Univerzitet u Sarajevu

Elektrotehnički fakultet

Odsjek za Telekomunikacije

Dizajn i implementacija TOR modela u NS-3 simulatoru

Simulacija procesa u telekomunikacijskim mrežama - Praktični dio

Radili:

Vedad Crnčalo, Amna Bumbul, Harun Dedović, Muhamed Crnčalo

26. februar 2025.

Sadržaj

1 Opis rješenja

Ovo rješenje implementira simulaciju TOR mreže u NS-3, koristeći višeslojnu enkripciju i poseban način rutiranja kako bi se osigurala anonimnost podataka u mrežnoj komunikaciji. Umjesto klasičnog prenosa podataka, gdje su izvor i odredište jasno vidljivi, TOR koristi metodu *"onion routing"*, pri kojoj se podaci omotavaju u više slojeva enkripcije. Svaki čvor u mreži dešifruje samo jedan sloj, otkrivajući samo informaciju o sljedećem koraku u ruti paketa, ali ne i njegovo krajnje odredište. Na taj način, niti jedan pojedinačni čvor ne može u potpunosti rekonstruisati komunikaciju, čime se postiže visok nivo privatnosti i sigurnosti.

XOR enkripcija („ekskluzivno ili“) predstavlja aditivnu enkripciju koja se zasniva na XOR operaciji, poznatoj i kao ekskluzivna disjunkcija u logici. Kao logička operacija, XOR predstavlja sabiranje po modulu 2, pri čemu je rezultat tačan samo kada su ulazi različiti. XOR šifra se često koristi u računalnim malverima radi otežavanja analize i obrnutog inžinjeringa. Kada je ključ slučajan i barem iste dužine kao poruka, šifra postaje znatno sigurnija nego u slučaju ponavljanja ključa unutar iste poruke. XOR algoritam za enkripciju je jednostavna, ali vrlo efikasna metoda simetrične enkripcije, pri čemu se isti ključ koristi i za enkripciju i za dekripciju poruke. Zbog svoje efikasnosti i jednostavnosti, često se koristi kao komponenta u složenijim algoritmima enkripcije. [1]

U TOR.cc implementaciji, XOR šifra se koristi za enkapsulaciju podataka dok prolaze kroz niz releja, čime se osigurava anonimnost pošiljatelja. Na svakom releju se primjenjuje XOR operacija pomoću različitih ključeva, čime se dodatno prikriva stvarna putanja paketa.

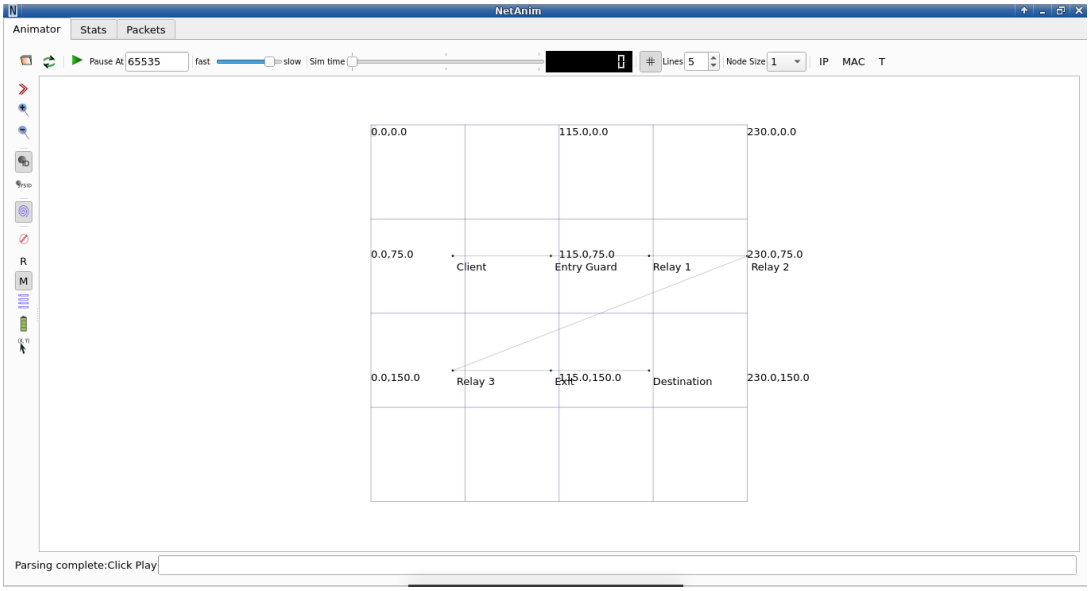
Ovaj projekt prikazuje dizajn i implementaciju pojednostavljenog modela TOR mreže korištenjem NS-3 simulatora. Cilj ove simulacije je demonstrirati osnovne principe anonimnog rutiranja kroz niz releja, čime se osigurava zaštita privatnosti korisnika i sakrivanje izvorišta podataka. Simulacija je izvedena pomoću statičkog rutiranja, a komunikacija se realizuje korištenjem UDP protokola sa UDP Echo Client i UDP Echo Server aplikacijama.

