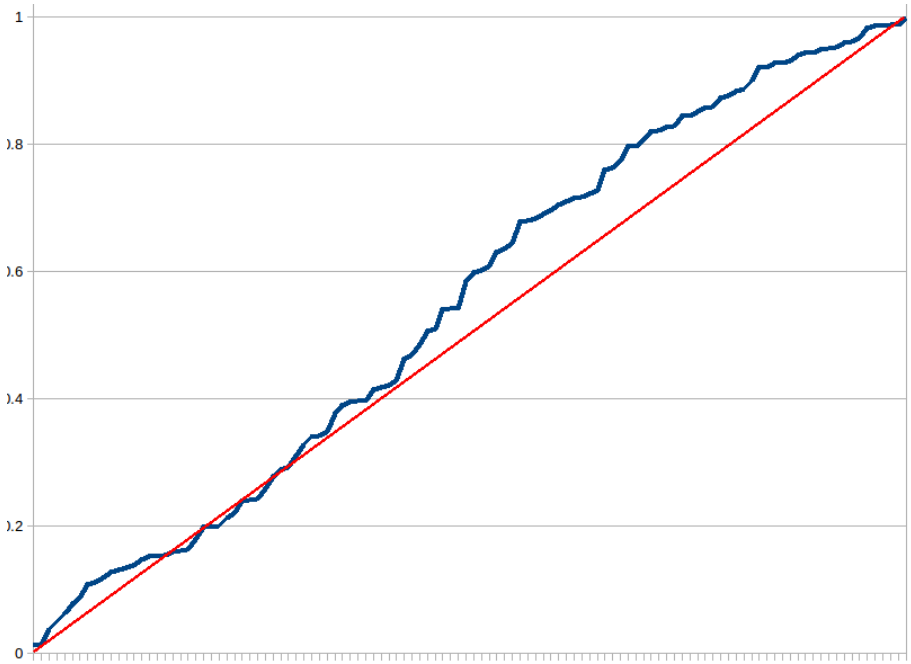
22. rgb_minimum_distance
23. rgb_permutations
24. rgb_lagged_sum
25. rgb_kstest_test
26. dab_bytedistrib
27. dab_dct
28. dab_filltree
29. dab_filltree2
30. dab_monobit2

Neki od ovih testova se u toku ispitivanja ponavljaju više puta, neki čak i do 32 puta. Tako da po izvršenim svim testovima dobija se skup p-vrednosti od kojih se po sortiranju može dobiti grafik raspodele koji je direktno uporediv sa referentnim graficima datim na slikama 24. i 25.

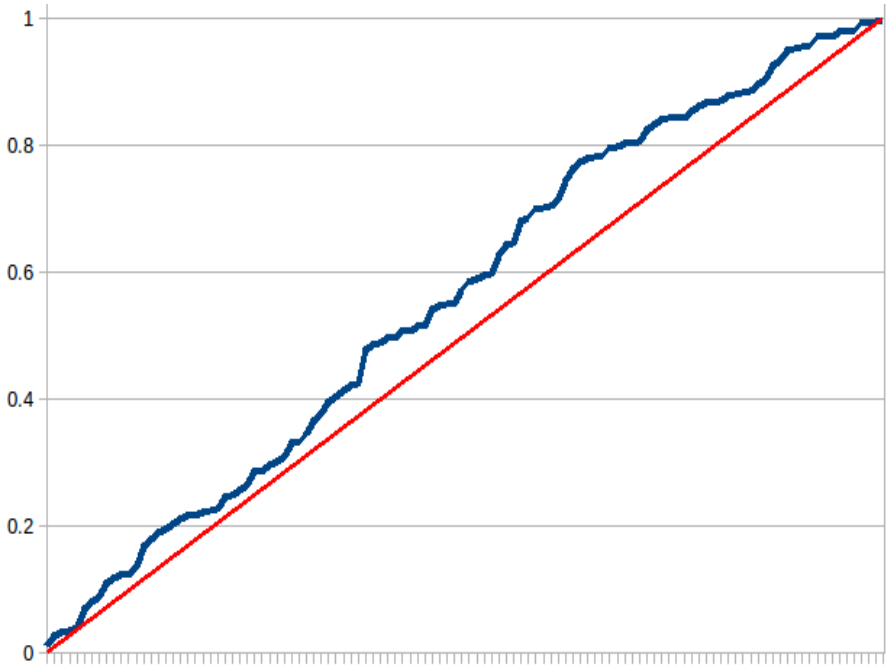
Detaljni rezultati ispitivanja svih slika su dati na pratećem CD-u u gore navedenom folderu, a na slikama 26.,27., i 28. su prikazani rezultirajući grafici od dobijenih p-vrednosti za .GIF, .JPG i .PNG slike u boji:




Slika 26. Grafik slučajne raspodele uzorka slike u .GIF formatu

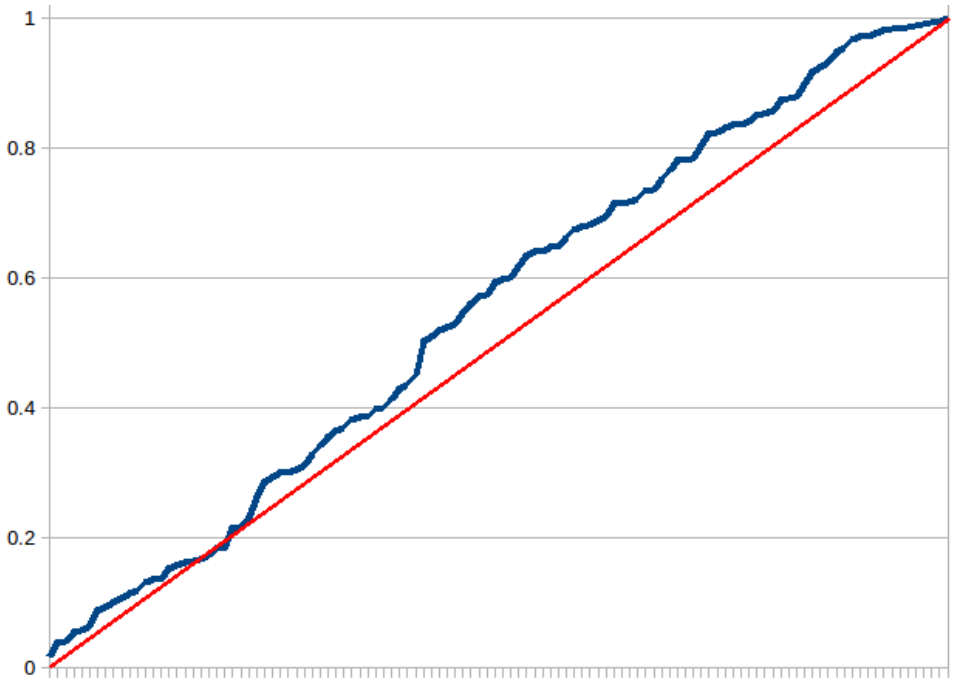



Slika 27. Grafik slučajne raspodele uzorka slike u .JPG formatu

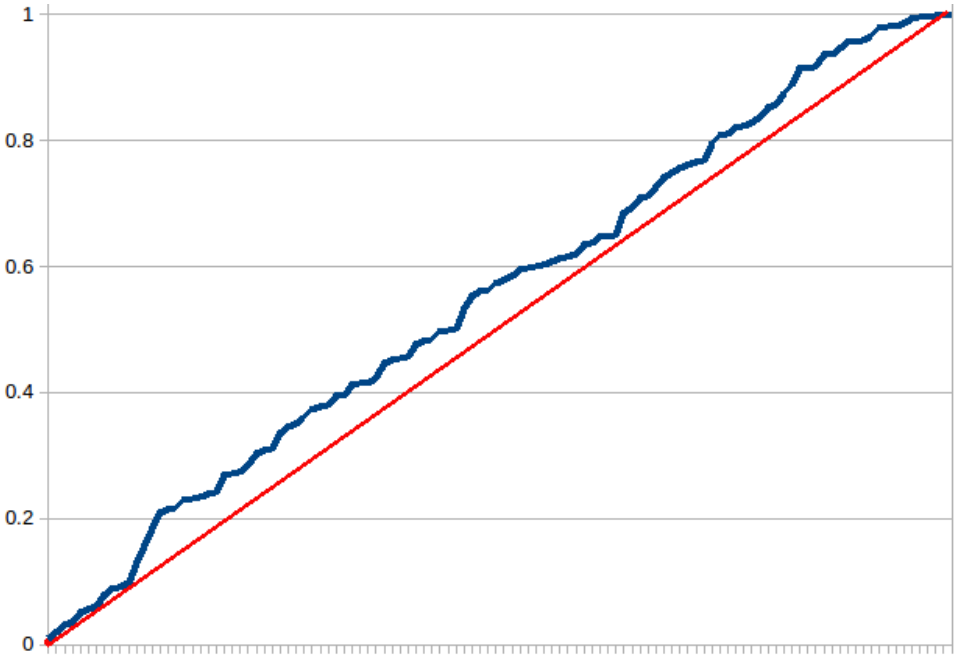



Slika 28. Grafik slučajne raspodele uzorka slike u .PNG formatu

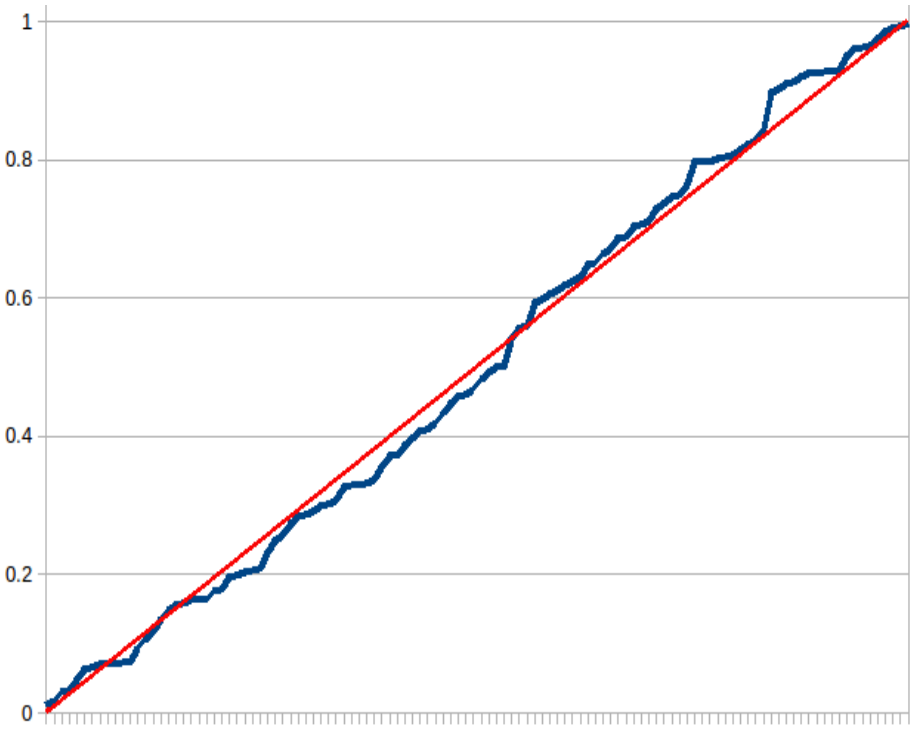
Na slikama 29., 30. i 31. su prikazani grafikoni od rezultirajućih p-vrednosti dobijenih izvršavanjem iste baterije testova u .GIF, .JPG, i .PNG formatu, ali ovoga puta istovetnih slika u crno-belom formatu.




Slika 29. Grafik slučajne raspodele uzorka slike u .GIF formatu (b&w)




Slika 30. Grafik slučajne raspodele uzorka slike u .JPG formatu (b&w)




Slika 31. Grafik slučajne raspodele uzorka slike u .PNG formatu (b&w)

Iz prethodno iznetog se može izvesti zaključak da su slike u kompresovanim formatima, bez obzira na sadržaj (čak je svejedno da li su crno-bele ili u boji) izvor veoma kvalitetnih nizova statistički slučajnih vrednosti, te kao takve se mogu koristiti i kao dugački jednokratni ključevi u šifarskim sistemima.

### III.2.3. AUDIO (.MP3) FAJLOVI KAO IZVOR KLjUČEVA

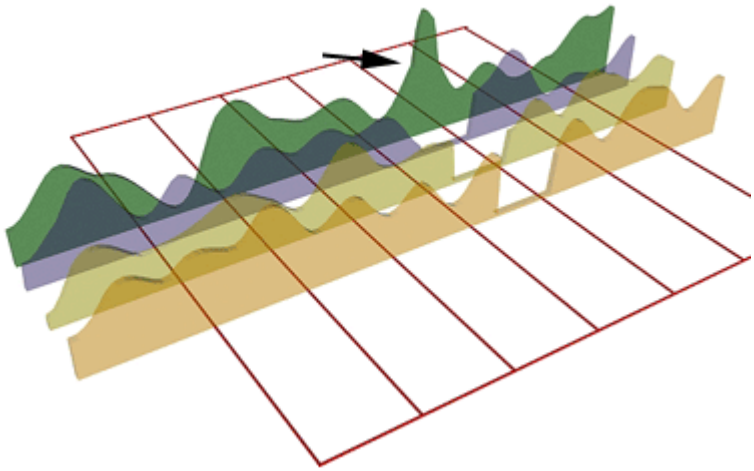
Zvučni zapisi se takođe mogu kompresovati kao i slike, ali iako je cilj isti (smanjiti fizičku veličinu fajla), metodologija kompresije je drastično drugačija. Naime kod percepcije zvuka odnosno skupa više zvukova (sazvučje više muzičkih instrumenata/glasova) uvodi se pojam „psihoakustike“[21][22]. Pojednostavljeno rečeno, dva faktora su glavna kod percepcije zvuka, tj, sazvučja više simultanih zvukova. Prvi je frekvencija pojedinačnih zvukova, a drugi je amplituda tj. jačina pojedinačnih zvukova u sazvučju. Samo ova dva faktora imaju veoma širok raspon međusobne interakcije koja rezultira određenom “percepcijom zvuka” od strane čoveka.

Suština je da je tehnički posmatran polifoni zvučni sadržaj često i drastično različit od onoga što ljudsko uho/mozak registruje. Polazeći od pretpostavke da ako bi se ono što

čovek ne percepira uopšte ili veoma zanemarljivo, izostavilo iz zvučnog sadržaja, ono što preostane biće dovoljno "verno originalu", bar onako kako to čovek čuje.

Osim "grubog" izdvajanja "slabo čulnih" frekvencija bliskih krajevima zvučnog opsega, posmatra se i jačina zvukova određene frekvencije ali u određenom trenutku. Ovo je bitno zbog fenomena "temporalnog maskiranja" iz psihoakustike[23]. Ako na primer u jednom trenutku zvučni materijal sadrži dva zvuka pojedinačnih frekvencija 1100Hz i 1000Hz, dakle oba zvuka koja su u „veoma čulnom" opsegu, i pojedinačno bi se oba jasno čula, u ovom slučaju jači zvuk će „maskirati" slabiji zvuk te se ovaj slabiji zvuk može zanemariti i odbaciti u procesu kompresije ovog zvučnog materijala, bez bojazni da će primetno degradirati ukupnu zvučnu percepciju od strane čoveka.

Na slici 32. je prikazan 3D model zvučnog materijala koji se sastoji od više simultanih zvukova, i kako se usled postojanja jednog glasnog zvuka određene frekvencije mogu zanemariti ostali zvukovi u tom trenutku/periodu.



Slika 32. 3D akustički model polifonog zvučnog signala

Koristeći ovo pravilo (i ne samo njega) algoritam kompresije zvuka se u stvari svodi na „kontrolera/selektora" delova zvučnog matrerijala koji se može zanemariti/odbaciti. A ono što ostane se kompresuje tradicionalnim algoritmima kompresije podataka. Ovo omogućava odnos kompresovanog materijala prema izvornom u odnosima 1/10 ili 1/12, bez subjektivnog gubitka sadržaja, iako striktno tehnički posmatrano izostavljanjem određenih delova zvučnog materjala isti je često i drastično siromašniji od izvornog materijala.

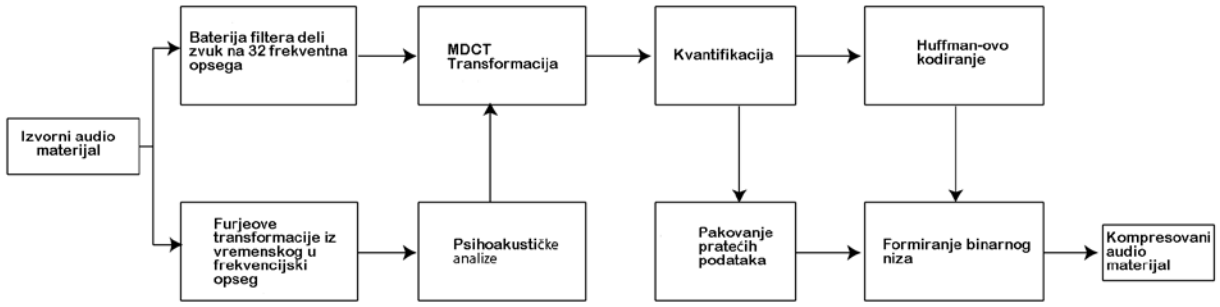
Istraživanja koja su rezultirala (ne samo) .mp3 formatom započela su kasnih 70'ih godina prošlog veka u Nemačkoj na Nirmberškom Univerzitetu. Tada su i računari i komunikacioni kanali imali veoma ograničene performanse gledano sa aspekta današnjih performansi kako hardvera, tako i telekomunikacione infrastrukture. Oni su istraživali mogućnost kompresije zvučnih zapisa vodeći se po principima psihoakustike. Zajedno sa

Fraunhofer insitutom su oformili MPEG (eng. Moving Picture Experts Group) telo, i po njemu su dobili zvanične (ISO) nazive modeli standarda za kompresiju zvuka i video materijala danas poznati kao MPEG-1,2,3 i 4.

