UNIVERZITET U SARAJEVU
ELEKTROTEHNIČKI FAKULTET
ODSJEK ZA TELEKOMUNIKACIJE

Dizajn i implementacija TOR modela u NS-3 simulatoru

Projektni zadatak iz predmeta Simulacija procesa u telekomunikacijskim mrežama
Teorijski dio

Crnčalo Vedad, 2293/2024
Crnčalo Muhamed, 2237/2024
Dedović Harun, 2294/2024
Bumbul Amna, 2292/2024

Sarajevo, 2024. godina

Sadržaj

Uvod

Potreba za anonimnosti tokom korištenja interneta, bila je jedan od glavnih prioriteta korisnika još od njegovog nastanka. U svrhu postizanja privatnosti na tako javnoj platformi, laboratorija za istraživanje mornarice Sjedinjenih Američkih Država razvila je koncept onion rutiranja, koji je osnova za tehnologiju poznatu kao "TOR." Ta tehnologija je puštena kao open source softver 2004. godine, finansiraju i održavaju ga širok spektar interesnih skupina, od vlade SAD-a do pojedinaca. [1]

TOR mreža predstavlja sistem servera koje održavaju volonteri, a omogućava korisnicima da povećaju svoju privatnost i sigurnost na internetu. Umjesto da uspostave direktnu vezu, korisnici se povezuju putem niza virtuelnih tunela, što im omogućava da razmjenjuju informacije preko javnih mreža bez ugrožavanja privatnosti. Pored zaštite privatnosti, Tor se koristi kao alat za zaobilaženje cenzure, omogućavajući pristup sadržajima ili odredištima koja su inače blokirana. Također, TOR predstavlja osnovu za razvoj novih komunikacionih alata koji imaju ugrađene funkcije zaštite privatnosti. [2]

TOR Browser ima širok spektar primjena, prvenstveno usmjerenih na zaštitu privatnosti i anonimnosti korisnika na internetu. Tor je također ključan za pristup dark webu, gdje se nalaze anonimne .onion stranice, te za sigurnu komunikaciju aktivista i novinara u zemljama s ograničenjem slobode govora. Osim toga, Tor se koristi u testiranju sigurnosnih aplikacija, omogućujući programerima da razvijaju i testiraju protokole u anonimnim uvjetima.

Glavni cilj ovog rada je teoretska obrada TOR pretraživača i onion rutiranja na kojem se zasniva. U ovim poglavljima poseban osvrt je na način njegovog rada, način funkcionisanja i razlog njegove primjene. U nastavku, rad prolazi kroz razloge modeliranja TOR mreže, gdje se navodi njena uloga u pružanju sigurnosti i anoniminosti prilikom korištenja interneta. Naredno poglavlje opisuje detaljan princip onion rutiranja, u kojem se enkriptovani podatci prijenose preko više nasumičnih čvorova. U okviru rada predstavljen je karakterističan scenarij TOR modela, koji uključuje njegovu topologiju i potrebne načine konfiguracije simulacije. Eksperimentalni dio rada fokusirati će se na mjerenje ključnih metrika kao što su latencija i propusnost, analizu rezultata te njihov prikaz u grafičkom obliku. Na kraju rada, opisuju se pristupi modeliranju TOR mreže koriteći simulacijske alate. Kao primjer simulacijskih alata uzet je ExperimenTor.

1 Razlog modeliranja TOR mreže

"Onion rutiranje" predstavlja distribuiranu mrežu koja je dizajnirana da učini anonimnim aplikacije baziranje na TCP-u kao što su web pretraživači i aplikacije za slanje poruka. Klijenti biraju put kroz mrežu u kojoj svaki čvor ili "onion ruter" na putu zna prethodi čvor i sljedeći čvor, ali ne zna ostale čvorove u mreži. [5]

TOR pripada kategoriji dizajna niskog kašnjenja koji pokušava interaktivni mrežni saobraćaj učiniti anonimnim. Također, omogućava pogodniji način dostave e-mail-a u poređenju s anonimne e-mail mreže sa znatnim kašnjenjem, zato što udaljeni mail server dostavlja blagovremenu potvrdu o dostavljanju. [5]