2 Arhitektura simulacije

Ovaj model simulira TOR (The Onion Router) mrežu koristeći sedam čvorova, koji zajedno omogućavaju anonimno i sigurno prosljeđivanje mrežnog saobraćaja kroz višeslojnu enkripciju i specijalizovano rutiranje.

- **Klijent** – Inicira mrežni saobraćaj generisanjem paketa koji sadrže podatke za slanje. Prije slanja, paket prolazi kroz proces višeslojne enkripcije, gdje se svaki sloj šifruje posebnim ključem.
- **Ulazni čvor** – Prvi čvor u TOR mreži, odgovoran za primanje paketa od klijenta i prosljeđivanje dalje kroz mrežu. Ulazni čvor može vidjeti IP adresu klijenta, ali ne i sadržaj paketa ili njegovo krajnje odredište, čime se osigurava prva faza anonimnosti.
- **Tri releja** – Posrednički čvorovi koji omogućavaju dodatno prikrivanje tragova paketa tako što ga preusmjeravaju između više lokacija.
- **Izlazni čvor** – Posljednji čvor prije odredišta vidi sadržaj paketa, ali ne zna identitet klijenta, čime se sprečava povezivanje korisnika s njegovim aktivnostima na mreži.
- **Odredište** – Dešifruje slojeve enkripcije i prima originalne podatke. Konačni čvor u mreži koji prima dešifrovane podatke i obrađuje ih. Ovo može biti web server, aplikacija ili bilo koji drugi entitet koji komunicira sa klijentom putem TOR mreže, a da pri tome ne zna njegovu stvarnu IP adresu.

Ovaj model simulira ključne karakteristike TOR mreže, omogućavajući analizu performansi, sigurnosti i efikasnosti anonimne komunikacije u različitim scenarijima. Opisana arhitektura se može vidjeti na slici ispod:



Slika 1: *Prikaz arhitekture simulacije u NetAnim-u*

3 Komparacija sa teoretskim rezultatima

3.1 Mjerenja ključnih metrika

Performanse TOR mreže analiziraju se kroz različite metrike, pri čemu su kašnjenje (delay) i propusnost (throughput) ključni pokazatelji efikasnosti prenosa podataka.

Kašnjenje predstavlja vrijeme potrebno da paket stigne od izvorišta do odredišta, što je posebno važno u TOR mreži zbog višestrukog usmjeravanja kroz releje radi očuvanja anonimnosti [2].

Propusnost, s druge strane, mjeri količinu podataka koji mogu biti preneseni kroz mrežu u određenom vremenskom periodu i odražava ukupnu efikasnost sistema [2].