Kao početna premisa razvijen je OCF algoritam (eng. Optimum Coding in Frequency), A daljim njegovim unapređenjem nastao je ASPEC (Adaptive Spectral Perceptual Entropy Encoding).

MPEG je objavio MPEG Layer-3 standard 1993. godine, i on je široko prihvaćen kako za samo skladištenje audio materijala, tako i za prenos preko interneta. 1994. Godine on je postao opšte poznat kao MP3.

Na slici 33. Je data blok-šema algoritma kompresije koji se koristi za mp3 format.




Slika 33. Blok šema kompresije .mp3 audio formata

Detaljno objašnjenje svih delova ovog algoritma bi zauzelo previše mesta, pa će razmatranje istog biti ograničeno na aspekte upotrebe ovako kompresovanog audio materijala kao izvora slučajnog niza velike dužine. Detalji o algoritmu kompresije su dostupni u literaturi[24].

Zbog prirode audio materijala, koji se prezentuje samo svojim "trenutnim" uzorkom u jedinici vremena, a ne u celini kao što je slučaj sa slikama, ni prilikom kompresije ni prilikom dekompresije se ne obrađuje ceo materijal u potpunosti, pa samim tim nije apsolutno isključena redudansa određenih takvih delova.

Konkretno svaki "deo" materijala se kompresuje nezavisno od ostatka audio materijala.

Svaki taj deo se tretira tako da njegova kompresija rezultira nezavisnim okvirom(paketom) (eng. frame) fiksne dužine, koja po MP3 standardu iznosi 1152 uzorka.

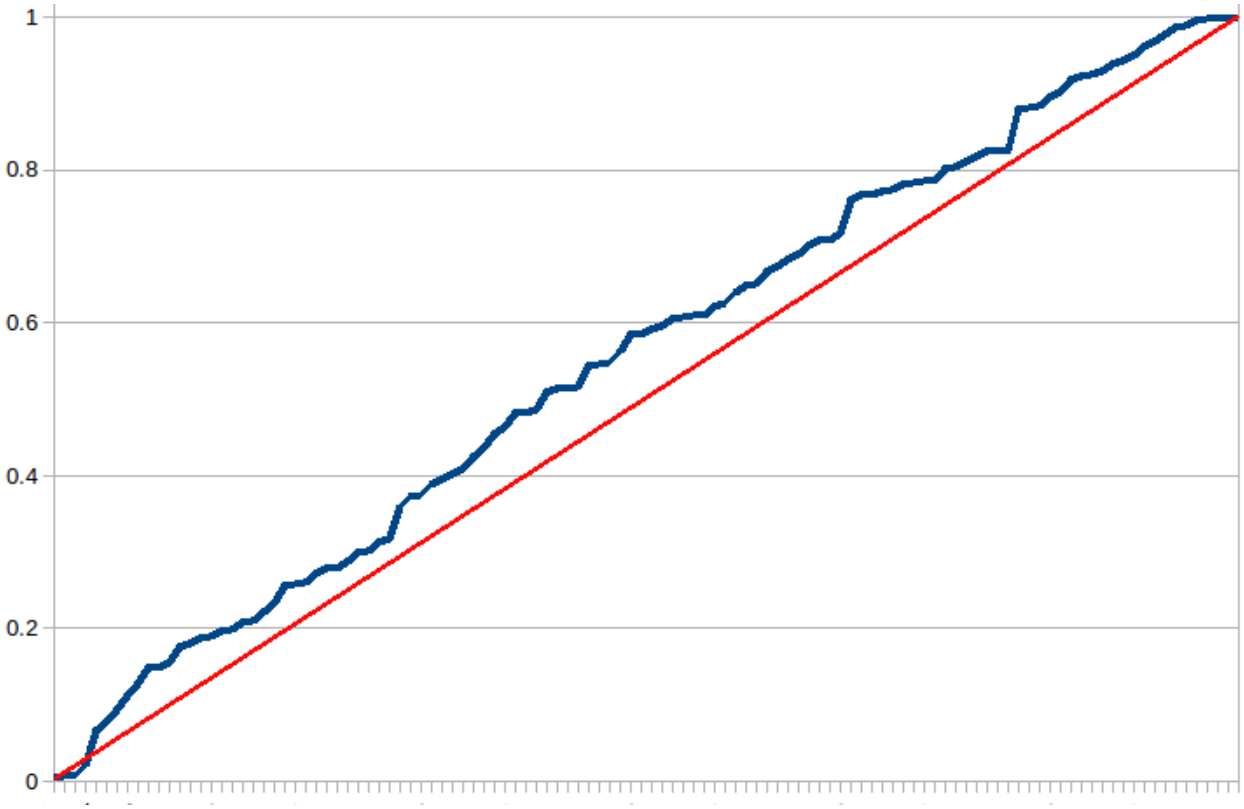
Međutim budući da je "drugi stub" MP3 kompresije bitrate, količina okvira po sekundi uzorkovanog materijala je takođe varijabilna.

MP3 podržava CBR (eng. **C**onstant **B**it **R**ate) i VBR (eng. **V**ariabile **B**it **R**ate) standarde. Ovo dodatno usložnjava ceo slučaj sa aspekta neke statističke analize.

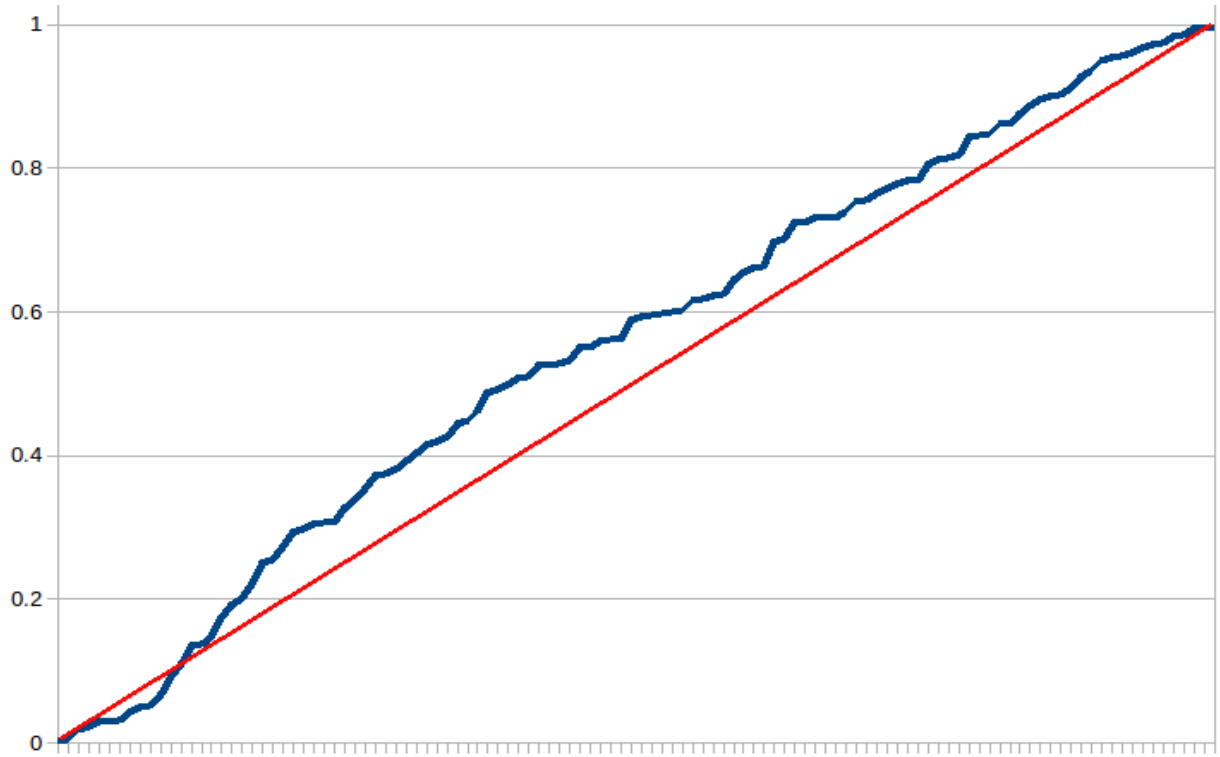
Testiran je uzorak od 10 .mp3 numera, svaka je odabrana iz različitih izvora, sa različitim kvalitetom uzorkovanja/kompresije.

Svaka od numera je na priloženom CD-u u folderu “uzorci materijala za ključeve”, podfolder mp3. Dobijeni rezultati ispitivanja su prikazani u folderu rezultati u obliku .xslx fajlova sa odgovarajućim nazivima.

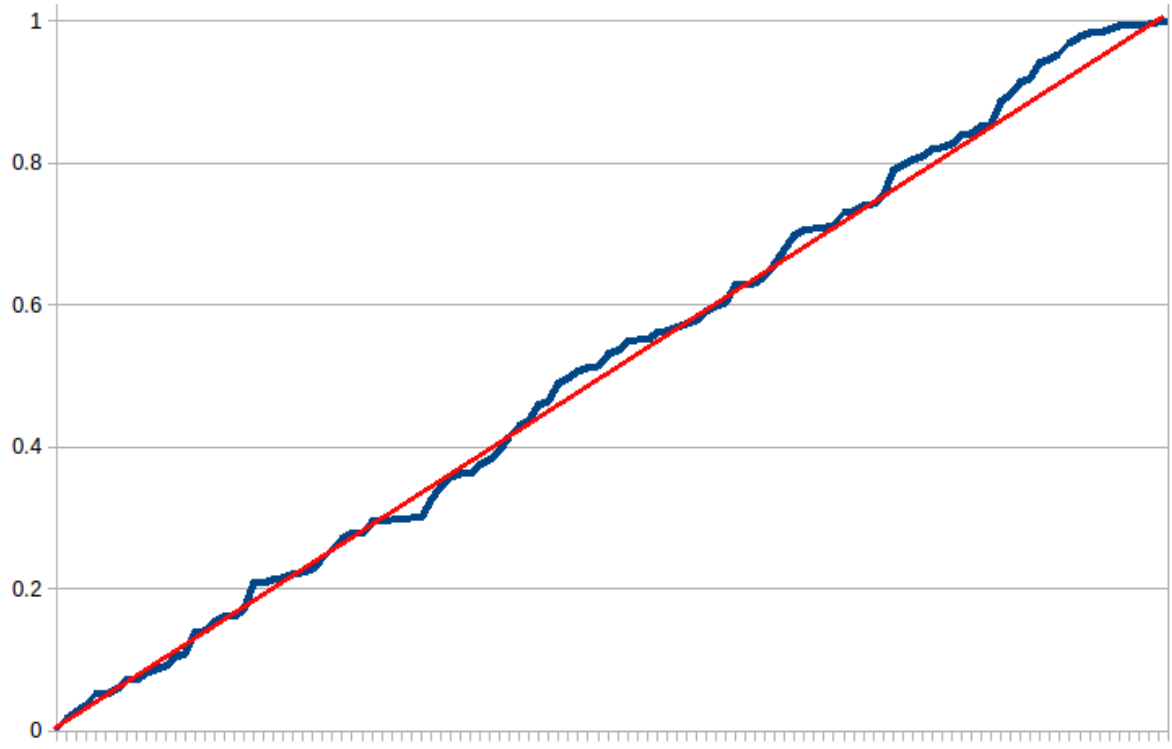
Na slikama 34,35,36,37 i 38. su prikazani reprezentativni rezultati ispitivanja po istoj metodologiji kao pri ispitivanju slika (potpuna baterija testova alata dieharder) u grafičkom obliku (preraspodela dobijenih p-vrednosti).



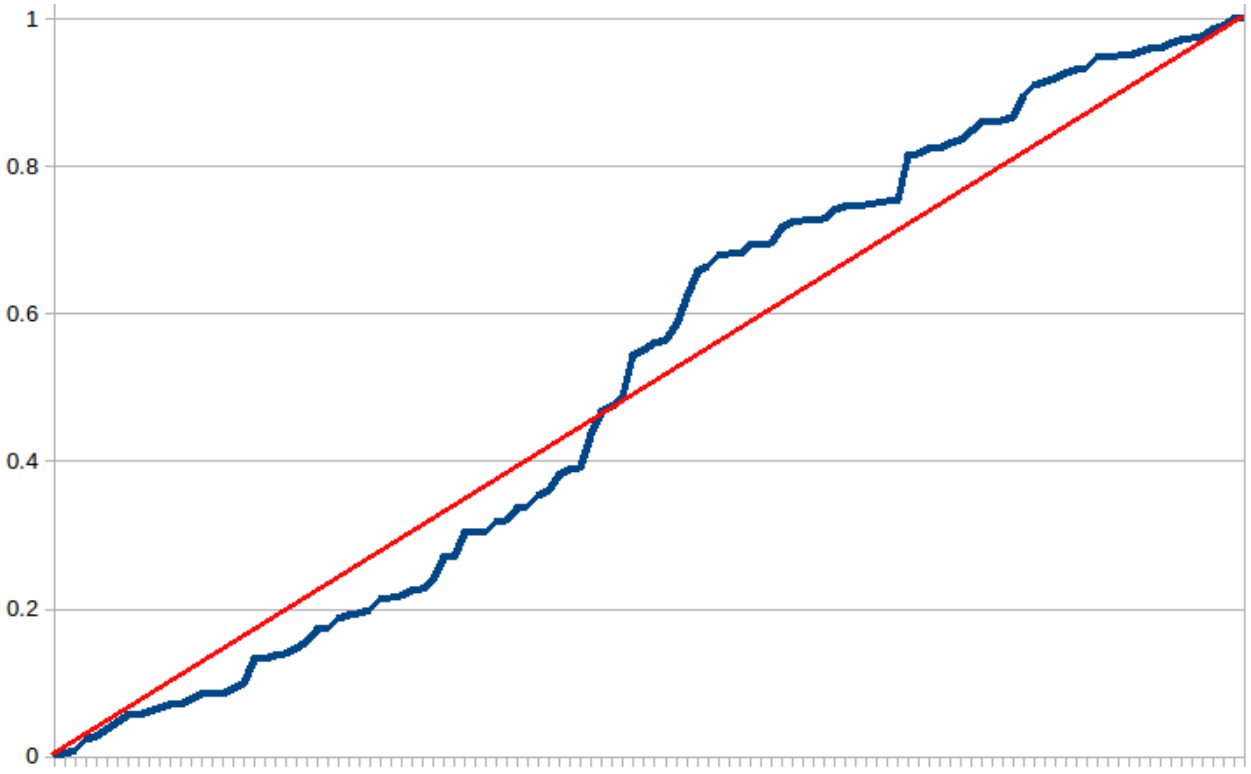

Slika 34. Grafik slučajne raspodele audio uzorka 1



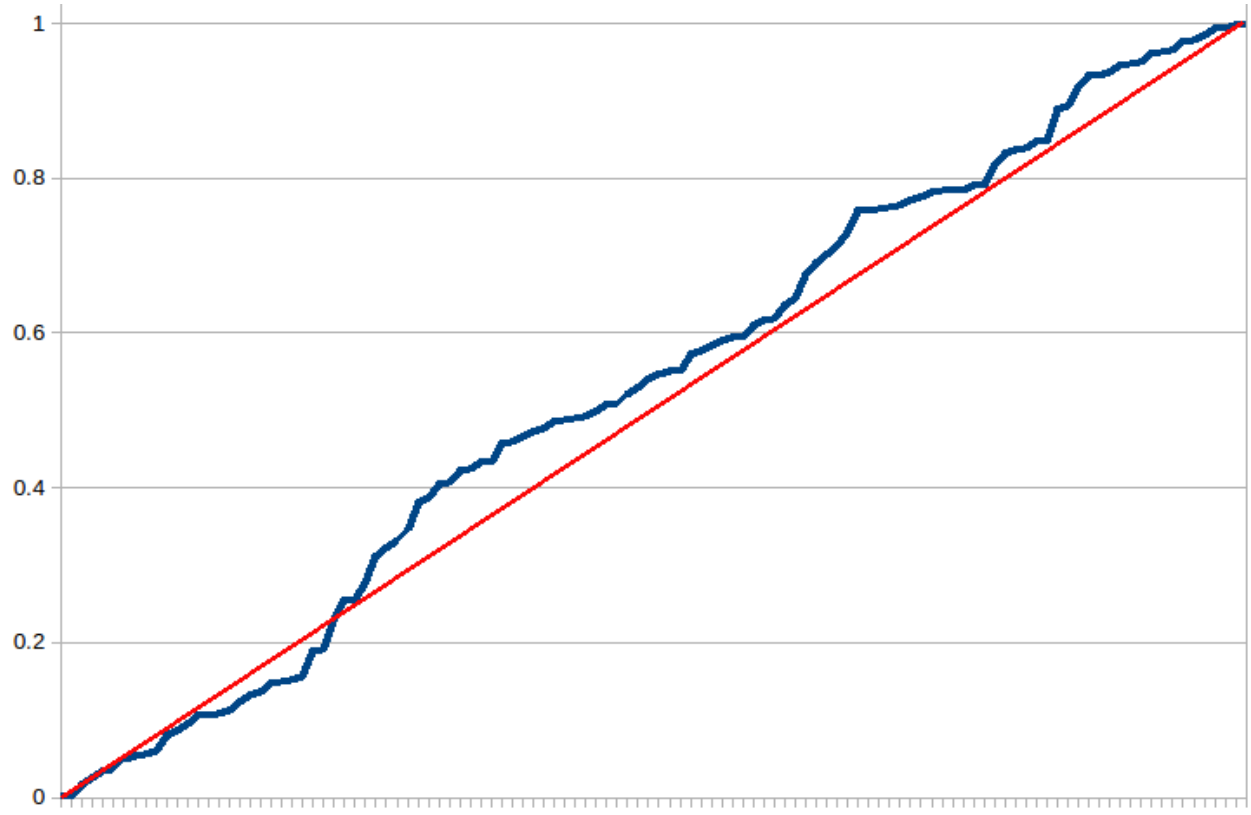

Slika 35. Grafik slučajne raspodele audio uzorka 2




Slika 36. Grafik slučajne raspodele audio uzorka 3




Slika 37. Grafik slučajne raspodele audio uzorka 4




Slika 38. Grafik slučajne raspodele audio uzorka 5

Iz priloženih rezultata ispitivanja, može se zaključiti da su mp3 audio fajlovi pogodni izvori nizova slučajnih vrednosti velike dužine. Oni se dakle mogu koristiti i kao dugački jednokratni ključevi u šifarskim sistemima.

