Analiza mogućnosti napredne metode za filtriranje paketa

Brajković, Sandro

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Sandro Brajković

ANALIZA MOGUĆNOSTI NAPREDNE METODE ZA FILTRIRANJE PAKETA

DIPLOMSKI RAD

Zagreb, 2016.

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

ANALIZA MOGUĆNOSTI NAPREDNE METODE ZA FILTRIRANJE PAKETA

ANALYSES OF DEEP PACKET INSPECTION FEATURES

Mentor: izv.prof.dr.sc. Štefica Mrvelj

Student: Sandro Brajković

JMBAG: 0135213915

Zagreb, srpanj 2016.

Analiza mogućnosti napredne metode za filtriranje paketa

Sažetak:

Ovaj diplomski rad opisuje mogućnosti trenutno najnaprednije metode za filtriranje i klasifikaciju prometa. *Deep Packet Inspection* je metoda filtriranja koja pregledava svih sedam slojeva OSI referentnog modela kod analize paketa te tako nudi najveću moguću točnost kod identifikacije paketa i prometa. U radu su opisani bitni pojmovi vezani uz funkcionalnosti DPI tehnologije kao i njene primjene u stvarnom svijetu. Budući da je ova tehnologija izazvala burne reakcije aktivista za zaštitu privatnosti, opisani su i analizirani načini korištenja ove tehnologije koji narušavaju privatnost. Također su analizirani podatci prikupljeni ovom metodom kako bi se prikazao jedan od načina primjene. Analizirani podatci daju uvid u najkorištenije aplikacije mobilnog podatkovnog prometa. Također su opisani kritični faktori koji utječu na performanse tih najkorištenijih aplikacija.

Ključne riječi: *Deep Packet Inspection*, filtriranje, klasifikacija

Analyses of Deep Packet Inspection Features

Abstract:

This Master's thesis describes the features of an advanced method of packet filtering and classification. Deep Packet Inspection is a filtering method that inspects all seven layer of OSI referent model while analyzing the packets and therefore offer the best way of identifying the packets and traffic. This paper also describes important terms that are related to DPI functions and it’s applications in the real world. Since this technology caused a lot of uproar from the privacy activists, the use cases of DPI where privacy is disturbed are also described and analyzed. The data collected using this method are also analyzed so one of the use cases could be closely shown. The analyzed data gives insight in most used application of mobile data traffic. Also, critical factors that affect the performance of user applications are also described.

Key words: Deep Packet Inspection, filtering, classification

Sadržaj

1. Uvod

U 21. stoljeću Internet je daleko najkorišteniji način komunikacije i prijenosa podataka. Kao takvim, kroz njega prolaze enormne količine podataka koje je relativno teško nadzirati. Budući da mrežni elementi ne gledaju sadržaj paketa koji se šalju, već samo zaglavlja, te ih na temelju njih prosljeđuju prema odredištu, postoje mnogi načini za slanje ilegalnih podataka putem Interneta.

Filtriranje podataka proces je pregledavanja paketa koji omogućava njihovo propuštanje u mrežu ili odbacivanje. Kao takav veoma je bitan zbog više aspekata među kojima je najvažnija sigurnost koja je kroz povijest najviše poticala razvoj filtriranja. Povećanjem količine podatkovnog prometa, mobilni operateri susreću se s brojim izazovima kada je u pitanju planiranje mreža i upravljanje prometom. Napredna metoda filtriranja paketa opisana u ovom radu trenutno je najnapredniji način za filtriranje i klasifikaciju. Kao takva ima široku upotrebu, pogotovo kod mrežnih operatera i davatelja usluga. U ovom radu opisani su pojmovi usko vezani uz *Deep Packet Inspection* (DPI), koji predstavlja naprednu metodu filtriranja podataka, te su prikazane različite upotrebe ove tehnologije kao i primjer analize samih podataka dobivenih ovom metodom filtriranja.

Svrha ovoga rada je objasniti naprednu metodu za filtriranje podataka i analizu prikupljenih podataka.

Cilj rada je prikazati skup mogućnosti koje nudi implementacija sustava baziranih na DPI-u. Poseban naglasak stavljen je na nadzor i analizu podataka koja omogućava detekciju kritičnih faktora koji mogu utjecati na performanse aplikacije krajnjeg korisnika.

Materija diplomskog rada izložena je u sedam poglavlja:

1. Uvod,
2. Osnovne značajke DPI-a,
3. Pravni aspekt nadzora prometa uz korištenje DPI-a,
4. Opis procedure nadzora prometa i prikupljanja podataka
5. Analiza prikupljenih podataka o prometu,

6. Detektiranje kritičnih faktora koji mogu utjecati na performanse aplikacije,
7. Zaključak

Drugo poglavlje pod nazivom *Osnovne Značajke DPI-a* predstavlja pojmove usko povezane s funkcijom DPI-a kao što su nadgledanje prometa i metode nadgledanja prometa, klasifikacija prometa, razine filtriranja prometa te osnovni pristupi korištenju DPI-a.

U trećem poglavlju koje se zove *Pravni aspekti nadzora prometa uz korištenje DPI-a* opisana je pravna strana upotrebe DPI-a. Tehnologija opisana u ovome radu izazvala je burne reakcije u javnosti, a pogotovo među aktivistima za zaštitu privatnosti, kada je obznanjeno da se koristi. U ovome poglavlju dan je pregled mogućnosti i načina upotrebe DPI-a koji je izazivao protivljenje određenih skupina ljudi.

U četvrtom poglavlju nazvanom *Opis procedure nadzora prometa i prikupljanje podataka* prikazani su slučajevi upotrebe i neki od procesa nadzora prometa i prikupljanja podataka uz korištenje DPI tehnologije.

Peto poglavlje, nazvano *Analiza prikupljenih podataka o prometu* prikazani su podatci prikupljeni od strane operatera koristeći DPI. Podatci su klasificirani te je opisano 10 najkorištenijih aplikacija koje koriste korisnici mobilnog podatkovnog prometa.

Šesto poglavlje naziva *Detektiranje kritičnih faktora koji mogu utjecati na performanse aplikacije* bavi se aplikacijama iz petog poglavlja ali ih se koristeći identifikatore klase kvalitete usluge, još jednom klasificira te su opisani kritični faktori koji utječu na kvalitetu usluge za svaku od navedenih aplikacija.

2. Osnovne značajke DPI-a (Deep Packet Inspection)

Deep Packet Inspection mrežna je tehnologija koju poslovni sektor i mrežni operateri koriste za nadgledanje aplikacija koje generiraju i primaju mrežni promet. Tokovi podataka na Internetu sastoje se od paketa, a paketi se sastoje od dva elementa: zaglavlja i korisničkih podataka (*paylaod*). Zaglavlje usmjeruje paket prema odredištu, kao što adresa na pismu usmjeruje pismo prema odredištu. Korisnički podatci su ono što korisnici ili aplikacije razmjenjuju, nastavno na analogiju s pismom, to su slika, tekst, boja, rukopis, stil pisanja itd. Prijašnje mrežne tehnologije analiziraju i filtriraju podatke ovisno o informacijama iz zaglavlja paketa. DPI sustavi omogućuju podobniju analizu paketa baziranu na njihovom sadržaju. DPI može modificirati sadržaj paketa i identificirati podatkovni promet čak i kada je on kriptiran. Pregledavanje sadržaja komunikacija, bio on kriptiran ili ne, njegovo modificiranje i potom ubrzavanje ili usporavanje ovisno o definiranim pravilima dovelo je do mnogih protivljenja i protesta u zajednici [1]. Pravna strana ove metode podobnije je opisana u trećem poglavlju rada.

Konstantan razvoj uređaja i procesorske moći koja može podnijeti obradu miliona paketa u sekundi potrebna je kako bi se zahtjevi za današnjim DPI-om ostvarili. Kako tehnologija prati cjenovnu krivulju Moorovog zakona [2] mogućnosti DPI-a se sve češće implementiraju u širok spektar mrežne opreme, od usmjerivača do specijaliziranih uređaja koje se postavljaju unutar manjih mreža.

Ova tehnologija ima širok spektar primjena koje će biti opisane u ovom radu. Za početak je, u nastavku, dan pregled osnovnih pojmova i tehnologija koje su usko vezane za DPI, a zatim je prikazan detaljniji opis principa rada i mogućnosti DPI-a.

2.1 Metode nadgledanja prometa

Nadgledanje mrežnog prometa može biti aktivno ili pasivno. Pasivno nadgledanje mrežnoga prometa čita podatke bez da utječe na sam promet. Aktivno nadgledanje daje mogućnost modificiranja podataka koje čita.

Postoji nekoliko načina pasivnog nadgledanja prometa. Jednostavno nadgledanje može biti lagano za manualnu procjenu, budući da se radi o manjoj količini promatranog prometa. Međutim, greške i napadi mogu jednostavno proći ne zamijećeno. Nadgledanje svih detalja o mreži i mrežnome prometu također ima nedostatke. Prikupljaju se svi podatci potrebni za analizu i detekciju napada ili grešaka, ali se oni izgube u velikoj količini podataka koja je prikupljena ovim načinom nadgledanja. Također, što više podataka se prikupi, to je tehnološki zahtjevnije pohraniti i obraditi te podatke. Stoga se različiti načini promatranja mrežnog prometa natječu jedan s drugim, svaki nudi određene prednosti u odnosu na ostale te se tako svaki od njih koristi u različitim situacijama i s različitom svrhom. Slika 1 prikazuje općenitu arhitekturu nadgledanja prometa [3] .

Slika 1 : Opća arhitektura nadgledanja prometa

Izvor: [3]

Proces nadgledanja mrežnog prometa sastoji se od dva glavna koraka. Prvi korak je dupliciranje prometa a drugi je analiza prometa. Ovi koraci detaljnije su opisani u nastavku.

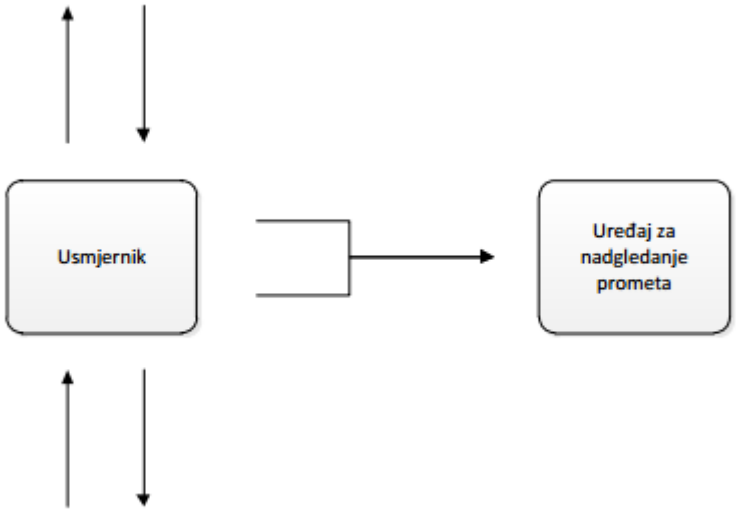
2.1.1 Dupliciranje prometa

Svi načini nadgledanja mrežnog prometa imaju jednu zajedničku osobinu, a to je da se promet duplicira kako bi se duplikat analizirao. Samo dupliciranje može se odvijati na dva načina: *inline* ili zrcaljenjem. Uređaj za dupliciranje prometa u *inline* modu postavlja se na vod, dok je kod zrcaljenja, mogućnost dupliciranja ugrađena u preklopnik ili usmjernik. Prema [4] postoji nekoliko načina zrcaljenja prometa:

- Zrcaljenje porta
- Korištenje uređaja za hvatanje paketa (Test Access Point - TAP)
- Korištenje uređaja za hvatanje paketa uz korištenje zaobilazne kartice mrežnog sučelja.

2.1.1.1 Zrcaljenje porta

Zrcaljenje porta je funkcionalnost koja se uobičajeno koristi u preklopnicima i usmjernicima u poduzetničkom okruženju. Promet koji prolazi određenim portom preklopnika ili usmjernika, zrcali se na drugi port. Port koji se koristi za dupliciran promet naziva se SPAN(*Switched Port ANalyzer*) portom. Slika 2 prikazuje proces nadziranja prometa pomoću zrcaljenja porta.



Slika 2 Princip zrcaljenja porta

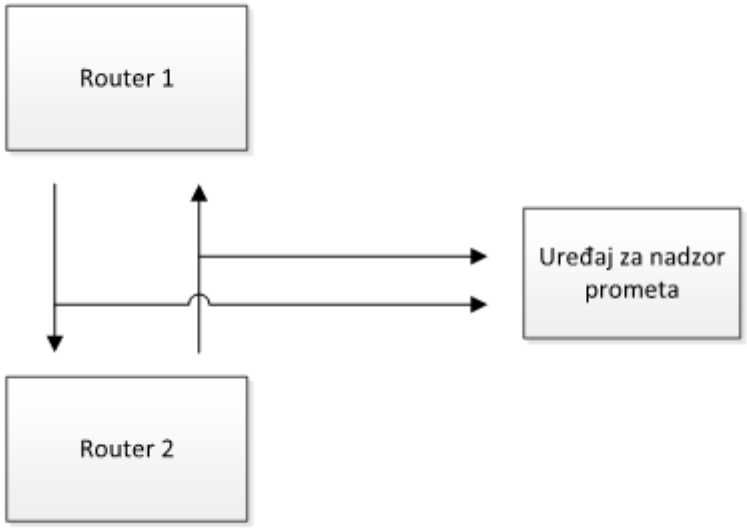
Izvor: [3]

Postoje dva nedostatka zrcaljenja portova. Prvi je mogućnost da suma propusnosti koja se zrcali na port bude veća od propusnosti tog porta pa dolazi do zagušenja i gubitka paketa. Puni dupleks se prenosi u jednom smjeru preko SPAN porta. To je do dva puta propusnosti pojedinog porta za dva porta koja koristi preklopnik, ili čak i više ako se koristi više od dva porta. Većina preklopnika ne posjeduje dovoljno procesorske moći da bi podnijeli i preklapanje i zrcaljene prometa. Primarna funkcija preklopnika je prioritetna tako da je moguće da zrcaljenje ne radi dobro tijekom vršnih sati [3].