Ove metrike su odabrane jer direktno utiču na korisničko iskustvo, veće kašnjenje može dovesti do sporog odziva aplikacija, dok niža propusnost može ograničiti brzinu prenosa podataka kroz mrežu.

3.1.1 Propusnost (Throughput) i Kašnjenje (Delay)

Teorijski, propusnost (throughput) u TOR mrežama zavisi od različitih faktora, uključujući mrežnu arhitekturu, kapacitet linkova i način na koji se podaci usmjeravaju kroz mrežu. Throughput se definiše kao količina podataka koji se prenesu kroz mrežu u određenom vremenskom intervalu i izražava se u bitima po sekundi (bps) [2]. Može se izračunati pomoću formule:

$$Throughput = \frac{\text{Ukupan broj primljenih paketa} \times \text{Veličina paketa (u bitima)}}{\text{Vrijeme simulacije}} \quad (1)$$

U idealnim uslovima, očekuje se da propusnost (throughput) bude visoka, uz minimalne gubitke paketa i kašnjenja (delay). Međutim, zbog arhitekture TOR mreža, koje koriste višestruke rute i slojevitu enkripciju podataka, dolazi do povećanja latencije i smanjenja ukupne propusnosti. Prema postojećim istraživanjima, TOR mreže često imaju veće kašnjenje u odnosu na klasične mreže, jer svaki paket prolazi kroz više čvorova prije nego što stigne do odredišta, čime se produžava vrijeme prenosa.

U simulaciji izvedenoj u NS-3 okruženju, dobiveni rezultati pokazuju da je ukupno preneseno 72 paketa, pri čemu nije bilo gubitaka, što rezultira 100% omjerom isporučenih paketa (Packet Delivery Ratio). Prosječno kašnjenje iznosi 0.150403 sekundi, što je relativno niska vrijednost. Kašnjenje (delay) se definiše kao prosječno vrijeme potrebno da paket stigne od izvorišta do odredišta i može se izračunati kao [2]:

$$Delay = \frac{\sum \text{Vremena dolaska paketa} - \sum \text{Vremena slanja paketa}}{\text{Ukupan broj primljenih paketa}} \quad (2)$$

Međutim, u poređenju sa teoretskim očekivanjima i rezultatima prikazanim u analiziranim radovima, primjetno je da simulacija pokazuje optimistične rezultate. Jedan od

ključnih razloga za ovo odstupanje je pojednostavljen model simulacije u NS-3, gdje nisu uzeti u obzir svi faktori koji utiču na performanse stvarne TOR mreže. Konkretno, u simulaciji nije simulirano stvarno zagušenje mreže, koje bi uzrokovalo povećano kašnjenje i smanjenje propusnosti. Takođe, simulacija ne uključuje dodatne kriptografske operacije koje se odvijaju na svakom čvoru u TOR mreži, što bi u realnim uslovima dodatno povećalo latenciju.

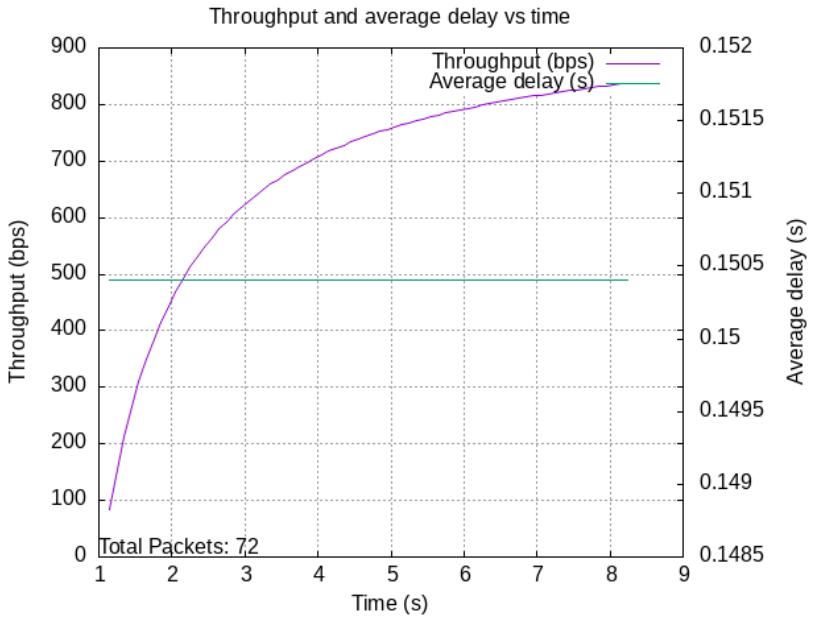
Pored toga, u NS-3 modelu korišteni su idealni linkovi bez dodatnih ometanja i varijacija u mrežnom kašnjenju, dok stvarne mreže imaju dinamiku koja uključuje varijabilne uslove kao što su paketna kašnjenja, mrežne greške i promjene u rutiranju. Ovi faktori bi u stvarnoj implementaciji doveli do povećanja delay-a i smanjenja throughput-a u odnosu na ono što je dobijeno u simulaciji.

