Mjerenje i predviđanje prometa u telekomunikacijskoj mreži

Tirić, Suzana

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Suzana Tirić

MJERENJE I PREDVIĐANJE PROMETA U TELEKOMUNIKACIJSKOJ MREŽI

ZAVRŠNI RAD

Zagreb, 2019.

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

MJERENJE I PREDVIĐANJE PROMETA U TELEKOMUNIKACIJSKOJ MREŽI

TRAFFIC MEASUREMENT AND FORECAST IN TELECOMMUNICATIONS NETWORK

Mentor: prof. dr. sc. Štefica Mrvelj

Student: Suzana Tirić
JMBAG: 0135229889

Zagreb, rujan 2019.

MJERENJE I PREDVIĐANJE PROMETA U TELEKOMUNIKACIJSKOJ MREŽI

SAŽETAK

Sve složenijom mrežnom topologijom, povećava se zagušenje mreže i neočekivane situacije u mreži. Kako bi se spriječilo navedeno, potrebno je mjerenje i predviđanje mrežnog prometa. Analiza mrežnog prometa je proces snimanja, pregledavanja i analiziranja mrežnog prometa. Koriste se različite tehnike analize, a opći okvir za mrežnu analizu uključuje pred-obradu, stvarnu analizu i otkrivanje uzoraka mrežnih podataka. Predviđanjem mrežnog prometa kontrolira se i sprječava zagušenje, a poboljšava se iskoristivost mreže. Točno i pouzdano predviđanje omogućuje planiranje kapaciteta mreže i održavanje zahtijevane kvalitete usluge. Kako bi se pravilno dimenzionirale mreže koriste se prometni modeli. Prometni modeli su skup mjerenih i izračunatih parametara na temelju kojih je moguće izračunavanje očekivanog mrežnog prometa te definiranje ponuđenog mrežnog prometa.

KLJUČNE RIJEČI: mjerenje mrežnog prometa; alati za mjerenje mrežnog prometa; predviđanje mrežnog prometa; modeli predviđanja mrežnog prometa

TRAFFIC MEASUREMENT AND FORECAST IN TELECOMMUNICATIONS NETWORK

SUMMARY

With an increasingly complex network topology, there is an increase in network congestion and unexpected network situations. To prevent this, network traffic measurement and prediction of network traffic are required. Network traffic analysis is the process of capturing, reviewing and network traffic analysis. There are different analysis techniques used and the general network analytics framework includes pretreatment, real analysis, and network data sample detection. With prediction of network traffic, congestion is being prevented and controlled while improving and utilizing the network. Accurate and reliable traffic predictability makes possible network capacity planning and maintenance of quality services. To properly size up networks, traffic models are used. Traffic models are gathered as calculated and measured parameters on the basis of which is possible calculation of expected network traffic while defining offered network traffic.

KEY WORDS: network traffic measuring; network traffic measuring tools; network traffic prediction; network traffic prediction models

SADRŽAJ

1. Uvod

Složenijom mrežnom topologijom, povećava se zagušenje mreže i neočekivane situacije u mreži. Kako bi se spriječilo navedeno, potrebno je mjerenje i predviđanje mrežnog prometa. Analiza mrežnog prometa je proces snimanja, pregledavanja i analiziranja mrežnog prometa. Svrha rada je prikazati različite tehnike mjerenja, analize i predviđanja mrežnog prometa te alate koji se koriste za analizu mrežnog prometa. Alati za analizu mrežnog prometa mogu se podijeliti na programske ili sklopovske. Sklopovski alati ugrađeni su u telekomunikacijsku opremu, dok su programska rješenja šire namjene, a sposobna su analizirati mnogo više protokola. Predviđanje telekomunikacijskog prometa omogućava kvalitetno planiranje odnosno dimenzioniranje potrebnih resursa kako bi se zadovoljila željena kvaliteta usluge. Za pravilno dimenzioniranje telekomunikacijskog sustava upotrebljavaju se prometni modeli.

Naslov završnog rada je: **Mjerenje i predviđanje prometa u telekomunikacijskoj mreži**. Rad je podijeljen u sedam cjelina:

1. Uvod
2. Analiza mrežnog prometa u telekomunikacijskoj mreži
3. Alati za analizu mrežnog prometa u telekomunikacijskoj mreži
4. Predviđanje mrežnog prometa u telekomunikacijskoj mreži
5. Problemi predviđanja mrežnog prometa u telekomunikacijskoj mreži
6. Poboljšanje procesa analize i predviđanja mrežnog prometa u telekomunikacijskoj mreži
7. Zaključak

U drugom poglavlju opisan je postupak mjerenja i analize mrežnog prometa. Metode mjerenja te faze analize mrežnog prometa.

Alati koji se koriste prilikom mjerenja i analize mrežnog prometa prikazani su u trećem poglavlju.

Poglavlje *Predviđanje mrežnog prometa u telekomunikacijskoj mreži* opisuje metode kojima se provodi predviđanje prometa.

U petom poglavlju opisani su problemi koji utječu na predviđanje mrežnog prometa u telekomunikacijskoj mreži.

Metode za poboljšanje predviđanja mrežnog prometa prikazane su u šestom poglavlju.

2. Analiza mrežnog prometa u telekomunikacijskoj mreži

Analiza mrežnog prometa je proces snimanja, pregledavanja i analiziranja mrežnog prometa u svrhu izvedbe, sigurnosti te općih mrežnih operacija i upravljanja. To je postupak korištenja ručnih i automatiziranih tehnika za pregled detaljnih podataka i statistika unutar mrežnog prometa. Analiza mrežnog prometa prvenstveno se vrši radi detaljnijeg uvida u vrstu prometa, odnosno mrežnih paketa ili podataka koji prolaze kroz mrežu. Analiza mrežnog prometa obično se vrši putem mrežnog *softvera* za nadgledanje propusnosti mreže. Statistika dobivena analizom mrežnog prometa pomaže prilikom razumijevanja i vrednovanja korištenja mreže, brzine prijenosa te kod određivanja vrste, veličine, podrijetla i odredišta sadržaja. Analiza mrežnog prometa koristi se i radi identifikacije zlonamjernih ili sumnjivih paketa unutar mreže. Također, nastoje se pratiti brzine preuzimanja, prijenosa, propusnost, sadržaj, itd. radi razumijevanja mrežnih operacija [1].

Analiza mrežnog prometa predstavlja postupak presretanja mrežnih paketa i podvrgavanje istih analizi. Nakon što se mrežni paket presretne, vrši se lokalno zapisivanje te se paket prosljeđuje na odredište. Analiza mrežnog prometa se vrši bez izmjene i blokiranja komunikacije [2].

Mjerenje i analiza mrežnog prometa ključni su za dizajn, rad i održavanje mreže širokog područja (WAN - *Wide Area Network*). Sa sve većom popularnošću *Interneta*, brzina prijenosa i vrijeme obrade predstavlja presudan problem. Infrastruktura WAN mreže daleko je od zahtjeva brzog, ogromnog i neprekidnog rasta mreže. Mrežna izvedba važna je zbog stvaranja uvida u mrežu što pomaže kod razvijanja mrežnih operacija i protokola. Sa stajališta analize, prometni modeli imaju značajnu ulogu jer poboljšavaju razumijevanje kompliciranih mrežnih karakteristika i ponašanja mreže te omogućuju proučavanje učinaka raznih parametara modela na mrežnoj izvedbi i simulaciju istih. Postoje mnogi alati za pronalaženje prometnih modela, a među najučinkovitijim je diskretna valna transformacija. Ključno pitanje kod dizajniranja i odabira shema upravljanja zagušenjem je uzorak prometa, a uzorci prometa ovise o aplikacijama [3].

Dobivanje podataka o mrežnom prometu iz stvarne WAN mreže ima važnu ulogu kod mjerenja mrežnog prometa, a sustavno prikupljenim podacima može se izvući zaključak o

mrežnom ponašanju. Prema [3] postoji nekoliko načina mjerenja mrežnog prometa u stvarnim mrežama:

- dnevnicima poslužitelja
- pasivnim mjerenjem
- aktivnim mjerenjem.

Prvi način mjerenja mrežnih podataka vrši se dnevnicima poslužitelja, tako što se *web* poslužitelji mogu konfigurirati za snimanje podataka koji uključuju sve zahtjeve klijenata. Većina *web* poslužitelja sadrži pristupnu datoteku, datoteku zapisa gdje se bilježe svi zahtjevi i odgovori poslužitelja. Svaki redak u dnevniku pristupa sadrži informacije o jednom zahtjevu za dokument. Iz svakog unosa moguće je utvrditi naziv računala domaćina koji podnosi zahtjev, vrijeme kada je zahtjev upućen i ime traženog dokumenta. Zapis također sadrži i neke informacije o odgovoru poslužitelja na zahtjev, da li je poslužitelj uspio udovoljiti zahtjevu (ako nije, uz odgovor je naveden razlog neuspješnog zahtjeva), broj bajtova koje je poslao poslužitelj, ako su preneseni. Podaci iz pristupnih datoteka koriste se za karakteriziranje mrežnog prometa.

Drugi način mjerenja mrežnog prometa je odabir odgovarajućeg mjesta za pasivno hvatanje svakog paketa. Važan je odabir dobrog mjesta za praćenje. Idealno mjesto za dobivanje uzoraka je ono kroz koji prolaze mnoge TCP (*Transmission Control Protocol*) veze. Iako je pasivno mjerenje mrežnog prometa jednostavno, ono ima nedostatke. Pasivnim mjerenjem mrežnog prometa mogu se zagubiti paketi ako propusnost sustava praćenja nije dovoljna. Još jedan problem pasivnog nadzora je da povremeno prihvaća pakete s pogreškama. Pasivno mjerenje mrežnog prometa daje pogled na izvedbu pojedinih veza ili čvorova.