### III.2.4 Video materijali kao izvor ključeva

Bez obzira što su ispitivanja pokazala da su slike i audio sadržaji u kompresovanim formatima pogodni za izvor jednokratnih ključeva šifarskih sistema, kada se radi o šifrovanju glasa oba prethodna izvora ipak imaju jedno značajno ograničenje: dužinu.

Kada bi se slike ili mp3 fajlovi koristili kao jednokratni ključevi za šifrovanje teksta, velika većina tekstova (u praksi skoro pa svi) bi bila moguća kvalitetno da se šifruje korišćenjem konkretne slike ili mp3 fajla, jer dužina poruka/uputstava čak i celih članaka (broj slova u konkretnom dokumentu) koji se prenose uz potrebe šifrovanja ne prelaze dužinu fajla koji sadrži konkretnu sliku ili audio fajl.

Međutim kod šifrovanja glasa u realnom vremenu, situacija je drugačija.

Konkretno, ako se za primer uzme jedan minut glasa, koji je digitalizovan sa frekvencijom uzorkovanja 22050Hz, 16-bit, što znači da jedna sekunda tako digitalizovanog glasa "zauzima" 44100 bajtova, ukupan broj bajtova jednog minuta tako digitalizovanog glasa je 60x44100= 2646000 bajtova. Ovo je često jednako ili veće od prosečne slike u nekom od često korišćenih kompresionih formata, odnosno u proseku polovina prosečne numere u mp3 formatu.

Uopšte formula za potrebnu dužinu kvalitetnog niza slučajnih vrednosti je:

$$D = \frac{f_s \times bitres}{8}$$

Gde je D=potrebna dužina ključa u bajtovima, $f_s$=frekvencija uzorkovanja glasa, bitres=rezolucija uzorkovanja A/D konvertera (8bit, 16bit, itd)

Ako pretpostavimo da prosečan razgovor traje nekoliko minuta, jasno je da je potreban duži jednokratni ključ od jedne slike ili zvučnog zapisa u kompresovanom formatu.

Video materijali su dakle, budući da je osnovno trajanje materijala u određenim uzorcima (dugometražni filmovi) i višesatno, a da su u današnje vreme aktuelni video materijali visoke rezolucije, fizička veličina fajlova koji sadrže takve video materijale čini ih više nego adekvatnim za korišćenje kao ključa za šifrovanje razgovora.

Temelje video kompresije je udario standard MPEG-2 1995. godine. Trenutno aktuelan je standard MPEG-4 AVC/H.264. On obuhvata više različitih tehnika za

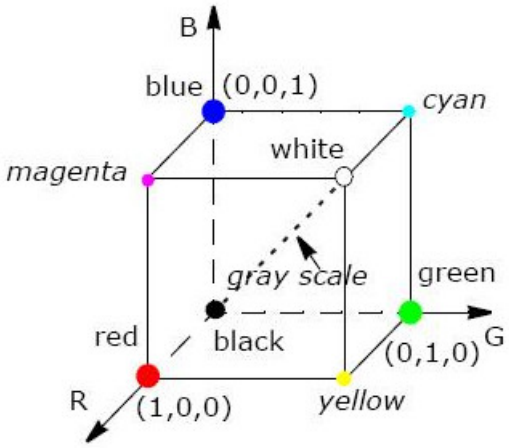
kompresovanje video materijala. Sam standard kompresije video zapisa je veoma kompleksna i velika oblast, i prevazilazi okvire teme ovoga rada, tako da će u njemu biti obrađeni i istaknuti samo oni, pre svega kvantitativni aspekti koji utiču na eliminaciju redudanse u rezultirajućem kompresovanom video materijalu, čime kvalitativno čine tako kompresovan video materijal upotrebljivim kao dugačkih nizova slučajnih vrednosti za jednokratne ključeve u šifarskim sistemima.

Osnovna premisa kompresije "pokretnih slika" je ponovo u izostavljanju "svega što se može izostaviti" bez vidnog narušavanja samog vizuelnog sadržaja. Ovde za razliku od psihoakustike, dolazi do izražaja moć opažanja ljudskog oka.

Prva bitna transformacija iz digitalne slike je transformacija slike iz RGB modela[] u YUV model[]. Naime, inicjialni model prikaza boja na računarskoj grafici je RGB model.

RGB model polazi od premise da se svaka boja iz vidljivog spektra može „dobiti" tj. prikazati na katodnom ekranu mešanim intenzitetom tri boje: Crvene (eng. **R**ed), Zelene (eng. **G**reen) i Plave (eng. **B**lue).

Na slici 39. [29] je prikazan vektorski RGB model boja.



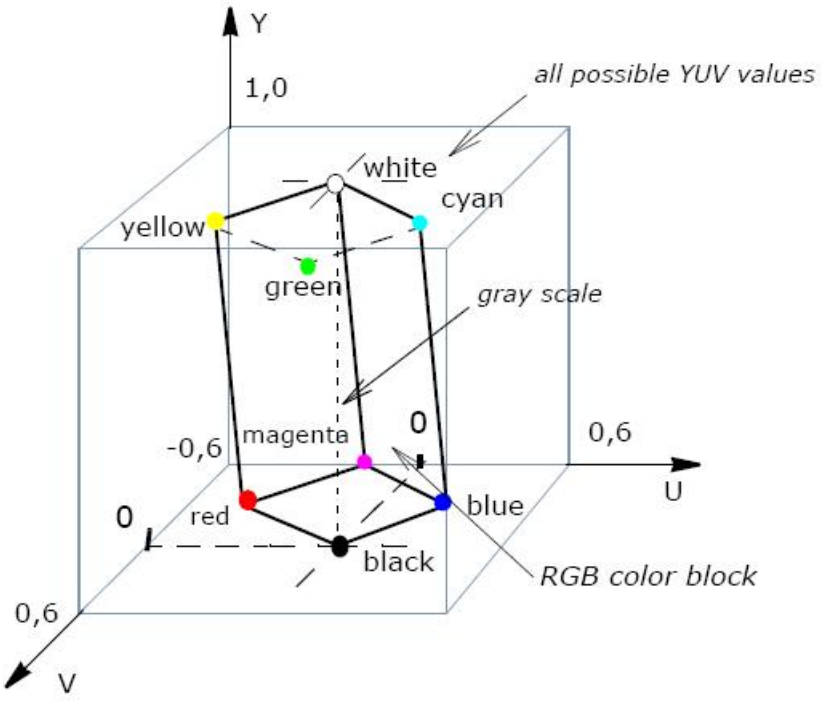

Slika 39. Vektorski RGB model boja

Ovaj model boja je zaista zadovoljavajući kako za prikaz statične slike na ekranu. Međutim, opet uvođenjem saznanja o percepciji ljudskog oka, dokazano je da je ljudsko oko mnogo osetljivije na svetlost nego na konkretnu nijansu boje.

Taj princip je primenjen još u začetku TV tehnike, gde se kod crno-belih TV prijemnika slika prenosila i prikazivala samo po nivo svetlosti, dakle crno, belo i sve nijanse sivog između njih.

Tako je nastao YUV sistem, čije komponente su "Luma" (Y-gama ili svetlo) i "Chroma" (UV-boja).

Na slici 40.[29] je prikazan vektorski YUV model boja:




Slika 40. Vektorski YUV model boja

U YUV sistemu boja se beleži „dvokomponentno“ (treća komponenta je osvetljaj) , za razliku od RGB modela koji beleži pojedinačnu boju koristeći 3 komponente.

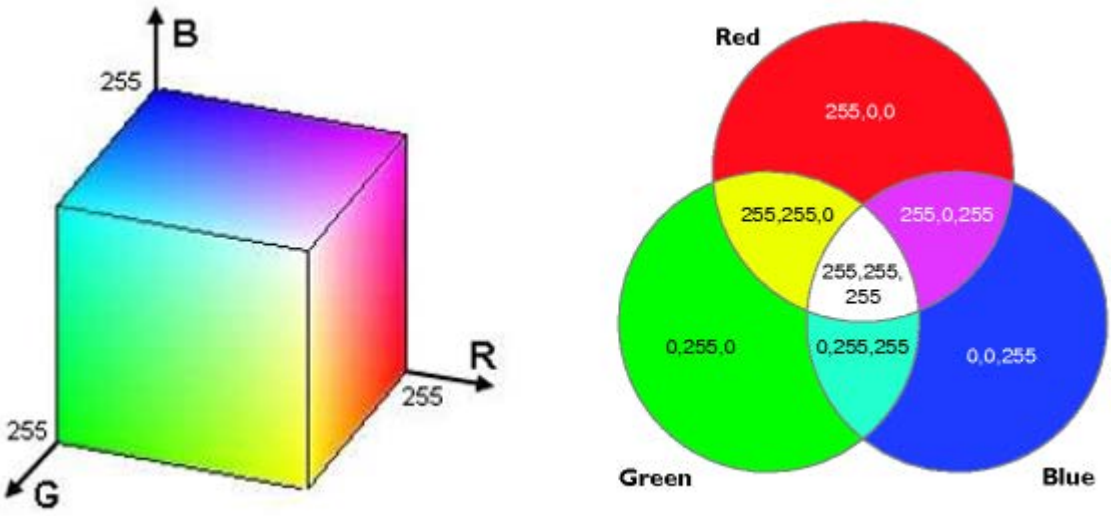
Konverzija RGB boje u YUV model se vrši po sledećim formulama:

$$Y = 0.299 \times R + 0.587 \times G + 0.114 \times B$$
$$U = -0.147 \times R - 0.289 \times G + 0.436B$$
$$V = 0.615 \times R - 0.515 \times G - 0.100 \times B$$

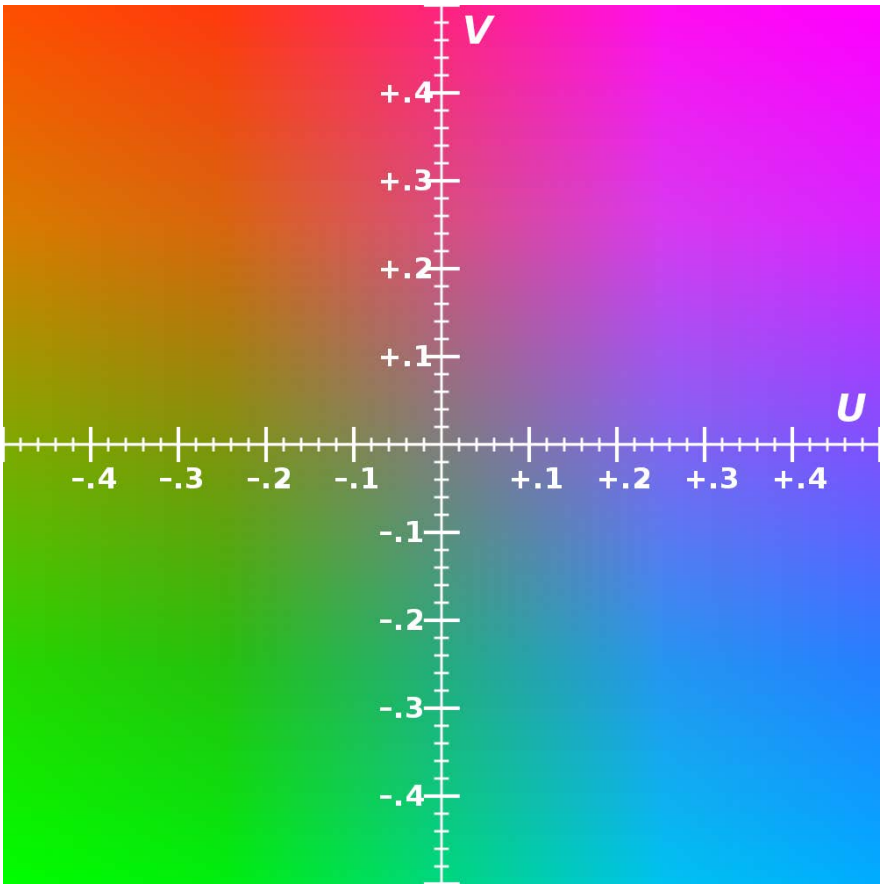
Konverzija pixel-a iz YUV modela u RGB model se analogno vrši po sledećim formulama:

$$R = Y + 1.140 \times V$$
$$G = Y - 0.394 \times U - 0.581 \times V$$
$$B = Y + 2.032 \times U$$

Sam smisao ovakve transformacije je razumljiviji ako se pogleda koordinatni prikaz RGB i YUV modela dat na slikama 41. i 42.




Slika 41. Koordinatni prikaz RGB modela



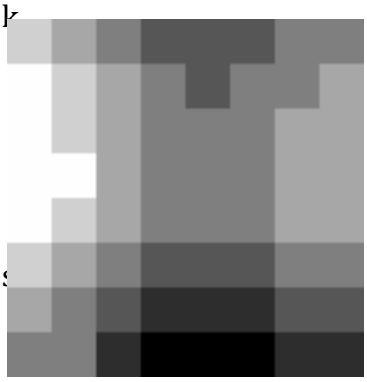

Slika 42. Koordinatni prikaz YUV modela

Osim ovakvog svođenja na manji broj podataka, kompresija video materijala koristi postojanje 2 osnovne redudantnosti koje eliminiše:

1. Vremenska redudansa (eng. temporal redundancy). Video materijal najčešće prikazuje 20-30 slika u sekundi (eng. frames per second –fps). Ako bi se takav video materijal pauzirao, i puštao po jednu sliku „na klik“, moglo bi se uočiti da su promene sadržaja dve sukcesivne slike najčešće neprimetne ili jedva primetne. Iako tako „gust“ uzorak upravo „srce iluzije pokretnih slika“, on ne mora biti tako skladišten da bi se ispravno reprodukovao rezultirajući istom iluzijom ljudskom oku. Naime umesto da se skladište podaci svih tačaka sa pojedinačnih slika sukcesivno, skladište se podaci o svim tačkama samo prve slike, a zatim samo podaci o onim tačkama koje su drugačije na sledećoj slici, čime se čini ogromna ušteda, i potpuno eliminiše redudansa (ponavljanje niza istih podataka).

2. Prostorna redudansa (eng. spatial redundancy) se ispoljava tako što je frekvencija promene boje pojedinih susednih tačaka veoma niska. Ovo znači da se u pojedinoj slici mogu uočiti čitavi „regioni“ slike koje čine tačke istovetne ili veoma slične boje. Konkretno kod MPEG-4 standarda koristi se DCT algoritam (eng. discrete cosine transform) na blokovima od 8x8 tačaka.

Primer kako DCT funkcioniše[30] može se dati na bloku od 8x8 tačaka uvećanih prikazanih na slici 43. Korišćenjem notacije 0=crno-255=belo, taj blok se može kvantifikovati kako je prikazano u tabeli 7.



Slika 43. Uzorak slike 8x8 tačaka

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 120 | 108 | 90 | 75 | 69 | 73 | 82 | 89 |
| 127 | 115 | 97 | 81 | 75 | 79 | 88 | 95 |
| 134 | 122 | 105 | 89 | 83 | 87 | 96 | 103 |
| 137 | 125 | 107 | 92 | 86 | 90 | 99 | 106 |
| 131 | 119 | 101 | 86 | 80 | 83 | 93 | 100 |
| 117 | 105 | 87 | 72 | 65 | 69 | 78 | 85 |
| 100 | 88 | 70 | 55 | 49 | 53 | 62 | 69 |
| 89 | 77 | 59 | 44 | 38 | 42 | 51 | 58 |

Tabela 7. Kvantifikovan uzorak

Formula za DCT transformaciju je sledeća:

$$F_{(u,v)} = \frac{C_u}{2}\frac{C_v}{2}\sum_{y=0}^{7}\sum_{x=0}^{7} f_{(x,y)} \times \cos\left[\frac{(2x+1)u\pi}{16}\right] \times cos\left[\frac{(2y+1)v\pi}{16}\right]$$

pri čemu su:

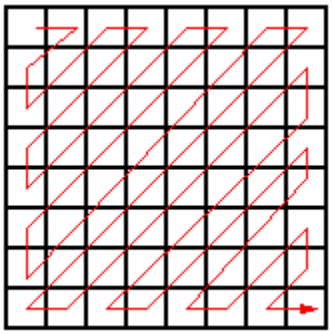
$$C_u = \begin{Bmatrix} \frac{1}{\sqrt{2}} & ako\ je\ u = 0 \\ 1 & \text{ako je u} > 0 \end{Bmatrix}, C_v = \begin{Bmatrix} \frac{1}{\sqrt{2}} & ako\ je\ v = 0 \\ 1 & \text{ako je v} > 0 \end{Bmatrix}$$

a $f_{(x,y)}$ je vrednosti (svetlosti) tačke na koordinatama x i y.