3.1.2 Prenos 72 paketa kroz mrežu

Propusnost na slici 2. pokazuje eksponencijalni rast na početku, koji se postepeno stabilizira oko 800 bps. Ovaj početni rast predstavlja fazu punjenja mreže, gdje se paketi ubrzano procesiraju dok mrežni baferi ne dostignu svoj kapacitet. Stabilizacija oko 8. sekunde ukazuje na to da je mreža dostigla svoj maksimalni kapacitet obrade podataka i da je optimizirana za ovakvo opterećenje. Maksimalna vrijednost propusnosti od približno 800 bps pokazuje da mreža može efikasno obraditi veći broj paketa tokom dužeg vremenskog perioda.

Prosječno kašnjenje na slici 2. ostaje konstantno na oko 0.150 s, što dovodi do zaključka da povećan broj paketa nije uzrokovao dodatno zagušenje niti povećano vrijeme čekanja. Ova stabilnost u kašnjenju, uz rast propusnosti, sugerira da TOR mreža koristi efikasan mehanizam za rutiranje i distribuciju opterećenja. Ovakvo ponašanje je posebno važno za TOR mreže, jer omogućava očuvanje anonimnosti bez kompromisa u performansama.

Općenito, mreža pokazuje sposobnost da podnese veći broj paketa bez značajnog uticaja na kašnjenje, što ukazuje na dobru skalabilnost. Propusnost raste dok mreža ne dostigne svoj maksimalni kapacitet, dok kašnjenje ostaje konstantno. Ovakav obrazac ukazuje na stabilne performanse i efikasno upravljanje saobraćaja čak i pri većem opterećenju.



Slika 2: *Prikaz dijagrama kašnjenja i propusnosti za 72 prenesena paketa*

```
=== TOR network statistics ===

Transmission summary:
-------------------------------------
Total bytes sent:          864
Total bytes received:      864
Total packets sent:        72
Total packets received:    72
Delivery ratio (bytes):    100%
Delivery ratio (packets):  100%
Troughput (bps):           345.6 bps
Troughput (kbps):          0.3456 kbps
Average end-to-end delay:  0.150403s
-------------------------------------
Created output file: output.txt
-------------------------------------
```