Treći način mjerenja mrežnog prometa je aktivnim pretraživanjem. Aktivno mjerenje mrežnog prometa pruža komplementarne prikaze polja izvođenja puta koji se sastoji od nekoliko veza i čvorova. Podaci mjerenja koriste se za prometni inženjering, uklanjanje pogrešaka na performansama, mrežne operacije i usklađenosti mjerenja s ciljevima izvedbe [3].

2.1 Metode mjerenja mrežnog prometa

Mjerenje mrežnog prometa obavlja se iz više razloga. Uključuju promet i karakterizaciju mreže, nadzor mreže i kontrolu mreže. Nadzor i kontrola mreže su usko povezane jedna s drugom, a razlikuju se samo u vremenskom intervalu na kojem djeluju. Glavni ciljevi mjerenja mrežnog prometa su identifikacija stanja mreže i otkrivanje kvarova.

Svako mjerenje ima dva faktora koji određuju mjernu populaciju: mjesto i rezolucija. Lokacija definira koji se dio mreže mjeri i koliki je promet uključen u mjerenja. Odabir lokacije mjerenja ima značajan utjecaj na korisnost mjerenja. Mjerenje lokacije mora biti reprezentativno za mjerenje prometa ili mreže. Na primjer, ako je potrebno mjeriti performanse mreže s „*kraja na kraj*“, mjerenje bi se trebalo izvršavati u dijelu pristupne mreže, dok se kod performansi jezgrene mreže mjerenja vrše na rubu jezgene mreže, a ne u pristupnim mrežama. Kod prikupljanja mjernih podataka na samim mrežnim uređajima, u obzir treba uzimati i opterećenje uzrokovano operativnim mrežnim elementima.

Opsežno prikupljanje statistike može rezultirati degradacijom performansi jer su mrežni elementi optimizirani za isporuku podataka. Sekundarne funkcije kao što su mjerenja i dijagnostički odgovori djeluju s nižim prioritetom u odnosu na funkcije prosljeđivanja podataka. Mrežni elementi optimizirani su za isporuku podataka. Sekundarne funkcije kao što su zahtjevi za odgovor, ignoriraju se ili se odgađaju, što može pokvariti krajnji rezultat mjerenja mrežnog prometa. Vanjska oprema za mjerenje mrežnog prometa nema ove nedostatke, osim što zauzima mrežni kapacitet za prijenos izmjerenih podataka i uvode dodatne troškove. Postoji nekoliko metoda mjerenja mrežnog prometa kako je navedeno u [4], a to su:

- mjerenja na osnovu vremena
- mjerenja na osnovu protoka
- mjerenja na mrežnim elementima
- mjerenja s čvora na čvor.

Mjerenje mrežnog prometa na osnovu vremena može se provoditi kontinuirano ili na temelju uzoraka. Neka mjerenja, poput brojanja bitova i paketa, mogu se provoditi kontinuirano čak i prilikom velikih brzina. Mjerenja zahtijevaju održavanje stanja

pojedinačnih tokova ili njihovih opterećenja. Neka se mjerenja temelje na uzorcima za testiranje gubitka paketa i kašnjenja slanjem testnog prometa. Druga skupina mjerenja koristi samo kao identificiranje razdoblja zauzetosti ili maksimalno opterećenje mreže.

Druga metoda mjerenja mrežnog prometa temelji se na protoku paketa. Paketi se grupiraju u tokove prema njihovim izvorišnim i odredišnim IP adresama, protokolu i broju izvorišta i odredišta. Za svaki tok se prikuplja niz detalja koji uključuju početnu vremensku oznaku protoka, trajanje protoka, broj paketa, broj bajtova, itd. Mjerenje mrežnog prometa na osnovu protoka raspoređeno je uglavnom na pristupnim mrežama. Broj istodobnih protoka je ograničen, a količina podataka unutar jednog protoka nije prevelika.

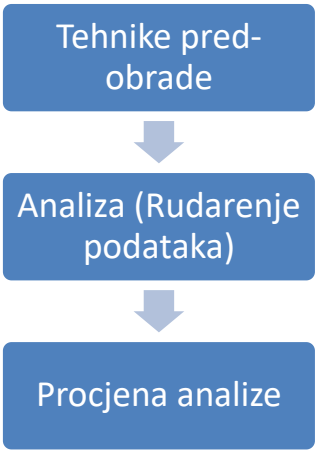
Treća metoda mjerenja je mjerenje na mrežnim elementima. Može biti pasivno i lokalno. Mreža se sastoji od mrežnih čvorova, a svaki čvor se sastoji od jedne ili više mrežnih sučelja koja su povezana na druga sučelja drugih čvorova. Mrežni čvorovi za svako sučelje održavaju brojače poslanih i primljenih podataka. Brojači sakupljaju podatke o broju paketa, broju bajtova i broju odbačenih paketa ili sa greškom. Mjerenje mrežnog prometa na mrežnim elementima ne daje cjelokupni prikaz stanja mreže ili izravne indikacije krajnjih performansi. Kombiniranjem statistike mjerenja više mrežnih elemenata, može se postići bolji prikaz mreže.

Četvrta metoda mjerenja mrežnog prometa s čvora na čvor ima najpopularniju primjenu. Tipična upotreba aktivnog mjerenja je slanje testnog prometa. Mjerenja se provode između krajnjih točaka radi mjerenja izvedbe s „kraja na kraj“ ili između posrednih točaka za nadgledanje nekog dijela mreže. Promet koji se koristi za mjerenje može biti stvarni promet aplikacije ili testni promet. ICMP (*Internet Control Message Protocol*) poruke mogu imati različitu obradu na krajnjim točkama i u usmjerivačima, što može rezultirati previše optimističnim ili pesimističnim rezultatima [4].

2.2 Faze analize mrežnog prometa

Za analizu mrežnog prometa koriste se različite tehnike. Opći okvir za mrežnu analizu uključuje pred-obradu, a zatim stvarnu analizu i motrenje te otkrivanje uzoraka mrežnih podataka. Analiza mrežnog prometa može se izvršiti na različite načine:

- na razini paketa
- na razini protoka
- na razini sigurnosnog mrežnog upravljanja.



Slika 1. Faze analize mrežnog prometa
Izvor: [5]

Slikom 1. prikazan je proces analize mrežnog prometa, a kako bi se procijenila učinkovitost analize mrežnog prometa, koriste se skupovi podataka. Prema [5] postoji nekoliko važnih skupova podataka koji se koriste za analizu mrežnog prometa:

- DARPA (*Defense Advanced Research Projects Agency*)
- KDD (*Knowledge discovery in databases*)
- NSL-KDD
- CAIDA (*Center for Applied Internet Data Analysis*)
- Waikato
- Berkeley Lab.

2.2.1 Tehnike pred-obrade

Pred-obrada je važna faza koja se koristi za rukovanje stvarnim mrežnim podacima iz svijeta u razumljivom obliku. Svakako, stvarni mrežni podaci iz svijeta su nepotpuni, nedosljedni te sadrže pogreške i vrijednosti odstupanja. Stoga su prije same analize mrežnog prometa, potrebne metode pred-obrade kako bi se poboljšala kvaliteta podataka za analizu,

čime se poboljšava točnost i učinkovitost rezultata određenog zadatka rudarenja podataka. Tehnike pred-obrade su bitne prilikom analize mrežnog prometa zbog uzoraka mrežnog prometa različitih vrste, formata i veličina.

Metoda diskretizacije spada pod tehnike pred-obrade. Diskretizacija je proces dokumentiranja kontinuiranih karakteristika u normalne karakteristike. Glavni cilj procesa diskretizacije je otkriti skup točaka presjeka koji dijeli raspon na mali broj intervala. Svaka točka presjeka je stvarna vrijednost unutar raspona kontinuiranih vrijednosti, koja dijeli raspon u dva intervala, jedan je veći od točke presjeka, a drugi je manji ili jednak vrijednosti točke presjeka. Proces diskretizacije je važna tehnika pred-obrade kako bi se skratilo trajanje analize mrežnog prometa. Prema [5] metode diskretizacije mogu biti svrstane u četiri kategorije:

- Metoda pod nadzorom i bez nadzora – metode pod nadzorom koriste oznake razreda kroz proces diskretizacije dok metode bez nadzora ne koriste informacije o oznakama razreda, nego generira diskretizaciju dijeljenjem vrijednosti karakteristika.
- Globalna i lokalna metoda – globalna koristi cijele numeričke karakteristike za diskretizaciju, dok lokalne metode koriste podskup primjera prilikom diskretizacije.
- Od dolje prema gore (razdvajanje) i od gore prema dolje (integriranje) – metoda od dolje prema gore započinje duljinom i vrijednošću intervala koje zatim dijeli u manje intervale prilikom svake iteracije, a metoda od gore prema dolje počinje sa većim brojem pod intervala i kombinira ih sve do postizanja optimalnog broja intervala.
- Izravna i inkrementalna metoda - izravnom metodom dijeli se raspon vrijednosti na jednak broj intervala i korisnik može odrediti broj intervala, a inkrementalna metoda počinje jednostavnom diskretizacijom i ide tijekom povećanja procedure sve dok ne dobije dobru diskretizaciju, kad ju zadobije, zaustavlja se diskretizacija.

Metoda odabira značajki je metoda pred-obrade koja se primjenjuje prije tehnike rudarenja podataka. Navedena metoda se koristi za poboljšanje tehnike rudarenja, uklanjanjem suvišnih karakteristika, generira novi skup karakteristika odabirom samo

podskupa izvorne karakteristike. Metoda odabira značajki se koristi uglavnom za smanjenje veličine skupa podataka kako bi se poboljšala analiza mrežnih podataka [5].