Najjednostavnije rješenje niskog kašnjenja predstavlja "single hop proxy" kao što je "Anonymizer", a to je jedan povjerljiv server koji uklanja podatke o ishodištu paketa prije njegovog prosljeđivanja. Ovi dizajni se mogu jednostavno analizirati, ali korisnici trebaju vjerovati tom proxy-ju. Koncentrisanje saobraćaja u jednu tačku povećava anonimni niz (osobe među kojima se korisnik krije), ali to predstavlja problem ako neko to zloupotrijebi i posmatra sav saobraćaj koji ulazi i izlazi iz proxy-ja.[5]

TOR mreža je posebna iz razloga što svaki "onion ruter" funkcioniše kao obični proces koji se izršava na nivou običnog korisnika bez viših privilegija. Svaki onion ruter održava TLS (Transport layer security) konekciju do svakog drugog onion rutera. Identifikacioni ključ se koristi kako bi se potpisali TLS certifikati i koristi se kako bi se dešifrovali korisnički zahtjevi za postavljanjem posebne mreže i za razmjenjivanje kratkotrajnih identifikacionih ključeva. [5]

Pored toga što je moguće inicirati anonimnu komunikaciju, klijenti također mogu odabrati način komunikacije koji im omogućava da ne otkrivaju svoj identitet ili lokaciju. [6]

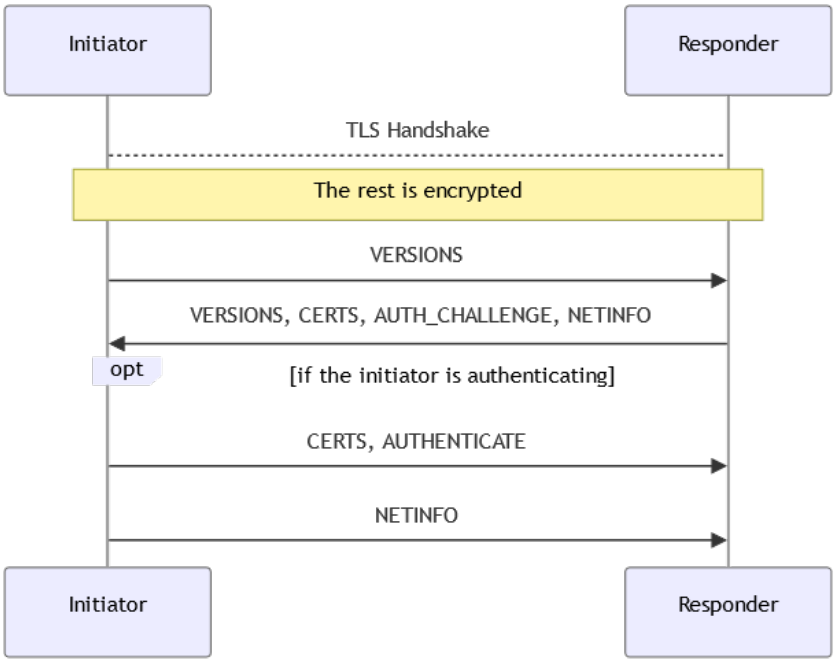
Koriste se kanali koji su direktna šifrirana konekcija između dva TOR releja ili između klijenta i releja. Kanali se implementiraju kao TLS sesije preko TCP-a. Klijenti i releji mogu imati otvorene nove kanale, ali samo relej može biti primalac kanala. Kako bi se uspješno uspostavio kanal, relej koji treba odgovoriti mora dokazati kriptografsko vlasništvo jednog ili više relej identiteta, koristeći "digitalno rukovanje" koje kombinira TLS i niz TOR ćelija. [6]

Trajanje kanala je ograničeno. Bilo koja strana (ili klijent ili server) može zatvoriti kanal ako nema uspostavljenih "kola" i ako je "KeepalivePeriod" koji obično traje 5 minuta, istekao od posljednjeg puta kada su se neki podaci prenijeli mrežom. [6]

Prethodno navedeno omogućava integritet podataka i privatnost, kao i autentikaciju, povjerljivost i otpornost na "man-in-the-middle" napada.