2.1.1.2 Korištenje uređaja za hvatanje paketa

Test Access Port (TAP) je uređaj za hvatanje paketa postavljen u *inline* modu budući da su promatrani vodovi odvojeni. TAP uređaj se spaja između dva odvojena dijela voda i promet se duplicira. Jedan TAP duplicira promet na jedan izlaz, koji se sastoji od dva fizička porta za silazni i uzlazni smjer na vodu s punim dupleksom. Regenerativni TAP duplicira promet u više

izlaza. Agregacijski TAP spaja oba kanala na jedan izlazni port. Postoje tri vrste TAP-a: bakreni, optički i virtualni. Slika 2 prikazuje pristup zrcaljenju prometa uz korištenje TAP-a [2].



Slika 3 Pristup zrcaljenju prometa koristeći TAP

Izvor: [3]

Pasivni bakreni TAP spaja se direktno na vod. Budući da pasivni TAP nema svoje napajanje, nestanak struje neće uzrokovati probleme na vodu. Nedostatak pasivnog bakrenog TAP-a je u tome što se može koristiti samo za 10 megabitne i 100 megabitne veze. Pasivna veza izobličuje signal na način da nije moguće koristiti TAP kod gigabitne veze [5].

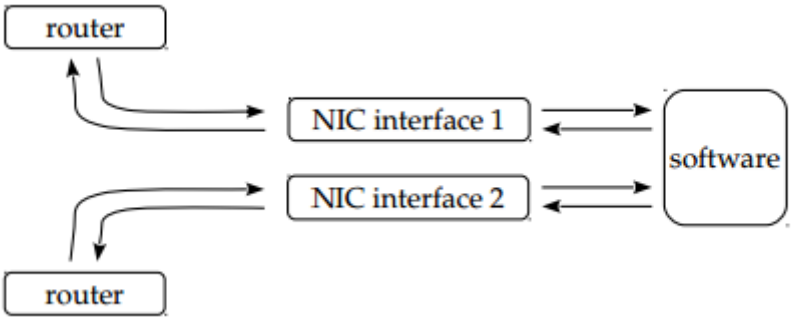
Aktivni bakreni TAP funkcionira na način da signal koji prolazi kroz TAP bude ponovno prenošen i dupliciran te tako nema distorzije signala. Nedostatak ovog načina je da nestanak napajanja u TAP-u uzrokuju prebacivanje na pasivnu opremu pa dolazi do kašnjenja od nekoliko stotina milisekundi.

Pasivni optički TAP preusmjerava dio originalnog signala na zrcalni port. Nedostatak mu je u tome što oslabljuje signal u vodu.

Regeneracijski optički TAP preusmjerava veoma mali dio originalnog signala na zrcalni izlaz te ga onda pojačava do pune snage. Nedostatak napajanja samo uzrokuje nesposobnost zrcaljenja te ne utječe na sam vod [3].

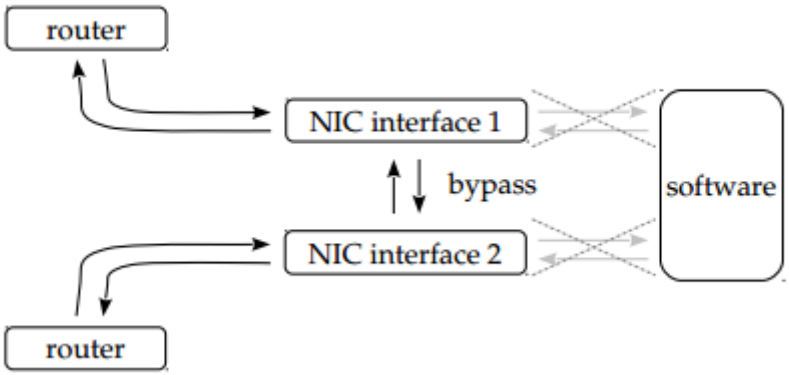
2.1.1.3 Korištenje uređaja za hvatanje paketa uz korištenje zaobilazne kartice mrežnog sučelja

Korištenjem kartice mrežnog sučelja (*Network Interface Card* - NIC) integrira se nadgledanje prometa s analizom prometa. Promatrani vod je odvojen. Oba dijela su spojena s NIC-om, te je NIC instaliran na računalo. Sučelja su konfigurirana kao mrežni premosnik. Kako se računalo ponaša kao premosnik, sav promet prolazi kroz njega i stoga je moguće vršiti analizu prometa.



Slika 4 Pristup zrcaljenju porta koristeći dva NIC-a, [3]

Zrcaljenje prometa na način da se upotrebljava NIC moguće je korištenjem komercijalnih NIC-ova ali oni tada postaju kritična točka. Kada dođe do prestanka rada računala ili programa na računalu, vodovi više nisu spojeni. Zato postoje posebni NIC-evi koji se nazivaju zaobilaznim NIC-evima (engl. *Bypass NIC*) koji imaju mogućnost zaobilaženja mrežnih sučelja kada dođe do prestanka rada računala ili programa.



Slika 5 Prikaz korištenja zaobilaznog NIC-a, [3]

Nedostatak ovih načina rada je u tome što moraju postati fizička računala koja moraju biti statična i ne mogu se micati, a isto tako, ako se ne koriste zaobilazni NIC-evi oni postaju kritična točka u sustavu [3].

2.1.2 Dohvaćanje paketa i analiza prometa

Dohvaćanje paketa (*Packet Capture*) ima tri značenja. Prvo je interaktivan pristup mrežnom nadgledanju. Drugo, *packet capture* je podatak generiran programom za praćenje prometa. Treće je sam čin dohvaćanja paketa iz mreže. Dohvaćeni podatci mogu se pohraniti ili mogu biti direktno pročitani od strane analizatora mrežnog prometa u stvarnom vremenu [6].

2.1.2.1 Dohvaćanje paketa kao metoda dupliciranja paketa

Mrežni promet je dohvaćen s promatranog mjesta. Nije bitno za dohvaćanje da je to mjesto privremeno i prostorno vezano za nadolazeću analizu budući da se dohvaćeni podatci pohranjuju.

Mogu se pohranjivati u privremene datoteke kao dijelovi cjelokupnog procesa mrežnog promatranja ili se mogu pohraniti kako bi se koristili i analizirali kasnije. Prikupljeni podatci jednaki su onima podatcima koji su se prenašali linkom. Proces dohvaćanja paketa može biti manualan ili automatiziran [7].

2.1.2.2 Dohvaćanje paketa kao pristup nadgledanja mrežnog prometa

Pristup nadgledanja mrežnog prometa koji koristi dohvaćanje paketa sastoji se od dva osnovna koraka. Prvi korak je dohvaćanje paketa i stvaranje datoteke s dohvaćenim podatcima, a drugi je provođenje analize nad prikupljenim podatcima. Ovaj pristup može biti manualan ili automatiziran. Automatizirani pristup se koristi kod otkrivanja malicioznog koda i promatranja ponašanja malicioznog koda. Naravno, kod takvog pristupa moguća je i daljnja manualna analiza odabranih dohvaćenih paketa.

Kod ovakve metode koristi se i grafičko sučelje i komandna linija. U nekim slučajevima moguće je koristiti skriptiranje kako bi se pojedine akcije automatizirale. Skripte se koriste kako bi korisnicima olakšale pretraživanje tako velike količine podataka. Ovaj način nadgledanja mrežnog prometa nudi najviše mogućnosti, ali također zahtijeva i najviše vremena i znanja budući da se radi s jako velikim količinama podataka. Manualno pregledavanje paketa od

velike je važnosti kod otkrivanja novih malicioznih kodova i njihovog ponašanja, zato što ih postojeći programi i algoritmi ne mogu detektirati kada nisi upoznati s njima [3].

2.1.3 Metoda promatranja toka

Metoda bazirana na promatranju toka (eng. *Flow observation*) razlikuje se od prethodne dvije opisane metode. Ovom metodom se ne analiziraju korisnički podatci, već samo zaglavlja paketa. Te informacije se tada skupljaju u tokove. RFC 7011 [8] definira tok: „Tok je definirani set paketa ili okvira koji prolaze kroz promatranu točku u mreži u vrijeme određenog vremenskog intervala. Svi paketi koji pripadaju određenom toku imaju skup zajedničkih svojstava."

Za razlikovanje tokova koriste se: izvorišna IP adresa, IP adresa odredišta, izvorišni IP port, odredišni IP port, protokol 4. sloja po OSI referentnom modelu. Budući da ne pregledava korisničke podatke, ova metoda je brža od DPI-a kada koristi isti hardver. Također, nepohranjivanjem korisničkih podataka ostvaraju se značajne uštede u prostoru za pohranu [3].

2.2 Klasifikacija mrežnog prometa

Klasifikacija mrežnog prometa, zadnjih je godina, postala jedan od velikih izazova u telekomunikacijama. Ona se bazira na dubokom razumijevanju kompozicije i dinamike mrežnog prometa, a esencijalna je kod upravljanja i nadgledanja infrastrukture mrežnih operatera. Nadalje, povećani kapacitet i dostupnost širokopojasnog pristupa Internetu doveli su do kompleksnog ponašanja tipičnih korisnika, veoma različitih od korisnika iz vremena *dial-up* veze.

Klasifikacija internetskog prometa daje uvid u mnoge aktivnosti potrebne za upravljanje mrežom, kao što su: planiranje kapaciteta, prometno inženjerstvo, analizu pogrešaka, performanse aplikacija, detekcija anomalija te naplata. Provedeno je više analiza i mjerenja Internet prometa, i većina ih upućuje na to da je najdominantnija vrsta prometa *peer-to-peer* (P2P) koji zauzima više od 80% prometa, ovisno o lokaciji i trenutku u promatranom danu. U zadnje vrijeme, video promet je ponekad zauzimao veći udio od P2P prometa, ponajviše zahvaljujući tzv. *live streaming*-u i uslugama dijeljenja videa. Točni podatci su i dalje nepoznati, ponajviše zato što je veoma teško točno mjeriti i analizirati Internet

promet. Najveći problemi kod takvoga mjerenja su ograničeno trajanje mjerenja, gubitak informacije tijekom procesa mjerenja i nemogućnost identifikacije korištene aplikacije.

Dodatno, dostupnost širokopojasnog pristupa Internetu konstantno raste, pogotovo kabelska televizija te ADSL infrastruktura i tehnologije a u razvijenim zemljama i optička veza. Takva pristupačnost otvara nove načine korištenja resursa, kako rezidencijalnim tako i poslovnim korisnicima. Kako je širokopojasni pristup sve više dostupan i budući da mu se povećava kvaliteta usluge, korisnici ga sve više koriste za širi spektar mogućnosti kao što su Internet pozivi, elektroničko poslovanje, Internet bankarstvo i dijeljenje podataka - ponajviše videa i glazbe. Drugim riječima, upravo su povećani kapacitet i pristupačnost doveli do kompleksnijeg ponašanja krajnjega korisnika. Novija istraživanja su pokazala da korisnici širokopojasnog pristupa Internetu, za razliku od onih s *dial-up* pristupom, više koriste Internet, provode više vremena stvarajući i dijeleći sadržaj kao i da više traže razne informacije. Stoga, davatelji mrežnih usluga bi trebali obratiti pažnju na to novo, kompleksnije ponašanje krajnjih korisnika [9].

Bez mogućnosti identificiranja i mjerenja mrežnog prometa, davatelji usluga ne mogu stvarati nove usluge, optimizirati dijeljene resurse niti osigurati točnu naplatu usluga. Klasifikacija prometa korak je dalje od same identifikacije, ona traži informacije o na primjer: rezoluciji videa, tipu medija, porijeklu te mjeri karakteristike kao što su: trajanje, broj ponavljanja, kvaliteta doživljaja itd.

2.2.1 Identifikacija prometa

Različiti proizvođači opreme i aplikacija, različito grupiraju promet, ali općenito se promet može svrstati u jednu od sljedećih kategorija:

- Protokol: skup pravila i formata koji definira kako će dva i/ili više elemenata dijeliti informacije (tok informacija može biti jednosmjeran ili dvosmjeran). Primjeri su: UDP,TCP,HTTP,SIP,FTP,SMTP.
- Aplikacija: promet koji je produkt nekog određenog programa. Primjeri su Skype, Netflix, *online* igre.
- Internetska stranica: sve internetske stranice su dio određene web domene i sav sadržaj koji se dijeli je dio neke domene.