2.2.2 Rudarenje podataka

Rudarenje podataka se koristi za pronalazak saznanja, a ima važnu ulogu u analizi mrežnog prometa. Namjera je predstaviti različite tehnike rudarenja podataka koje se koriste za analizu mrežnog prometa. Prema [5] tehnike rudarenja podataka su podijeljene u okviru četiri široke kategorije:

- grupiranje
- razvrstavanje
- hibridna
- asocijacijska.

Tehnika grupiranja je proces podjele podataka u dvije skupine prema određenim karakteristikama te dijeli podatke u skupine sličnih objekata. Svaka grupa se sastoji od članova koji su vrlo slični, dok su članovi različitih grupa različiti jedni od drugih. Metode grupiranja se koriste za formiranje grupa mrežnih podataka radi analize mrežnog prometa.

Razvrstavanje predstavlja drugu tehniku analize podataka koji uzima svaki primjerak skupa podataka i dodjeljuje ga određenoj klasi. Analiza mrežnog prometa zasnovana na razvrstavanju pokušava razvrstati sve prometne podatke kao normalne ili zlonamjerne. Izazov razvrstavanja je smanjiti broj lažnih pozitivnih rezultata, odnosno prepoznavanje normalnog mrežnog prometa kao nenormalnog i otkrivanje zlonamjernog mrežnog prometa kao normalnog.

Treća kategorija tehnike rudarenja je hibridni model, a on predstavlja kombinaciju dvaju ili više tehnika pristupa za analizu, a postiže dobre rezultate u analizi mrežnog prometa.

Četvrta kategorija tehnike rudarenja je pravilo asocijacije, što znači da povezuje atribute u parove. Predstavlja skupljanje stavki označenih kao skup predmeta u jednom mrežnom zahtjevu. Pravila asocijacije koriste se za prepoznavanje obrasca ili odnosa među atributima baze podataka, a vrlo su važna za analizu mrežnog prometa [5].

2.2.3 Procjena analize

Kod tehnike rudarenja podataka koristi se mnogo različitih mjernih podataka za istraživanje tehnika pretraživanja podataka. Mjerni podaci o stupnju detekcije, lažne pozitivne stope, točnost i vremenski trošak koriste se kod mjerenja performansi razvrstavanja na različite skupove podataka. Postoji niz mjernih podataka kako bi se izrazila točnost predviđanja, a mjerni podaci se koriste pomoću konfuzijske matrice. Svaka mjerna vrijednost prema [5] definirana je kako slijedi:

- Prava negativna vrijednost (TN – *True Negatives*) predstavlja ukupan broj normalnih paketa ispravno razvrstanih.
- Prava pozitivna vrijednost (TP – *True Positives*) predstavlja ukupan broj zlonamjernih paketa ispravno razvrstanih.
- Lažna negativna vrijednost (FN – *False Negatives*) predstavlja ukupan broj zlonamjernih paketa koji su pogrešno razvrstani kao normalni ispravni paketi.
- Lažna pozitivna vrijednost (FP – *False Positives*) predstavlja ukupan broj normalnih ispravnih paketa koji su pogrešno razvrstani kao zlonamjerni paketi.
- Stopa detekcije (DR – *Detection rate*) predstavlja omjer ukupnog broja otkrivenih napada podijeljen s ukupnim brojem lažnih pozitivnih vrijednosti zbrojene ukupnim brojem pravih negativnih vrijednosti.

3. Alati za analizu mrežnog prometa u telekomunikacijskoj mreži

Alati za analizu mrežnog prometa zovu se analizatori paketa, odnosno *snifferi*. Služe za dekodiranje informacije i prikazivanje u čitljivom obliku. *Snifferi* imaju dva načina analize prometa, a to su pasivno osluškivanje više-odredišnih poruka (npr. bežićni mrežni promet) te presretanje prometa.

Pojedini alati kako je navedeno u [6] posjeduju i dodatne mogućnosti kao što su:

- automatska detekcija pogreške u prijenosu
- otkrivanje uzroka takve greške
- prikaz podataka u grafičkom obliku (vremenski grafovi propusnosti, količine prometa i sl.)
- generiranje ispitnih paketa, ispravnih ili neispravnih (u svrhu provjere ispravnosti prijenosa ili sposobnosti oporavka od pogreške).

Analizom mrežnog prometa i statističkom obradom dobivaju se korisne informacije o ponašanju i iskoristivosti mreže. Praćenjem aktivnošću određenih računala, moguće je identificirati veća opterećenja na pojedinim dijelovima mreže ili identificirati računala kojima se generiraju veće količine sumnjivog prometa [7].

Alate za analizu mrežnog prometa moguće je podijeliti na programske ili sklopovske. Sklopovski alati za analizu mrežnog prometa su uske namjene, ugrađena su u telekomunikacijsku opremu te imaju sposobnost vrlo brze analize prometa. Programska rješenja su šire namjene, a sposobna su analizirati mnogo više protokola te se koriste u instancama kada je potrebno otkrivanje uzoraka određene anomalije [2].

Kako je navedeno u [2] primjeri korištenja *sniffera* su:

- detekcija mrežnih pogreški
- detekcija pokušaja upada na sustav
- izolacija sustava sa mrežnim kvarom
- nadzor podataka u prijenosu mrežom
- prikupljanje statistike mrežnog prometa i sl.

Alati za analizu mrežnog prometa omogućuju promatranje mrežnog prometa i prikupljanje podataka kako bi se isti kasnije analizirali. Olakšavaju otkrivanje grešaka kod mrežnih protokola i omogućavaju njihovo brže otklanjanje [6].

3.1 Tipovi alata za mjerenje mrežnog prometa

S vremenom se razvija sve više alata za mjerenje mrežnog prometa u svrhu rješavanja trenutnih mrežnih problema. Alati se i dalje razvijaju kako bi bili što općenitiji i jednostavniji za upotrebu. Napredniji alati mogu upotrebljavati informacije iz više izvora, poput baza podataka o raspodjeli IP adresa, uz izravna mjerenja [4].

3.1.1 Alati za dostupnost i kašnjenje

Vjerojatno najčešće korišteni mrežni alat za mjerenje je *ping* jer je lako dostupan na većini sustava. Osnovna verzija šalje ICMP pakete sa zahtjevima za povratak, a za svaki primljeni odgovor povratnog paketa ispisuje se red koji naznačuje redni broj paketa i proteklo vrijeme za svaki primljeni paket. Na kraju ispisuje liniju sažetka naznačujući minimalnu, srednju i maksimalnu odgodu i stopu gubitka paketa. Točnost vremena ovisi o matičnom operativnom sustavu. Uobičajena rezolucija je oko jedne milisekunde na modernim sustavima [4].

3.1.2 Alati za karakterizaciju skoka

Ovi se alati temelje na slanju UDP (*User Datagram Protocol*) datagrama na nekorišteno sučelje s različitim TTL (*Time to live*) vrijednostima u IP datagramu. Kad usmjerivač smanji TTL polje i ustanovi da je nula, on vraća poruku prekoračenog ICMP vremena. Za ovu poruku program će naučiti sljedeći skok na ruti i poslati još jedan paket s TTL poljem za jedno povećanje. Kada poruka dođe do odredišta i u tom UDP-u nema procesa slušanja, domaćin će odgovoriti ICMP sučelju nedostupnom porukom. Izvorni *traceroute* ima nekoliko varijanti

koje imaju određena poboljšanja performansi ili prikazuju neke dodatne informacije, poput brojeva autonomnog sustava. Neke inačice koriste ICMP poruke povratnih zahtjeva, umjesto UDP paketa [4].

3.1.3 Alati za mjerenje propusnosti

Za mjerenje propusnosti mogu postojati dva različita cilja. Prvi je mjeriti trenutačno raspoloživu propusnost u postojećim mrežnim uvjetima, a drugi je mjeriti najveću dostižnu propusnost u nedostatku konkurentskog prometa. Prva se koristi za procjenu protoka aplikacija, a druga se koristi za karakterizaciju mrežne opreme. Mjerenje propusnosti može biti nametljivo ako alat za mjerenje ne izvrši sličnu prilagodbu brzine kao protokoli aplikacije. Ako se za mjerenje koristi stvarni aplikacijski protokol, samo relativno veliki broj istodobnih mjerenja odvraća pozornost od ostalih korisnika mreže [4].

3.1.4 Alati za skupljanje tragova paketa

Najpopularniji sakupljač paketa je *tcpdump* koji koristi jako pokretljive *libpcap* knjižnice za hvatanje paketa, što skriva razlike u operativnom sustavu od *softvera* za hvatanje. *Tcpdump* je dostupan za više operativnih sustava. Datoteke praćenja koje je napisao *tcpdump* "*pcap*" je uobičajeni format za razmjenu tragova paketa, međutim ima određena ograničenja u svom formatu. Potrebno je osiguravanje samostalnih, ali i nekih pomoćnih podataka da bi se podaci pravilno analizirali. Primjerice, vremenske oznake imaju ograničenu točnost [4].

3.2 *Wireshark* programski alat

Wireshark je alat za analizu mrežnog prometa, napisan u programskom jeziku C. Kasnijim nadogradnjama pisan je i u drugim programskim jezicima. Glavna uloga *Wireshark* alata je

hvatanje mrežnih paketa, analiza i rad s paketima. Moguće ga je koristiti za administraciju i povećanje sigurnosti mreže i njenih korisnika.