TLS funkcioniše na sljedeći način:

- Onaj ko inicira "digitalno rukovanje" to uspijeva otvaranjem TLS konekcije.
- Obje strane šalju "VERSIONS" kako bi se dogovorile koju verziju protokola bi trebale koristiti.
- Strana koja odgovara šalje "CERTS ćeliju" strani koja je inicirala komunikaciju kako bi ta strana dobila certifikate koji su joj potrebni da sazna identitet strane koja odgovara, AUTH_CHALLENGE ćeliju za autentikaciju i NETINFO ćeliju za uspostavljanje IP adresa.
- Strana koja inicira komunikaciju provjerava da li je CERTS ćelija ispravna i odlučuje da li da pređe na autentikaciju.
- Ako strana koja inicira komunikaciju ne može autenticirati sebe, šalje NETINFO ćeliju.
- Ako strana koja inicira komunikaciju može inicirati samu sebe, šalje CERTS ćeliju, AUTHENTICATE ćeliju i NETINFO ćeliju.[6]



Slika 1: *TLS rukovanje između inicijatora i odgovarača.*[6]

Ključni razlozi zbog kojih je **TOR** odličan primjer za modeliranje su:

- **Skalabilnost:** Naglašava jednostavnost dizajna i novi načini poboljšavanja dizajna se nastavljaju otkrivati;
- **Kontrola zagušenja:** TOR koristi decentraliziranu kontrolu i koristi potvrdu s kraja na kraj kako bi se zadržala anonimnost dok se čvorovima na rubu mreže omogućava detektovanje zagušenja ili preplavljivanja te se potom šalje manje podataka dok zagušenje ne prestane;
- **Omogućeno multipleksiranje više TCP tokova:** TOR ovo omogućava kako bi se poboljšala efikasnost i povećala anonimnost;
- **Podržavanje mnogih programa baziranih na TCP-u bez modifikacije;**
- **Provjeravanje integriteta podataka:** Provjera se obavlja prije nego što podaci napuste mrežu;
- **Serveri direktorija:** Određeni čvorovi imaju ulogu servera direktorija i oni obezbjeđuju potpisane direktorije koji opisuju poznate rutere i njihovo trenutno stanje, a korisnici ih periodično preuzimaju;
- **Bez zahtjeva za zakrpama jezgre OS-a:** TOR ne zahtijeva zakrpe jezgre operativnog sistema niti podršku za *network stack*.

2 Princip rada Onion rutiranja

Nakon definisanja TOR-a, prirodno se postavlja pitanje kako on radi. Onion rutiranje je infrastruktura za privatnu komunikaciju putem javnih mreža. Omogućava anonimne veze koje su izuzetno otporne na presretanje i analizu saobraćaja. Ove anonimne veze su dvosmjerne, i mogu se koristiti bilo gdje je moguća upotreba standardne mrežne veze. U onion rutiranju, ne uspostavlja se direktna veza između izvorišnog i odredišnog uređaja. Već se komunikaciji vrši preko niza mrežnih uređaja poznatih kao onion čvorišta. [3]

Onion ruting mreža se pristupa putem niza proxy servera. Aplikacija koja inicira vezu uspostavlja socket vezu sa aplikacijskim proxy-jem, koji zatim prilagođava format poruke o konekciji i podatke koji će se prenositi u oblik koji može biti proslijeđen kroz onion ruter mrežu. Ovaj proxy se potom povezuje sa onion proxy-jem, koji definira rutu kroz mrežu kreiranjem složene strukture podataka zvane "onion". [3]

Ti releji su nasumično odabrani, dok podaci koji će prolaziti kroz njih su prvo enkriptovani kriptografijom eliptičke krive. Kako podaci prolaze kroz ulazni relej prvi sloj enkripcije se uklanja, te podaci nastavljaju put prema srednjem releju. Srednji relej uklanja još jedan sloj enkripcije i prosljeđuje enkriptovane podatke posljednjem releju (izlazni relej). Izlazni relej tada uspostavlja vezu sa željenim odredištem korisnika putem nezaštićene veze. [4] Zbog ovog postepenog uklanjanja slojeva enkripcije na relejima, ova tehnika je i dobila ime onion rutiranje (onion.prev.eng luk).

Važno je naglasiti da relej može identifikovati samo prethodni i naredni relej u nizu, što komunikaciju između uređaja čini još težom za pratiti. Identifikaciju dodatno komplikuje to što se odabrani releji mijenjaju svakih 10 minuta. Podaci koji se prijenose preko releju, zbog stalnog uklanjanja slojeva, izgledaju drukčiji nakon svakog hop-a.