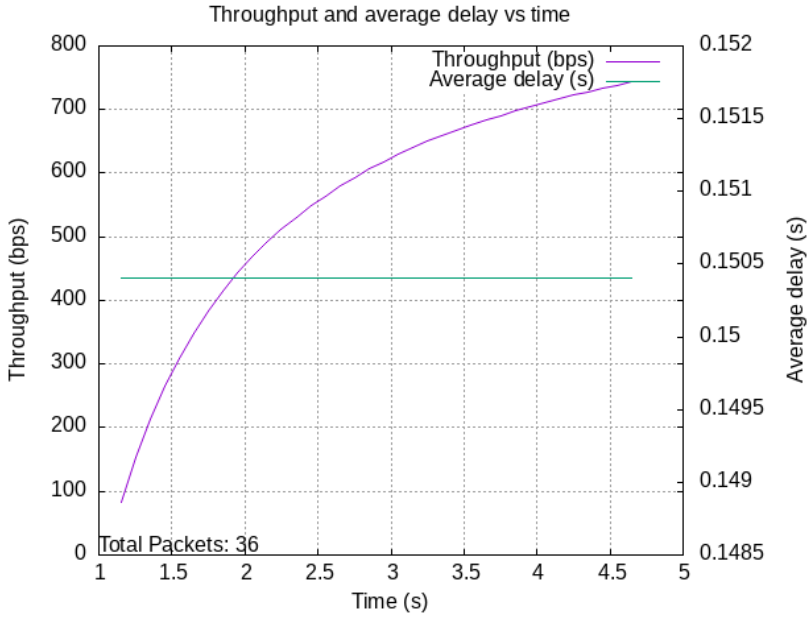
Slika 3: *Prikaz ispisa terminala za prenos 72 paketa*

3.1.3 Prenos 36 paketa kroz mrežu

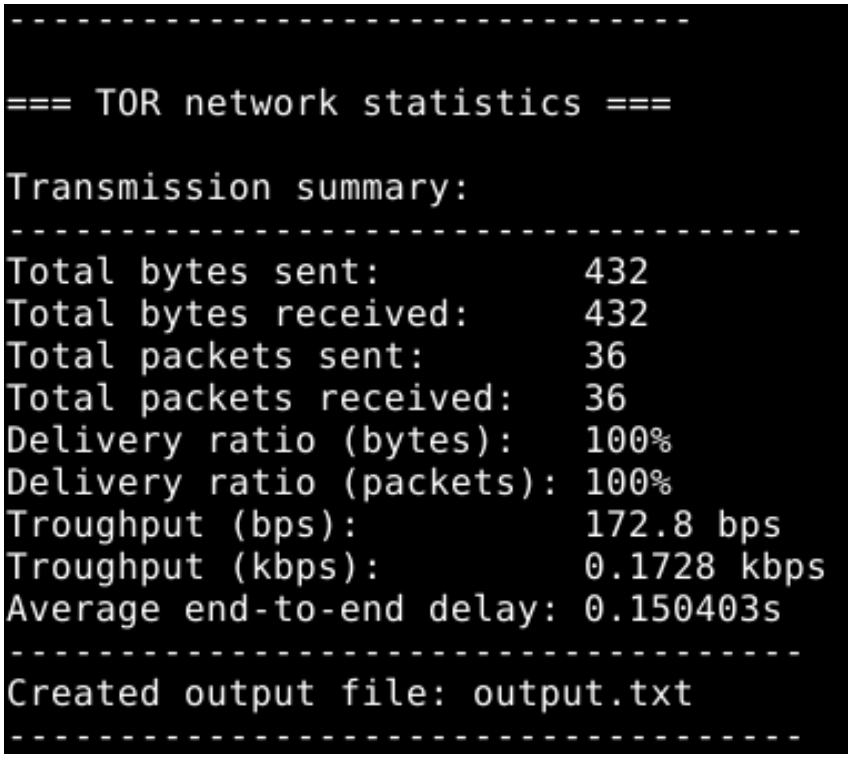
Na slici 4., propusnost također pokazuje eksponencijalni rast na početku, ali dostiže stabilizaciju mnogo brže nego na slici 2. (otprilike oko 4,5 sekunde). Ovaj brži rast je posljedica manjeg broja paketa, što omogućava mreži da brže obradi dolazne podatke. Maksimalna propusnost dostiže oko 700 bps, što je nešto kod prneosa 72 paketa zbog manjeg ukupnog opterećenja. Mreža se brzo prilagođava ovom manjem opterećenju, što pokazuje njenu efikasnost i agilnost u obradi podataka.