Programski alat hvata pakete koji putuju mrežom i prikazuje ih detaljno. Prema [8] neki od primjera korištenja ovog alata su:

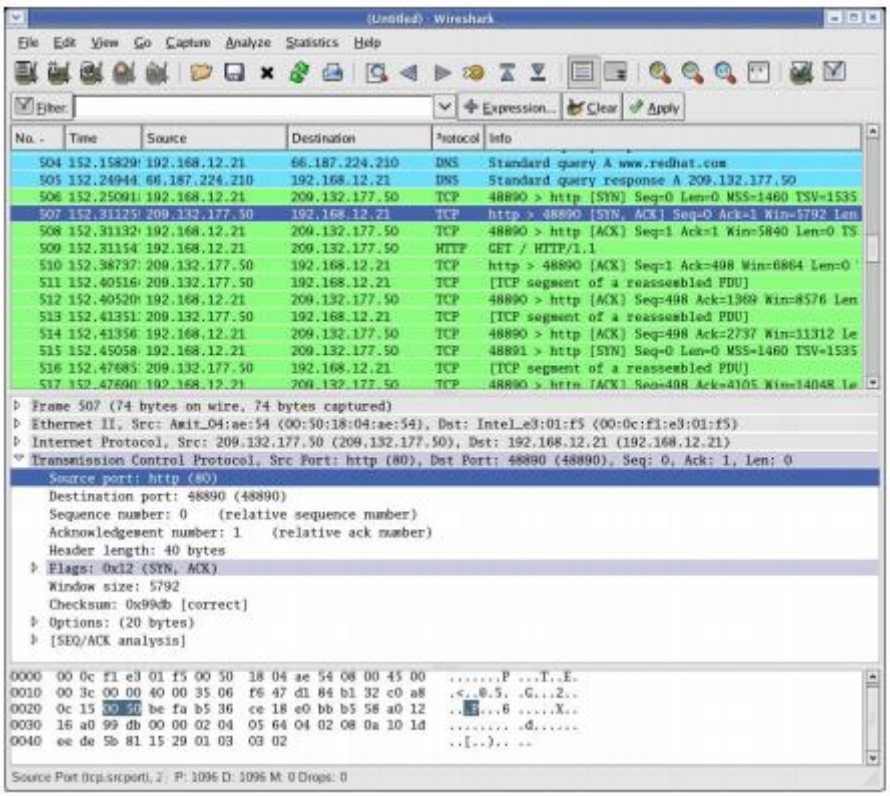
- otklanjanje problema na mreži
- analiza sigurnosnih ranjivosti
- razvoj i implementacija novih protokola
- učenje o mrežnim protokolima.

Wireshark može raditi na različitim platformama, a osim što radi na operacijskom sustavu *Microsoft Windows* podržan je i na *Unix* operacijskim sustavima. Postoji i inačica *Wireshark* alata bez grafičkog sučelja *Tshark* [8].

Prema [9] funkcije Wireshark alata su:

- hvatanje paketa
- filtriranje paketa
- uvoz i izvoz paketa
- prekid hvatanja paketa
- reduciranje količine uhvaćenih paketa
- hvatanje u različitim mrežama i sl.

Wireshark je jednostavan alat za rukovanje jer ima grafičko sučelje što je prikazano slikom 2. Za hvatanje paketa potreban je odabir jednog ili više uređaja sa kojeg će se izvršavati hvatanje paketa. Kad se završi hvatanje paketa, izvršava se filtriranje paketa. Filtriranje paketa se vrši na temelju IP adrese, veličine paketa, određenih podataka u paketu, sličnosti između paketa i sl. *Wireshark* može čitati pakete spremljene u datoteke, nakon što se paketi uhvate ili nakon što se datoteka s informacijama o prethodno uhvaćenim paketima učitana, popis paketa vidljiv je u listi paketa [9].



Slika 2. Grafičko sučelje programskog alata *Wireshark*, [6]

3.3 *NetworkMiner* programski alat

NetworkMiner je programski alat za analizu mrežnog prometa. Funkcija alata je snimanje mrežnog prometa i analiza iz spremljenih PCAP datoteka (programsko sučelje za hvatanje mrežnog prometa). Alat pasivnim funkcijama vrši identifikaciju operacijskih sustava iz mrežnog prometa sa preddefiniranim pravilima i bez generiranja dodatnog prometa.

Prikazom svih detektiranih IP adresa mogu se ispisati detaljnije informacije za svaku IP adresu kao što su generirani promet, otvorena sučelja, MAC adresa i sl. Također može sastavljati datoteke iz prikupljenog mrežnog prometa [10].

NetworkMiner je jednostavniji alat za korištenje od *Wireshark* alata te dobro obavlja posao u analizi mrežnog prometa unutra i vani [11].

3.4 *Scapy* programski alat

Scapy je programski alat za analizu mrežnog prometa koji omogućuje interaktivno kreiranje i manipulaciju mrežnih paketa. Može se koristiti kod jednostavnijih zahtjeva kao što je generiranje i slanje proizvoljnih mrežnih paketa ili prisluškivanje mrežnog prometa, no može se koristit i kod kompliciranijih zahtjeva kao što su pregledavanje mrežnih sučelja, identifikacija operacijskih sustava na udaljenim računalima i sl. Alat za korisničko sučelje koristi *interpreter Python* programski jezik. Zbog svoje funkcionalosti, može se koristiti kao zamjena za alate poput: *ttlscan*, *nmap*, *hping*, *queso, p0f, xprobe, arping, arp-sk, arpspoof, firewalk i irpas*. Kako je navedeno u [12] *Scapy* programski alat se primjenjuje u sljedećim područjima:

- testiranje i istraživanje
- pregledavanje mreža, sučelja i mrežnih protokola
- ispitivanje ruta, *firewalla*, prepoznavanje operacijskih sustava
- izvođenje mrežnih napada.

Scapy programski alat može generirati izvještaje s rezultatima pregledavanja u HTML-u, LATEX-u i tekstualnom obliku. Koncept rada alata je jednostavan, pomoću *Python interpretera* korisnik definira mrežne pakete koji se zatim šalju, a osluškuju se odgovori na poslani paket. Zaprimljeni paketi se uparuju sa poslanim zahtjevima i korisniku se šalje lista parova paketa te zahtjevi i odgovori koji su ostali bez para. Jednostavnim pristupom moguće je kasnije dodavanje složenijih funkcija koje mogu obavljati pregled mreže i izvoditi mrežne napade.

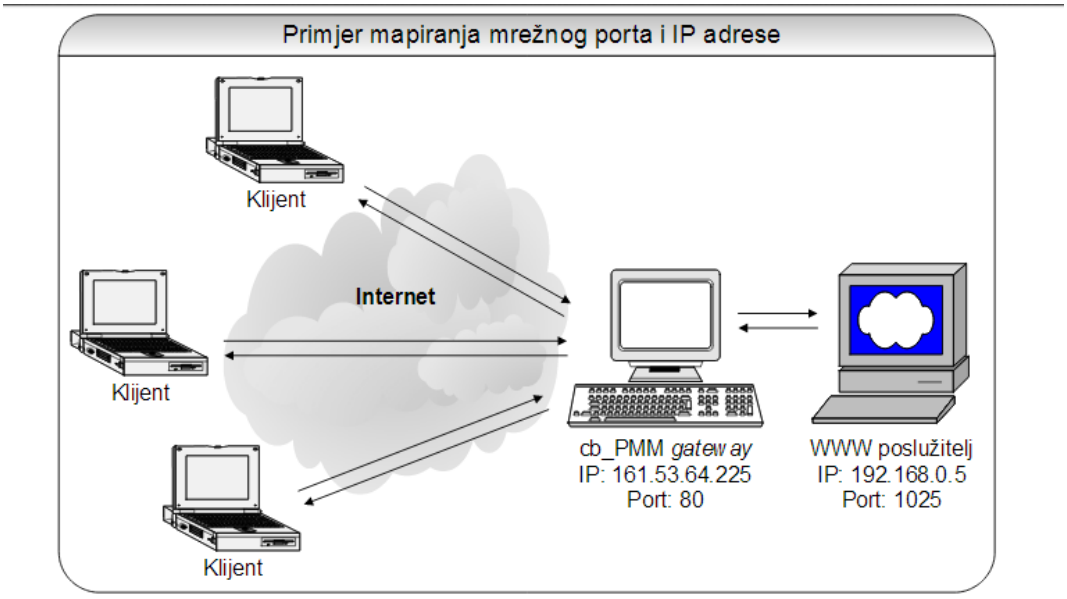
Još jedna od funkcija *Scapy* alata je pasivno pregledavanje radi identifikacije operacijskog sustava na udaljenom računalu. Pasivnom tehnikom nastoje se analizirati TCP/IP paketi nastali kao odgovorom na zahtjev (HTTP ili SMTP). Kako se implementacija TCP/IP razlikuje od sustava do sustava, svaki od odgovora na zahtjev će sadržavati određene specifične parametre u paketu. Usporedbom pristiglog paketa i definiranim pravilima može se odrediti vrsta udaljenog operacijskog sustava.

Scapy je namijenjen stručnjacima za sigurnost radi olakšavanja analize i manipulacije mrežnih paketa te izvođenje složenijih radnji poput pasivnog i aktivnog pregledavanja mreže [12].

3.5 *Cb_PMM* programski alat

Programski alat *cb_PMM* koristi se za praćenje i analizu TCP mrežnog prometa putem mapiranja sučelja i tuneliranja TCP konekcija. Alat se ponaša kao usmjerivač TCP prometa, pri čemu je moguće njegovo bilježenje i pohranjivanje u različitim formatima. *Cb_PMM* ima dvije osnovne funkcije, mapiranje TCP sučelja i IP adresa te praćenje TCP konekcija.

Mapiranje mrežnih sučelja omogućuje prosljeđivanje konekcija koje su upućene na odredišnu IP adresu te mrežno sučelje na neko drugo sučelje i IP adresu. Tako alat radi kao *gateway* na razini TCP protokola. Primjer mapiranja mrežnih portova i IP adresa prikazano je slikom 3.