Primenom gornje transformacije na vrednosti iz primera date u tabeli 7., dobijaju se sledeći rezultati koji se takođe mogu prestaviti u tabeli 8x8, dati u tabeli 8.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 700 | 90 | 100 | 0 | 0 | 0 | 0 | 0 |
| 90 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| -89 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Tabela 9. Rezultat transformacije



Slika 44. ZigZag redosled obrade

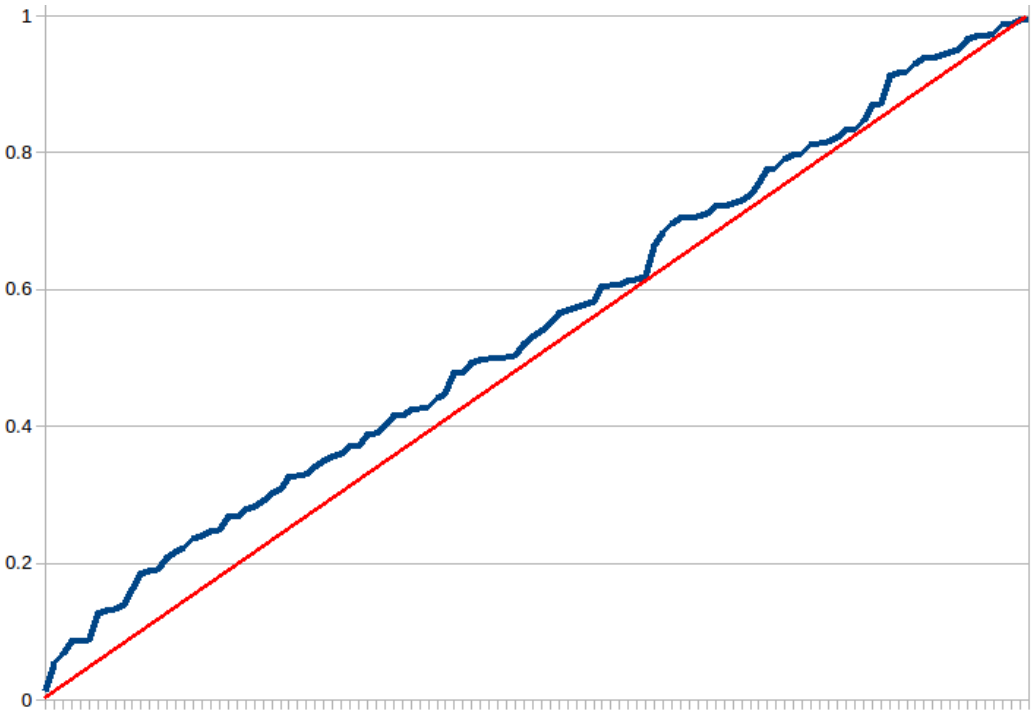
Uočljivo je da je samo 5 brojeva različito od nule. Zbog svojstva ovakve transformacije da su nule grupisane u desnom-donjem delu, odnosno relevantne vrednosti u gornjem-levom delu, vrednosti se serijski upisuju u rezultirajući niz u cik-cak porektu prikazanom na slici 44[30]. Naravno nule se ne upisuju u rezultirajući niz nego se kraj regiona markira sa specijalnom vrednošću koja označava kraj bloka (eng. end of block).

Na ovaj način umesto 64 (8x8) vrednosti, skladišti se samo 5, što je ogromna ušteda, a vizuelni gubitak je zanemarljiv, tj. subjektivno neuočljiv.

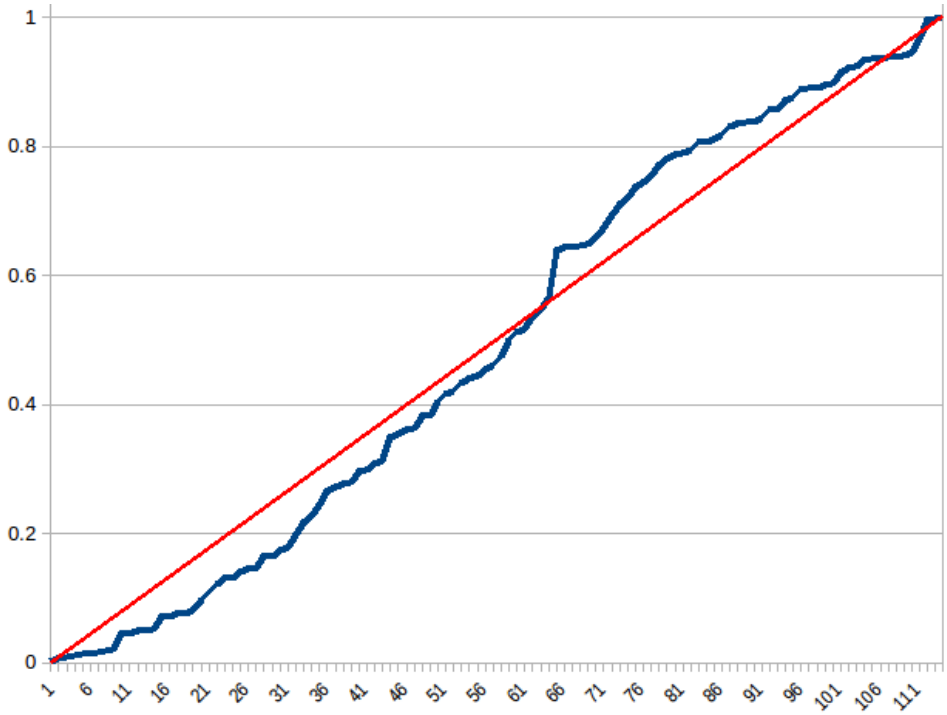
Naravno, na ovaj metod koji koristi eliminaciju prostorne redudanse, nadovezuje se standardni model kompresije, te ako se cela pojedinačna slika (scena) sastoji od više istovetnih ili dovoljno (vizuelno) sličnih blokova, oni se neće ponavljati u rezultirajućem nizu, i kada se na ovo sve primeni i metod eliminacije vremenske redudanse (ako se u sledećoj slici (sceni) ili više njih ponavlja istovetan ili dovoljno (vizuelno) sličnih blokvoa, opet se neće ponavljati, tako da je rezultirajući veoma dugački niz vrednosti sa veoma niskom, skoro nepostojećom redudansom (ponavljanjem) što je osnovni kriterijum slučajnog niza.

Korišćenjem baterije testova dieharder alata, testirano je 10 uzoraka video materijala, različitog sadržaja i kvaliteta (rezolucije) od najniže do Full HD rezolucije. Ispitivani video materijali su priloženi na pratećem CD-u, u folderu “materijali za ključeve”, podfolder “video” , a rezultati testiranja u podfolderu “rezultati” u .xlsx fajlovima istovetnog naziva.

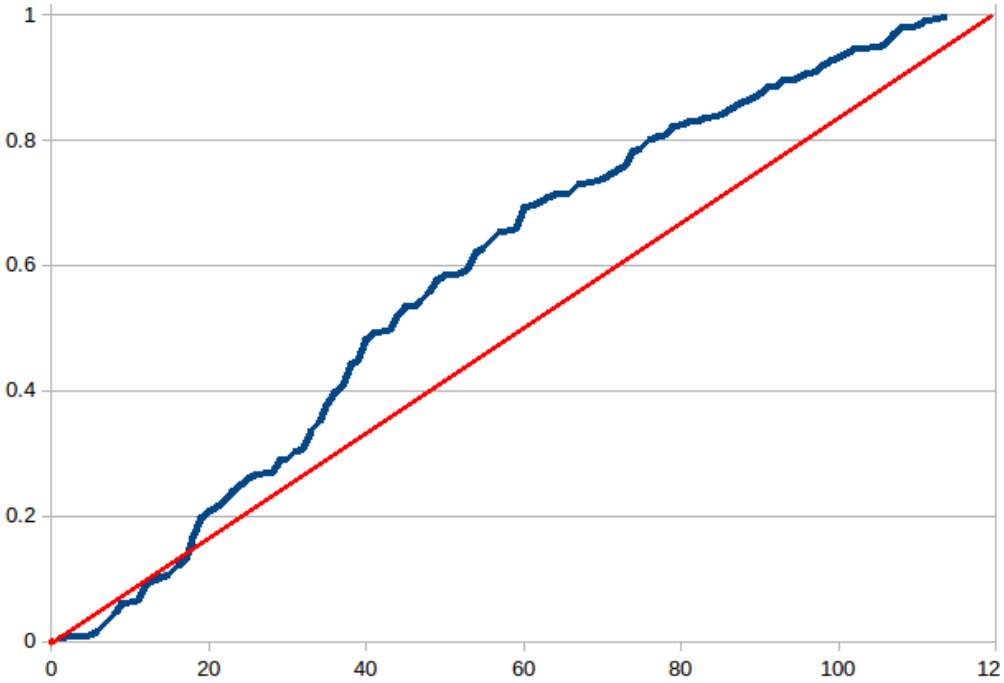
Karakteristični rezultati u obliku grafikona dobijenih p-vrednosti dati su na slikama 45-49.



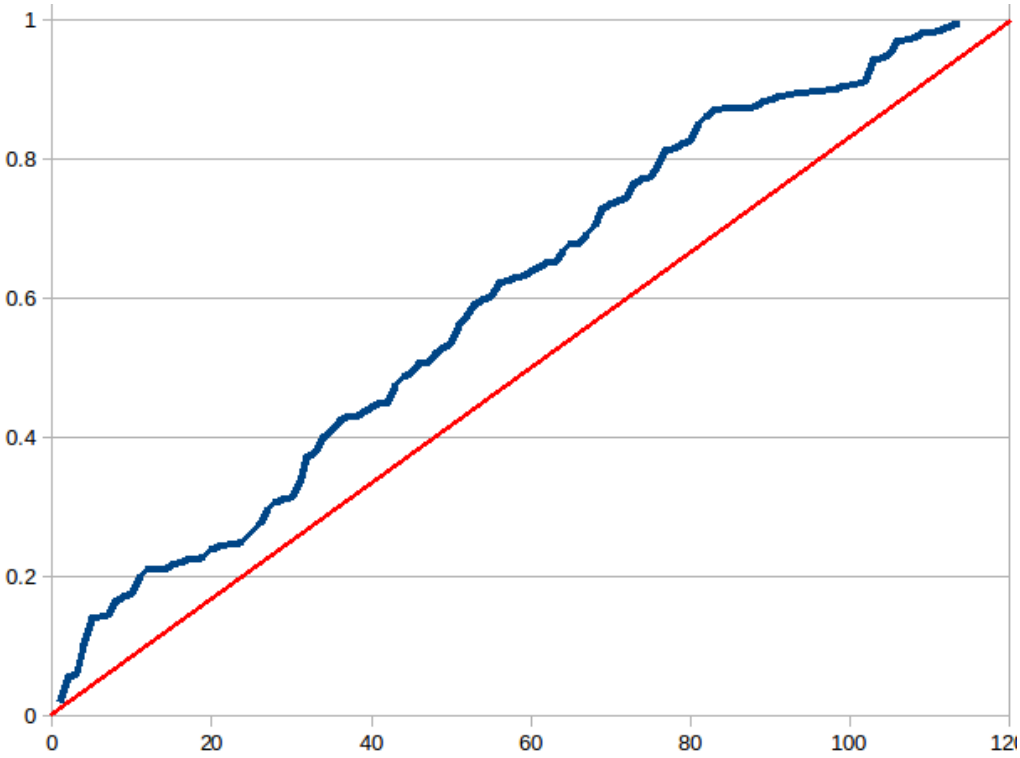

Slika 45. Grafik slučajne raspodele video uzorka 1



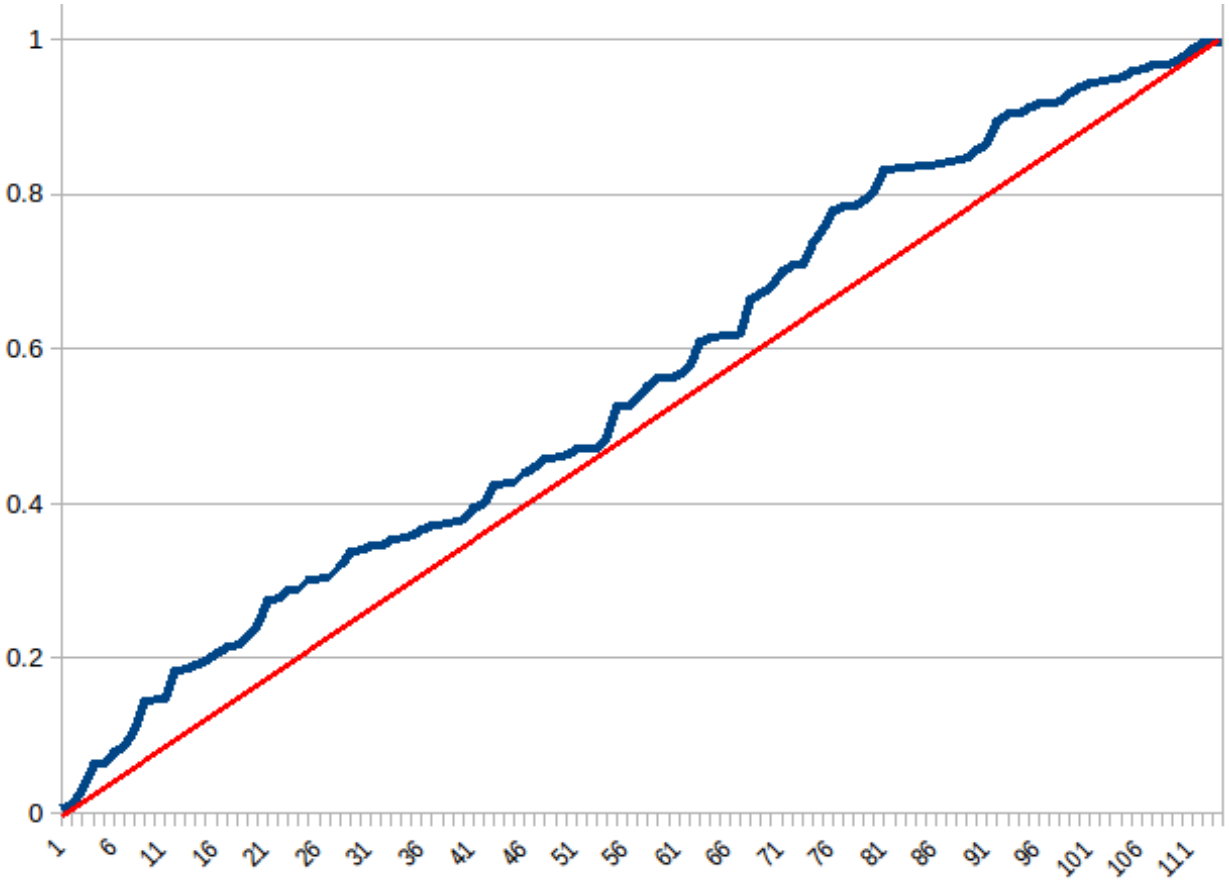

Slika 46. Grafik slučajne raspodele video uzorka 2




Slika 47. Grafik slučajne raspodele video uzorka 3




Slika 48. Grafik slučajne raspodele video uzorka 4




Slika 49. Grafik slučajne raspodele video uzorka 5

# IV POSTAVKE SISTEMA ŠIFROVANE KOMUNIKACIJE

Da bi se uspostavila veza između dva sagovornika na internetu, potrebno je da obe strane znaju "adresu" druge strane. U ovom slučaju IP adresu sagovornika. Budući da ceo sistem gubi na značaju (a i na sigurnosti) ako je makar jedna strana, a svakako ako su obe strane "stacionarne", tj. sa fiksnim, unapred poznatim IP adresama. Ovo otvara neograničene mogućnosti kako presretanja i naknadne analize saobraćaja, kako i za razne oblike DoS (eng. denial of service) napada.

Dakle, polazna premisa po ovom pitanju je da su oba sagovornika u ovom sistemu mobilna, sa nekim nasumičnim IP adresama koje im je u tom trenutku dodelio njihov mobilni operater/interet provajder.

Tehnički tu je potrebno rešiti tri zadatka:

1. Omogućiti međusobno "pronalaženje" sagovornika
2. Omogućiti da se sagovornici po iniciranju razgovora usaglase o šifarskom ključu koji će koristiti
3. Omogućiti da se šifrovana komunikacija transportuje direktno između sagovornika, bez posrednika u oba smera.

Na ovaj način se izbegava funkcija posrednika-"telefonske centrale" kroz koju prolazi sav saobraćaj i koja je idealna "tačka napada" . Ukratko, **ne može se izvršiti napad na ono što ne postoji.**

Takođe, izuzetno osetljiva je faza iniciranja komunikacije u kojoj se strane učesnici u razgovoru usaglašavaju o upotrebi konkretnog šifarskog ključa. Sam ključ, po pravilu ne sme biti predmet komunikacije, već samo neko interno obeležje koje jednoznačno identifikuje ključ, da bi obe strane mogle ispravno da dešifruju primljeni sadržaj koji je adekvatno šifrovan. U nastavku rada biće detaljno obrađena sva tri gore pomenuta zadatka i predloženo adekvatno rešenje za svaki od njih.