- Usluge: općeniti naziv za stranice kao što su Twitter, Facebook, servisi u oblaku, mrežno pohranjivanje podataka i ostali.

Davatelji usluge: obično se koriste kako bi se razlikovali brandovi unutar određene vrste prometa. Tako neki davatelji video usluge koriste *Real-Time Messaging Protocol* (RTMP), a veći broj govornih servisa koristi *Session Iniciation Protocol* (SIP).

Čak i u ovoj podjeli, postoji potencijal preklapanja koji je očit. Ovi pojmovi su veoma blisko povezani pa je lako naći argumente da bi neki određeni tip prometa trebao pripadati nekoj drugoj klasifikaciji: npr. BitTorrent je softver koji koristi BitTorrent protokol kao dio BitTorrent mreže. Nadalje, veliki dio Internet videa prenosi se RTMP-om, unutar HTTP-a, koji je TCP - tako da je svaki od tip protokola točna identifikacija, ali ovisi o razini informacije koja je potreba.

Većina ovih pojmova se često koristi kao generalni pojam za više pojmova. Zbog važne i tehničke naravi tematike, kada god postoji sumnja u pravo značenje, pametno je postaviti specifično pitanje i precizno definirati kontekst. Također, često se dodaju dodatne pod klase kako bi se detaljnije opisala određena podjela. Tako se YouTube može identificirati kao HD ili neHD, dok BitTorrent može biti kriptiran ili nekriptiran. Dodavanje pod klasa daje dodatnu razinu informacija u podjelu [10].

2.2.2 Kategorije prometa

Tipično, protokoli, aplikacije, internetske stranice i usluge su dio kategorizacijske hijerarhije. Ta hijerarhija se naravno može mijenjati ovisno o potrebama, ova promatrana u nastavku je hijerarhija jednog od vodećih prodavača aplikacije za upravljanje mrežnim prometom, Sandvine-a.

Tablica 1. opisuje kategorije prometa prema Sandvine-u te daje njihov opis i najčešće korištene primjere.

Tablica 1 Kategorije po Sandvine proizvođaču

Prometna kategorija	Opis	Primjer
Pohrana	Prijenos velike količine podataka i online pohrana	FTP,NNTP,Dropbox
Igre	Konzole i PC igre	Nintendo Wii, Xbox Live, Playstation Live, World of Warcraft
Trgovine	Trgovine aplikacija i sadržaja za preuzimanje	Google Play Store, Apple iTunes, Windows Update
Administracija	Protokoli korišteni za upravljanje mrežom	DNS, ICMP, NTP, SNMP
Dijeljenje podataka	Aplikacije za dijeljenje podataka, *peer-to-peer* ili direktno dijeljenje	BitTorrent, Ares, Pando, Foxy
Komunikacija	Aplikacije, servisi i protokoli koji omogućuju email, pisanu , govornu ili video komunikaciju	Skype, ICQ, SIP, IRC, WhatsApp, Gmail, SMTP
Stvarno vremenska zabava	Aplikacije i protokoli koji omogućuju zabavu na zahtjev	Pandora, Google, Twitch.tv, Netflix
Tuneliranje	Protokoli i usluge koji omogućuju pristup udaljenim mrežnim resursima ili nude enkripciju ili enkapsulaciju	SSL, SSH, L2TP, Remote Desktop, PC Anywhere, Teamviewer
Društvene mreže	internetske stranice i usluge fokusirani na omogućavanje interakcije i dijeljenje podataka	Facebook, Twitter, Instagram
Pretraživanje	Protokoli i usluge koji omogućuju pretragu Interneta	HTTP, WAP browsing

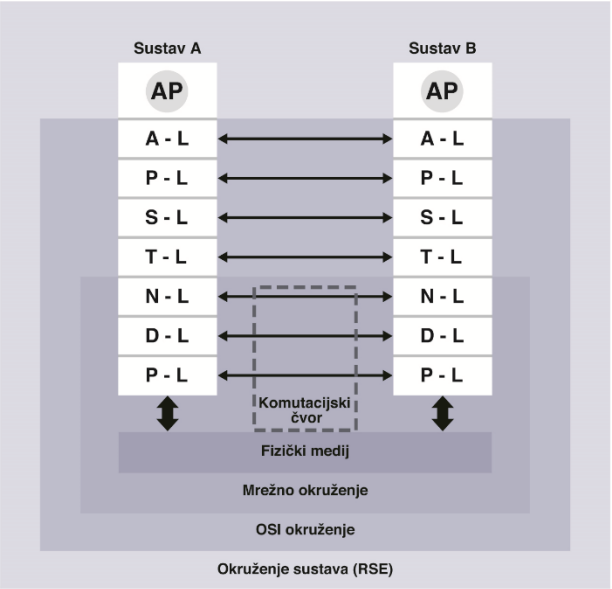
Izvor: [10]

2.3 Razine filtriranja podataka

Temeljem koncepta i općih načela slojevitog strukturiranja kompleksa komunikacija, razvijen je referentni model povezivanja otvorenih sustava (*Open System Interconnection – Reference Model*). Izbor sedam razina rezultat je iscrpnih evaluacija (prijedlozi su bili u rasponu 5 - 11). OSI-RM službeno je prihvaćen u listopadu 1984. godine kao ISO-norma dokumentom ISO7948, te kao preporuka CCITT (ITU-T) X.200 na Plenarnoj sjednici CCITT (također u listopadu 1984. g.) [11].

OSI referentni model definira sedam protokolnih razina, od najvišeg sloja razina, od najvišeg sloja primjene ili aplikacije do najnižeg fizičkog sloja. Slojevi OSI referentnog modela su prikazani na slici 6.

1. **Fizički sloj *(Physical Layer)***
2. **Sloj podatkovne veze *(Data Link Layer)***
3. **Sloj mreže *(Network Layer)***
4. **Sloj transporta *(Transport Layer)***
5. **Sloj sesije *(Session Layer)***
6. **Sloj prezentacije *(Presentation Layer)***
7. **Sloj primjene *(Application Layer)***



Slika 6 Opis OSI referentnog modela
Izvor: [12]

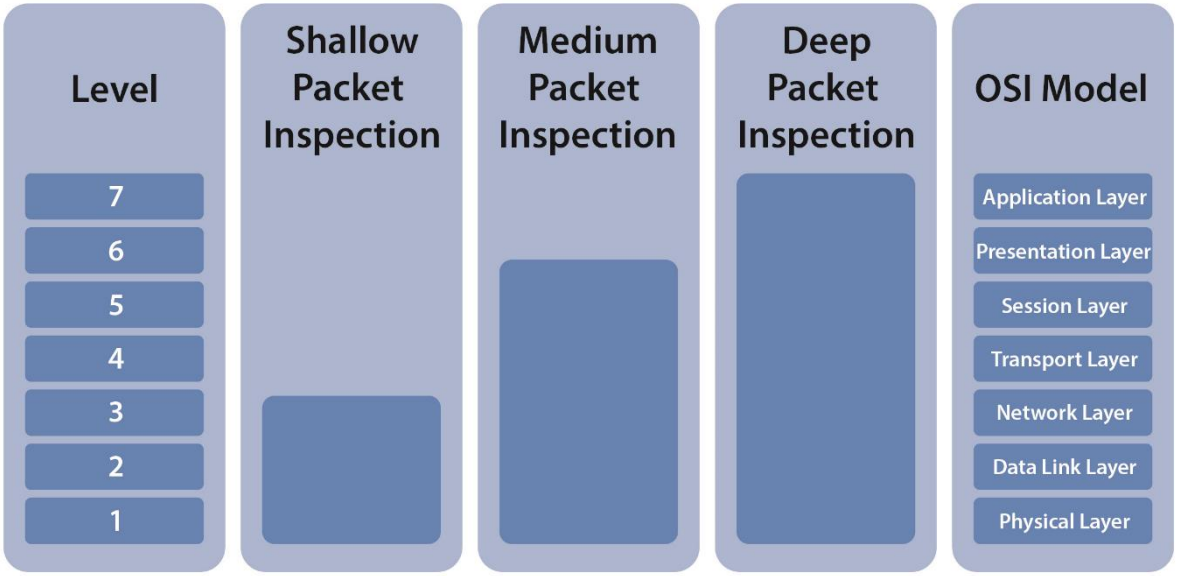
Prva tri sloja mrežno su ovisna i orijentirani su na protokole asocirane s podatkovnom telekomunikacijskom mrežom koja se koristi za povezivanje dvaju sustava.

Suprotno njima, tri gornja sloja su aplikacijsko ovisna i sadrže protokole koji omogućuju interakciju aplikacijskih procesa krajnjih korisnika [12].

Mrežni paketi se uglavnom dijele na zaglavlje i korisničke podatke koji se prenose. IP zaglavlje sadrži razne podatke potrebne u prijenosu paketa: verzija, duljina zaglavlja, tip servisa, ukupna duljina, identifikacija, zastavice, ofset fragmenta, TLL vrijeme, protokol, *checksum* zaglavlja, izvorišna adresa, odredišna adresa i opcionalne podatke. . Pored IP zaglavlja nalazi se TCP zaglavlje koje ima funkciju identifikacije adrese odredišnog terminala i prijavljivanje greške kada se paket izgubi.

Razina filtriranja podataka ovisi o broju slojeva koji se provjeravaju. Iako ne postoje strogo definirane kategorije, Parsons je 2008. godine kategorizirao tri razine [11].

Tri razine filtriranja su *Shallow Packet Inspection* (SPI), *Medium Packet Inspection* (MPI) i *Deep Packet Inspection* (DPI). Slika 7 prikazuje razine koje svaka od navednih metoda pretražuje.



Slika 7 Razina filtriranja podataka

Izvor: [11]

SPI čita zaglavlje paketa i odbacuje pakete ako je informacija iz zaglavlja na crnoj listi, tj. na listi na kojoj je administrator odredio što ne želi da prolazi mrežom. SPI ne može čitati sesijski, prezentacijski ili aplikacijski sloj, pa tako ne može ni čitati same korisničke podatke. Budući da čita samo informacije iz zaglavlja, ova metoda je pogodna za brzo procesiranje velike količine podataka.

MPI aplikacija ne prima podatke direktno, već ih obrađuje pomoću *proxy*-a. Podatci se spremaju u privremenu memoriju gdje MPI obrađuje zaglavlja prema uputama. *Proxy* je sinkroniziran s mrežnim elementima tako da administrator mreže može postaviti prethodno definirana pravila o paketima koji će se slati mrežom. Odluku o propuštanju paketa kroz mrežu, SPI donosi samo na temelju zaglavlja, dok MPI u obzir uzima i format podataka i internetsku adresu. Na primjer, moguće je odrediti pravilo da se samo *flash* datoteke i slike s društvenih mreža ne otvaraju na poslovnim računalima. S druge strane, MPI sustavi nemaju dovoljno skalabilnosti i zahtijevaju poseban aplikacijski poveznik za svaku aplikaciju, a ako se

radi s više aplikacija i poveznika, tada se unosi kašnjenje u sustav. Stoga ovi sustavi nisu od koristi davateljima usluga koji rade s velikim količinama mrežnih podataka i podržavaju veći broj aplikacija [11].

Za razliku od SPI-a i MPI-a, DPI se koristi u velikim mrežnim okolinama budući da je dizajniran da procesira stotine tisuća paketa i određuje koji program generira te pakete, sve u što kraćem vremenu. DPI sustavi pohranjuju stotine tisuća paketa u memoriju dok ne skupi dovoljno informacija da svrstaju određeni paket pod već identificiranu vrstu paketa. Kada je paket identificiran, sustav određuje što će s njime napraviti koristeći prethodno definirana pravila te tako odlučuje da li će paket biti poslan mrežom ili odbačen. Ako DPI sustav ne može identificirati aplikaciju niti nakon pretraživanja zaglavlja i korisničkih podataka, provjerava uzorak da bi se odredilo kako paket putuje između računala [11].

DPI tehnologijom moguće je analizirati internetski promet u stvarnom vremenu i procesirati ga diferencijalno. Takav sustav sadrži mnoge funkcionalnosti. Može ga se koristiti u različite svrhe kao što su sigurnost, upravljanje prometom, blokiranje malicioznog sadržaja, upravljanje oglasima itd [11].

Više o samoj DPI tehnologiji opisano je u nastavku rada.

2.4 Deep Packet Inspection

Kako bi se prebrodila ograničenja filtriranja podataka, SPI-a i nepotpune klasifikacije prometa, razvijena je DPI tehnologija. Kao što je već navedeno u prijašnjem poglavlju, DPI pregledava sve slojeve OSI modela. DPI sustavi pregledavaju cijeli IP paket i na temelju zadanih pravila u bazama pravila, donose odluke te poduzimaju određene mjere s prometom. Nekoliko je načina na koje DPI klasificira promet, najkorišteniji su *pattern-matching* i analiza temeljena na događajima u mreži, ali koriste se i statistički i bihevioristički algoritmi. Analizu zaglavlja paketa moguće je napraviti ekonomično,s strane procesorske snage potrebne za obradu podataka, budući da su zaglavlja ograničena standardiziranim protokolima. Međutim, korisnički sadržaj mnogo je teže pretraživati budući da nije pohranjen u standardiziranom obliku. Zato takva pretraga zahtijeva puno više procesorske moći. Tome problemu pristupa se razvojem posebnog *softver* baziranog na Boyer-Moore-ovom algoritmu i hardverskim rješenjima baziranim na algoritmu Bloom-ovog filtera. U nastavku su opisane dvije najčešće metode filtriranja i klasificiranja prometa na kojima se temelji rad DPI-a [13].