Slika 3. Primjer mapiranja mrežnog sučelja i IP adrese, [13]

U primjeru računalo sa programskim alatom *cb_PMM* spojeno je na internet i ima javnu IP adresu 161.53.64.225. Sa interneta se šalju *web* zahtjevi na tu adresu i sučelje 80. *cb_PMM* prima sve pakete sa odredišnim sučeljem 80 i prosljeđuje ih na privatnu IP adresu 192.168.0.5 gdje je pokrenut *web* poslužitelj na sučelju 1025.

cb_PMM omogućuje simultano mapiranje do osam mrežnih sučelja i IP adresa. Druga funkcija je analiza mrežnog prometa i zapisivanje TCP podataka koji prolaze kroz mapirane konekcije. Podaci se mogu pratiti u stvarnom vremenu ili se mogu snimati u *log* datoteke. Program omogućava praćenje svih podataka sadržanih u TCP paketu [13].

3.6 *IPAudit* programski alat

IPAudit je programski alat za prikupljanje i analizu mrežnog prometa. Praćenje i generiranje podataka mrežnog prometa vrši se pomoću *libpcap* programske biblioteke. *IPAudit* programski alat prikuplja sav mrežni promet na lokalnoj mreži postavljanjem mrežnog sučelja u promiskuitetni način rada. Podržava analizu prometa na više mrežnih sučelja.

Alat omogućuje analizu svih paketa koji prolaze lokalnom mrežom i nudi detalje o računalima, mrežnim sučeljima i protokolima. *IPAudit* može služiti za analizu mrežne propusnosti i detekciju kompromitiranih računala te otkrivanje adresa s kojih se vrši skeniranje mreže [7].

3.7 Programski alati za otkrivanje neovlaštene analize mrežnog prometa

Antisniff programski alat jedan je od programskih alata za detekciju neovlaštenog promatranja mrežnog prometa. *AntiSniff* radi sa *Ethernet* i DSL mrežama.

Sljedeći alat je portabilni C programski paket pod imenom *ifstatus*. *Ifstatus* programski alat izvršava testiranje mrežnih sučelja na lokalnom sustavu i pregledava da li su neka sučelja u '*promisciuous*' modu, što predstavlja indikaciju u promatranju mrežnog prometa. Alat je praktičan kada se koristi u kombinaciji sa *cron demon* programskim alatom. *Crond* programski alat se konfigurira na način da u određenim vremenskim razdobljima pokreće *ifstatus* programski alat, koji će u slučaju primijećenih neregularnosti prijavljuje upozorenje.

CPM programski alat je isto jedan od alata za detekciju neovlaštene analize mrežnog prometa, a ima identičan način rada kao i *ifstatus* programski alat.

LSOF je programski alat iz sustava izvlači sve one informacije koje mogu biti indikator neovlaštenih aktivnosti jer će mrežni promatrači vrlo često na sustavu ostaviti otiske u obliku *log* datoteka ili nešto slično kao posljedicu neovlaštene analize i promatranja mrežnog prometa, što se u ovom slučaju pokušava iskoristiti kao pomoćno sredstvo za otkrivanje neovlaštenih aktivnosti [6].

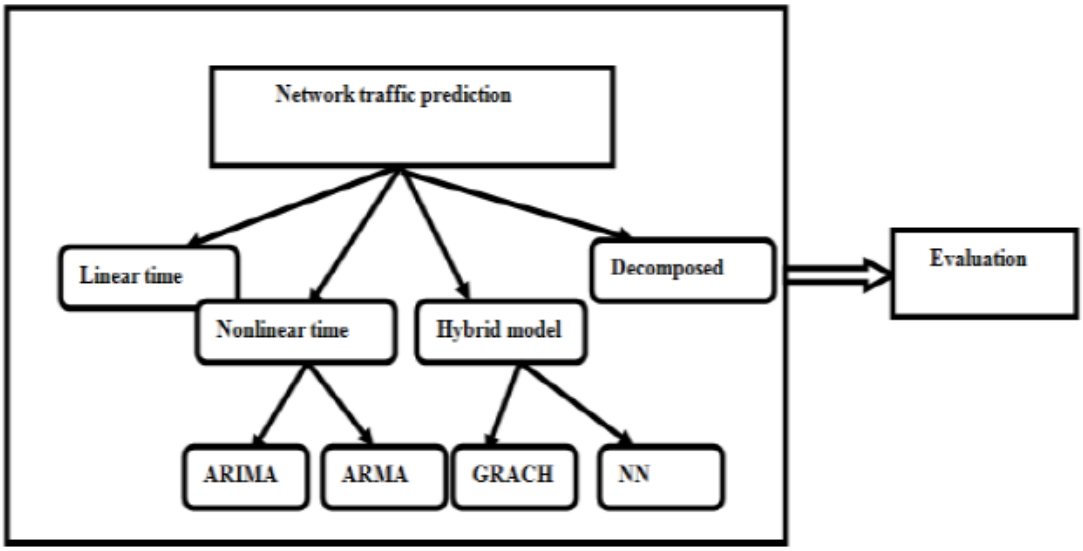
4. Predviđanje mrežnog prometa u telekomunikacijskoj mreži

Predviđanje telekomunikacijskog prometa omogućava kvalitetno planiranje odnosno dimenzioniranje potrebnih resursa (prijenosnih kapaciteta te kapaciteta komutacijskih sustava) kako bi se zadovoljila željena kvaliteta usluge. Stalno praćenje odnosno mjerenje i analiza telekomunikacijskog prometa omogućava optimizaciju postojećih mrežnih resursa što u konačnici rezultira zadovoljavajućom kvalitetom usluge. Telekomunikacijski promet promatranog sustava ili mreže varira ovisno o dobu dana, tjedna pa i godišnjem dobu te o specifičnim događajima kao što su praznici, razna TV ili radio glasovanja, igre, itd. [14].

Predviđanje mrežnog prometa ima vrlo važnu ulogu, a neki od razloga su izbjegavanje zagušenja, nadziranje mrežne sigurnosti i povećanje brzine na mreži [5].

Za predviđanje telekomunikacijskog prometa odnosno pravilno dimenzioniranje telekomunikacijskog sustava upotrebljavaju se prometni modeli. Prometni model je skup mjerenih te izračunatih parametara koji ukazuju na ponašanje korisnika mreže, a na temelju kojeg je moguće izračunati očekivani telekomunikacijski promet te definirati ponuđeni telekomunikacijski promet. Parametri prometnog modela ovise o vrsti sustava koji se dimenzionira. Primjerice, za dimenzioniranje komutacijskog sustava u javnim mobilnim mrežama jedan od parametara prometnog modela je „broj isporučenih SMS poruka po korisniku u promatranom vremenskom periodu“ dok je za dimenzioniranje komutacijskog sustava koji poslužuje podatkovni promet jedan od parametara prometnog modela „broj“ iniciranih sesija od strane korisnika u promatranom vremenskom periodu. Pri proračunu prometnog modela potrebno je uzeti u obzir trenutno ponašanje korisnika sustava odnosno mreže u glavnom prometnom satu te očekivanu promjenu ponašanja korisnika sustava/mreže u vremenu za koje se dimenzionira sustav. Telekomunikacijski sustav se dimenzionira na temelju definiranog prometnog modela koji se računa za glavni prometni sat. Međutim, pri dimenzioniranju je potrebno uzeti u obzir specifične događaje uslijed kojih određeni parametri prometnog modela izlaze iz definiranih okvira, primjerice broj govornih poziva za Novu Godinu u javnim telekomunikacijskim mrežama. Stoga je pri dimenzioniranju sustava potrebno uzeti u obzir specifičnosti ovakvih događaja [14].

Postoje različite tehnike predviđanja mrežnog prometa, a između ostalih to su: linearni model vremenskih serija, nelinearni model vremenskih serija, hibridni model i model rastavljanja [5].



Slika 4: Tehnike predviđanja mrežnog prometa, [5]

4.1 Definicija predviđanja mrežnog prometa

U predviđanju mrežnog prometa mogu se razmatrati dvije metrike:

- kolikom će se brzinom u budućnosti predviđati mrežni promet sa ograničenom pogreškom
- koja je minimalna pogreška predviđanja određenog vremenskog intervala predviđanja.

Navedeno može biti razmotreno korištenjem dva modela prometa: *Auto-regressive moving average* i *Markov-modulated poisson process.* Cilj nije predlaganje najboljeg modela predviđanja prometa jer je to veoma teško pitanje, nego je fokus na procjeni predviđanja prometa s pretpostavkom te točnost modeliranja. Specifični vremenski raspon ili iskorištavanje propusne širine za kontrolu predviđanja mreže tvore ograničenja. Ova dva modela, iako su oba kratkog dosega, mogu dohvatiti statistiku sličnog prometa prilično precizno za ograničene vremenske intervale mjerenja temeljenih na upravljanju prometom. Primjenjivost predviđanja prometa ograničena je pogoršanjem točnosti predviđanja sa

povećanjem intervala predviđanja. Iz analitičkih i numeričkih studija mogu se istražiti različite uloge statistike prometa, bilo prvog ili drugog reda, u predviđanju mrežnog prometa. Statističko multipleksiranje i pravilno mjerenje prometa uzorkovanjem ili filtriranjem pokazuje pozitivne učinke. Eksperimentalni rezultati predlažu obećavajući oslonac u predviđanju prometa i općenito poboljšano predviđanje ako su male promjene prometa u vremenskim intervalima, koje su obično od manje važnosti za dodjelu propusne širine i kontrolu prijema poziva jer su filtrirane.