Prosječno kašnjenje ostaje konstantno na 0.150 s, što je identično kao na prvoj slici. Ova konzistentnost u kašnjenju, bez obzira na količinu podataka, ukazuje na efikasan protokol prijenosa podataka unutar TOR mreže. Takva stabilnost kašnjenja je izuzetno važna za održavanje kvaliteta usluge, posebno u kontekstu anonimnosti i sigurnosti koju TOR mreže pružaju.

Mreža pokazuje da može brzo dostići stabilizaciju propusnosti kada je opterećenje manje, ali maksimalna vrijednost propusnosti je nešto niža u poređenju s prvim slučajem (700 bps u odnosu na 800 bps). Ipak, prosječno kašnjenje ostaje stabilno, jer mreža efikasno upravlja saobraćajem bez obzira na količinu podataka.



Slika 4: *Prikaz dijagrama kašnjenja i propusnosti za 36 prenesena paketa*

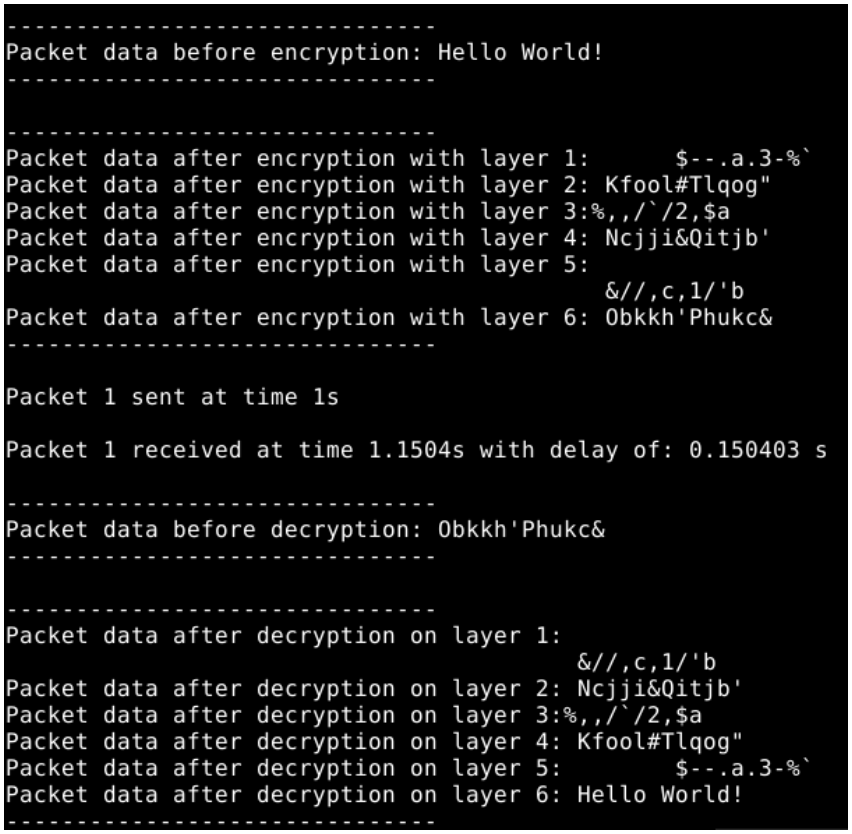


Slika 5: *Prikaz ispisa terminala za prenos 36 paketa*

Prema tome zaključujemo da scenarij sa 36 paketa pokazuje stabilnije karakteristike kašnjenja uz očuvanu propusnost mreže, što ukazuje na to da manji broj prenesenih paketa može rezultirati predvidljivijim mrežnim ponašanjem.

3.2 Enkripcija

U svrhu enkriptovanja podataka, koristi se UDP protokol koji omogućava komunikaciju između klijenta i servera. Pri toj komunikaciji, podaci će se prije slanja šifrirati kroz više slojeva. Ovaj pristup služi kao pojednostavljena reprezentacija enkripcije u TOR modelu, gdje se višeslojna enkripcija koristi za postizanje anonimnosti i sigurnosti podataka.