2.4.1 Metoda uspoređivanja uzoraka

Metoda uspoređivanja uzoraka (*Patter-matching)* je metoda koja podrazumijeva pretraživanje cijeloga mrežnog prometa u potrazi za poznatim nizovima byte-ova ili za regularnim izrazom (*regular expression*). Potraga se može ograničiti na određene dijelove paketa ili na specifične pakete. Relativna jednostavnost ovog pristupa mu je velika prednost, upravo zato je ovo popularna metoda koju koristi DPI.

Problem nastaje kada se pokušavaju pretražiti uzorci koje nije moguće opisati regularnim izrazom. Ako je podatke potrebo dekodirati prije *pattern matching*-a a funkcionalnost dekodiranja nije ugrađena u mrežni element, tada postaje nemoguće kreirati regularni izraz koji obavlja dekodiranje. Kompresija je primjer takvog dekodiranja koje je potrebno obaviti prije *pattern matching*-a. Složena logika odluka je također neisplativa koristeći regularne izraze. Današnje mrežno nadgledanje prometa koristi *pattern-matching* DPI metodu za dekodiranje često korištenih protokola [14].

Pattern matching je spor u odnosu na pristup temeljen na promatranju toka prometa koji je opisan u nastavku ovog poglavlja. Konkretno, *patter matching* implementacija za 10

Gb/s prometa zahtijeva hardversko ubrzanje koristeći FPGA. Nasuprot tome, metoda promatranje prometa bez hardverskog ubrzanja može obrađivati 40 Gbps.

2.4.2 Analiza temeljena na događajima

Zbog nemogućnosti *pattern matching*-a da dekodira promet ili donosi višestruke odluke razrađena je arhitektura temeljena na analizi događaja (*event-based analysis*).

U pristupu DPI-a koji se bazira na analizi događaja, paketi se procesiraju u događaje koji se zatim procesiraju pomoću skripti. Skripte mogu implementirati kompleksne procesne algoritme i dodati nove DPI funkcionalnosti. Arhitektura takvog pristupa zamjenjuje dio *pattern matching*-a s algoritmima implementiranima kao računalni programi. Algoritmi mogu biti *statefull* i *stateless*. *Stateless* algoritmi su neposredna reakcija ili lanac reakcija na određeni događaj. *Stateful* algoritmi mogu koristiti programske varijable kako bi zapamtili stanja između više događaja [14].

2.4.3. Upotreba DPI-a

DPI danas ima veoma širok spektar mogućnosti, pa se tako može koristiti u razne svrhe. Neke od najbitnijih i najčešćih načina upotrebe opisani su u ovom dijelu rada. Primjene DPI-a uključuju: provođenje politika (*Policy Enforcement*), mrežnu sigurnost, analizu mreže i korisnika, nadgledanje i presretanje prometa, optimizaciju sadržaja, naplatu i mjerenje, distribuciju aplikacija i raspodjelu opterećenja prometa (*Load Balancing*) i modifikaciju i umetanje podataka u pakete [14].

Već dulje vrijeme postoje aplikacije koje koriste DPI ali korisnici ni javnost toga nisu bili svjesni dok se nisu pojavili protivnici korištenja DPI-a u svrhu zaštite privatnosti. Primjeri tih aplikaciju su: filtriranje neženjene elektroničke pošte, antivirusi za elektroničku poštu, sustav detekcije i prevencije upada, vatrozidi (*Firewall*), mrežne sonde za nadgledanje prometa itd. [15].

2.4.3.1 Upravljanje prometom

Poznato je da različite mrežne aplikacije imaju različite zahtjeve za kvalitetom usluge. Internet telefonija i online igre najbolje rade bez kašnjenja i kolebanja kašnjenja (*jitter*), ali ne zahtijevaju puno propusnosti. S druge strane, kod preuzimanja velikih količina podataka, *jitter*

i kašnjenje neće degradirati uslugu, već je samo bitna što veća propusnost. Nažalost, Internet nema jedinstvenu tehniku za garantiranjem kvalitete usluge. Prijašnji sustavi za garantiranjem kvalitete usluge bazirali su se na označavanju paketa kako bi daljnji usmjernici u mreži mogli prioritetno usmjeravati neke pakete. Jedan od problema takvog sustava je nesuradnja svih davatelja usluga. A drugi je mogućnost pogrešnog označavanja određenog tipa prometa što bi uzrokovalo velike probleme u mreži.

DPI može efikasno riješiti problem označavanja prometa zato što može točno odrediti vrstu aplikacije i na temelju nje klasificirati promet. Tako označavanje paketa postaje mrežna funkcionalnost a ne funkcionalnost određenih uređaja te bi se tako izbjegla mogućnost pogrešnog označavanja. Za točnu klasifikaciju prometa nužan je DPI, budući da pregledavanje samo zaglavlja – čitanje porta u TCP i UDP zaglavljima – nije dovoljno za pouzdanu klasifikaciju protokola ili aplikacije zato što mnoge moderne aplikacije koriste dinamičke portove ili portove koje su tradicionalno koristile neke druge aplikacije.

Klasifikacija protokola i aplikacija pomoći DPI-a bazira se na raznim tehnikama, [15]:

- *Pattern matching* koji je opisan u potpoglavlju 2.4.1
- Bihevioralna analiza kod koje se traže uzorci u komunikacijskom ponašanju aplikacije kao što su apsolutna i relativna veličina paketa, količina podataka u toku, broj tokova itd.
- Statistička analiza pomoću koje se računaju statistički indikatori koji se mogu koristiti za identifikaciju vrste transmisije (stvarno vremenska, tekstualna, video, audio itd.).

Kada je klasifikacija odrađena, sustav upravljanja prometom instaliran na određenim točkama u mreži postat će uska grla mreže tijekom perioda velikog mrežnog opterećenja ali će barem moći pružiti *soft* garanciju kvalitete usluge, sličnu kao *DiffServ*. *Soft* znači da bi garancija bila samo lokalna – ondje gdje je sustav upravljanja prometom instaliran. Dok ova metoda ne uspijeva riješiti problem cjelokupnog davanja podrške za kvalitetom usluge, može riješiti najčešći problem današnje Internet infrastrukture: zagušenje pristupnih mrežnih *link*-ova.

Neki od primjera gdje bi se morao koristiti DPI za upravljanje prometom su:

- prioritiziranje interaktivnog stvarno vremenskog sadržaja kao što su Internet telefonija, *online* igre ili udaljeni pristup
- ograničavanje resursa aplikacijama koje koriste velike količine resursa u vrijeme vršnih sati
- blokiranje neželjenih aplikacija kao što su *peer-to-peer* dijeljene podataka u poslovnoj okolini.

DPI upravljanje prometom je relativno nova tehnologija. Često navođen razlog za to je što je hardver koji ima mogućnosti i procesorsku moć obrade tolike količine podataka postao dostupan tek u zadnjih nekoliko godina. Međutim, to nije točan razlog, zato što je količina prometa u zadnjih nekoliko godina rasla mnogo brže od razvoja samih komponenti i procesorskih sustava, tako da je implementacija DPI-a bila lakša prije desetak godina. Pravi razlog je što se s povećanim količinama prometa i sve većim brojem novih aplikacija i protokola koji koriste TCP i UDP portove za razmjenu podataka, postalo nemoguće klasificirati promet u svrhu upravljanja prometom i planiranja kapaciteta [15].

2.4.3.2 Mrežna sigurnost

DPI je originalno razvijen u svrhu mrežne sigurnosti. Tradicionalni vatrozidi prate aplikacije koje su unutar neke lokalne mreže i ostvarile su konekciju s određenim poslužiteljem na Internetu. Oni dakle, mogu kontrolirani nezahtijevano povezivanje izvan lokalne mreže i također mogu blokirati koje ne koriste standardne aplikacije (kao što su port 80 za http i port 25 za SMTP). S ovim pristupom postoje barem dva problema. Prvi je taj što je, na primjer, port 80 uvijek otvoren pa su ga razne aplikacije počele koristiti za svoj promet. *Skype* je primjer poznate aplikacije koja uspijeva proći kroz većinu vatrozida. Drugi problem je trend seljenja prema web uslugama i računalstvu u oblaku a time granica između lokalne mreže i ostatka interneta praktički nestaje. Zbog toga se mrežni administratori susreću s problemima koji ih primoraju da kompletno ispituju pakete kako bi saznali radi li se doista o aplikacijama i tokovima podataka kakvi se čine [16].

Mnogi DPI proizvođači nude rješenja koja kombiniraju razne mogućnosti kao što su detekcija i prevencija upada i mogućnosti vatrozida zajedno s potpunim pregledavanjem prometa.

Njihovi uređaju skeniraju promet s poznatim uzorcima virusa, crva i ostalog malicioznog koda, te blokiraju njihov pristup lokalnoj mreži [16].

DoS (*Denial of Service*) napadi su klasičan primjer napada kod kojeg su operatori u odličnom položaju da se obrane. Takav napad se događa kada jedno računalo preoptereti drugo računalo podatcima te mu tako istroši i zauzme resurse te ono nije u mogućnosti raditi. DDoS (*Distributed Denial of Service*) napadi oni kod kojeg više računala napada jednu ili više meta s velikim količinama prometa. Ovakvi napadi mogu biti ozbiljne prijetnje mrežama zato što mogu opteretiti mrežu s tisućama mega bita prometa. Takve napade je potrebno blokirati što prije, zato što dublje oni dopru u mrežu, više štete učine. Tako da ako ih operatori spremno detektiraju u ranim fazama tada nema problema za korisnike. Operatori rutinski odbijaju stotine takvih napada dnevno.

DPI nije samo bitan za sigurnost pojedinih računala ili mreža, već svojim čitanjem korisničkih podataka daje odlično oružje u borbi protiv kriminalnih aktivnosti na Internetu. Tako su operatori obvezni zakonom čuvati podatke o pozivima i porukama kako bi ih organi vlasti mogli koristiti u svrhe lociranja pojedinih osoba ili u svrhu dokaza kod utvrđivanja kriminalnih radnji [17].

2.4.3.3 Ciljano oglašavanje

Ciljano oglašavanje označava pojam gdje marketinška ili medijska kompanija prati i skuplja podatke o potencijalnim kupcima kako bi naučila njihove navike i želje te tako odlučila koje proizvode ponuditi određenim korisnicima [18].

Online oglašavajuće kompanije godinama koriste mrežne tehnologije kao što su kolačići (*cookies*) kako bi pratili stranice koje korisnici posjećuju. Na taj način stvaraju se korisnički profili koji prikazuju korisnikovo ponašanje i omogućuju ponudu sadržaja za koji je korisnik zainteresiran. DPI daje sličnu mogućnost i samim operatorima na način da identificira stranice koje korisnici posjećuju, sadržaj tih stranica i ostale aplikacije koje korisnik koristi. Operatori i njihovi partneri na taj način mogu stvarati veoma detaljne profile korisnika koji se kasnije koriste za prikazivanje točno onih oglasa koji bi mogli zanimati određenog korisnika [19].

Na facebook-u, ciljano oglašavanje je standardna opcija i korisnici su primoreni sudjelovati u ciljanom oglašavanju prije nego sami odaberu opcije koje iz isključuju iz njega.. Kao takvo, ciljano oglašavanje na facebook-u bilo je tema mnogih pritužbi pa i sudskih postupaka te je za određene dijelove svijeta, kao što je EU, sudski naloženo da se korisnicima mora omogućiti ne sudjelovanje u ovakvoj vrsti oglašavanja [20].

3. Pravni aspekt nadzora prometa uz korištenje DPI-a

Trenutno DPI nije niti legalan niti ilegalan. Legalnost ove tehnologije ovisi o tome tko ju koristi i u koje svrhe ju koristi. Dvije strane s kojih se može promatrati takav problem su transparentnost i sloboda govora.

Transparentnost je ključna u legalnosti korištenja DPI-a kao tehnologije, budući da se jedino tako uklapa u zakone o privatnosti i zaštiti podataka diljem svijeta. Kao što je vidljivo iz višestrukih pravnih sporova u svijetu, problematične su bile činjenice da su operatori koristili DPI bez informiranja korisnika o tome ili bez traženja pristanka od strane korisnika. Do problema i dalje dolazi kada se radi o povjerljivim podatcima, ali kada se radi o ograničenom korištenju, kao što je u slučaju nadgledanja mreže, tada ne postoje pravne prepreke za korištenje ove tehnologije. Problem konkurentnosti na tržištu je također prisutan i tiče se najviše Američkog tržišta gdje je manji broj operatora pa postoji mogućnost za degradacijom konkurentske usluge [21].

Što se tiče slobode govora, dok se zakoni diljem svijeta koji nisu formulirani kako bi obuhvatili korištenje DPI-a ne promijene, slobodni govor neće biti adekvatno zaštićen od operatora koji koriste DPI. Međutim operatori kao takvi su privatne osobe i nemaju obvezu štititi slobodu govora svojih korisnika, dok se zakoni koji ju reguliraju ne promjene [21][22].