## IV.1. "LOCIRANjE SAGOVORNIKA"

Kada u klasičnoj komunikaciji neko želi da uspostavi vezu sa nekim drugim on na uređaju bira njegov broj telefona. Kada računarski program želi da komunicira preko interneta sa drugim programom on mora znati IP adresu uređaja na kome je pokrenut taj drugi program.

Budući da su adrese na mobilnim uređajima po pravilu dinamičke (ne fiksne, znači često i nikako predvidljivo promenjive), potrebno je da negde postoji treći program koji će da vodi evidenciju o svakoj instanci određenog programa, na kojoj IP adresi se nalazi u realnom vremenu. Taj treći program pak mora biti na nekoj fiksnoj IP adresi, tako da svaki pojedinačni program za komunikaciju može da mu se direktno obrati i time mu prosledi svoju IP adresu, a da može od njega da dobije i trenutnu IP adresu bilo koje druge instance komunikacionog programa iz tog sistema.

Ovakav pristup nije nov i rasprostranjeno se koristi u p2p i VoIP programima (Skype, Viber i sl.). **Međutim ovakav pristup bi očigledno bio neprihvatljiv za sistem šifrovane komunikacije**, jer bi postojanje programa -"centralnog registra" na fiksnoj IP adresi bio potpuni bezbednosni propust.

Postojanje takvog "centralnog registra" na fiksnoj IP adresi bi odmah i bez dodatnog truda napadaču dalo podatke o IP adresama svih korisnika sistema, što otvara vrata za nebrojene napade navedene u uvodnom razmatranju IV glave ovog rada.

Dakle da bi se ispunio prvi zadatak tj. bezbedno se pojedini učesnici u komunikaciji informisali o IP adresama drugih učesnika u šifrovanoj komunikaciji, pošto se postojanje "centralnog registra" tehnički ne može izbeći, mora se izbeći da taj "centralni registar" bude javno dostupan, tj. mora se sakriti njegova lokacija, čime se onemogućava ozbiljna bezbednosna degradacija celog sistema.

Da bi sigurnost sistema bila podignuta na još viši nivo, može se postaviti i dodatni "podzadatak", tj. zahtev da u slučaju da jedan od sagovornika (uređaj, program, korisnik, nebitno) padne u "neprijateljske ruke", bilo voljno ili silom, lokacija "centralnog registra" se **ne može saznati** korišćenjem sledećih metoda:

- reverznim inženjeringom programa
- pokretanjem programa pa nadziranjem njegovog saobraćaja tj. obraćanja "centralnom registru"
- Dobijanjem informacija o načinu korišćenja od korisnika uređaja/programa

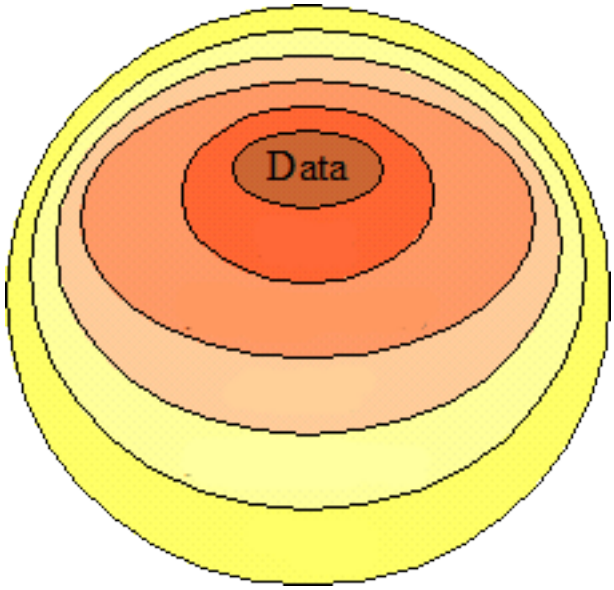
Na ovaj način, sistem postaje veoma pouzdan i onemogućena je njegova "provala" kao sistema u slučaju da jedan ili bilo koliko korisnika sistema/uređaja/programa dospe u "neprijateljske ruke".

Tehnička podloga za rešenje ovog zadatka već postoji, nije striktno razvijana za ove potrebe, ali je idealno jer ispunjava sve gore navedene uslove. Radi se o protokolu "skrivenih servisa" (eng. hidden services)[31] u okviru Tor mreže[32].

### IV.1.1 TOR –ISTORIJAT I PRINCIP RADA

Tor je nastao kao projekat Američke pomorske obaveštajne službe, pod imenom „Onion routing" (Onion=crni luk (eng)). Kao takav je patentiran 1998. Godine.

2004. godine javnosti je prezentovana 2. generacija onion routing-a[32]. Ceo koncept je u suštini koristio mehanizam „višestruko zatvorenih adresiranih koverti". Otud aluzija na glavicu crnog luka koja u svom poprečnom preseku ima više slojeva, kao što je ilustrovano na slici 50[33].



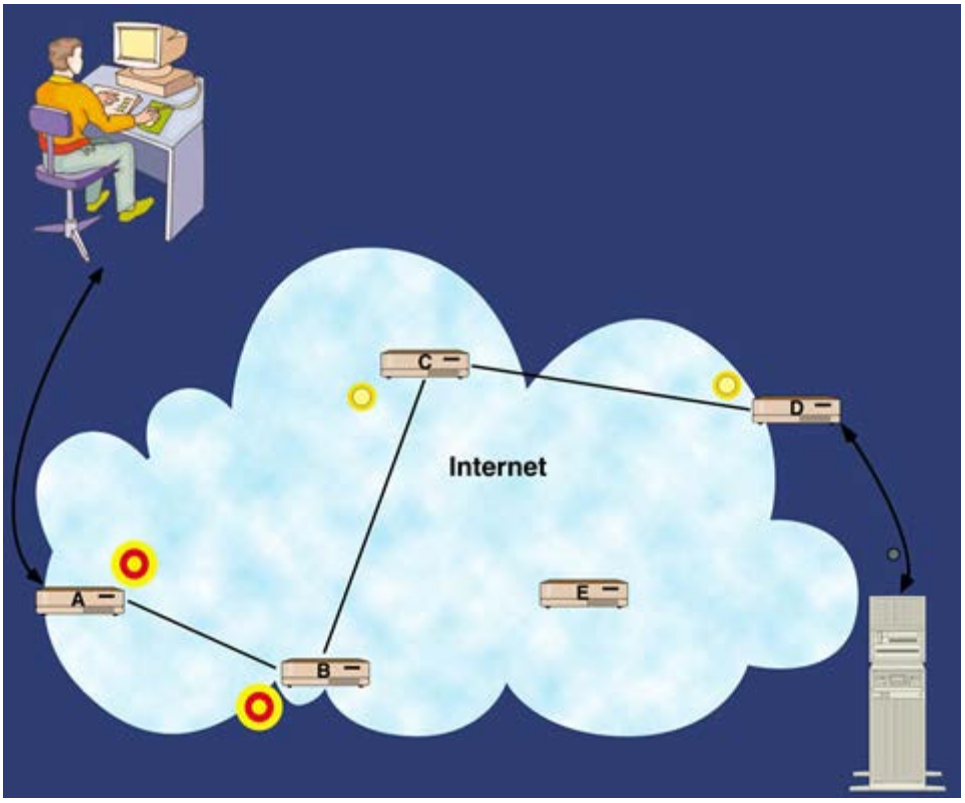

Slika 50. Prikaz višeslojnog šifrovanja u Onion Routing-u

Iz priložene ilustracije lako se može uočiti da oko samog podataka koji se prenosi kroz Tor mrežu, postoji više slojeva zaštite, konkretno šifrovanja. Dakle, podatak je n-puta šifrovan, i toliko puta će biti dešifrovan do svoga konačnog odredišta.

Analogni primer iz stvarnog sveta bi bio kada bi se neka poruka zapisala na papir koji bi zatim bio zapakovan u kutiju koja bi bila obezbeđena katancem od koga ključ ima samo krajnji primalac poruke. I na kutiji bi se napisala adresa primaoca iste. Zatim bi ta kutija bila spakovana unutar sledeće kutije sa sledećim katancem od koga ključ ima samo posredni kurir koji će odneti poslednju kutiju do konačnog odredišta.

Taj postupak bi se ponavljao još nekoliko puta, i to bi rezultiralo sa jednom kutijom koja je obezbeđena katancem od koga ključ ima samo prvi kurir koji preuzima tu kutiju od pošiljaoca. On po prijemu kutije, svojim ključem može samo da otvori tu kutiju i da sledeću kutiju unutar "svoje" kutije prosledi na adresu sledećeg kurira. Na ovaj način samo prvi kurir može da ima saznanje o pošiljaocu poruke, ali ne i o krajnoj destinaciji iste niti o sadržaju iste. Takođe poslednji kurir u lancu može da ima saznanje o primaocu poruke, ali ne i o izvornom pošiljaocu niti o sadržaju iste. A svi ostali kuriri u lancu mogu samo da znaju od kog kurira su je dobili i kom kuriru su je isporučili.

Primer ovakvog lanca je dat na slici 51[33].




Slika 51. Primer Tor lanca

Ovakav "lanac" prenosa poruke onemogućava jednostavan nadzor pošiljaoca ili primaoca "od interesa". Npr. ako bi bezbednosna služba neke zemlje želela da zna ko sve sa njene teritorije razmenjuje podatke sa nekom obaveštajnom agencijom neke druge zemlje, sve što bi trebala da učini je da beleži sve internet konekcije sa svoje teritorije prema određenim serverima u inostranstvu. Međutim ako pojedinci takve komunikacije vrše kroz Tor mrežu nikada direktno ne stupaju u kontakt sa "inkriminišućim serverima", ovakav način "pecanja" strane agenture je onemogućen u potpunosti.

### IV.1.2 TOR SKRIVENI SERVISI

Međutim za potrebe "tajnog centralnog registra", jedan poseban protokol Tor mreže je izuzetno pogodan: Tor hidden services. Ovaj protokol omogućava sledeće:

- Da se neki server/servis postavi na internetu, i da mu se može pristupiti kroz Tor mrežu bez saznanja IP adrese samog servera
- Korisnici se konektuju na ovaj server/servis preko „tačke sastanka" (eng. rendezvouz point) tako da nemaju saznanje o samoj lokaciji (IP adresi) servera, a pritom ne odaju ni svoju lokaciju (IP adresu).
- Svi podaci koji se prenose od klijenta/korisnika ka serveru/servisu i u suprotnom smeru su višestruko šifrovani i postoji više Tor čvorova između korisnika i tačke sastanka i od tačke sastanka do servera.
- Sama serverska aplikacija/servis je potpuno transparentno izložena Tor mreži. Ovo znači da se postojeći serverski softver koji se želi koristiti kao hidden service može koristiti bez ikakvih izmena programskog koda.

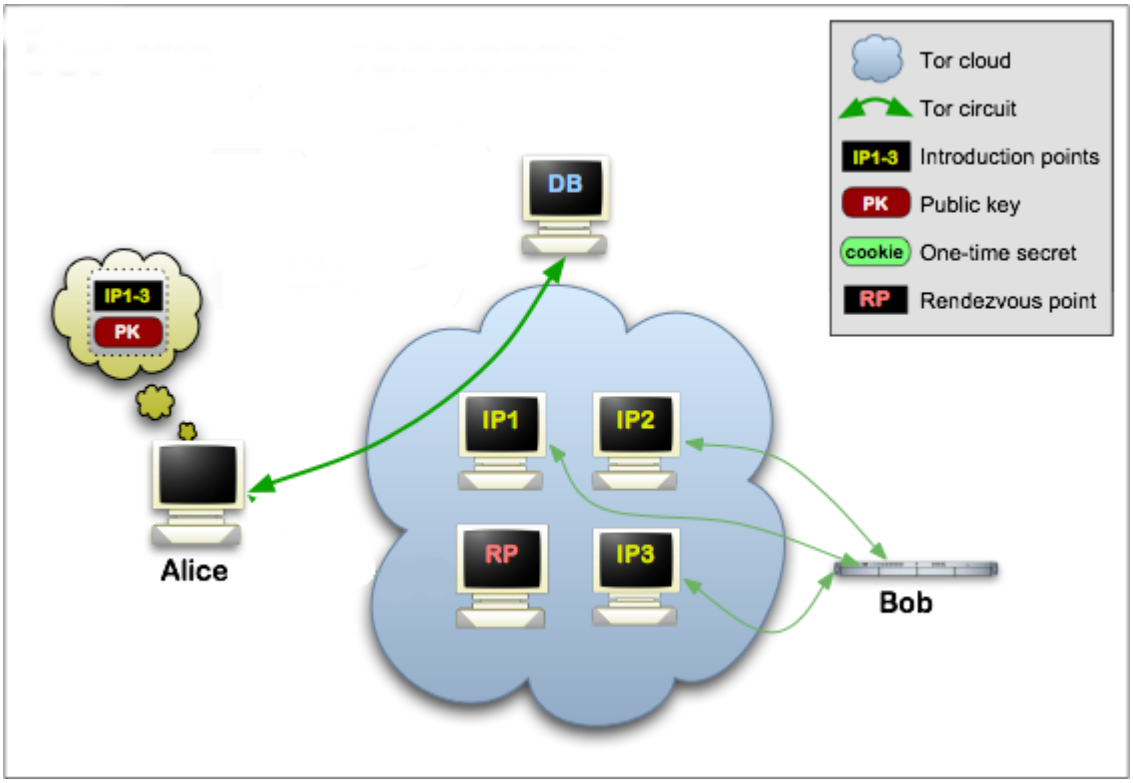
Ovo je maksimalno uprošćeno opisan ovaj protokol[34]. Da bi se potpuno opšte razumeo način funkcionisanja ovog protokola, potrebno je definisati nekoliko pojmova iz opšte Tor mreže:

- OP-Onion proxy ili Tor klijent. Softver koji je istovremeno „priključak" određenog računara na Tor mrežu istovremeno vrši funkciju opšteg Tor čvora, kroz koga će prolaziti i saobraćaj drugih Tor klijenata, mimo njegove kontrole/izbora.
- Tačka kontakta (eng. Introduction point)–srednjeročno odabrani čvorovi Tor mreže na kojima se Tor klijenti mogu obratiti (samo za inicijalni kontakt) određenom skrivenom servisu.
- Tačka sastanka (eng. eng. rendezvouz point) –jednokratni nasumično odabrani Tor čvor koji radi kao relejni prenosnik podataka između dva Tor lanca (klijenta i servera).
- "Onion adresa" skrivenog servera. U literaturi poznata i kao deskriptor skrivenog servera/servisa. Ona je u fiksnom formatu XXXXXXXXXXXXXXXX.onion:port, i ne može se korisnički birati, već se automatski generiše prilikom inicjalnog kreiranja skrivenog servera na samom serveru. Sastoji se od 16 karaktera koji su izvedeni iz generisanog javnog ključa skrivenog servera, zatim ekstenzije .onion i IP porta na kome skriveni servis "očekuje konekciju".
- Javni ključ skrivenog servera, koji se automatski generiše prilikom inicjalnog postavljanja(objavljivanja) skrivenog servera na Tor mreži.

- Privatni ključ skrivenog servera, koji se generiše u paru sa svojim javnim ključem. Princip korišćenja javnog/privatnog servera je identičan načinu kako to funkcioniše sa parom javni/privatni ključ definisanim u RSA algoritmu[35].
- Jednokratna tajna, kojom se klijent štiti od lažnog „skrivenog servera“.
- Tor lanac –Lanac od više Tor čvorova kojim poruka putuje od pošiljaoca do primaoca, „umotana“ u onoliko slojeva šifrovanja/adresovanja koliko čvorova ima u lancu.