Jedno od ključnih pitanja na temelju mjerenja u upravljanju prometom je predviđanje potrebne širine pojasa u sljedećem kontrolnom vremenskom intervalu na temelju mrežnih mjerenja prometnih karakteristika. Cilj predviđanja mrežnog prometa je predviđanje buduće stope varijacije prometa što je preciznije moguće, na temelju povijesti mjerenja. Predviđanje prometa označava mogućnost predviđanja za zadovoljavanje nekih zahtjeva preciznosti nad željenim vremenskim intervalom predviđanja i kontrole.

S jedne strane, potreban je veliki interval predviđanja da bi se osiguralo dovoljno vrijeme za kontrolne radnje i za nadoknadu neizbježnih kašnjenja uzrokovanih mjerenjem prometa (uzorkovanjem i filtriranjem) i predviđanjem prometa (modeliranjem i računanjem). S druge strane mala pogreška predviđanja poželjna je iz sljedećeg razloga, kontrolne radnje temeljene na pogrešnom predviđanju mogu nenamjerno ugroziti performanse upravljanja. Radi postignuća veće iskoristivosti resursa, mrežni administratori radije odabiru precizno predviđanje mrežnog prometa. Nažalost, točnost predviđanja se pogoršava kako se interval predviđanja povećava. Postoji veza između velikog intervala predviđanja i male pogreške predviđanja, koji odražava vezu između kontrolnog vremenskog intervala i mrežne učinkovitosti. Različite vrste prometa zahtijevaju svoja svojstvena prirodna predviđanja. Iz tog razloga je važno okarakterizirati statistiku prometa u predviđanju po stupnju prioriteta. Isti promet može pokazati različiti rezultat predviđanja, ako se gledaju drugačije vremenske skale. Dolazni mrežni promet izražava se stohastičkim procesom s kontinuiranim vremenom [15].

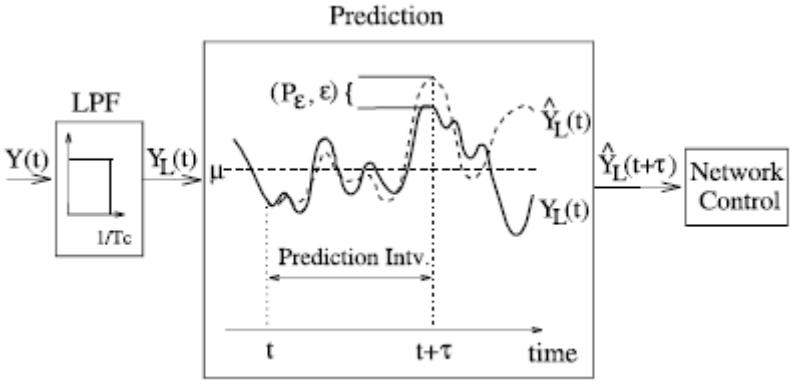
Dolazni mrežni promet kako je navedeno u [5] računa se korištenjem formule (1):

$$\{Y(t) = X(t) + \mu\} \tag{1}$$

gdje oznake imaju sljedeće značenje:

- *Y(t)* – dolazni mrežni promet
- μ – prosječna stopa prometa
- *X(t)* – čisti slučajni regularni proces s kontinuiranim integriranim spektrom i nulte srednje vrijednosti.

ARMA i MMPP postupci se baziraju na ovoj formuli. U idealnom slučaju, bilo koje determinističke komponente se mogu izvući iz prometa prema *Lebesegue teoremu raspadanja* i ukloniti iz analize predviđanja. Pitanje predviđanja prometa prikazano je slikom 5. Prikazuje postupak kontrole međuspremnika, temeljen na mjerenju, čije je maksimalno lokalno kašnjenje d_{max} oko 30 ms. Postupak čekanja u redu može se okarakterizirati pomoću nisko propusnog filtera (LPF) s frekvencijom isključivanja $1/T_c$, odnosno kritične vremenske skale (CTS – *Critical Time Scale*). Samo visokofrekventna (HF) dinamika ulaznog prometa apsorbira se u privremenoj pohrani, dok niskofrekventni (LF) dio ne mijenja stanje privremene pohrane. Takav T_c može se koristiti za uzorkovanje i kao interval izglađivanja za mjerenje mrežnog prometa. Dakle, čvor se može pojednostaviti kao prijenosni sustav bez međuspremnika za filtrirani ulaz $Y_L(t)$ [15].



Slika 5. Okvir predviđanja mrežnog prometa, [15]

Slikom 5 prikazan je okvirni postupak predviđanja mrežnog prometa, a oznake imaju sljedeće značenje:

- Y(t) – dolazni mrežni promet
- T_c – brzina filtriranja
- $Y_L(t)$ – intenzitet filtriranog prometa
- μ – prosječni prometni intenzitet
- $(P_\varepsilon,\varepsilon)$ – ograničenje pogreške predviđanja

- $\hat{Y}_L(t + \tau) - \tau$ – korak predviđanja.

Svrha predviđanja mrežnog prometa je istraživanje potencijala ili optimalne granice predviđanja u više koraka u prometnom inženjerstvu. Poseban interes je vezan uz izvedbu gornje i donje vrijednosti intervala predviđanja ili pogreška za prikupljene predstavničke uzorke prometa iz stvarnih mreža. Imati vezano rješenje je ekvivalent postizanju optimalnog predviđanja svakog uzorka prometa. Tada se može koristiti za procjenu specifičnih kontrolnih performansi ili za odabir određenih kontrolnih parametara kao što je kontrola vremenske skale ili ciljane vrijednosti iskorištenja širine pojasa. Kompromis između velikog MPI i male pogreške predviđanja, pokazuju kompromis između odabrane kontrolne vremenske skale i odgovarajuće učinkovitosti upravljanja. Pravilnim mjerenjem prometa, odnosno nisko propusnim filtriranjem i multipleksiranjem, poboljšava se predviđanje prometa. Statistike i prvog i drugog reda su važne prilikom analize, zbog određenih prometnih svojstava, poput višestruke korelacije vremenskih skala, velikog koeficijenta varijacije i SRD ograničenja predviđanja. Opsežna numerička istraživanja stvarnih uzoraka potvrđuju ta analitička opažanja. Model predviđanja pogodniji za agregirani promet nego za pojedinačne tokove na ograničenoj vremenskoj skali [15].

Linearne tehnike uključuju vremensko-serijske modele, model *Kalmanovog* filtriranja, i slično. Nelinearni modeli uključuju metodu najbližeg susjeda (eng. *K-nearest neighbor*), umjetnu neuronsku mrežu. Naivne metode nemaju nikakvo znanje o modelu i najčešće se koristi metoda povijesnog prosjeka (eng. *historical averages*) i metoda klasteriranja (eng. *clustering*) [16].

4.2 Tehnika linearne serije

Tehnike linearnih vremenskih serija su kovarijantne strukture u vremenskoj seriji. Postoje dvije popularne podskupine modela linearnih vremenskih serija: automatski regresivni (AR) i pomični prosjek (MA), koji se mogu kombinirati kako bi se napravili automatski regresivni modeli pokretnih prosjeka. Linearna vremenska serija tradicionalna je tehnika predviđanja mrežnog prometa [5].

Obilježja linearnih modela su preddefinirana struktura i konačan skup parametara. Znanje o procesu koji se modelira može se ugraditi u strukturu modela i time poboljšati točnost predviđanja. Skup podataka je manji u usporedbi s nelinearnim metodama. Na osnovu tog skupa podataka utvrđuju se vrijednosti parametara. Kako je navedeno u [16] modeli linearnih tehnika podijeljeni su na:

- simulaciju prometa (eng. *traffic simulation models*)
- vremenske serije (eng. *time series*).

Modeli simulacije prometa mogu se podijeliti prema:

- razini detalja na: makroskopske, mezoskopske i mikroskopske
- skali nezavisnih varijabli na: kontinuirane, diskretne i polu-diskretne
- predstavljanju procesa na determinističke i nedeterminističke.

Modeli koji se zasnivaju na vremenskim serijama predviđaju vrijednost varijable na temelju povijesnih mjerenja. Modeliranje vremenskim serijama zahtijeva da je proces stacionaran. Taj uvjet prometni tok ne zadovoljava, pa se umjesto teorije o prometnom toku koristi statika. Prema [16] modeli koji koriste vremenske serije za predviđanje su:

- linearna regresija (eng. *linear regression*)
- ARIMA (eng. *autoregressive integrated moving average*)
- *Kalmanov* filtar.

Model ARMA (*Autoregressive Moving Average*) kombinira se i iz AR i iz MA kako bi se dobio točan model. Automatski progresivni prosjek je statistička upotreba modela s modelom vremenskih serija za predviđanje. Model ARMA primijenjen je na dobro realizirane podatke vremenskih serija. ARMA model smatra se prikladnim za predviđanje podataka koji integriraju slučajne slučajeve. Model linearne vremenske serije ARMA vrlo je značajan za predviđanje mrežnog prometa.

Model ARIMA (*Autoregressive Integrated Moving Average Model*) predstavlja integrirani ARMA model. ARIMA igra važnu ulogu s modelom vremenskih serija za predviđanje mrežnog prometa. ARIMA model se najviše koristi za predviđanje mrežnog prometa [5].

4.3 Tehnika nelinearne serije

Nelinearni vremenski nizovi generiraju se nelinearnim dinamičkim jednadžbama. Oni pokazuju značajke koje se ne mogu modelirati linearnim procesom poput varijance promjene vremena, asimetričnog ciklusa, strukture višeg momenta, pragova i lomova. Ovaj model predviđanja mrežnog prometa koristi se različitim tehnikama, poput neuronske mreže i neizrazite logike.

U odnosu na linearne serije njihov glavni nedostatak je potrebna količina podataka. Nelinearnim modelima je potrebno mnogo više podataka. Prednost se krije u mogućnosti modeliranja dinamičnih i nestacionarnih procesa, poput prometnog toka. Rijetki i specifični događaji (poput nastanka incidenta) mogu prouzročiti greške u predviđanju prometnog toka [16].