3.1 Net neutrality

Jedna od najčešćih razloga protiv DPI-a i nadgledanju prometa koji se bazira na njemu je taj što krši pravila *net neutrality*-a. Ali standardizirana definicija *net neutrality*-a ne postoji, pa ga se tako drukčije definira ovisno o regiji, socijalnim ili znanstvenim statusima. Osnovna premisa *net neutrality*-a je da se sav Internet promet treba tretirati jednako. Više tehnička definicija bila bi da se svi IP paketi obrađuju jednako po principi *best-effort* na kojemu radi IP protokol. Ali *net neutrality* nije tehnički princip već socijalna paradigma koja teži očuvanju Interneta onakvim kakav je i danas, s maksimalnom slobodom i jednakošću među njegovim sudionicima. Stoga će društvo morati odlučiti o količini slobode i jednakosti koja će u budućnosti biti na Internetu.

Ako se *net neutrality* tumači kao jednakost pristupa svim korisnicima, tada Internet danas zasigurno nije neutralan. Statistički podatci prikupljeni iz mnogih regija tijekom više godina, pokazuju da manje od 20% korisnika generira više od 80% ukupnog prometa. Taj

fenomen je moguće objasniti samo razlikama u potražnji. Korisnici koji su bolje upoznati s tehnologijom mogu iskoristiti mnogo više od svog jednakog dijela propusnosti, koja je najkritičnija u vremenima mrežnog zagušenja kada ta nejednakost u korištenju utječe na performanse ostalih korisnika. Dobar primjer su P2P aplikacije za razmjenu podatka kao što je BitTorrent. Kako bi se maksimizirala brzina preuzimanja podataka, takve aplikacije uspostavljaju stotine paralelnih veza s različitim korisnicima. Starije aplikacije koje komuniciraju samo sa serverom, uspostavljaju jednu vezu s jednim serverom ili par veza s par servera. Aplikacija koja koristi veliki broj veza će uvijek pobijediti u natjecanju za mrežnim resursima u mrežama bez upravljanja propusnosti. Još gore, takve aplikacije mogu učiniti potpuno neiskoristivima aplikacije koje koriste male količine podataka u stvarnom vremenu kao što su Internet telefonija ili *online* igre. Upravo zbog toga, neregulirana mreža ne može se zvati neutralnom kada ne garantira jednakost među korisnicima.

Upravljanje prometom može riješiti takve probleme današnjeg Interneta. Tako bi bilo moguće jednoliko rasporediti raspoložive količine mrežnih resursa, pogotovo za vrijeme zagušenja mreže. Najjednostavniji način bi bila jednaka raspodjela resursa među svim korisnicima mreže. Za takav pristup čak ne bi bilo potrebno koristiti DPI. Međutim, takav pristup nije uvijek najpametniji, budući da se zahtjevi za kvalitetom usluge razlikuju ovisno o aplikaciji. Na primjer, Internet telefonija zahtijeva veoma malo resursa ali ima određeni minimum koji bi trebao biti zadovoljen u svakome trenutku kako ne bi bilo prekida ili degradacije usluge. Aplikacije za dijeljenje podataka zahtijevaju što više resursa, ali također mogu podnijeti i periode s malom količinom resursa bez primjetljive degradacije kvalitete usluge. Kako je prije spomenuto, Internet nema mogućnosti rezervacije i garancije određene kvalitete usluge. Upravljanje prometom koje je svjesno samih aplikacija koje se koriste, može poboljšati trenutnu situaciju pružanjem garantirane minimalne količine resursa, prioritizacijom ili kombinacijom oboje tehnologije. Takav način upravljanja prometom zahtijeva korištenje DPI-a, pogotovo kod klasifikacije prometa aplikacija za dijeljenje podataka koje koriste višestruke veze i time prikrivaju svoje aktivnosti od ostalih sustava za nadgledanje prometa. DPI zajedno s bihevioralnom i statističkom analizom pruža jedini pouzdan način za klasificiranje prometa i vrsta aplikacija današnjeg Interneta.

Najjednostavniji način upravljanja prometom s obzirom na specifične aplikacije je dodjeljivanje različitih prioriteta različitim aplikacijama. Na primjer Internet telefoniji se

dodijeli najveći prioritet, interaktivnim aplikacijama visoki prioritet, neinteraktivnim aplikacijama kao što su elektronička pošta dodjeli se srednji prioritet, te se aplikacijama za dijeljenje podataka (npr. P2P aplikacije) dodjeli nizak prioritet. Važno je napomenuti da dodjeljivanje prioriteta ne utječe nužno na degradaciju usluge s nižom razinom prioriteta. Na ovom primjeru, davanje višeg prioriteta Internet telefoniji u odnosu na P2P promet ne će utjecati na resurse koje traži P2P. To je zato što Internet telefonija zauzima samo 1% ukupnog Internet prometa dok P2P promet zauzima skoro 50%. Povećana količina resursa za Internet telefoniju će u ovom slučaju biti nezamjetna u odnosu na količinu P2P prometa. Stoga je strah da će aplikacije nižeg prioriteta automatski imati lošiju kvalitetu neutemeljen.

Međutim, ako postoje dvije vrste aplikacija koje koriste velike količine resursa kao što su P2P i Internet TV, tada prioritiziranje jedne utječe na kvalitetu usluge one aplikacije kojoj je dodijeljen niži prioritet. U ovom slučaju Internet TV zahtijeva mnogo resursa pa većina davatelja takvih usluga gradi zasebnu infrastrukturu samo za usluge Internet TV-a.

Očito je da je prioritiziranje prometa potrebno u budućem Internetu, međutim ostaje pitanje tko će odlučivati o samom prioritiziranju usluga. Jedna opcija je da korisnici sami biraju prioritete. Ova opcija ima dva problema. Prvi problem je što tako nešto zahtijeva određenu razinu znanja o zahtjevima za kvalitetom usluga i mrežnim protokolima, a drugi je taj što bi korisnici obično previše prioritizirali one usluge koje oni koriste. Druga opcija je da operatori određuju prioritete. U tom slučaju bilo bi bitno da se takva prioritiziranja ne baziraju na koristi određenog operatora već da se baziraju na zahtjevima određenih aplikacija za kvalitetom usluge. Tako da se kao dobra ideja čini internacionalna standardizacija za koju bi moglo trebati dosta vremena da se uvede.

Potpuno drukčiji način rješavanja problema jednakosti među korisnicima bio bi povratak na plaćanje Interneta ovisno o potrošnji. Ovaj način bi pružio jednakost, veliki dio korisnika, oko 80%, bi čak plaćali i manje račune nego sada, ali bi se tim načinom veoma ograničio potencijal za rastom i inovacijama koje se stvaraju upravo zbog neograničenog korištenja Interneta [23].

3.2 Privatnost

Pitanje privatnosti je obično među prvim zamjerkama DPI-a budući da se pregledavaju svi podatci vezani uz ponašanje korisnika na Internetu. Narušavanje privatnosti očito je kod korištenja DPI-a u svrhe ciljanog oglašavanja i nadgledanja.

U Europi, privatnost je zaštićena osmim člankom Europske povelje o ljudskim pravima, a odnosi se primarno na države EU iako ju je Europski sud za ljudska prava široko interpretirao. Također je zaštićena i Europskim zakonom o zaštiti podataka koji regulira obradu privatnih podataka i tiče se organizacija u privatnom i poslovnom sektoru. Kada se osobni podatci obrađuju, to mora biti napravljeno na transparentan način, vlasnik podataka mora biti o tom obaviješten i mora na to pristati. Općenito, DPI se treba pridržavati zakona pojedine države u kojoj se koristi [24].

Vezano uz korištenje DPI-a za ciljano oglašavanje, Europska Komisija otvorila je slučaj protiv Ujedinjenog Kraljevstva vezano uz korištenje DPI-a, nakon što su se Britanski korisnici Interneta žalili da se Ujedinjeno Kraljevstvo ne pridržava Europskih zakona o zaštiti podataka [25].

U SAD-u postoje razni slučajevi vezani uz korištenje softvera koji se koristi za ciljano oglašavanje a koristi DPI i time krši prava korisnika koja su u SAD-u zaštićena 4. Amandmanom.

3.3 Sloboda govora

Problem slobode govora na Internetu smatra se korištenje DPI-a, od strane operatora, u svrhu upravljanja mrežama na neneutralan način. Tim Wu je tako predložio da se operatorima zabrani odlučivanje o tome što korisnici mogu pretraživati na Internetu [26].

Lessig i McChensney spominju probleme slobode govora kod upravljanja mrežom korištenjem DPI-a. Smatraju da klasifikacija prometa ili korisnika bez pravila *net neutrality*-a može dovesti do toga da će kompanije prodavati brzi pristup Internetu onima koji ga mogu priuštiti dok će ostali korisnici imati samo ograničeni pristup Internetu. Takav problem je očit kod Američkih davatelja usluge kabelske televizije, koji danas diktiraju što će korisnici gledati i za koju cijenu [27].

3.4 Tržišno natjecanje / konkurencija

Korištenje DPI-a od strane operatora može također izazvati tržišne probleme. Budući da operatori mogu koristiti DPI kako bi prioritizirali svoje usluge ili usluge svojih sestrinskih kompanija, diskriminacija različitih vrsta prometa dovela bi do nepoštenog tržišta.

Takav problem je realniji u Sjedinjenim Američkim Državama budući da na tom tržištu vlada *duopol* pa je relativno lagano jednom operatoru diskriminirati tuđi promet. U Europi je situacija bolja zato što postoji mnogo više operatora pa je tako i tržište razvijenije i otvorenije. S druge strane, niti na jednom od ovih tržišta se zakon *net neutrality*-a ne provodi pa operatori mogu inovacijama u poslovanju ili tehnologijama diskriminirati tuđi promet sve dok se to ne protivi zakonima pojedine države u kojoj se koristi [27].

3.5 Filtrianje sadržaja zaštićenog autorskim pravima

Kako DPI čita sav sadržaj svakog paketa koji analizira, uvijek je postojala mogućnost filtriranja i blokiranja (odbacivanja) određenog prometa.

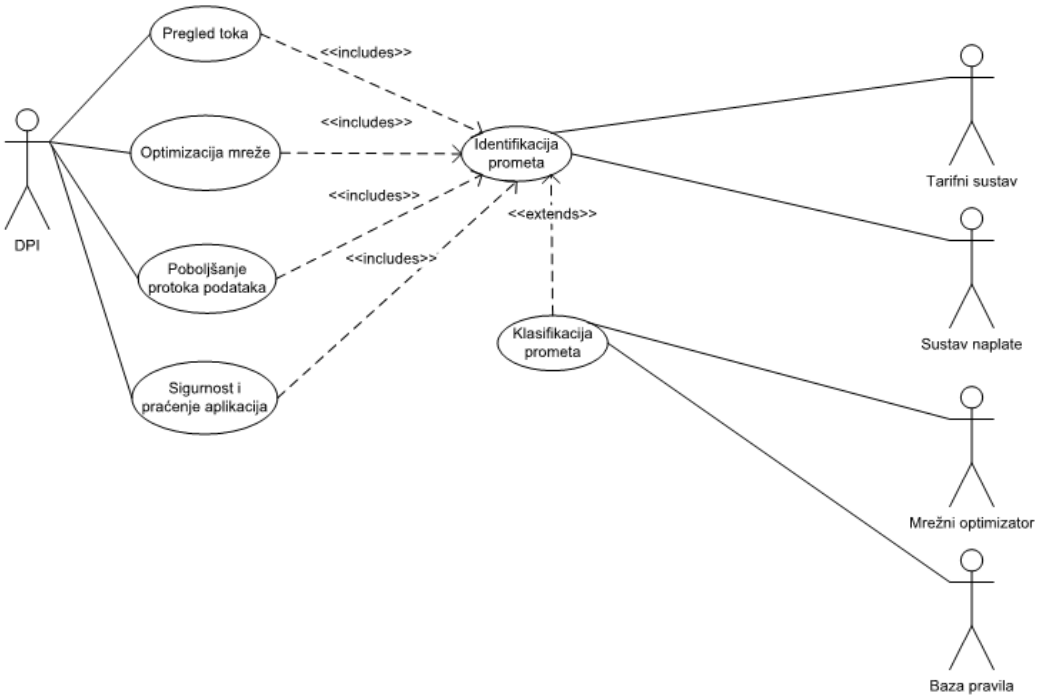
Filtriranje ilegalnog distribuiranih podataka posebno je zanimljiv način upotrebe DPI-a zato što je imalo svojih dobrih i loših trenutaka, a danas se sve više čini kako neće opstati kao legalan način filtriranja. Još od 2004. godine europska glazbena industrija pravnim je postupcima pokušala izboriti pravo da nametne operatorima filtriranje sadržaja zaštićenog autorskim pravima tako da korisnici ne bi mogli dijeliti takve podatke. U suprotnom, smatrali su, da bi operatori trebali biti odgovorni za postupke svojih korisnika u slučaju da dijele ilegalan sadržaj. Cilj je bio natjerati operatore da koriste tehnologije za filtriranje kako bi detektirali i blokirali zaštićeni glazbeni sadržaj. To se smatralo alternativom identifikaciji pojedinih korisnika koji razmjenjuju takav sadržaj.