Detaljan opis uspostavljanja komunikacije klijenta sa skrivenim serverom je dat u nastavku sa ilustracijama[36]

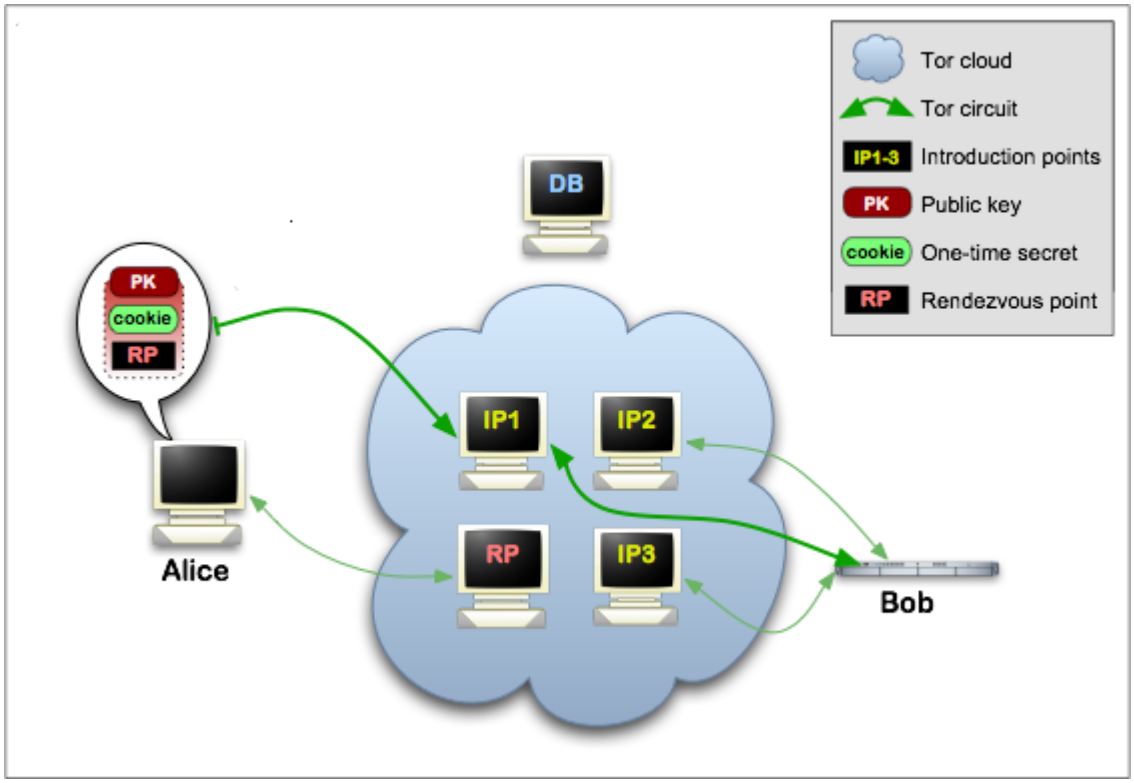
1. OP klijenta znajući samo onion adresu skrivenog servera se obraća jednom od više javno dostupnih “Tor imenika” (eng. directory authority). U slučaju da je onion adresa validna, i server aktivan, klijent dobija javni ključ skrivenog servera i više mogućih “tačaka kontakta” kako je prikazano na slici 52.




Slika 52. Uspostavljanje bezbedne komunikacije sa Tor hidden service-om 1. Korak

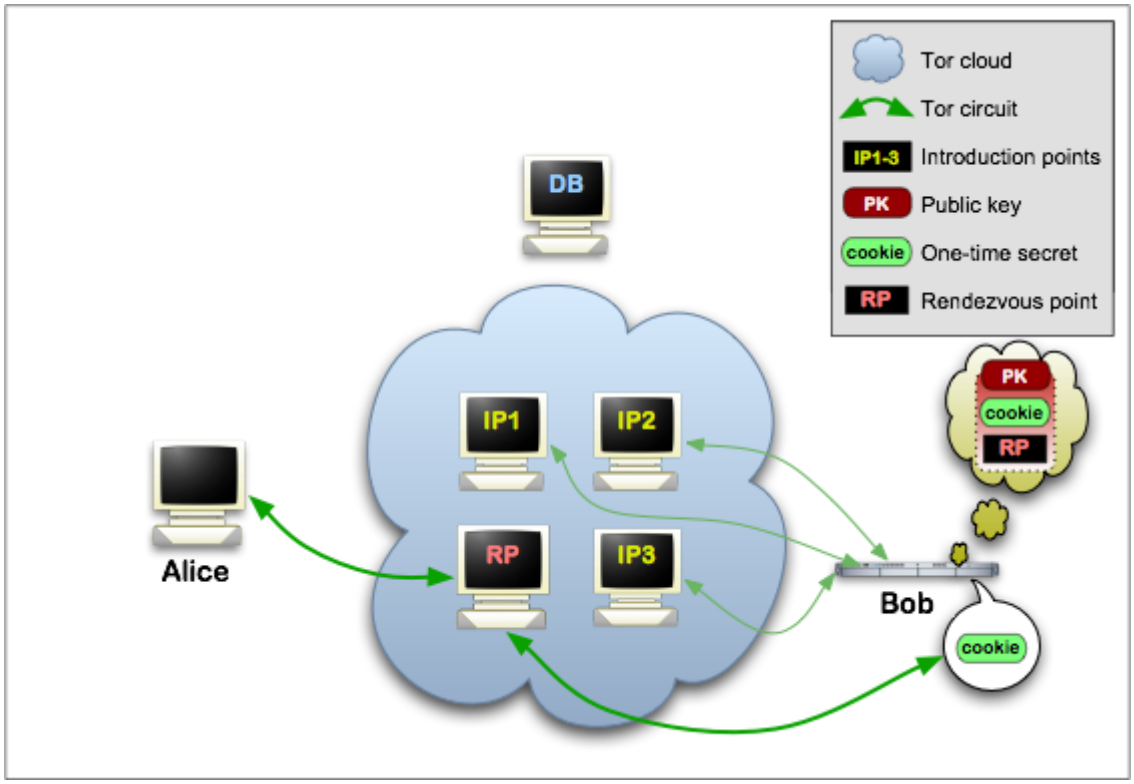
2. Klijent odabira tačku sastanka, kreira “uvodnu poruku” koja sadrži IP adresu predložene tačke sastanka (nasumično je bira klijent) i jednokratnu tajnu. Cela uvodna poruka se šifruje javnim ključem skrivenog servera i biva prosleđena slučajnim Tor lancem do jedne od tačaka kontakata skrivenog servera. Na ovaj način se osigurava da se IP adresa skrivenog servera ne otkriva učesnicima u lancu komunikacije. I sam skriveni server

je različitim tor lancima povezan sa svakom od svojih tačaka kontakta. Istovremeno klijent šalje uvodnu poruku koja sadrži jednokratnu tajnu do odabrane tačke sastanka, opet šifrovanu sa javnim ključem skrivenog servera, a kroz nasumično formirani Tor lanac.. (slika 53.)




Slika 53. Uspostavljanje bezbedne komunikacije sa Tor hidden service-om 2. Korak

3. Skriveni server dobija šifrovanu uvodnu poruku od klijenta preko Tor lanca od svoje tačke kontakta, dešifruje je svojim privatnim ključem, i tako saznaje IP adresu tačke sastanka i jednokratnu tajnu. On zatim uspostavlja svoj slučajni Tor lanac prema tačci sastanka i kroz njega šalje jednokratnu tajnu tačci sastanka. Tačka sastanka pošto uporedi jednokratnu tajnu dobijenu nezavisnim Tor lancima od klijenta i od skrivenog servera, i utvrdi njihovu identičnost postaje samo relej između dva postojeća Tor lanca klijenta i skrivenog servera (slika 54.)



Slika 54. Uspostavljanje bezbedne komunikacije sa Tor hidden service-om 3. Korak

Na ovaj način klijent može da komunicira sa serverom, bez znanja lokacije servera, što je od značaja za predmetnu primenu. Štaviše neograničen broj klijenata može simultano razmenjivati podatke sa tako "skrivenim" serverom, bez mogućnosti otkrivanja njegove IP adrese. Takođe sam sadržaj komunikacije je višeslojno šifrovan, i time realno više nego dobro zaštićen od analize sadržaja, te je ovakav vid komunikacije pogodan i za razmenu poverljivih podataka koji su takođe zaštićeni od svake "zainteresovane treće strane".

## IV.2. RAZMENA/SINHRONIZACIJA ŠIFARSKOG KLjUČA

Koliko god bili značajni algoritmi šifarskog sistema i sam šifarski ključ, način odabira jednokratnog ključa kod obe strane u komunikaciji i njihovo saopštavanje je proces od jednake vitalne važnosti za sigurnost samog šifarskog sistema. Budući da je u uvodnom razmatranju o šifarskim sistemima rečeno da je sistem "jednokratne" beležnice idealno siguran šifarski sistem, a materijala za ključeve ima dovoljno kako je pokazano u III odeljku, preostaje još samo rešenje sigurnog "ugovaranja" jednokratnog ključa za svaku pojedinačnu komunikaciju dve strane, i to samo jedinstvene dve strane.

Na ovaj način se obezbeđuje dodatna "bezbednosna izolacija" u slučaju delimične provale sistema. Ako npr. jedan uređaj/klijent padnu u neprijateljske ruke, može biti kompromitovana samo komunikacija tog uređaja/klijenta sa njegovim parom. Onoga trenutka kada se prestane verovati uređaju/klijentu, isti biva "isključen iz mreže sigurnih sagovornika" i više nema pristup sistemu.

U datom predloženom rešenju, odabir jednokratnih ključeva funkcioniše na sledećim principima:

1. Svi korisnici moraju imati ključeve "na gotovs", uskladištene na svojim lokalnim uređajima vremenski izolovano od same komunikacije. Ovo je bitno iz dva razloga: 1. Ne koristi se transportni komunikacioni kanal tj. njegov kapacitet se ne zauzima za vreme komunikacije, te je komunikacioni kanal u potpunosti slobodan za prenos šifrovanog glasa. 2. Ozbiljan bezbednosni propust bi bio da se "u etru" tj. neobezbeđenom komunikacionom kanalu simultano transportuju i šifrat i ključ, budući da je tajnost šifarskog sistema bazirana na ključu.
2. "Centralni registar" osim što vodi evidenciju korisnika, vodi i centralnu evidenciju o šifarskim ključevima. Ova evidencija obuhvata:
   - ID ključa (interno dodeljeni jedinstveni broj)
   - Tačan link do samog ključa (pogodnog materijala na internetu)
   - Kontrolni verifikacioni kod sadržaja ključa. U suštini to je 128-bitna vrednost sračunata po MD5 algoritmu[37] koja može da se koristi kao digitalni otisak prsta određenog sadržaja na osnovu koga se može proveriti/potvrditi identitet odnosno nepromenjivost sadržaja.

   U posebnoj evidenciji centralni registar bi vodio evidenciju „upotrebljenih ključeva", tako da se ne bi desilo da bilo koji klijent bilo kada ponovo upotrebi ključ koji je već jednom iskoristio.
3. Kada bilo koji pojedinačni klijent „prijavljuje na sistem", on centralnom registru prosleđuje svoj alias i IP adresu na kojoj je aktivan. Takođe, klijent proverava da li u svojoj memoriji ima spreman šifarski ključ. Ako ga nema, on se obraća centralnom registru za dodelu ključa. Centralni registar nasumično bira odgovarajući

materijal na internetu, računa njegov MD5 potpis, i sve to skladišti u svojoj evidenciji kao novi raspoloživi ključ. On zatim prosleđuje link i rezultirajući MD5 potpis klijentu.

Budući da se sva ova komunikacija obavlja kroz Tor mrežu, svi komunikacioni paketi koji sadrže ove poverljive podatke putuju kroz internet višeslojno šifrovani, i svaki put različitom putanjom, te nisu izloženi napadu.

Klijent po dobijanju „dodeljenog ključa“ započinje preuzimanje tog materijala sa interneta. Ovo se ne dešava kroz Tor mrežu, već direktno, ali pristup pojedinačnog klijenta nekom randomalnom multimedijalnom sadržaju na internetu je samo jedan od milijardu takvih simultanih pristupa multimedijalnim sadržajima, praktično „zrno peska u pustinji“, i verovatnoća da napadač uspe da uoči i izdvoji baš taj inkriminišući pristup na osnovu koga bi došao do ključa je jednaka šansi da se u pustinji uoči i izdvoji baš određeno jedinstveno zrno peska. Takođe prenos veće količine podataka preko Tor mreže je veoma spor i neefikasan.

Po završetku preuzimanja dodeljenog sadržaja klijent izračunava MD5 potpis preuzetog sadržaja, i upoređuje ga sa MD5 potpisom dobijenim od centralnog registra. U slučaju da se MD5 potpisi ne slažu, klijent o tome obaveštava centralni registar.

Centralni registar po prijemu obaveštenja da se MD5 potpis određenog opredeljenog šifarskog ključa razlikuje, što može biti iz nekih sporednih legitimnih razloga (npr. neko je u međuvremenu ažurirao taj materijal na internetu) ili iz razloga nekog sofisticiranog napada na sistem (npr. pokušaj poturanja ključa od strane treće strane), ne uklanja taj „ključ“ iz svoje evidencije, već ga samo markira kao „nepouzdan“ iz razloga da bi mogao blagovremeno da spreči upotrebu tog ključa kod nekog drugog klijenta kome je već isti isporučen za neku buduću komunikaciju. A klijent u tom slučaju ponavlja celu proceduru „trebovanja ključa“ od centralnog registra.

Ako pak klijent u svojoj memoriji ima uskladišten materijal za šifarski ključ koji nije prethodno (klijent) koristio, on je spreman za komunikaciju.

4. Kada pojedinačni klijent inicira komunikaciju sa drugim klijentom on prvo mora od centralnog registra da zatraži informaciju o dostupnosti i IP adresi drugog klijenta, i pritom da obavesti centralni registar o svom raspoloživom ključu (njegov ID i MD5 potpis).

Centralni registar proverava da li je drugi klijent (po zahtevanom aliasu) na mreži i da li je ključ koji poseduje prvi klijent validan (upoređivanjem MD5 sume). U slučaju nevalidnosti ključa prvog klijenta, zahtev za šifrovanu komunikaciju se odbija, a klijent započinje proceduru trebovanja novog ključa od centralnog registra.

Kada centralni registar konstatuje da je predloženi ključ prvog klijenta validan, on obaveštava drugog klijenta (sa kojim je prvi inicira komunikaciju) o dodeljenom jednokratnom ključu za predstojeću komunikaciju. Procedura obaveštavanja, preuzimanja i

duple validacije ključa (od strane klijenta i centralnog registra) kod drugog klijenta je istovetna kao u koraku 3.

Kada drugi klijent uskladišti i verifikuje dodeljeni jednokratni ključ, centralni registar im omogućava direktnu komunikaciju tako što im prosleđuje njihove međusobne IP adrese i nasumično odabrane IP portove na kojima će se komunikacija odvijati.

## IV.3. DIREKTNA ZAŠTIĆENA (ŠIFROVANA) KOMUNIKACIJA

Kao što je rečeno u uvodnom delu, da bi komunikacija bila sigurna, ona mora biti što manje izložena mogućnostima napada pa samim tim i nadzora same komunikacije. Jedna od potencijalnih slabih tačaka je "centralni čvor komunikacije", kroz koga bi dva klijenta razmenjivala podatke. Problem kod komunikacije na internetu je međusobno povezivanje, problem koji je delimično obrađen u poglavlju IV.1 ovoga rada.

Delimično, jer je rešen samo zadatak bezbednog inicijalnog lociranja međusobnih učesnika. Drugi deo zadatka je da učesnici zaštićeni sadržaj razmenjuju direktno bez posrednika, koji bi bio izuzetno ranjiva tačka sistema u smislu presretanja ili direktnog napada na sistem.

Ovaj drugi deo zadatka je rešen oslanjanjem na svojstvo UDP protokola koji je po svojoj prirodi "stateless"[38], što znači da paketi koji se šalju UDP protokolom nemaju status, i ne može se pratiti/potvrditi da je paket isporučen ili ne na odredište.

Ovo svojstvo može delovati kao mana UDP protkokola, što ona svakako jeste za određene namene, ali za potrebe masovnog transporta glasovnih paketa u kojima (kao što je ustanovljeno u poglavljima II.4.2 i II.5. ovoga rada) sporadični „gubitak" pojedinih paketa ne utiče suštinski na kvalitet prenete informacije.

Poznati p2p programi (sa posebnim osvrtom na VoIP programe kao što su Skype ili Viber) takođe koriste direktnu komunikaciju između dva klijenta, ne iz bezbednosnog već iz krajnje praktičnog razloga: Ne opterećuju svoju infrastrukturu relejnim prenošenjem informacija između klijenata, jer bi to zahtevalo virtuelno neograničenu propusnu moć tog centralnog kanala komunikacije koji bi prenosio(prosleđivao) sve informacije između svih klijenata simultano. Na stranu hardverski zahtevi za farmom servera koji bi imali dovoljan kapacitet obrade i prosleđivanja tolike količine podataka u realnom vremenu. Čak i kada bi sve ovo bilo tehnološki moguće, cena tog takvog „centralnog releja" i koštanje njegovog korišćenja bi bila enormna, i ovakve usluge sigurno ne bi bile besplatne kao što jesu.

Za ove potrebe koristi se tehnika u literaturi poznata pod nazivom[43]:

### IV.3.1 UDP Hole Punching

Kako mu i samo ime kaže, ova tehnika „buši rupu“ u zaštitnom zidu internet rutera određenog uređaja, konkretno radi se o tehnici koja funkcioniše „u paru“, dakle potrebne su 2 tačke komunikacije. Ova tehnika je bitna, odnosno neophodna da bi se ostvarila direktna komunikacija između dva entiteta na internetu. Pošto je logično pretpostaviti da (u najmanju ruku) često dva korisnika sistema zaštićene komunikacije nisu u istoj lokalnoj računarskoj mreži.

To dakle podrazumeva da ta dva entiteta imaju svoje lokalne IP adrese u svojim lokalnim mrežama, i da na internet „izlaze“ preko nekog lokalnog gateway uređaja. Tek taj gateway uređaj je „direktno“ na internetu, tj. ima „javnu“ IP adresu. Iako je IPv6[44] standard već naveliko u upotrebi, IPv4[45] standard je i dalje sveprisutan, pa budući da je kod njega problem „adresnog opsega“ drastično izražen, on će biti uzet kao referenca za razmatranje modela privatna/javna IP adresa[46].