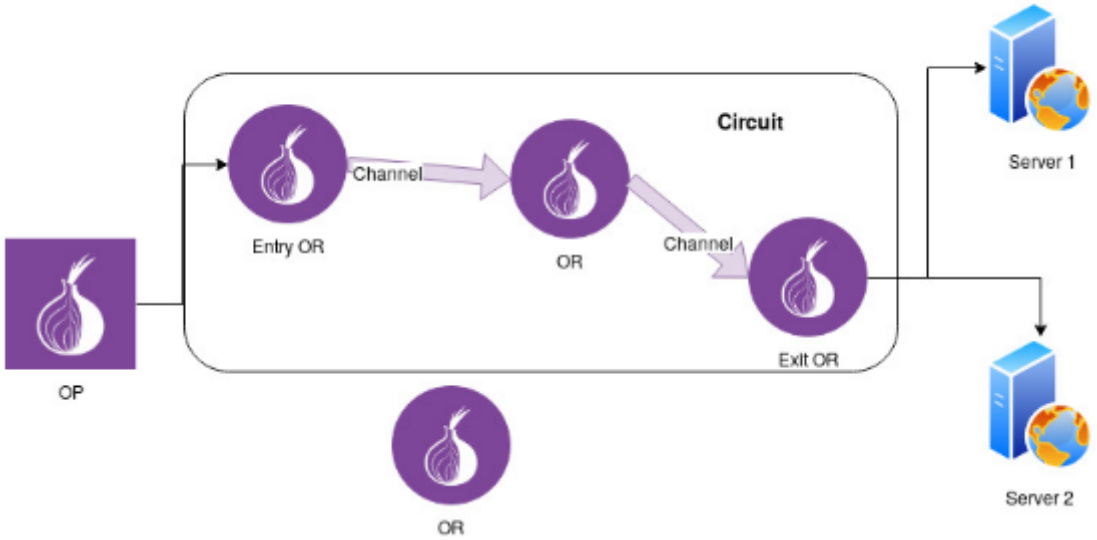
Dizajn TOR mreže podrazumijeva da su IP adrese TOR releja (početni, srednji i izlazni) javne. Međutim, jedan od načina na koji vlasti ili internet provajderi (ISP-ovi) mogu blokirati TOR jeste blokiranjem IP adresa ovih javnih TOR releja. TOR bridge-ovi su releji unutar mreže koji nisu uključeni u javni TOR direktorijum, što otežava njihovo blokiranje od strane ISP-ova i vlasti. [2]

Iako za prolazak podataka onion ruting mrežu zovemo rutiranje, on se ne obavlja na mrežnom sloju, već na aplikacijskom. Specifično, za usmjeravanje podataka kroz dugoročne socket veze koristimo IP rutiranje. Anonimna veza se sastoji od dijelova više međusobno povezanih dugoročnih multipleksiranih socket veza. Iako je niz onion releja u anonimnoj vezi fiksiran tokom njenog trajanja, ruta kojom podaci putuju između tih releja zavisi od osnovne IP mreže. Stoga se onion rutiranje može usporediti sa slobodnim usmjerenjem izvora. [3]

3 Karakterističan scenarij za testiranje TOR modela

Internet komunikacije postaju predmet nadzora i napada koji ugrožavaju sigurnost i privatnost korisnika interneta. Vlada može uspostaviti nadzor saobraćaja u nekim slučajevima kako bi uklonila sadržaj opozicije ili kako bi nekoga locirala.

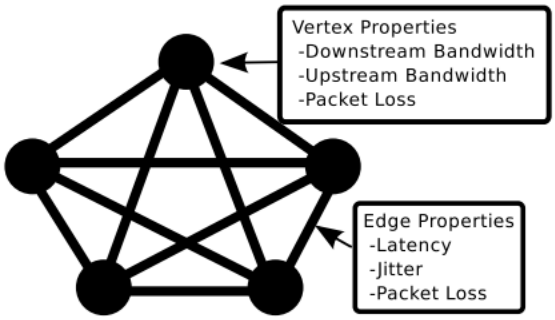
Kako bi se zaštitila privatnost korisnika, TOR mreža ima za cilj sačuvati privatnost i sigurnost korisnika tokom pretraživanja interneta. Tipični izgled TOR mreže je prikazan na slici 2. ispod.



Slika 2: *Tipični izgled TOR mreže.*[7]

3.1 Topologija karakterističnog slučaja

Karakteristike čvorova su: dolazna širina propusnog opsega, odlazna širina propusnog opsega, gubitak paketa. Karakteristike rubova su: kašnjenje, jitter i gubitak paketa.



Slika 3: *Topologija karakterističnog slučaja.*[8]

Prvo razmatramo strukturu naše eksperimentalne mreže. U idealnom slučaju, naša mrežna topologija replicirala bi internet arhitekturu, uključujući sve autonomne sisteme kao što su: jezgro, okosnica, ruteri, i sve veze između njih. Takva struktura bi dala najpreciznji pogled na internet eksperimentalni okvir.