Takva tehnologija prvo je bila korištena u Belgiji 2007. godine kada je glazbena industrija sudskim putem tražila od operatora *Scarlet* da instalira takav sustav. Sud u Briselu podržao je taj korak. Nakon toga, ta tehnologija pokušala je biti nametnuta Irskim operatorima. Međutim sudski slučajevi su odbačeni kada je izašlo na vidjelo da je muzička industrija zavaravala sud s informacijama o korištenju tehnologije za filtriranje pa su tako operatori oslobođeni takve obveze u obje zemlje.

Operatori su u ovakvim slučajevima u veoma povoljnim situacija zato što su vlasnici infrastrukture i mreže pa samim time mogu raznim testiranjima dokazivati slučajeve koji idu njima u korist. Slična situacija je i kod filtriranja ilegalnog sadržaja i dječje pornografije, operatori također imaju superiornu poziciju. Tako je Australski operator objavio da će sudjelovati u testiranjima takvih tehnologija samo kako bi dokazao da one ne djeluju [16].

4. Opis procedure nadzora prometa i prikupljanje podataka

U ovom poglavlju su, uz pomoć UML dijagrama, opisani slučajevi upotrebe i određene aktivnosti DPI-a. Prvi dijagram prikazuje četiri slučaja upotrebe.



Dijagram 1 Dijagram slučaja upotrebe

Prvi navedeni slučaj upotrebe, pregled toka, analizira promet ovisno o tokovima podataka između klijenta i servera. Te veze se analiziraju i klasificiraju kako bi se primijenile politike operatera i nosivih usluga. Na taj način je moguće nadzirati opterećenje mreže i pojedinih aplikacija. Ova slučaj upotrebe koristio se za prikupljanje podataka analiziranih u sljedećem poglavlju.

Drugi slučaj upotrebe koji se zove optimizacija mreže, opisuje korištenje DPI-a u svrhu sprječavanja prekida usluge uzrokovanih preopterećenjem mreže. Prekidi usluge mogu veoma naštetiti kvaliteti usluge pa je tako veoma bitno spriječiti ih kada je to moguće.

Slučaj upotrebe nazvan poboljšanje protoka podataka, opisuje način korištenja DPI-a u svrhu prikupljanja podataka o prometu u mreži. Tako je moguće odrediti najkorištenije aplikacije i te podatke koristiti kako bi se bolje prioritizirale određene usluge.

Posljednji navedeni slučaj upotrebe, sigurnost i praćenje aplikacija, podrazumijeva korištenje DPI-a u svrhu praćenja i analize prometa kako bi se spriječili sigurnosni incidenti. Takvo korištenje najčešće se nalazi u poslovnim okolinama kada se nadziru zaposlenici.

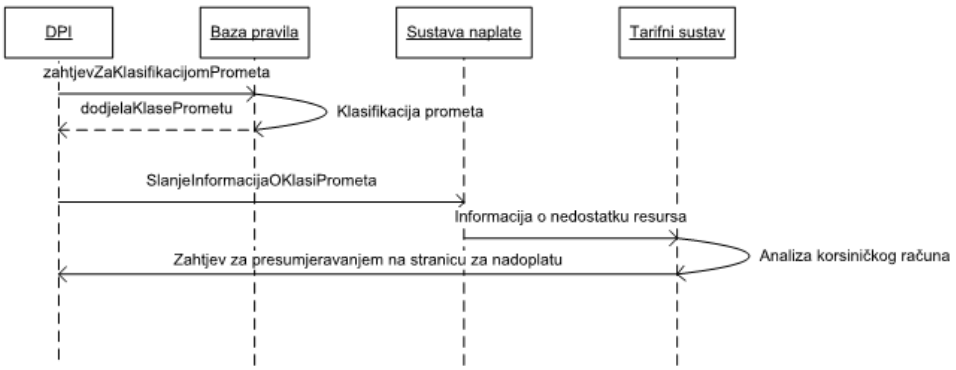
Dijagram 2 prikazuje općenite aktivnosti DPI tehnologije.

Dijagram 2 Dijagram aktivnosti

Dijagram aktivnosti prikazuje aktivnosti koje prolazi DPI kada se radi o svim slučajevima upotrebe. Prva aktivnost je promatranje prometa, to je aktivnost u kojoj paket dolazi do DPI-a koji zatim počinje analizu tih paketa. Sljedeći korak je identifikacija prometa, a nakon što je paket identificira, koristeći baze pravila, DPI klasificira paket u jednu od unaprijed definiranih klasa. Nakon klasifikacije, podatci o analiziranom paketu šalju se okolnim sustavima kako bi ti

sustavi mogli odrađivati svoj posao ovisno o podatcima o pojedinom paketu. Na kraju DPI pohranjuje podatke o analiziranom paketu u svrhu daljnje analize kada ona bude potrebna.

Iz ovog dijagrama vidljivo je kako su DPI-ove aktivnosti veoma jednosmjerne, tj. DPI kao sustav nema mnogo odluka koje donosi. Njegova velika prednost je upravo u tome što ima pristup okolnim, udaljenim bazama podataka i pomoću svih dostupnih informacija može opsluživati razne sustave sa točnim podatcima koji su tim sustavima potrebni kako bi ispunjavali svoju svrhu.



Dijagram 3 Dijagram međudjelovanja

Dijagram 3 prikazuje međudjelovanje objekata u sustavu operatere u slučaju kada korisnik nema dovoljno sredstva na računu kako bi nastavio korištenje podatkovnog prometa, pa se od DPI-a traži da promijeni zaglavlje slijedećeg paketa tog korisnika i preusmjeri ga na stranicu na kojoj ga se upozori na stanje na njegovom računu i nudi mu se nadoplatu sredstava.

5. Analiza prikupljenih podataka o prometu

U ovom poglavlju analiziran je promet jednog hrvatskog mobilnog operatora. Dobiveni podatci prikupljeni su koristeći DPI tehnologiju koja je dio PCRF (*Policy and charging rules function*) sustava spojenog na glavni *gateway* operatora. PCRF je sustav koji upravlja raznim pravilima u mreži kao što su zahtjevi za kvalitetom usluge, pravilima vezanim uz naplatu, dijagnostika mreže itd. Takav sustav ima pristup bazama podataka okolnih sustava kako bi donosio odluke i slao podatke tim istim okolnim sustavima. Jedna od komponenti PCRF-a je i DPI dio koji ima zadatak filtriranja i klasificiranja prometa koji prolazi kroz mrežu i opsluživanje okolnih sustava tim podatcima. Na temelju pravila pohranjenim u bazama pravila, ostali sustavi tretiraju promet s obzirom na klasu i skup pravila koju im dodijele DPI i PCRF.

Promet za analizu potrebnu u ovom radu mjeren je 3 uzastopna dana za vrijeme vršnog sata toga dana. Općenito, vršni sat mobilnog podatkovnog prometa u Hrvatskoj je između 13:00 i 17:00. Rezultati mjerenja i analiza s obzirom na učestalost prometa od pojedine aplikacije u ukupnom prometu prikazani su u tablicama 2 do 4.

Tablica 2. DPI mjerenje prvog dana

Aplikacija	Odlazni promet (Byte)	Dolazni promet (Byte)	Udio u ukupnom odlaznom prometu	Udio u ukupnom dolaznom prometu
Bittorrent	189 924 212 119	462 479 219 828	26,65571%	6,05792%
Google	113 511 299 147	364 290 514 945	15,93122%	4,77177%
Facebook	103 712 330 078	1 425 880 247 717	14,55594%	18,67732%
Skype	52 862 532 809	59 189 575 259	7,41921%	0,77531%
Amazoncloud	51 875 385 353	34 067 690 220	7,28067%	0,44625%
Whatsapp	27 867 463 693	38 803 083 187	3,91118%	0,50827%
Youtube	21 466 018 338	2 454 426 208 720	3,01274%	32,15004%
Viber	19 395 303 690	42 872 886 124	2,72211%	0,56158%
Gmail	18 416 135 786	42 353 749 533	2,58469%	0,55478%
Imessage	15 353 596 381	913 707 091	2,15486%	0,01197%

Tablica 3. DPI mjerenje drugog dana

Aplikacija	Odlazni promet (Byte)	Dolazni promet (Byte)	Udio u ukupnom odlaznom prometu	Udio u ukupnom dolaznom prometu
Bittorrent	185 407 550 718	446 180 576 005	32,90660%	7,70377%
Google	80 530 359 575	255 717 990 138	14,29273%	4,41524%
Facebook	74 957 777 692	1 030 870 046 713	13,30370%	17,79904%
Skype	44 662 226 944	49 067 099 590	7,92677%	0,84719%
Amazoncloud	39 878 929 367	22 971 843 655	7,07781%	0,39663%
Whatsapp	18 498 005 215	26 558 348 306	3,28307%	0,45856%
Youtube	16 669 451 387	1 900 777 137 429	2,95854%	32,81889%
Viber	13 144 199 997	29 245 487 287	2,33287%	0,50495%
Imessage	12 364 865 246	540 252 663	2,19455%	0,00933%
Gmail	11 352 969 088	26 973 968 851	2,01495%	0,46573%

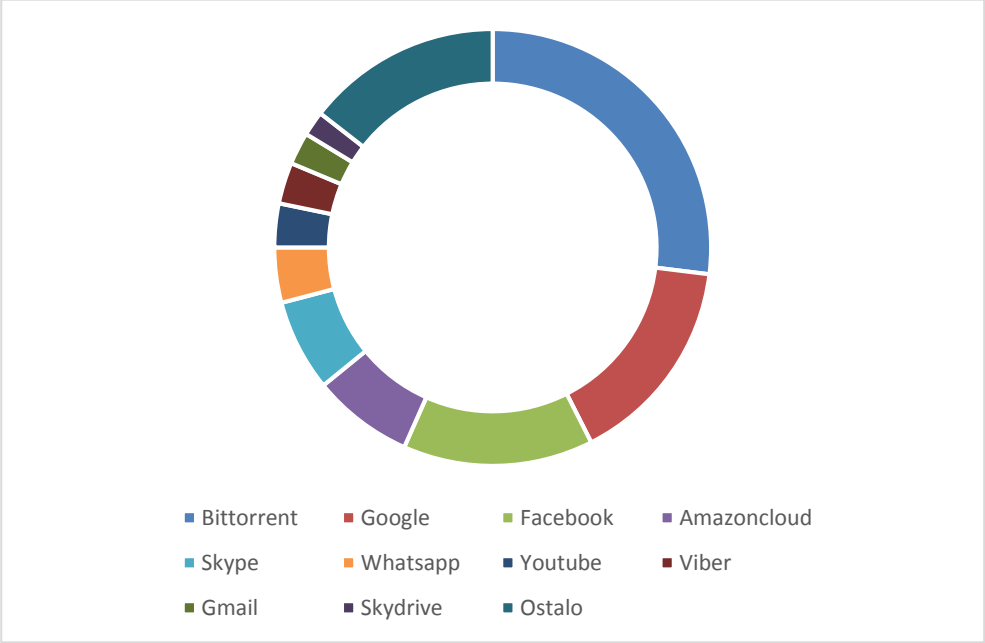
Tablica 4. DPI mjerenje trećeg dana

Aplikacija	Odlazni promet (Byte)	Dolazni promet (Byte)	Udio u ukupnom odlaznom prometu	Udio u ukupnom dolaznom prometu
Bittorrent	3 936 374 874 221	10 996 838 461 939	26,96177%	7,17285%
Google	2 275 895 446 070	6 670 548 355 719	15,58850%	4,35096%
Facebook	2 056 912 020 916	28 584 919 906 273	14,08860%	18,64493%
Amazoncloud	1 092 181 393 053	550 001 036 952	7,48078%	0,35875%
Skype	993 428 162 386	1 154 774 505 734	6,80438%	0,75322%
Whatsapp	595 553 130 401	844 942 833 896	4,07918%	0,55113%
Youtube	473 537 400 773	54 202 948 372 753	3,24344%	35,35465%
Viber	446 420 788 546	975 893 835 769	3,05771%	0,63654%
Gmail	349 153 552 206	731 788 287 728	2,39149%	0,47732%
Skydrive	266 969 063 341	117 922 521 814	1,82858%	0,07692%

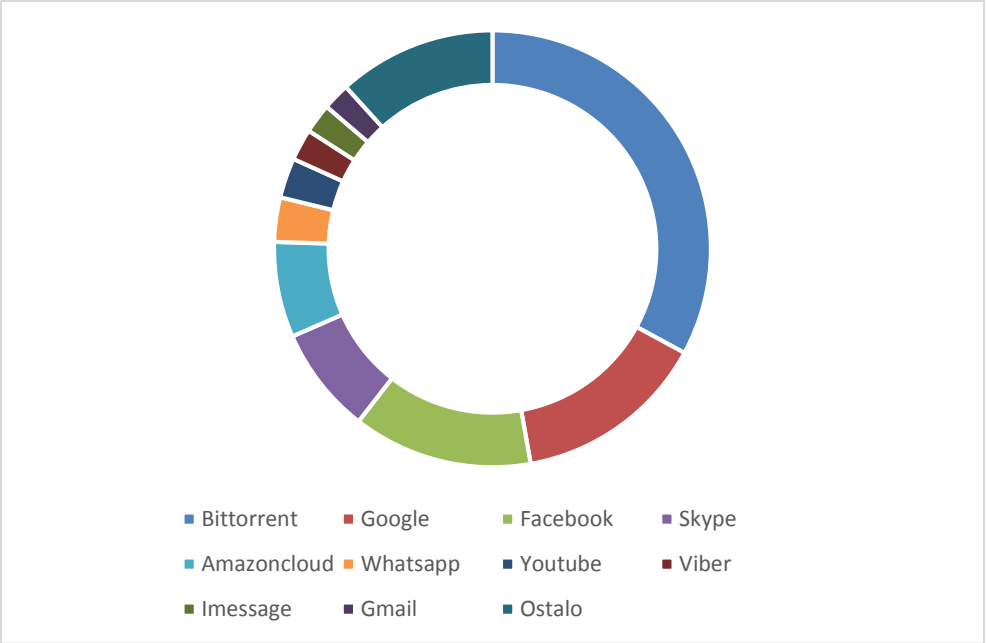
Prvi stupac u tablicama označava aplikaciju koju je klasificirao DPI, sljedeća dva stupca su odlazni i dolazni promet mjereni u *Byte*ovima, dok zadnja dva stupca prikazuju udio količine prometa pojedine aplikacije u ukupnom izmjerenom prometu u tome razdoblju. Podatci su sortirani po količini odlaznoga prometa, od one aplikacije koja ga generira najviše prema onima koje generiraju manje. U ovoj analizi obuhvaćeno je samo prvih 10 aplikacija koje zauzimaju najveću količinu resursa. To je zato što nakon 10 najkorištenijih aplikacija u

rezultatima, nalaze se aplikacije koje zauzimaju veoma male udjele u ukupnom prometu. Tako je i u prvih 10 aplikacija vidljiv veliki pad udjela između prve i desete aplikacije.