Slika 6: *Prikaz ispisa terminala enkriptovanih podtaka u prenosu*

Ako se promatra primjer sa slike iznad, vidljivo je da *"Hello World!"* enkripovana sa šest slojeva na predajniku, te nakon prenosa dekriptovana na prijemniku. Za svaki od tih šest slojeva koristi se drugačiji ključ za šifriranje. Nakon što paket stigne na odredište, dekripcija se odvija u obrnutom redoslijedu, pri čemu svaki sloj koristi isti ključ za dekripciju koji je korišten za enkripciju. Proces je simetričan, što znači da svaki sloj koristi iste metode za dešifriranje kao i za šifriranje.

Ovaj pristup enkripciji pruža dodatni nivo sigurnosti jer čak i ako napadač presretne paket, mora proći kroz šest različitih slojeva dekripcije da bi došao do originalne poruke. Korištenje UDP protokola omogućava brzu i efikasnu komunikaciju bez uspostavljanja sesije, ali uz dodatni rizik od gubitka paketa. UDP echo server i klijent koriste se za testiranje mrežne komunikacije, te olakšavaju provjeru ispravnosti višeslojne enkripcije i dekripcije, jer povratak identičnih podataka potvrđuje uspješnu dekripciju na odredištu.

4 Diskusija i Zaključak

U ovom radu implementiran je pojednostavljeni model TOR mreže u NS-3 simulatoru, što je omogućilo analizu performansi u kontekstu kašnjenja i propusnosti podataka. Rezultati simulacije pokazuju visok omjer isporučenih paketa i relativno nisko prosječno kašnjenje, što ukazuje na efikasnost modela u kontrolisanim uslovima. Ipak, prilikom poređenja sa teorijskim rezultatima, primijećeno je da simulacija pokazuje optimističnije performanse zbog pojednostavljenog modeliranja mreže.

Faktori poput stvarnog mrežnog zagušenja, dinamičkog rutiranja i dodatnih kriptografskih tehnika nisu u potpunosti uključeni u simulaciju, što bi moglo dovesti to razlika u performansama kada se model primijeni u stvarnim uslovima. Također, implementirana ekripcija nema uklanjanja slojeva eknripcije po hop-ovima, već se svi slojevi enkripcije uklanjaju na odredištu.

Na osnovu dobijenih rezultata može se zaključiti da implementacija TOR modela u NS-3 simulatoru uspješno demonstrira princip višeslojne enkripcije i anonimnog rutiranja, što doprinosi boljem razumijevanju sigurnosnih aspekata mrežne anonimnosti. Simulacija prikazuje da TOR mreža može osigurati efikasan prenos podataka uz visoku stopu isporučenih podataka sa niskim kašnjenjem, ali i da postoje izazovi koji se odnose na realne mrežne uslove i dodatne sigurnosne faktore.

Daljna istraživanja ove tematike trebala bi se fokusirati na uvođenje stvarnih (real life) scenarija kao i naprednijih kriptografskih operacija kako bi se dodatna validirala efikasnost TOR modela u realnim situacijama. Također, optimizacija enkripcije i poboljšanje mehanizma rutiranja mogli bi dodatno smanjiti kašnjenje i povećati propusnost, čime bi se unaprijedila sigurnost i pouzdanost anonimne komunikacije u TOR mreži.

Literatura

[1] G Golovko, A Matiashenko, and N Solopihin. Data encryption using xor cipher. , *'.* , 1(63):81–83, 2021.

[2] Kyle Hogan, Sacha Servan-Schreiber, Zachary Newman, Ben Weintraub, Cristina Nita-Rotaru, and Srinivas Devadas. Shortor: Improving tor network latency via multi-hop overlay routing. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1933–1952. IEEE, 2022.