Nažalost, tačna struktura interneta je nepoznata, a čak i da je poznata, bila bi prevelika i to bi bilo neefikasno za replicirati kada su u pitanju eksperimentalne svrhe. Stoga, koristit ćemo manji, upravljiv model interneta.

Mrežni čvorovi: U našem grupisanom pristupu, kreiramo mrežni čvor za svaku zemlju. Svakom čvoru je dodijeljen podrazumijevani odlazni propusni opseg, dolazni propusni opseg, i svojstva gubitaka paketa, dobijena iz podataka Ookla Net Indeksa.

Mrežni rubovi: Svaki čvor u topologiji je povezan sa svakim drugim, formirajući kompletan grafikon. Svaka od ovih povezanosti predstavlja se kao mrežna ivica. Dodjeljujemo svakoj mrežnoj ivici sljedeće svojstva: kašnjenje (s kraja na kraj paketa), jitter (varijacija u odlaganju paketa), i gubitak paketa (djelić paketa koji se odbacuje).

Kada podesimo topologiju, onda podesimo host uređaje koji rade u toj topologiji. U kontekstu TOR mreže, najbitniji su TOR releji, TOR klijenti, TOR vlasti i internet web/serveri datoteka. Zbog hardverskih ograničenja, broj releja i klijenata biva smanjen.[8]

Da bismo utvrdili tačnost i bili uvjereniji u naš TOR mrežni model, koristimo sljedeće eksperimentalne alate TOR-a: Shadow i ExperimenTor.

Testiramo naš model sa dvije različite veličine mreže, od kojih su smanjene verzije TOR mreže. U našoj manjoj mreži, podešavamo 50 releja i 500 klijenata koji komuniciraju sa 50 HTTP servera datoteka. U našoj velikoj mreži, podešavamo 100 releja i 1000 klijenata koji komuniciraju sa 100 HTTP servera datoteka.

Modeliranje distribuiranog sistema je složen proces. Tokom ovog procesa otkrili smo da je važno koristiti prava internet i sistemska mjerenja kako bi se eliminisale proizvoljne odluke o modeliranju, s obzirom da to teži značajnom utjecaju na to kako precizno eksperimentalno okruženje umnožava stvarni distribuirani sistem. Mjerenja se ne bi trebala koristiti dok se u potpunosti ne razumiju, ili sve dok im se ne može potvrditi preciznost.[8]

4 Cilj i metodologija eksperimenata

Kroz ovaj projektni zadatak, fokus će biti na analizi utjecaja broja hopova u TOR mreži na ključne performanse i sigurnosne karakteristike. TOR mreža, kao decentralizirana platforma za anonimnu komunikaciju, oslanja se na koncept višestrukog prosljeđivanja podataka kroz mrežne čvorove(relej-e), čime se osigurava visok nivo privatnosti i anonimnosti. Eksperiment će biti dizajniran tako da uključuje simulaciju različitih scenarija TOR mreže s varijabilnim brojem hopova. Svaki scenarij predstavlja specifičnu konfiguraciju rute podataka između klijenta i destinacije, pri čemu broj hopova označava koliko čvorova učestvuje u prosljeđivanju i šifriranju podataka. Simulacija će se izvoditi u kontrolisanom okruženju uz primjenu odgovarajućih alata (NS- simulatora) koji omogućava detaljno praćenje performansi mreže.[11]

4.1 Mjerenje ključnih metrika

Za svaki eksperimentalni scenario pratit će se i kvantitativno analizirati sljedeće metrike:

- **Kašnjenje (latency)**: Mjeri se ukupno vrijeme prijenosa podataka od klijenta do odredišta. Veći broj hopova može povećati kašnjenje zbog dodatnih procesorskih operacija (šifriranje/dešifriranje) i mrežnih kašnjenja na svakom čvoru.
- **Propusnost (throughput)**: Analizira se količina podataka koja se uspješno prenosi u jedinici vremena. Promjene u propusnosti mogu ukazivati na uticaj dodatnih hopova na efikasnost mreže.
- **Sigurnosni parametri (security metrics)**: Procjenjuje se nivo anonimnosti i otpornost na identifikaciju korisnika u zavisnosti od broja hopova. Veći broj hopova obično povećava sigurnost, ali može izazvati degradaciju performansi.
- **Šum u podacima (noise)**: Proučava se efekat dodatnih slojeva enkripcije na kvalitet i integritet podataka u mreži, uz razmatranje mogućnosti gubitka podataka uslijed kompleksnih operacija.[11]

4.2 Analiza rezultata

Očekuje se da analiza pokaže jasnu povezanost između broja hopova i performansi TOR mreže, te omogući identifikaciju optimalnog broja hopova za balansiranje sigurnosti i efikasnosti.