Budući da IP adresa sadrži 4 bajta (XXX.XXX.XXX.XXX) maksimalan broj različitih IP adresa je $255^4 = 4{,}228{,}250{,}625$. Od ovog ukupnog broja IP adresa treba oduzeti tri predefinisana opsega za privatne IP adrese prema standardu definsanom u RFC1918 i prikazane u tabeli 9.:

| Rb. | Podmreža | Opseg adresa | Ukupan broj adresa |
|---|---|---|---|
| 1. | 10.0.0.0/8 | 10.0.0.1-10.255.255.254 | $2^{24} = 16{,}777{,}216$ |
| 2. | 172.16.0.0/12 | 172.16.0.1-172.31.255.254 | $2^{20} = 1{,}048{,}576$ |
| 3. | 192.168.0.0/16 | 192.168.0.1-192.168.255.254 | $2^{16} = 65{,}536$ |
| UKUPNO ADRESA: | | | 17,891,328 |

Tabela 10. Opsezi privatnih IP adresa

Iz izloženog se vidi da je ukupan broj dostupnih IP adresa tek nešto preko 4 milijarde. Da se ne koristi koncept privatnih/javnih IP adresa ovaj broj IP adresa ne bi bio dovoljan i internet ne bi bio globalni resurs dostupan svakome. Ideja koja valorizuje ovaj koncept privatnih/javnih IP adresa je sledeća: Svi uređaji koji se konektuju na internet su grupisani u svoje lokalne mreže (svi računari neke firme npr, ili računari, telefoni i svi smart uređaji u jednom domu) i svi oni imaju svoju lokalnu IP adresu iz privatnog adresnog prostora u bilo kojem mrežnom opsegu iz tabele 9.

U lokalnoj (privatnoj) mreži postoji jedan specifičan uređaj koji ima funkciju „internet kapije“ (eng. Gateway) i kome svi entiteti iz lokalne mreže šalju svoje „zahteve“ prema internetu, i preko koga primaju odgovore na te svoje zahteve. Dakle sav „spoljni“ (van lokalne mreže) saobraćaj ide preko tog uređaja. Taj uređaj je po pravilu ruter koji osim svoje lokalne IP adrese ima i javnu IP adresu koja je u suštini IP adresa „cele lokalne mreže“.

Na ovaj način postignuto je da veći broj uređaja može deljenjem iste javne IP adrese interagovati sa drugim entitetima na internetu, bez da svaki od njih zauzima pojedinačnu javnu IP adresu.

Čak i sa ovakvom „uštedom“ adresni prostor IP adresa je postao pretanak, ali to nije predmet ovoga rada[47].

Da bi ovakav način „deljenja“ javne IP adrese mogao da funkcioniše ispravno i opslužuje simultano veći broj klijenata iz privatne mreže, osmišljen je čitav niz protkola koji direktno ili indirektno to omogućavaju.

Jedan od tih protokola je naročito interesantan za potrebe omogućavanja direktne komunikacije dva uređaja iz različitih privatnih mreža preko interneta. To je NAT (eng. Network Address Translation) protokol[48].

Sam NAT protokol je veoma kompleksan, ali jedna od njegovih funkcija tzv. preklapanje (eng. NAT overloading) je od značaja za dalje razmatranje u ovom radu.

Naime, ova NAT funkcija koristi svojstvo TCP/IP protokol steka –multipleksiranje (eng. multiplexing) koja omogućava većem broju entiteta iz lokalne (privatne) mreže da održavaju više simultanih sesija sa udaljenim entitetom ili više njih, kroz različite IP portove. Budući da u svakom IP paketu u zaglavlju postoje (između ostalih) sledeće informacije:

- **Izvornu adresu** - IP adresu entiteta koji šalje paket
- **Izvorni port** - TCP ili UDP port koji proizvoljno odabira entitet koji šalje paket
- **Odredišnu adresu** - IP adresu entiteta kome je upućen paket
- **Odredišni port** - TCP ili UDP port za koji se očekuje da na njemu entitet kome je upućen paket treba da ga primi.

Same adrese određuju samo dva entiteta koja komuniciraju, dok sami IP portovi omogućavaju da konkretna konekcija (sesija) između ta dva entiteta bude jedinstveno identifikovana. Tek sva ova četiri podatka zajedno određuju konkretnu TCP/IP konekciju.

IP port je 16-bitna vrednost što znači da na raspolaganju postoji 65536 različitih portova. Neki portovi već imaju predodređene namene, tako da se za ovakve potrebe koriste u principu portovi od 1025-65535.

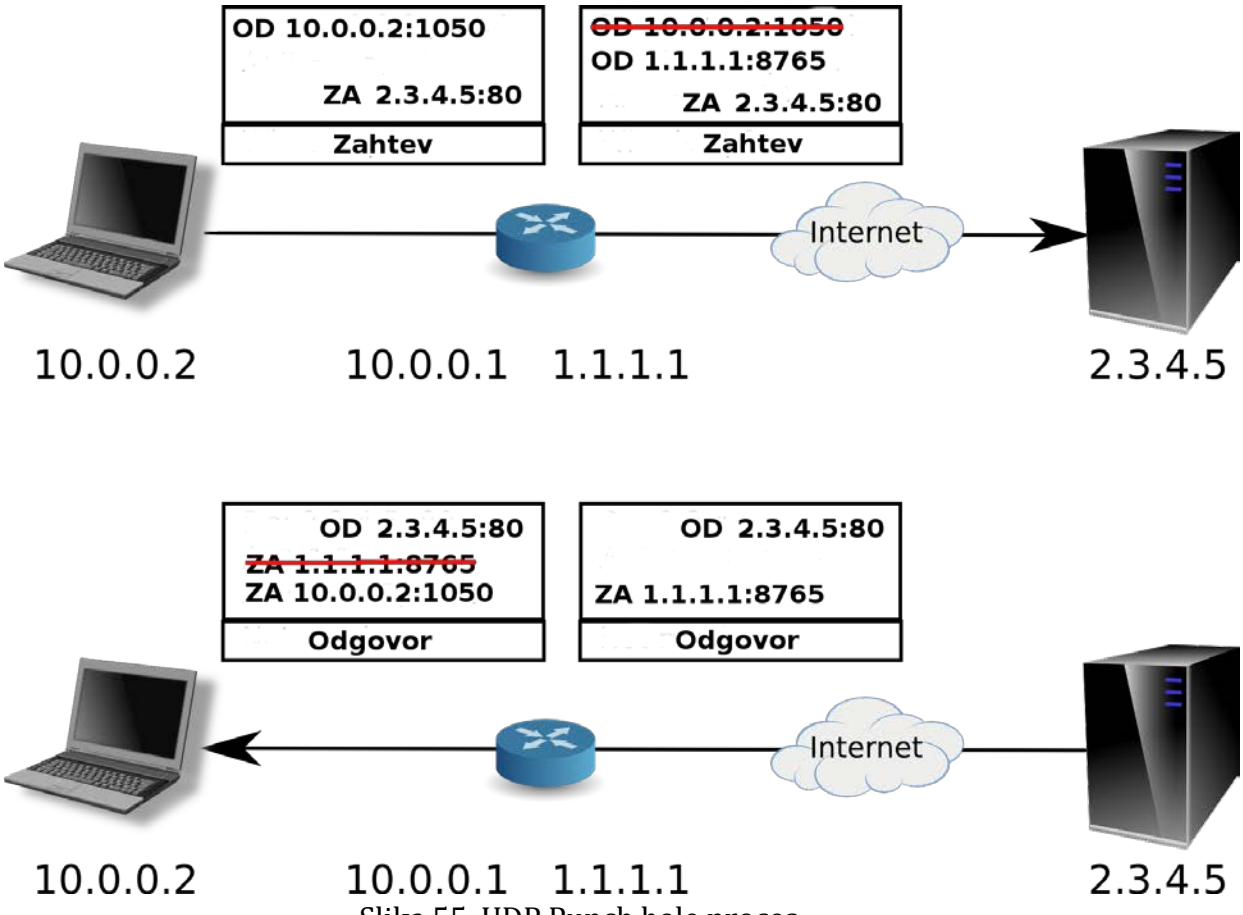
NAT preklapanje funkcioniše na sledeći način:

- Entitet iz lokalne mreže hoće da se poveže sa nekim entitetom van lokalne mreže (npr. web serverom). On već (direktno ili korišćenjem DNS-a) zna javnu IP adresu tog servera.
- Ruter (internet kapija) lokalne mreže prima taj paket od lokalnog entiteta.
- Ruter beleži lokalnu IP adresu i port iz tog paketa, kao i odredišnu IP adresu i port u svoju “tabelu za prevođenje adresa” (eng. address translation table).

- Ruter zamenjuje lokalnu IP adresu lokalnog entiteta svojom javnom IP adresom u predmetnom paketu. Takođe on zamenjuje i izvorni IP port predmetnog paketa sa portom koji odgovara portu u stavci tabele koju je sačuvao za tu konekciju. Tako izmenjen paket odlazi kroz internet do svoga odredišta.
- Kada povratni paket (odgovor) sa interneta stigne do rutera (jer je odgovor adresiran na javnu IP adresu rutera),ruter traži odredišni port predmetnog paketa u svojoj tabeli za prevođenje adresa, i pošto pronađe zapis ima tačnu lokalnu IP adresu entiteta kome treba da prosledi taj paket. Potom on menja odredišnu IP adresu dajući joj vrednost lokalne IP adrese predmetnog entieta i prosleđuje paket tom entitetu.
- Lokalni entitet prima prosleđeni paket od rutera u kome su polazna adresa i port istovetni odredišnoj adresi i portu inicijalnog zahteva, te taj paket tumači kao odgovor na isti što on i jeste kao da ga je dobio direktno od web servera kome je uputio zahtev.

Ovaj proces se ponavlja sve dok lokalni entitet komunicira sa tim "spoljnim serverom". Ali sve dok ova komunikacija traje, ruter će zadržati isti zapis za prevođenje adrese u svojoj predmetnoj tabeli. Ako aktivnost (komunikacija) izostane duže od vremena isteka konekcije, ruter će jednostavno obrisati taj zapis iz svoje tabele kao više nepotreban i osloboditi korišćeni port za buduću upotrebu.

Na slici 55. je dat primer gore opisane aktivnosti:

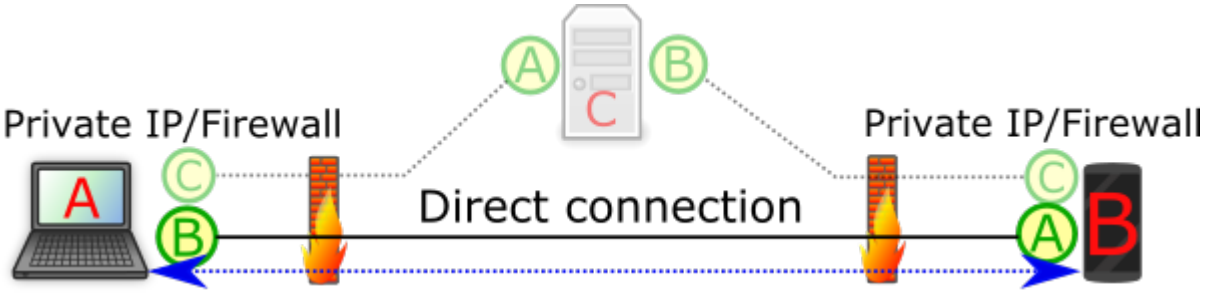



Slika 55. UDP Punch hole proces

Ovo svojstvo NAT funkcije da „prepisuje“ izvornu IP adresu/port omogućava da se uspostavi direktna komunikacija između dva entiteta na internetu (eng. peer to peer)[49].

Postupak je sledeći:

Da bi dva entiteta (A i B) koja su na različitim privatnim mrežama (koji dakle nemaju svoje sopstvene javne IP adrese) ostvarila direktnu komunikaciju, potreban je treći entitet koji ima sopstvenu javnu IP adresu (C) i koja je poznata obema entitetima (A i B), kao što je prikazano na slici 56.




Slika 56. Uspostavljanje direktne komunikacije

Entitet C je potreban samo za “upoznavanje” entiteta A i B. Pošto se obavi incijalno “upoznavanje” na način koji će biti detaljno opisan u nastavku, i nema nikakvu ulogu u samoj konkretnoj komunikaciji između entiteta A i B.

Uzmimo za primer da entitet A uspostavlja UDP konekciju prema entitetu C.

Po prijemu paketa od entiteta A, entitet C zna sada javnu IP adresu i port entiteta A, nebitno da li je to njegova direktna adresa ili NAT-ovana preko njegove internet kapije/zaštitnog zida (eng. firewall).

Entitet B uspostavlja UDP konekciju prema entitetu C.

Po prijemu paketa od entiteta B, entitet C zna sada javnu IP adresu i port entiteta B, nebitno da li je to njegova direktna adresa ili NAT-ovana preko njegove internet kapije/zaštitnog zida (eng. firewall).

Sada entitet C može da prosledi podatke o javnoj IP adresi/portu entiteta A entitetu B i obrnuto.

Entitet A šalje UDP paket na javnu IP adresu/port entiteta B. Naravno zaštitni zid entiteta B će ovaj paket odbaciti, ali zaštitni zip entiteta A to ne zna, i u NAT tabeli kreira zapis o ovoj konekciji, tako da će svi paketi koji dolaze od entiteta B na entitet A bići propušteni kroz zaštitni zid i prosleđeni entitetu A kao legitiman odgovor na onaj zahtev inicijalne konekcije entitetu B.

Isto se dešava i na drugoj strani, i time je omogućeno da se ostvari direktna komunikacija između ta dva entiteta.

Bitna napomena je da će prvi paket poslat sa entiteta A direktno entitetu B i prvi paket od entiteta B ka entitetu A biti odbačeni, pa se mora računati sa time da se prvim paketom ne šalju nikakvi podaci bitni za dalju komunikaciju.

Budući da UDP paketi nemaju status, bitno je da svaki paket u ovakvoj razmeni bude samostalna/samodovoljna celina za sebe, bez zavisnosti od prethodnog/ih paketa.

## IV.4 IMPLEMENTACIJA "CENTRALNOG REGISTRA"

Uzevši u obzir prethodno izneto, sam program koji bi vršio ulogu "centralnog registra" ili imenika u realnom vremenu bi dakle vršio sledeće funkcije:

1. Vodio spisak svih aktivnih (trenutno online) uređaja tj. klijenata na kojima je pokrenut namenski softver za šifrovanje glasa. U tom spisku on bi čuvao sledeće podatke o aktuelnim klijentima:
   - Alijas klijenta (npr. Vlada, Bojan, Ivana) po kome bi se pojedinačni korisnci međusobno razaznavali
   - Aktuelnu IP adresu klijentskog uređaja kada je isti online i prijavljen "na system".

2. Omogućavao pojedinačnim klijentima da saznaju IP adresu drugog klijenta sa kime žele da uspostave komunikaciju.

   Takođe on bi po zahtevu za ostvarivanje komunikacije između klijenata birao slučajni IP port za svakog od klijenata koji bi koristili te jednokratno određene portove za međusobnu direktnu komunikaciju.

3. Bio "pouzdani posrednik" za inicijalni "dogovor" dva klijenta o izboru šifarskih ključeva pre započinjanja šifrovane komunikacije. Ova funkcionalnost obuhvata i vođenje tačne evidencije (u svojoj centralnoj bazi podataka) o jednom upotrebljenom ključu, da bi se obezbedilo da se jednom upotrebljeni ključ ne upotrebi ponovo u nekoj sledećoj komunikaciji.

Takođe je bitno napomenuti da je potrebno periodično (frekvencija učestalosti srazmerna frekvenciji upotrebe sistema) „migrirati" centralni registar (serverski softver) na uvek novu „lokaciju" (IP adresu) i ažurirati Tor hidden service u skladu sa time.

Ova operativna mera je u stvari kontramera za eventualne masovne napade na Tor mrežu metodama zauzimanja što većeg broja čvorova i statističkog praćenja saobraćaja[50][51].

Dovoljno čestim „izmeštanjem" centralnog registra, drastično se smanjuju šanse za otkrivanje tj. identifikovanje centralnog registra što bi moglo da kompromituje ceo sistem u smislu mogućnosti DDoS napada, ne toliko i u smislu probijanja sistema kriptozaštite jer se sve informacije ka i od centralnog servera prenose takođe u zaštićenom obliku, ali bi to bila idealna početna tačka napada/analize.

Konkretna implementacija centralnog registra može biti JAVA Web aplikacija, funkcionalno servlet[52], koji bi opsluživao neograničen broj klijenata simultano u multi-thread modelu.

Sam servlet bi funkcionisao kao klasični HTTP server, što dodatno „maskira“ predmetni sadržaj komunikacije, jer ga je kao takvog izuzetno teško uočiti i izolovati „u šumi“ saobraćaja Tor mreže.

Funkcije koje bi obrađivao servlet bi bile:

-Registracija klijenta „na mrežu“.

Ova funkcija bi samo beležila klijentovu (dostavljenu kroz zahtev) javnu IP adresu i alias, i to beležila u svojoj bazi aktivnih klijenata. Ovde je „pokriven“ bitan bezbednosni aspekt da se javna IP adresa klijenta nikako „ne oglašava i ne kompromituje“ u smislu da se sva komunikacija između klijenta i centralnog registra obavlja takođe transferom podataka (višestruko) šifrovano kroz Tor mrežu, tako da se ne može filtriranjem mrežnog saobraćaja uočiti klijent, budući da on ne uspostavlja vezu direktno sa centralnim registrom, već kroz Tor mrežu, a adresa centralnog registra je takođe „skrivena“ u Tor mreži na način detaljno opisan u odeljku IV.1.2. Na taj način čak i neka treća strana koja bi se „infiltrirala“ u Tor mrežu, čak i ako bi se desio slučaj da neki od predmetnih paketa „prođe“ kroz njega, on niti može znati polaznu niti odredišnu IP adresu niti sam sadržaj paketa, što sistem čini veoma pouzdanim i otpornim.