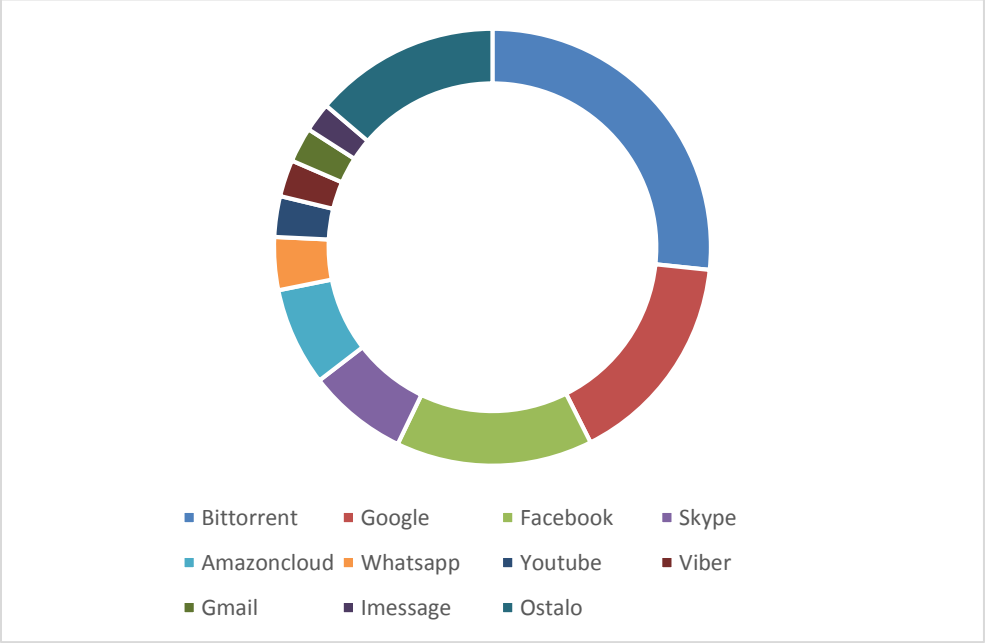
Iz dobivenih podataka vidljivo je da se najkorištenije aplikacije ne mijenjaju značajno. Najveći korisnici resursa su tako isti u svakom mjerenom razdoblju, a to su Bittorrent, Google i Facebook u odlaznom prometu, dok su Youtube i Facebook najveći korisnici u dolaznom prometu. Također je vidljivo kako se udjeli aplikacija u ukupnom prometu ne mijenjaju značajno.



Dijagram 4 Udio prometa od pojedine aplikacije u ukupnom izmjerenom odlaznom prometu prvog dana

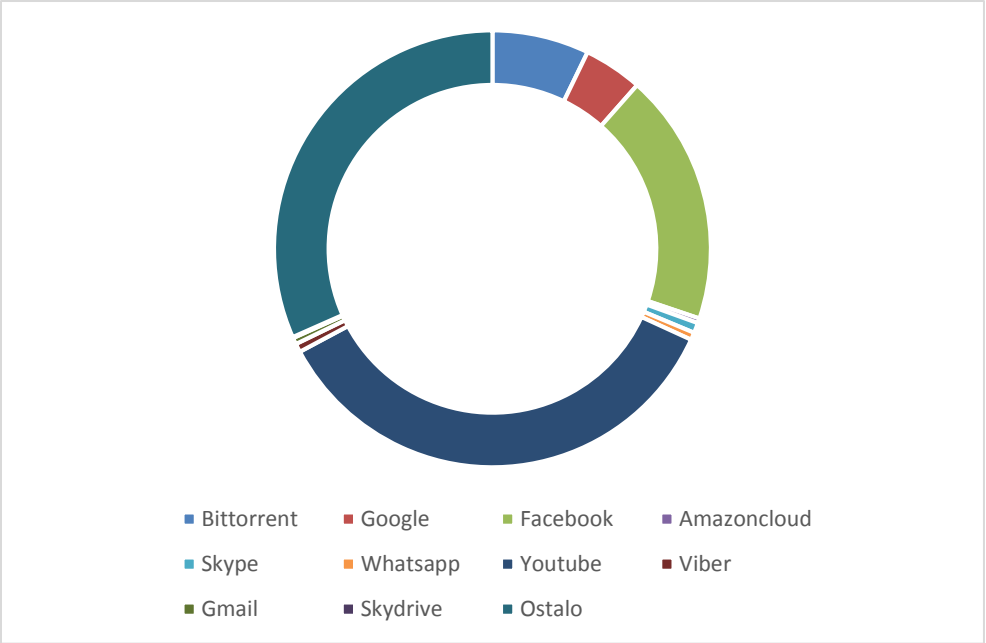


Dijagram 5 Udio prometa od pojedine aplikacije u ukupnom izmjerenom odlaznom prometu drugog dana

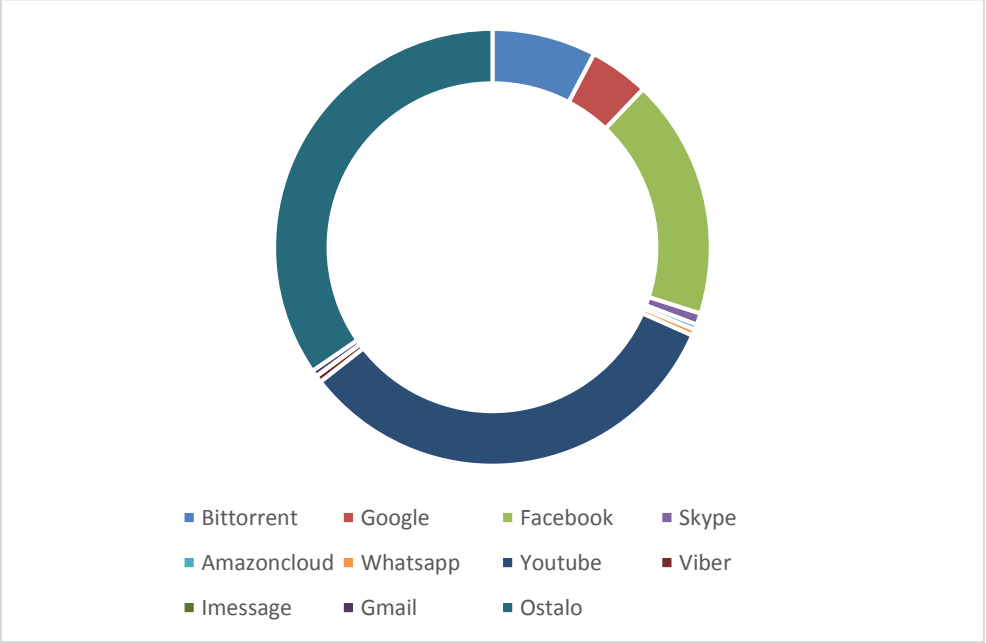


Dijagram 6 Udio prometa od pojedine aplikacije u ukupnom izmjerenom odlaznom prometu trećeg dana

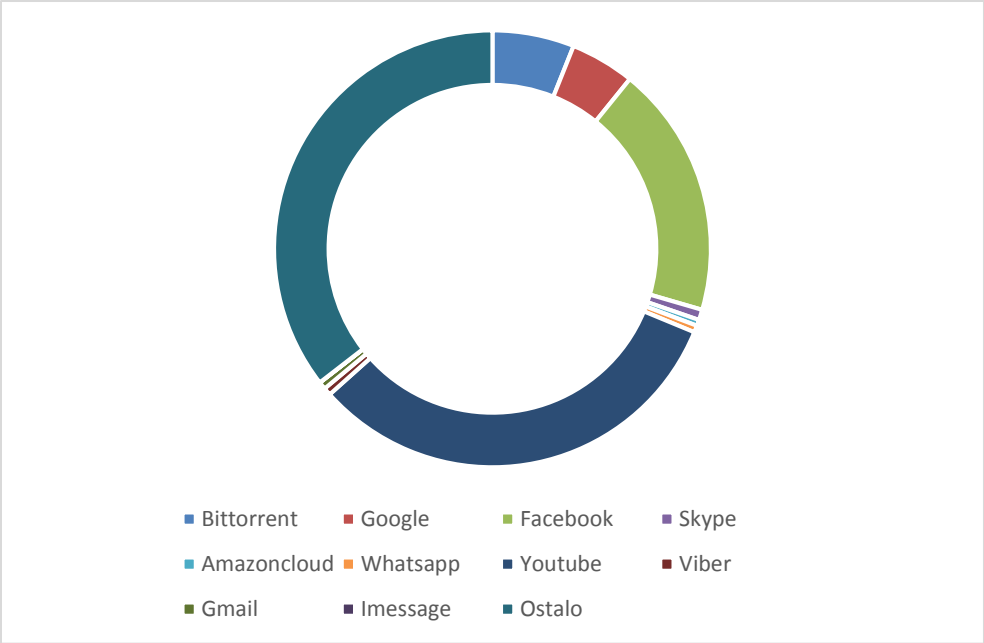
Dijagrami 4, 5 i 6 prikazuju odlazni promet, te potvrđuju da se udio najkorištenijih aplikacija u ukupnom prometu ne mijenjaju značajno ovisno o danu mjerenja.



Dijagram 7 Udio prometa od pojedine aplikacije u ukupnom izmjerenom dolaznom prometu prvog dana



Dijagram 8 Udio prometa od pojedine aplikacije u ukupnom izmjerenom dolaznom prometu drugog dana



Dijagram 9 Udio prometa od pojedine aplikacije u ukupnom izmjerenom dolaznom prometu trećeg dana

Dijagrami 7, 8 i 9 prikazuju dolazni promet te također potvrđuju da se udio najkorištenijih aplikacija u ukupnom prometu ne mijenja iz dana u dan. Ovim se dijagramima također dokazuje da je promet ujednačen iz dana u dan.

Iz rezultata je vidljivo da je najveći korisnik u odlaznom prometu Bittorent, P2P protokol za dijeljenje podataka. Dok najveći dio dolaznog prometa zauzima Youtube, servis za dijeljenje i pregledavanje video sadržaja.

Ako se promatra svaka aplikacija zasebno dolazi se do sljedećih zaključaka:

Bittorrent koji ima najveći udio u odlaznome prometu ima mali udio u dolaznome prometu, u odnosu na količinu odlaznoga prometa koji generira. To je zato što velik broj korisnika preuzme sadržaj bez da ga nastavlja dijeliti.

Google, kao najpoznatiji i najkorišteniji servis za pretragu Interneta generira pozamašnu količinu prometa u oba smjera, međutim odlazni promet mu je u prosijeku tri puta veći od dolaznog.

Facebook, najkorištenija društvena mreža, ima sličan udio odlaznoga prometa kao i Google. Međutim većina prometa koji generira Facebook je dolazna, tako Facebook zauzima drugo mjesto po količini dolaznoga prometa. Ovdje je također vidljiva i velika razlika u odlaznome i dolaznome prometu jedne aplikacije. Facebook generira i deset puta više dolaznog prometa u

odnosu na odlazni promet, što se može objasniti time da veći broj korisnika pregledava sadržaj dok samo jedna desetina objavljuje i dijeli sadržaj, pogotovo sadržaj koji generira više prometa kao što je video.

Skype je aplikacija koja se koristi za ostvarivanje poziva i video konferencija, a također može služiti i za razmjenu manjih podataka. Budući da je većina komunikacije koja se odvija Skype-om dvosmjerna, vidljivo je da su odlazni i dolazni promet približno jednaki.

Amazoncloud je usluga u oblaku koji nudi mnoštvo mogućnosti, od pohrane podataka, alata za analizu, alata za razvoj, sigurnosnih funkcija do razvoja i usluge poslužitelja video igara. Upravo zato ima toliko veći obujam prometa od ostalih usluga u oblaku [28].