Nakon prikupljenih podataka, rezultati će se detaljno analizirati kako bi se identifikovali kompromisi između:

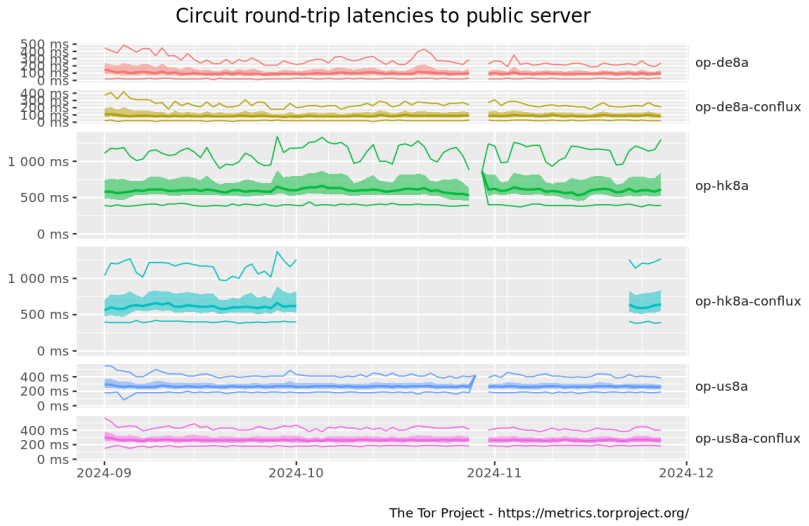
- **Sigurnosti**: Koliko dobro mreža štiti identitet korisnika uz različit broj hopova.
- **Efikasnosti**: Koliko brz i pouzdan ostaje prijenos podataka kroz mrežu.
- **Resursne potrošnje**: Utjecaj broja hopova na procesorsku i memorijsku efikasnost svakog čvora.[11]

4.3 Prikaz rezultata

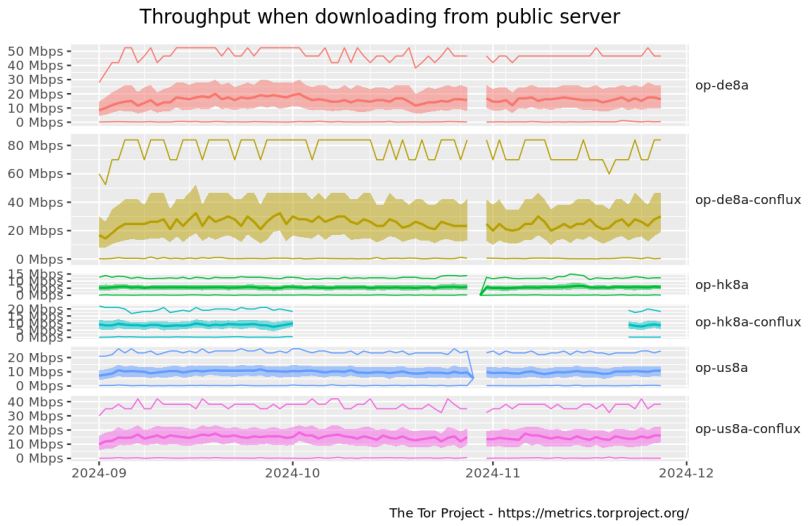
Za prikaz krajnjih rezultata u ovom projektnom zadatku koristit će se kombinacija grafičkih i numeričkih prikaza kako bi se omogućila jasna i intuitivna interpretacija rezultata.