-Zahtev klijenta za zaštićenom komunikacijom sa drugim klijentom.

Ova funkcija podrazumeva da centralni registar uvidom u svoju internu evidenciju pronađe IP adresu drugog klijenta, obavesti ga o zahtevu prvog i ako drugi odgovori pozitivno, odabira materijal za jednokratni šifarski ključ i prosleđuje informacije o istom ka oba klijenta, kako je detaljno opisano u odeljku IV.2.

Po dobavljanju ključa oba klijenta nezavisno upoređuju dobijeni MD5 sa stvarnim i ako se sve slaže obaveštavaju centralni registar da su spremni za komunikaciju. Centralni registar prosleđuje parametre komunikacije na oba klijenta (IP adresu i port onog drugog klijenta), beleži da je konkretni materijal za šifarski ključ “potrošen”, u svoju evidenciju da bi se izbeglo ponovno korišćenje istog šifarskog ključa ikada u budućnosti.

## IV.5. IMPLEMENTACIJA KLIJENTA

Klijent u ovom sistemu je realizovan kao Android aplikacija, kao najreprezentativniji, no po istovetnim principima može se realizovati na bilo kojoj drugoj hardversko/ softverskoj platformi.

Funkcije koje bi, u skladu sa prethodno definisanim parametrima i načinom funkcionisanja celog sistema, klijent imao su:

-Uzorkovanje i digitalizacija glasa u realnom vremenu u potrebnom kvalitetu.

-Ugrađene mehanizme (rutine) za uspostavljanje veze sa Tor hidden service serverom i komunikaciju korišćenjem Tor mreže.

-Preuzimanje određenog sadržaja sa interneta i njegovo skladištenje.

-Šifrovanje digitalizovanog glasa u pojedinačnim sekvencijalnim i sukcesivnim paketima i njihovo odašiljanje preko interneta direktno na odredište bez posrednika.

-Svaki od pojedinačnih takvih paketa bi u svom zaglavlju sadržao podatak o "indeksu ključa", koji nije u linearnoj zavisnosti od rednog broja paketa, a na osnovu kog podatka bi se mogao korišćenjem istog ključa sa zadate pozicije (indeksa) iz paketa da se izvrši dešifrovanje primljenog digitalizovanog glasa iz paketa i isti reprodukuje na odredištu u originalnom sadržaju bez gubitka kvaliteta.

Ovakva "sinhronizacija ključa" u svakom pojedinačnom paketu obezbeđuje "sinhronizaciju" dugačkog šifarskog ključa, u slučaju da neki od sekvencijalnih šifrovanih paketa ne stigne na odredište zbog bilo kakvih komunikacionih problema. U ovom slučaju dešifrovanje sledećih paketa bez obzira na broj prethodno "propuštenih" paketa će se odvijati normalno.

Čak i u slučaju presretanja ove komunikacije i posedovanja znanja o formatu paketa/digitalizacije, indeksa ključa u zaglavlju svakog paketa, dešifrovanje paketa i cele komunikacije je nemoguće bez posedovanja korišćenog ključa koji ne može biti "presretnut" u ovom kanalu komunikacije.

# V ZAKLjUČAK

## V.1 DOPRINOS

Glavni zadatak ovog rada je da predstavi i analizira novi pristup zaštićenoj VoIP komunikaciji. U okviru rada prikazan je i realni sistem, i praktična realizacija celog sistema u skladu sa predloženim pristupom.

Glavne hipoteza koja je postavljena i ispitana u radu je da sistem zaštićene komunikacije mora biti višeslojan, sa međusobnom funkcionalnom izloacijom takvom da "pad" pojedinih delova sistema/korisnika ne kompromituje sistem u celosti.

Takođe, detaljno je ispitano i empirijski testirano funkcionisanje sistema u "neidealnim" uslovima komunikacione infrastrukture, kao i izvor dostupnih sadržaja na internetu, i mogućnost korišćenja istih kao jednokratnih šifarskih ključeva.

Izolacija delova/funkcija sistema je postignuta na sledeći način:

- Centralni registar korisnika preko koga klijenti "ugovaraju" komunikaciju se nalazi duboko skriven u Tor mreži i ni jedan klijent nema informaciju o njegovoj stvarnoj lokaciji.
- Registracija klijenata i "ugovaranje" zaštićene komunikacije, te dogovor oko izbora jednokratnog ključa se obavlja kroz Tor mrežu ne direktno između klijenata već opet kroz Tor mrežu. Na ovaj način se onemogućava jednoznačno filtriranje internet saobraćaja u cilju identifikacije klijenata u sistemu/centralnog registra. Ovaj ceo mehanizam je opisan u odeljku IV.1.2. ovoga rada.
- Sama zaštićena (šifrovana) komunikacija se izvodi na slučajno odabranom IP portu direktno između klijenata korišćenjem mehanizama opisanih u odeljku IV.3.1. ovog rada. Kroz ovaj komunikacioni kanal dakle prolazi samo šifrovani sadržaj, ne i ključ, tako da i u slučaju da ova komunikacija bude presretnuta, nije moguće dešifrovati sadržaj bez ključa. Čak i ako bi napadač uspeo da dešifruje konkretnu komunikaciju, to je izolovani slučaj te konkretne komunikacije, i ostatak sistema ostaje da funkcioniše bezbedno.

Doprinos je dat i u realizaciji šifarskog koncepta "jednokratne beležnice" korišćenjem novih dostupnih tehnologija (Interneta, računara i Smart telefona), tako da strane u komunikaciji ne moraju da poseduju "beležnice" koje bi se koristile za veći broj jednokratnih komunikacija kod sebe te rizikuju da "padom" beležnice kod bilo kog klijenta kompromituju ceo sistem.

Predloženi i evaluirani sistem uvodi unapređeni koncept jednokratne beležnice koji podrazumeva da nijedan element sistema (ni pojedinačni klijent ni centralni registar) kod sebe nemaju  šifarski ključ uskladišten sve do početka same zaštićene komunikacije, te isti (šifarski) ne može biti kompromitovan unapred.

Takođe u radu se detaljno obrađuju i evaluiraju raspoloživi materijali na internetu u smislu slika, audio i video materijala, te ocenjuje njihova podobnost za potrebe šifarskog ključa.

U suštini sam kvalitet "slučajnosti" niza koji se koristi kao šifarski ključ je od sekundarne važnosti, jer je i sam govor/glas u komunikaciji dovoljno neodređen/slučajan posmatrano na primer u odnosu na tekstualni sadržaj. Jer u tekstu svako napisano (otkucano) slovo ima isti kod u računarskom skladištenju/transportu/reprezentaciji, dok glas čak i iste osobe kada izgovara iste reči/fraze/rečenice nikada neće rezultirati istovetnim nizom vrednosti u procesu digitalizacije. Na taj način se u sistem dodaje element "prirodne" slučajnosti koji daje značajno na "snazi" same kriptozaštite.

Sam glas/govor, naročito sa računarske tačke gledišta, predstavlja veoma moćnu šifru. Banalan, ali jako ilustrativan primer je upotreba pripadnika nacije Navaho Indijanaca od strane Sjedinjenih Američkih Država u svojim redovima u II svetskom ratu, gde su, suočeni sa sofisticiranim tehnikama Japanaca da dešifruju radio komunikaciju protivniče strane, u svoje redove mobilisali Navaho Indijance koji su obavljali dužnost radio operatera na Pacifičkom frontu, gde se umesto bilo kakve šifre, koristio nativni govor Navaho Indijanaca u direktnoj komunikaciji. Sam taj govor je bio potpuno nova, neprobojna šifra za Japansku stranu.  Naravno ovo rešenje je imalo ogromni bezbednosi rizik od zarobljavanja bilo kojeg Navaho radio operatera od protivničke strane što bi kompromitovalo ceo sistem u potpunosti.

Prikazani rezultati evaluacije kako pojedinih delova sistema, tako i sistema u celini pokazuju da se može efikasno zaštititi glasovna komunikacija implementirajući predložene principe. Višeslojnost rešenja efikasno podiže nivo efikasnosti zaštite, i poništava mogućnost „opšte provale sistema" i u slučaju pada bilo kog pojedinačnog dela sistema.

## V.2 DALjI RAD

Dalji rad na implementaciji rešenja koja su zasnovana na predloženom rešenju omogućava širok spektar raznolikih unapređenja, uz obaveznu analizu sigurnosti kako same kriptozaštite u užem smislu, tako i trendova u napretku računarskih tehnologija, u

smislu da se sa protokom vremena može proizvesti toliko moćan računar koji bi mogao u realnom vremenu primenom “grube računske sile” (eng. brute force) da dešifruje presretnutu komunikaciju. Ovakav računar je danas još uvek u domenu teorije, ali uzevši u obzir eksponencijalni rast računske moći novih procesora, i računarske tehnike uopšte, to je “damaklov mač” koji visi iznad svakog sigurnosnog sistema u računarskom domenu, i svi kreatori zaštitnih sistema moraju biti stalno na oprezu, i pratiti nove tehnologije.

Glavni adut koji govori u prilog bezbednosti sistema kriptozaštićene glasovne komunikacije je baš u tome što nije moguće automatsko dešifrovanje tj. evaulacija uspešnosti potencijalnog dešifrovanja, za razliku od evaluacije dešifrovanja tekstualnog sadržaja[53]. Kod evaluacije uspešnosti dešifrovanja tekstualnog sadržaja može se vršiti upoređivanje rezultirajućih (potencijalno dešifrovanih) reči sa postojećim već uskladištenim rečnikom ciljnog jezika, ili više njih. Međutim kod rezultirajućeg (potencijalnog dešifrovanog) glasa, prepoznavanje dobijenog zvuka je mnogo kompleksniji problem, i veoma je neizvesno, naročito u realnom vremenu “identifikovati” rezultat računarski[54]. Neki poluatomatski sistem evaluacije dešifrovanja glasa bi podrazumevao da računar vrši dešifrovanje glasa i reprodukuje rezultat, a “živ operater” za računarom bi po preslušavanju sadržaja ocenjivao da li je rezultat zaista dešifrovani glas ili ne, pa davao povratnu informaciju računaru da li da “proba sledeću kombinaciju” ili je to “dobitna kombinacija” dešifrovanja.

Uporedo sa razvojem tehnologija i interneta, privatnost svakog subjekta postaje sve ogoljenija, a tajnost polako zalazi u domen imaginacije. Analogno tome raste i značaj tehnologija i rešenja koja omogućavaju privatnost/tajnost kako podataka tako i komunikacije.

# LITERATURA


[1] Harry Hollien, Donald Dew, and Patricia Philips: "Phonational Frequency Ranges of Adults", Journal of Speech, Language, and Hearing Research, December 1971, Vol. 14, 755-760. doi:10.1044/jshr.1404.755

[2] Aftab Ahmad: "DATA COMMUNICATION PRINCIPLES *For Fixed and Wireless Networks",* Kluwer academic publishers, 2003, 81-90

[3] http://www.telenor.rs/info/pokrivenost, pristupano 25.06.2016.

[4] https://www.mts.rs/privatni/internet/mobilni-internet/mapa, pristupano 25.06.2016.

[5] http://www.vipmobile.rs/o-vipu/vip-mreza/mapa-pokrivenosti.1634.html, pristupano 25.06.2016.

[6] Stephen R.W. Discher: "Router OS by Example", 2011.

[7]Wei Meng Lee:"Android 4 -Razvoj aplikacija", Wiley Publishing Inc, 2012.

[8] Bruce Schneier:"Primenjena Kriptografija", Wiley Publishing Inc, 1996.

[9] https://www.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html, pristupano 8.7.2016.

[10] C.E. Shannon:"Predication and Entropy in printed English", Bell System Technical Journal, vol. 30, 1951., str. 50-64.

[11] G.W. Hart:"To decode short cryptograms", Communications of the ACM, vol.37, 1994,str. 102-108.

[12] W.F. Friedman:"Methods for the solution of running key chipers", Riverbank publication #16, Riverbank labs, 1918.

[13] D.Kahn:"The codebrakers: The story of secret writing", Macmillan Publishing, 1967.

[14] R.N. Williams:"An extermely fast Ziv-Lempel data compression algorithm", Data Compression Conference, 1991., str 362-371.

[15] M. J. Weinberger, G. Seroussi, G. Sapiro:" The LOCO-I lossless image compression algorithm: principles and standardization into JPEG-LS", IEEE Transactions on Image Processing (Volume:9 , Issue: 8 ), 2000., str. 1309-1324.

[16] Mark Nelson, Jean-loup Gailly:"The data compression book", University of Bahrain, College of applied studies, 1996.

[17] https://www.phy.duke.edu/~rgb/General/dieharder.php, pristupano 7.7.2016.

[18] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker:" A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", NIST Special Publication 800-22, 2001.

[19] J. O. Berger, T. Sellke:" Testing a Point Null Hypothesis: The Irreconcilability of *P*-Values and Evidence", Journal of the American Statistical Association, vol 82, 1987., str 112-122

[20] https://www.reddit.com/r/crypto/comments/2d4m1v/how_random_is_your_data_on_interpreting_diehard/, pristupano 7.7.2016.

[21] A. Klapuri :" Sound onset detection by applying psychoacoustic knowledge", Acoustics, Speech, and Signal Processing, 1999. Proceedings., 1999 IEEE International Conference, vol 6., str. 3089-3092

[22] E. Zwicker,H. Fastl:"*Psychoacoustics -Facts and Models"*, Springler Verlag, 1990

[23] Herre, Jurgen, Johnston, D. James:" Enhancing the Performance of Perceptual Audio Coders by Using Temporal Noise Shaping", AES Convention,1996.

[24] http://digitalsoundandmusic.com/5-3-8-algorithms-for-audio-companding-and-compression/ , pristupano 14.7.2016.

[25] https://www.w3.org/Graphics/Color/sRGB.html, pristupano 14.7.2016.

[26] T. Sikora:" The MPEG-4 video standard verification model", Heinrich-Hertz-Inst. for Commun. Technol., Berlin, Germany, 1997.

[27] Mohammed Ghanbari:" Standard Codecs: Image Compression to Advanced Video Coding",

[28] C. Poynton:" Digital video and HDTV algorithms and interfaces", Morgan Kaufmann, 2003.

[29] https://software.intel.com/en-us/node/503873, pristupano 14.7.2016.

[30] https://vsr.informatik.tu-chemnitz.de/~jan/MPEG/HTML/mpeg_tech.html, pristupano 14.7.2016.

[31] A. Biryukov, I. Pustogarov, F. Thill, R-P Weinmann:"Content and Popularity Analysis of Tor Hidden Services", IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW), 2014, str. 188-193

[32] R. Dingledine, N. Mathewson, P. Syverson:"Tor: The Second-Generation Onion Router", NAVAL RESEARCH LAB WASHINGTON DC, 2004.

[33] V. Stanojević: „Anonimnost na internetu –Tor rešenje", Master rad, Univerzitet Singidunum, 2013.

[34] https://gitweb.torproject.org/torspec.git/tree/rend-spec.txt

[35] U. Somani, K. Lakhani, M. Mundra:" Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing", 1st International Conference on Parallel Distributed and Grid Computing (PDGC), 2010, str. 211-216

[36]https://www.torproject.org/docs/hidden-services.html.en, pristupano 16.7.2016.

[37] https://tools.ietf.org/html/rfc1321, pristupano 16.7.2016.

[38] http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/udp.html, pristupano 16.7.2016.

[39] H. Zimmerman, „OSI Reference Model – The ISO Model of Architecture for Open Systems Interconnection" IEEE Transactions on Communications, Vol. COM-28, No 4., April 1980.

[40] Y. Rekhter, B. Moskowitz, D. Karrenber, G. J. De Groot, E. Lear:“RFC 1918: Address Allocation for Private Internets“, IETF 1996,

[41] S. Davidoff, J. Ham, „Network Forensics“, Prentice hall 2012.

[42] B. Sosinsky, „Networking Bible“, Wiley Publishing, 2009.

[43] http://resources.infosecinstitute.com/udp-hole-punching/ , pristupano 16.7.2016.

[44] https://tools.ietf.org/html/rfc2460, pristupano 16.7.2016.

[45] https://tools.ietf.org/html/rfc791, pristupano 16.72016.

[46] https://technet.microsoft.com/en-us/library/cc958825.aspx, pristupano 17.7.2016.

[47] S. Lawson: „IPv6 Doomsday Won’t hit in 2012, Experts say.”, PCWorld, 29. decembar 2011.

[48] https://tools.ietf.org/html/rfc2766

[49] W. Nejdi, B.Wolf, C. Qu, S.Decker, M. Sintek, A. Naeve, M. Nilsson, M. Palmer, T. Risch:”EDUTELLA a P2P network based on RFD”, www proceedings of the 11th international conference on world wide web, New York 2002.

[50] H.R. Nemati,L. Yang:”Applied Cryptography for Cyber Security and Defense”, Information Science Reference, 2011., str. 17-19.

[51] K. Müller:” Defending End-to-End Confirmation Attacks against the Tor Network”, Master’s Thesis, Gjøvik University College, 2015

[52] H. Brown:”Core Servlets & JavaServer Pages”, 2nd edition,Prentice Hall, 2011.

[53] G.H. Khaskari, A.L. Wijesinha, R.K. Karne:” Secure VoIP Using a Bare PC”, 3rd International Conference on New Technologies, Mobility and Security, 2009.

[54] D. Van Lancker, J. Kreiman, K. Emmorey:” Familiar voice recognition: Patterns and parameters”, Journal of Phonetics, Vol 13(1), 1985, str. 19-38.