Model GARCH (*Generalized Auto Regressive Conditional Heteroskedasticity*) koristi se za snimanje naleta internetskog prometa. Koristi se metoda predviđanja u jednom koraku, gdje god je predviđanje rekurzivno završeno kako bi se u odgovarajuće vrijeme slijedile vrijednosti predviđanja. GARCH i ARCH modeli se koriste za mjerenje uspješnosti njihovih tehnika [5].

Neuronska mreža sastoji se od funkcija koje se nazivaju neuroni. Ti neuroni imaju veze za dobivanjem ulaza i prosljeđivanjem izlaza drugih neurona. Svaka veza ima težinu koja je s njom povezana, a težina određuje performanse NN-a. Neuronsku mrežu za mrežni promet istražili su brojni istraživači. Neuronske mreže pružaju rješenje problema predviđanja mrežnog prometa primjenom brojnih tehnika. Neuronske mreže za predviđanje mrežnog prometa najprije su uvedene kao alternativa statističkim tehnikama mrežnog prometa.

Osim linearne i nelinearne tehnike predviđanja, postoji hibridni model, a on predstavlja kombinaciju dva ili više modela. Hibridni modeli su vrlo precizni u predviđanju mrežnog prometa. Kombinacija linearnih i nelinearnih modela naziva se hibridni model. Daje dobre rezultate u predviđanju i analizi mrežnog prometa [5].

4.4 Tehnika razlaganja

Kod tehnike razlaganja, vremenski nizovi se razlažu na četiri komponente. Svaka komponenta definirana je u nastavku.

Komponenta trenda je dugoročna sklonost, povećanje i smanjenje podataka o vremenskim serijama. Komponenta trenda predstavlja strukturne varijacije niskofrekventnih vremenskih serija.

Kod cikličke komponente, ciklički uzorak ukazuje na srednjoročnu fluktuaciju. Ciklički uzorak se povećava i opada bez određenog razdoblja.

Sezonska komponenta su razlike u podacima vremenskih serija koje su utjecale na sezonske čimbenike kao što su godina, kvartal, mjesec, tjedan, dan, sat. Podaci za sezonsku varijaciju imaju stabilne varijacije unutar vremenskih serija.

Nepravilna komponenta je preostala vremenska serija nakon uklanjanja komponente trenda i sezonskih komponenata [5].

5. Problemi predviđanja mrežnog prometa u telekomunikacijskoj mreži

Postoje razni modeli kojim se može vršiti predviđanje mrežnog prometa, a svaki od njih ima svoje pozitivne učinke. Međutim, dosadašnjim istraživanjima nijedan od modela predviđanja nije razvijen dovoljno da bi bio prihvaćen kao najbolji model efikasnog predviđanja za stvarnovremenske aktivnosti mrežnog prometa. Iz navedenog razloga se nameće i potreba za poboljšanim pristupom, kombiniranjem više modela predviđanja zajedno u više perioda [16].

Mjerenje ima veliki utjecaj na predviđanje prometa i potrebno ih je vezati zajedno kako bi se svi problemi predviđanja mogli sažeti u sljedeća pitanja:

1. Koliko daleko u budućnosti se može predviđati mrežni promet povjerljivim zahtjevom? Odnosno koji je maksimalni interval predviđanja pod određenim ograničenjem pogreške?
2. Koliko mrežnih resursa mora biti rezervirano da bi se apsorbiralo nepouzdano predviđanje, ako je interval predviđanja određen kao i vremenski interval mrežne kontrole?
3. Koja svojstva prometa, statistički dobivena iz mjerenja karakteriziraju svojstva predviđanja te kako multipleksiranje i uzorkovanje prometa utječe na procjenu predviđanja prometa?

U idealnom slučaju, ako su poznate buduće promjene prometa, upravljanje mrežom bez zagušenja moglo bi se pojednostaviti dinamičkim raspoređivanjem propusnosti prema rezultatima predviđanja. Ako stopa predviđanja premašuje raspoloživu širinu pojasa, bilo da je potrebna dodatna širina pojasa ili razni upravljački mehanizmi, potrebno je preusmjeriti putem postojećih tokova, smanjiti izvornu stopu ugovaranjem ili blokirati nove dolaske poziva. Vremenski interval kontrole snažno ovisi o pojedinačnom upravljačkom mehanizmu. Vremenski interval je relativno mali za kontrolu zagušenja na čvorovima i dinamičku širinu pojasa, a veći za prijem lokalnog kontrolnog poziva i znatno veći za ponovno usmjeravanje. Što je veći vremenski interval, to se veća pogreška predviđanja može tolerirati u pojasnoj

širini, shemama pojačane kontrole ili pretplate. Zbog toga bi se predviđanje prometa trebalo povezati sa zahtjevima mrežne kontrole u pogledu vremenskih skala i cilja korištenja resursa.

Obrnuto, može se procijeniti predviđanje prometa pod određenim ograničenjima, koji proizlaze iz zahtjeva za kontrolom. Rezultati se mogu upotrijebiti za kontrolne postavke, na primjer, za odabir cilja korištenja i s njim povezanih kontrolnih vremenskih intervala.

Potrebno je analizirati neizvjesno predviđanje prometa sa više koraka kvantizacije s obzirom na potpunu povijest prometa i njegov stacionaran model. Dakle, rezultat predstavlja gornju granicu za predviđanje mrežnog prometa sa određenim ograničenjem pogreške ili sa očekivanim intervalom predviđanja. Da bi se odgovorilo na pitanje „Je li promet predvidljiv?'' potrebno je uzeti u obzir čimbenike kao što su upravljanje mrežom u određenom vremenskom intervalu, cilj korištenja resursa, statistika prometa i mjerenje prometa na određenoj vremenskoj skali. Drugim riječima, procjena predviđanja prometa, ovisi o tome kako čovjek želi koristiti rezultate predviđanja kako bi se ispunilo kontrolno očekivanje ili ograničenje.

Tragovi prometa mogu biti nepokretni, a u tom slučaju se njihove karakteristike opisuju statistikama prvog i drugog reda, odnosno graničnom funkcijom distribucije (CDF – *Cumulative distribution function*) i funkcijom snage spektralne gustoće (PSD – *Power spectral density function*). Nadalje, promet može biti adekvatno predstavljen stacionarnim modelom kao što je *Auto-regressive moving average* (ARMA) ili *Markov-modulated poisson process* (MMPP). Poznato je da su sličnosti i dugoročna ovisnost LRD *(Long range dependence*) sveprisutna svojstva mrežnog prometa, uključujući i *Ethernet*, MPEG, JPEG videozapise i *www* promet. U praksi, u kritičnom okruženju za kontrolu, poput mreža bankomata, područje interesa je veličina prometa u ograničenim vremenskim intervalima [15].

U telekomunikacijskom prometu, pojavljivanjem komutirane paketne mreže i transformacijom telefonskih mreža u višeuslužne sustave, krajnjem korisniku pružaju se nove mogućnosti korištenja mreže. Sa višeuslužnim sustavima mijenja se arhitektura mreže i statička priroda telekomunikacijskog prometa koji je karakterističan s efektima samo-sličnosti i dugoročne ovisnosti. Povećanjem složenosti mrežne topologije povećava se mrežno zagušenje i neočekivane situacije u mreži. Kako bi se spriječilo navedeno, potrebno je mjerenje i predviđanje mrežnog prometa. Predviđanje može spriječiti i kontrolirati

zagušenje te poboljšati iskoristivost mreže. Predviđanje mrežnog prometa ima važnu ulogu u dizajnu, menadžmentu te optimizaciji modernih telekomunikacijskih sustava. Pouzdanim predviđanjem omogućuje se planiranje kapaciteta mreže i održavanje zahtijevane kvalitete usluge [16].

6. Poboljšanje procesa analize i predviđanja mrežnog prometa u telekomunikacijskoj mreži

Proračun protoka paketa u mreži daje korisne informacije o promjeni protoka paketa za neko buduće razdoblje, što je način za poboljšanje sposobnosti analize mrežnog prometa. Tisuće tvrtki ima svoje *web* stranice koje ovise o analizi mrežnog prometa zbog poboljšanja mrežnih promjena, smanjenja troškova marketinga, olakšanja optimizacije mreže, ubrzanja mreže, nadgledanja poslovanja i pružanja više razine usluge klijentima i partnerima.

Intelligent-based hybrid model predstavlja model za predviđanje prijenosa podataka unutar mreže, koji je osmišljen kombiniranjem *Adaptive neuro-fuzzy inference system* (ANFIS) sa *Nonlinear generalized autoregressive conditional heteroscedasticity* (NGARCH) optimalno regulirana s *Adaptive support vector regression* (ASVR). *Intelligent-based hybrid model* izabran je za istodobno rješavanje problema prelijevanja i grupiranja prekoračenja kako bi se poboljšala točnost predviđanja prometa, a obilježen je kao ASVR-ANFIS/NGARCH.

Spomenutim modelom moguće je napraviti proračun predviđanja protoka paketa na mreži što *web* pružatelju usluga može pomoći prilikom poboljšanja raspodjele propusnosti mreže učinkovito i djelotvorno, optimizacije određene *web* lokacije, praćenja poslovanja te povećanja marketinških promjena do najveće točke.

Kao što je poznato, analiza mrežnog prometa postala je pouzdana i standardna zadaća statistike *web* stranicama za razne *Internet* kompanije kao što su stranice za putovanja, upoznavanje i *online* trgovine.