Grafički prikazi su sljedeći:

- **Bar chart** - za uspoređivanje mjernih vrijednosti (kašnjenja, propusnosti, sigurnosti) za različite brojeve hopova.
- **Line chart** - za prikaz promjena performansi kada se broj hopova povećava.
- **Heatmap** - za kombinacije broja hopova, kašnjenje i sigurnost, za prikazivanje intenziteta



Slika 4: *Kašnjenja kružnih ruta (latenciju) za Tor mrežu*[12]



Slika 5: *Propusnost (throughput)*[12]

5 Načini modeliranja simulacijskog rješenja

Prethodne metode za eksperimentaciju Tor mreža:

- **Analitičko modeliranje** : Ovo predstavlja apstraktno modeliranje procesa odabira TOR rutera i procjena očekivane vjerovatnoće napada u smislu da napadači presretnu vezu i kontrolišu ulazne i izlazne pozicije TOR mreže kroz napade uskraćivanja usluga (DDOS). Iako ova analiza pruža vrijedne uvide u ovaj napad, ovaj analitički model pretpostavlja da klijenti biraju TOR rutere na osnovu modela uniformnong odabira. Tor klijenti zapravo biraju rutere po propusnosti, stoga je neizvjesno da li će precizno ponašanje koje je zapaženo biti takvo u stvarnoj mreži.[9]

- **Simulacije** : TOR-ov algoritam odabira rutera je veoma kompleksan i veoma je teško apstrahirati model, tako da je neophodno implementirati mehanizam odabira u simulaciji i posmatrati stope kompromisa „kola“ mreže. Simulator je koristo podatke TOR servera datoteka za modeliranje TOR rutera. Alternativno, ovaj vid analize se može izvršiti putem emulacije TOR klijenata koji pokreću stvarni TOR kod u „testbed“ okruženju.

- **PlanetLab eksperimentalna platforma** : Veliki nedostatak PlanetLab-a kao eksperimentalne platforme je to što se rezultati često ne mogu reproducirati. Ipak, mnogi istraživači su koristili PlanetLab za proučavanje TOR-a.

- **Simulacije malih razmjera** : Iako bi ovakve simulacije bile dovoljne kako bi se demonstrirao, recimo neki napad ili presretanje mreže, kako bi se osiguralo duboko razumijevanje kako napad izgleda u praksi, može biti potrebno skalirati eskperiment više od onoga što je do tada dostupno

- **Stvarni eksperimenti** : Mnoga prijašnja Tor istraživanja su sprovodila eksperimente, mjerenja i analizu koja je uključivala korištenje stvarne Tor mreže, što pruža bolji uvid u pravo ponašanje Tor mreže, međutim, uvidjelo se da sva ta istraživanja imaju određena ograničenja i potencijalne opasnosti[9]

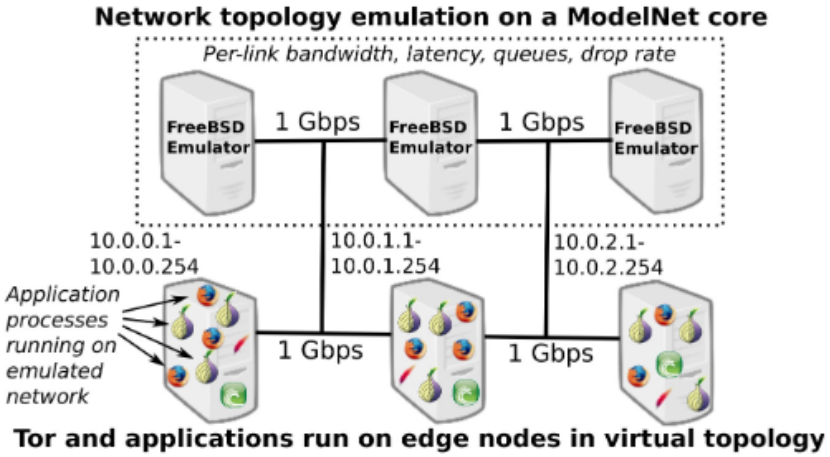
5.1 Experimentacija sa ExperimenTor-om

Kako bi se mogli sprovoditi eksperimenti velikih razmjera putem TOR mreže na način koji osigurava sigurnost stvarnim TOR korisnicima, implementacija ExperimenTor-a predstavlja rješenje. To je TOR testbed baziran na mrežnoj simulaciji sa pripadajućim eksperimentalnim setom alata.

Modeliranje stvarne TOR mreže je izuzetno teško, a kako bi se napravio testbed koji vjerno prikazuje stvarnu TOR mrežu, ključno je precizno modelirati distribuciju propusnosti Tor rutera. Pored preciznih modela TOR rutera, također je neophodno precizno modelirati TOR klijente. Takvi modeli bi trebali precizno opisivati broj TOR klijenata i njihov odlazni saobraćaj u pogledu distribucije aplikacija, broja konekcija i saobraćaja.