Sustav baziran na protoku paketa razvijenog u analizi mrežnog prometa koristi tehnike prikupljanja, pohranjivanja i analiziranja informacija o mrežnom prometu. Nadzor učinkovitosti i svojstava IP mreža koje se temelje na točnosti i napredna mjerenja prometa, stoga je potrebno istražiti nove načine za praćenje mrežnog prometa, a zatim saznati njegov pravilan pristup.

Poneki poznati modeli predviđanja prometa izazvali su nekoliko ključnih problema. Na primjer, sivi model (GM) naišao je na problem prekoračenja. *Autoregressive moving-average* (ARMA), *artificial neural network* (ANN), *adaptive neuro-fuzzy inference system* (ANFIS)

modeli ne mogu izbjeći problem grupiranja prekoračenja čime se pogoršava rezultat točnosti predviđanja. Iz navedenog razloga je uvedeno ugrađivanje N*onlinear generalized autoregressive conditional heteroscedasticity* (NGARCH) u *Adaptive neuro-fuzzy inference system* (ANFIS) sa svrhom istodobnog rješavanja problema prelijevanja i grupiranja prekoračenja tijekom predviđanja [17].

Predloženi složeni model ANFIS/NAGRCH je optimalno podešen pomoću *adaptive support vector regression* (ASVR) radi formiranja linearne kombinacije na takav način da ona ne samo da praktično pojednostavljuje složeni sustav, nego i značajno poboljšava točnost predviđanja zbog istovremenog rješavanja problema prelijevanja i grupiranja prekoračenja.

U pogledu upravljanja, predviđanjem protoka paketa, priljeva i odljeva, može se poboljšati i analiza mrežnog prometa. Analiza mrežnog prometa s predviđanjem protoka paketa pruža vrijedne informacije mrežnim administratorima kako bi što bolje prilagodili usluge *web* stranica.

Prvi je uveden *Intelligent-based hybrid model* (ANFIS/NAGRCH) koji se primjenjuje na vremenske serije za prognoziranje kao jedna od ključnih komponenti analize mrežnog prometa. Zatim se koristi *Adaptive support vector regression* (ASVR) za optimalno podešavanje kompozitnog modela ANFIS/NAGRCH. Praćenje mrežnog prometa vrši se sa i bez predviđanja protoka paketa na web stranicama.

Analiza mrežnog prometa pruža vrijedne informacije za administratore *web* stranica koji služe za prilagodbu informacija na njihovim serverima kako bi dosegnuli veću količinu pregleda. Dakle, kako bi se poboljšala analiza mrežnog prometa u stvarnom vremenu, posebno precizno predviđanje je zahtijevalo funkciju predviđanja priljeva i odljeva paketa što pomaže administratoru u upravljanju i učinkovitoj raspodjeli propusnosti mreže.

Intelligent-based hybrid model (ASVR-ANFIS/NGARCH) zamišljen je kao model koji predviđa mogućnost promjene protoka paketa u sljedećem nadolazećem razdoblju što rezultira visokom preciznošću predviđanja jer se istodobno mogu riješiti problemi grupiranja prekoračenja i prelijevanja. Kontrola protoka u pogledu omjera predviđenog i nepredviđenog prometa bila je vrlo velika te se *Intelligent-based hybrid* modelom poboljšava učinkovitost preko 20% čime navedeni model može djelovati kao jedan od glavnih komponenti analize

mrežnog prometa zbog dobre izvedbe za pomoć u poboljšanju kontrole mrežnog prometa [17].

7. Zaključak

Mjerenje i analiza mrežnog prometa važni su zbog dizajna, rada i održavanja WAN mreže. Kako mrežna topologija postaje sve složenija, povećava se zagušenje mreže kao i neočekivane situacije u mreži. Analiza mrežnog prometa predstavlja postupak presretanja mrežnih paketa i podvrgavanje istih analizi. Prvenstveno se vrši radi detaljnijeg uvida u vrstu prometa, odnosno mrežnih paketa ili podataka koji prolaze kroz mrežu. Mrežna izvedba važna je zbog stvaranja uvida u mrežu što pomaže kod razvijanja vještih mrežnih operacija i protokola. Dobivanje podataka o mrežnom prometu iz stvarne mreže ima važnu ulogu kod mjerenja mrežnog prometa, čime se mogu izvući informacije o mrežnom ponašanju.

Postoji nekoliko metoda mjerenja mrežnog prometa: na osnovu vremena i protoka, na mrežnim elementima i s čvora na čvor. Postoje tri faze kod analize mrežnog prometa: pred-obrada, rudarenje podataka i procjena analize. Analizom mrežnog prometa dobivaju se korisne informacije o ponašanju i iskoristivosti mreže. Praćenjem aktivnošću određenih dijelova mreže, moguće je identificirati veća opterećenja na pojedinim dijelovima.

Razvijeno je mnogo alata za mjerenje mrežnog prometa u svrhu rješavanja trenutnih mrežnih problema. Jedan od najčešće korištenih je *Wireshark*.

Predviđanje mrežnog prometa omogućuje kvalitetno planiranje i dimenzioniranje potrebnih resursa kako bi se zadovoljila željena kvaliteta usluge. Za predviđanje mrežnog prometa koriste se prometni modeli. Prometni modeli su skup mjerenih te izračunatih parametara koji ukazuju na ponašanje korisnika mreže, a na temelju kojeg je moguće izračunati očekivani mrežni promet te definirati ponuđeni mrežni promet.

Svrha predviđanja mrežnog prometa je istraživanje potencijala ili optimalne granice predviđanja u više koraka u prometnom inženjerstvu. Predviđanjem se može spriječiti i kontrolirati zagušenje te poboljšati iskoristivost mreže. Pouzdanim predviđanjem omogućuje se planiranje kapaciteta mreže i održavanje zahtijevane kvalitete usluge.

Popis literature

1. Technopedia. *Network Traffic Analysis*. Preuzeto sa: https://www.techopedia.com/definition/29976/network-traffic-analysis [Pristupljeno: kolovoz 2019.]
2. Centar informacijske sigurnosti. *Praćenje mrežnog prometa.* Preuzeto sa: https://www.cis.hr/www.edicija/AnalizaIPAuditalata.html [Pristupljeno: kolovoz 2019.]
3. Zhiwei C, Chuanshan G, Suo C, Liangxiu H. *Measurement and analysis of IP network traffic.* Shanghai: Fudan University; 2003. Preuzeto sa: https://www.researchgate.net/publication/229025260_MEASUREMENT_AND_ANALYSIS_OF_IP_NETWORK_TRAFFIC [Pristupljeno: kolovoz 2019.]
4. Peuhkuri M. *Internet traffic measurements – aims, methodology, and discoveries*. Helsinki: University of Technology; 2002. Preuzeto sa: http://www.netlab.tkk.fi/u/puhuri/publications/li.pdf [Pristupljeno: kolovoz 2019.]
5. Joshi MR, Hadi TH. *A Review of Network Traffic Analysis and Prediction Techniques*. ArXiv; 2015. Preuzeto sa: https://arxiv.org/abs/1507.05722 [Pristupljeno: kolovoz 2019.]
6. CARNet CERT, LS&S. *Analiza sniffing alata i zaštite*. CIS; 2001. Preuzeto sa: https://www.cis.hr/www.edicija/Analizasniffingalataizatite.html [Pristupljeno: kolovoz 2019.]
7. CARNet CERT, *LS&S. Analiza IPAudit alata.* CIS; 2005. Preuzeto sa: https://www.cis.hr/www.edicija/AnalizaIPAuditalata.html [Pristupljeno: kolovoz 2019.]
8. CARNet CERT, LS&S. *Analiza alata Wireshark*. CIS; 2010. Preuzeto sa: https://www.cis.hr/www.edicija/AnalizaalataWireshark.html [Pristupljeno: kolovoz 2019.]
9. Grgurić T. *Analiza mrežnog prometa primjenom programske podrške Wireshark*. Završni rad. Fakultet prometnih znanosti Sveučilišta u Zagrebu; 2016.
10. CERT. *NetworkMiner*. Preuzeto sa: https://www.cert.hr/27405/ [Pristupljeno: kolovoz 2019.]

11. Split Horizont. *Kako vidjeti tko je spojen na računalo.* Preuzeto sa: https://www.splithorizont.com/kako-vidjeti-tko-je-spojen-na-racunalo/ [Pristupljeno: kolovoz 2019.]
12. CARNet CERT, LS&S. *Analiza SCAPY alata*. CIS; 2004. Preuzeto sa: https://www.cis.hr/www.edicija/AnalizaSCAPYalata.html [Pristupljeno: kolovoz 2019.]
13. CARNet CERT, LS&S. *Analiza cb_PMM programskog alata*. CIS; 2003. Preuzeto sa: https://www.cis.hr/www.edicija/Analizacb_PMMprogramskogalata.html [Pristupljeno: kolovoz 2019.]
14. Visković I. *Komutacija i upravljanje u telekomunikacijskoj mreži*. Nastavni materijali. Sveučilišni studijski centar za stručne studije Sveučilišta u Splitu; 2011.
15. Sang A, Li S. *A predictability analysis of network traffic*. University of Texas at Austin; 2002. Preuzeto sa: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1.6154&rep=rep1&type=pdf [Pristupljeno: kolovoz 2019.]
16. Ravnjak M. *Predviđanje količine prometa zasnovano na neuronskoj mreži*. Diplomski rad. Fakultet prometnih znanosti Sveučilišta u Zagrebu; 2015.
17. Chang BR, Tsai HF. *Improving network traffic analysis by foreseeing data-packet-flow with hybridfuzzy-based model prediction*. Expert Syst. Appl; 2009. Pristupljeno sa: https://www.researchgate.net/publication/222014315 [Pristupljeno: kolovoz 2019.]

Popis slika

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom **Mjerenje i predviđanje mrežnog prometa u telekomunikacijskoj mreži**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 09.09.19

Student/ica:

(potpis)