Također je neophodno precizno modelirati temeljnu mrežu. DETER i Emulab imaju ograničene resurse za obradu podataka i ograničene mrežne resurse, što ih ograničava na eksperimente malih razmjera koji se mogu izvoditi na testbed-ovima.[9]

Prvi korak prije sprovođenja bilo kakvog eksperimenta u testbed-u je generisanje mrežne topologije i njeno raspoređivanje na ModelNet emulator.



Slika 6: *ExperimenTor sistemska arhitektura*[9]

Kako bi se precizno modelirala distribucija propusnosti TOR mrežnog rutera, konfiguracijski alat prvo dobija informaciju rutera od TOR servera direktorija i „izvlači“ kapacitet svakog rutera. Zatim, mapira svaki ruter na krajnji host uređaj koji se nalazi unutar virtuelne topologije i dodjeljuje stvarnu vrijednost propusnosti. Naposljetku, set alata dodjeljuje realistična mrežna kašnjenja svakom krajnjem host uređaju.

Nakon što je kreirana virtuelna topologija, neophodno je rasporediti TOR rutere. Prvi korak je kreiranje servera direktorija za testbed TOR eksperiment, što se postiže tako što se jednostavno generiše par javnog i privatnog ključa za svaki server direktorij koji će se koristiti u testbed-u (pet direktorija je dovoljno da se distribuira opterećenje saobraćaja zahtjeva TOR klijenata). Kako bi se osiguralo da svi simulirani TOR klijenti i ruteri koriste direktorije testbed-a umjesto stvarnih direktorija, neophodno je sačuvati svaki javni ključ testbed direktorij-a i to se distribuira TOR-ovim ruterima i klijentima u testbed-u.

Konfigurisanje TOR klijenata i aplikacija i pokretanje i analiziranje eksperimenata predstavljaju posljednje korake simulacije. Eksperimentor set alata sadrži sve što je neophodno za konfigurisanje mrežne topologije, servera direktorija, TOR rutera i TOR klijenata. Dodatno, set alata upravlja izvršavanjem eksperimenata. Jedna glavna skripta kreira instancu testbed-a, pokreće eksperimente, zaustavlja ih nakon specificiranog vremena i prikuplja podatke koji su generisani tokom eksperimenta. Testbed pomaže u otklanjanju problema performansi.[9]

Zaključak

U zaključku ovog rada, izvršena je rekapitulacija teorijske obrade TOR modela i onion rutiranja na kojem se on zasniva. Kroz rad je potvrđena efikasnost onion rutiranja kao infrastrukture za anonimnu i sigurnu komunikaciju putem javnih mreža, koja je otporna na presretanje i analizu saobraćaja.

U radu se vrži obrada teme, od teorijske istraživanja samog koncepta, prolaska kroz simulaciju mrežnih topologija, pa sve do eksperimentalne analize metrika kao što su latencija, propusnost, te gubitak paketa. Ovi nalazi pružaju osnovu za buduća istraživanja, koja bi mogla unaprijediti sigurnost i efikasnost TOR mreže, posebno u kontekstu otpornosti na napade i optimizacije resursa. Pružen je i primjer simulacijskog alata ExperimenTor, koji je omogućava precizno testiranje raznih scenarija i tako pruža smjernice za unapređenje TOR mreže.

Spisak slika

Literatura

[1] https://georgetownlawtechreview.org/onion-routing-and-tor/GLTR-11-2016/

[2] https://2019.www.torproject.org/about/overview(torproject.org)

[3] "Anonymous Connections and Onion Routing"Michael G. Reed, Member, IEEE, Paul F. Syverson, and David M. Goldschlag

[4] Hiding Behind the Keyboard: Uncovering Covert Communication Methods with Forensic Analysis

[5] https://journals.ala.org/index.php/rusq/article/view/5704/7093

[6] https://css.csail.mit.edu/6.858/2022/readings/tor-design.pdf

[7] https://spec.torproject.org/tor-spec/channels.html

[8] https://www-users.cse.umn.edu/~hoppernj/tormodel-cset2012.pdf

[9] https://css.csail.mit.edu/6.858/2023/readings/tor-traffic-analysis.pdf

[10] https://seclab.cs.georgetown.edu/papers/experimentor.pdf

[11] ŠhorTor: Improving Tor Network Latency via Multi-hop Overlay Routing"2022 IEEE Symposium on Security and Privacy (SP)

[12] https://metrics.torproject.org/networksize.html