Whatsapp i Viber su mobilne aplikacije za razmjenu poruka, pozive i dijeljenje manjih podataka. Posljednjih godina slične aplikacije postaju sve popularnije, a danas već imaju i milijarde korisnika. Zbog velikog broja korisnika, operatori moraju obraditi veliku količinu prometa pa nadziranje takvih usluga predstavlja probleme manjim operaterima. Također, u 2016. godini ovakve usluge počeli su kriptirati promet kako bi zaštitili privatnost korisnika [29].

Youtube je najkorištenija i najpopularnija usluga za dijeljenje video sadržaja, što i dokazuje količina prometa koju generira. Vidljiva je velika razlika u odlaznom i dolaznom prometu, što se može opisati činjenicom da velika većina korisnika samo pregledava sadržaj dok mali broj (u odnosu na sve koji koriste ovaj servis) korisnika stvara i dijeli sadržaj. Ovu web stranicu posjećuju milijarde korisnika pa se tako i generira velika količina prometa [30].

Gmail je najkorištenija, besplatna usluga elektroničke pošte. Količina generiranog prometa proizlazi iz velikog broja korisnika koji koriste ovu uslugu. Izmjereno je da mjesečno ovaj servis koristi više od milijarde korisnika [31].

Imessage je aplikacija za razmjenu poruka koju je razvio Apple. Koristi se na Apple-ovim uređajima i u novijim verzijama se koristi i za čitanje i slanje SMS poruka. Količina prometa također dolazi zbog broja korisnika, koji u prosjeku razmjenjuju 28 000 poruka u sekundi [32].

Vidljiva je očita poveznica između količine prometa i broja korisnika određene aplikacije. Tako u ovih 10 najkorištenijih aplikacija sve osim Imessage-a imaju barem milijardu aktivnih korisnika. Zbog toga i Google koji je servis za pretragu Interneta, koji ne generira velike količine prometa svojim korištenjem, dolazi na ovako visokog mjesto po količini prometa.

Ovi podatci sami po sebi ne pomažu operateru, ali uloga DPI-a ne staje na klasifikaciji prometa. Kada se promet klasificira, DPI na temelju svojih baza pravila, obavještava druge sustave kako da tretiraju određene pakete. Tako će servis naplate znati kako naplatiti domaći a kako *roaming* promet, a servis upravljanja mrežom će znati kada određenom korisniku smanjiti brzinu prijenosa itd. DPI sam po sebi ne utječe na mrežu i njene performanse, ali pruža informacije koje ne može pružiti ni jedan drugi sustav, a uz potporu sustava kao što je PCRF, takve informacije može pružati u stvarnome vremenu.

6. Detektiranje kritičnih faktora koji mogu utjecati na performanse aplikacije

Ubrzanim razvojem mobilnih mreža pojavio se velik broj novih usluga, među kojima i onih interaktivnih i onih koje se odvijaju u stvarnom vremenu, pa su zahtjevi za kvalitetom usluge postali sve veći. Kako bi se pristupilo različitim zahtjevima za kvalitetom usluge koriste se nosive usluge (engl. *bearer*). Nosive usluge pružaju prijenos podataka između dvije točke u mreži, najčešće korisničke opreme i *gateway*-a, po definiranim pravilima o kvaliteti usluge.

Svaka nosiva usluga sadrži skup pravila o kvaliteti usluge, svojstvima transportnog kanala kao što su brzina prijenosa, dozvoljeno kašnjenje, gubitak paketa itd. Svaka nosiva usluga ima dva ili četiri parametra kvalitete usluge, ovisno o tome radi li se o stvarno-vremenskoj usluzi ili ne. Parametri kvalitete usluge prema [33] su:

- identifikator klase kvalitete usluge (QCI[1])
- prioritet raspodjele (ARP[2])
- garantirana brzina – samo za stvarno vremenske usluge
- najveća brzina – samo za stvarno vremenske usluge.

6.1 Identifikator klase kvalitete usluge

Identifikatori klase kvalitete usluge određuju način tretiranja IP paketa koji se prenose nosivom mrežnom uslugom. 3GPP (*The 3rd Generation Partnership Project*) je definirao identifikatore klasa koji su prikazani u tablici 5. Većina operatera u početku koristi tri osnovne klase: govornu, kontrolno signalnu i *best-effort* usluge. Kasnije se određuju dodatne klase kako bi se nudile specifične usluge kao što je usluga video telefonije visoke kvalitete.

[1] QoS Class Indicator
[2] Allocation and Retention Priority

Tablica 5 Identifikatori klase usluga po 3GPP

QCI	Tip resursa	Prioritet	Dopušteno kašnjenje [ms]	Dopušteni gubitak paketa	Primjer usluge
1	Garantirani resursi	2	100	10-2	Govorna usluga
2		4	150	10-3	Video usluga u stvarnom vremenu
3		3	50	10-3	Stvarno vremenske igre
4	Ne garantirani resursi	5	300	10-5	Video usluga u stvarnom vremenu
5		1	100	10-3	IMS signalizacija
6		6	300	10-5	Video (s bufferom), TCP
7		7	100	10-5	Glasovne usluge, stvarno vremenske video usluge, interaktivne igre
8		8	300	10-3	Video (s bufferom), TCP
9		9	300	10-5	

Izvor: [31]

Tablica 5 prikazuje klase različitih usluga i njihove prioritete u mreži. Također daje informacije o dopuštenoj količini gubitka paketa i dopuštenog kašnjenja bez degradacije usluge [33].

6.2 Kritični faktori usluga

Kao što je vidljivo u tablici 5, različite usluge imaju različite zahtjeve za kvalitetom usluge. U ovom poglavlju biti će analizirane aplikacije iz 5. poglavlja te će im biti određeni faktori koji utječu na kvalitetu usluge.

Prva analizirana aplikacija je Bittorrent, P2P usluga za dijeljenje podataka. Takva usluga ima QCI 9 po tablici 5, te ima prioritet 9 što znači da ima najmanje zahtjeve za kvalitetom usluge. TCP aplikacije za dijeljenje podataka uvijek imaju najmanji prioritet zato što ustvari i nemaju zahtjeve za kvalitetom usluge, moraju samo imati vezu između korisnika i tada će trošiti sve raspoložive resurse za prijenos podataka. Kašnjenje neće uzrokovati degradaciju budući da se ne radi o stvarno vremenskoj usluzi, a gubitak paketa će biti ispravljen retransmisijom izgubljenog paketa. Druga i treća analizirana aplikacija, Google i Facebook, također spadaju u ovu kategoriju i nemaju posebni zahtjeva za kvalitetom usluge.

Aplikacije za prijenos poruka i elektroničke pošte također nemaju posebne zahtjeve za kvalitetom usluge budući da se gubitak paketa jednostavno ispravlja retransmisijom a kašnjenje ne utječe na samu kvalitetu usluge.

Zanimljivije su sljedeće analizirane usluge, kao što je aplikacija za pozive i video pozive – Skype. Takve aplikacije imaju QCI 1 i 2 po tablici 5. Stvarno vremenske aplikacije uvelike se razlikuju od aplikacija baziranih na TCP-u. Zato takve aplikacije zahtijevaju garantiranu brzinu i imaju dodatne zahtjeve za kvalitetu usluge vezane uz kašnjenje, kolebanje kašnjenja i gubitak paketa. Uz kašnjenje i gubitak paketa čije su dozvoljene vrijednosti vidljive u tablici, govorne usluge također zahtijevaju i malo kolebanje kašnjenja – do 30 milisekundi. Ako ti uvjeti nisu zadovoljeni dolazi do degradacije usluge i mogućeg prekida usluge. Što se tiče video usluga, zahtjevi su slični kao i kod govornih usluga, samo što nisu osjetljive na kolebanje signala već na latentnost koja ne bi trebala biti veća od 5 milisekundi, ovisno o buffer-u koji se koristi [34].

Youtube je također zanimljiv, a nudi nekoliko usluga s različitim kritičnim faktorima i različitim QCI faktorima. Osnovna usluga Youtube-a je pregledavanje pohranjenog video sadržaja, kao takva nema posebne zahtjeve za kvalitetom usluge, kao ni prijašnje opisane usluge bazirane na TCP-u. Međutim, također je podržana i usluga stvarno vremenskog prijenosa videa (*live-streaming*) koja je mnogo osjetljivija i ima veće zahtjeve za kvalitetom usluge. Posebni zahtjevi *live-streaming*-a su jednosmjeran tok podataka i očuvanje vremenskog perioda između paketa. Naravno sama kvaliteta također ovisi i o *buffer*-ima koji se koriste od strane davatelja takve usluge. *Live-stream* usluga ima prioritet 7 po tablici 5. što ju svrstava među usluge nižeg prioriteta, međutim ovisno o operatoru, ovakve usluge mogu imati puno veći prioritet. Povećavanje prioriteta određene usluge, i samim time garantiranje njezine kvalitete, uvelike ovisi o dogovorima operatora s kompanijama koje nude usluge prijenosa videa i marketinškim ponudama samog operatora. Stvarno vremenski prijenos videa relativno je nova usluga na tržištu pa se operatori s vremenom prilagođavaju i odlučuju žele li osiguravati veću kvalitetu takvih usluga [35].

7. Zaključak

Filtriranje i klasifikacija prometa, pogotovo u stvarnome vremenu, veliki je izazov s kojim se susreću operateri i kompanije koje se bave s velikim količinama podatkovnog prometa. Metoda opisana u ovome radu vrhunac je trenutnog razvoja za filtriranje i klasifikaciju prometa u takvim uvjetima. Svojim mogućnostima nudi nove usluge i načine manipulacije prometom. Tako se koristi u razne svrhe, od sigurnosti i nadgledanja prometa, do više specifičnih akcija kao što je naplata podatkovnog prometa.

Za potrebe diplomskog rada analizirani su podatci prikupljeni od strane mobilnog operatera. Podatci su klasificirani te su dobiveni rezultati prezentirani u petome poglavlju. Analizirano deset najkorištenijih aplikacija koje generiraju mobilni podatkovni promet. Analiza je pokazala relativno očekivane rezultate koji pokazuju da su aplikacije koje koriste najviše mrežnih resursa upravo one koje ili koristi najveći broj ljudi, ili su takve prirode da troše što je moguće veću količinu resursa, kao što je BitTorrent.

Na kraju rada određeni su kritični faktori koji utječu na performanse samih najkorištenijih aplikacija. Analiza tih faktora pokazuje kako među najkorištenijim aplikacijama nema mnogo onih koje imaju jako velike zahtjeve od samih davatelja usluga. Ti podatci pokazuju kako barem operateri s područja Hrvatske, barem za sada, nemaju problema s mrežnim kapacitetima.

Mogućnosti DPI tehnologije su velike, kao takve nažalost nisu dovoljno iskorištene. Upotreba DPI-a na strateškim mjestima u mreži mogu omogućiti povećanje kvalitete i sigurnosti usluga, a također mogu davateljima usluga pružiti veoma točne i relevantne podatke o ponašanju korisnika.

POPIS LITERATURE:

[1] Parsons C. Literature Review of Deep Packet Inspection: Prepared for the New Transparency Project's Cyber-Surveillance Workshop. March. 2011;6:2.

[2] Moore GE. Cramming more components onto integrated circuits, Reprinted from Electronics, volume 38, number 8, April 19, 1965, pp. 114 ff. IEEE Solid-State Circuits Newsletter. 2006;3(20):33-5.

[3] Svoboda J. Network Traffic Analysis with Deep Packet Inspection Method. Available from: http://is.muni.cz/th/250890/fi_m/dp-svoboda.pdf (16.8.2016.)

[4] Worrall AC, Carter BR, Widley G, inventors; Xyratex Technology Limited, assignee. Network monitor and method. United States patent US 7,411,946. 2008 Aug 12.

[5] https://wiki.wireshark.org/CaptureSetup/Ethernet (16.8.2016.)

[6] Shepard TJ. TCP packet trace analysis. MASSACHUSETTS INST OF TECH CAMBRIDGE LAB FOR COMPUTER SCIENCE; 1991 Feb.

[7] Baecher P, Koetter M, Holz T, Dornseif M, Freiling F. The nepenthes platform: An efficient approach to collect malware. InInternational Workshop on Recent Advances in Intrusion Detection 2006 Sep 20 (pp. 165-184). Springer Berlin Heidelberg.

[8] https://tools.ietf.org/html/rfc7011 (20.9.2016.)

[9] Callado A, Kamienski C, Szabó G, Gero BP, Kelner J, Fernandes S, Sadok D. A survey on internet traffic identification. IEEE Communications Surveys & Tutorials. 2009 Jul 1;11(3):37-52.

[10] https://www.sandvine.com/downloads/general/sandvine-technology-showcases/traffic-classification-identifying-and-measuring-internet-traffic.pdf (18.8.2016)

[11] Moon CS, Kim SH. A study on the integrated security system based real-time network packet deep inspection. International Journal of Security and Its Applications. 2014;8(1):113-22.

[12] Mrvelj Š. Predavanja iz predmeta Tehnologija telekomunikacijskog prometa 1: Slojevite arhitekture i norme umrežavanja otvorenih sustava, FPZ, studeni 2013. str17

[13] http://www.symantec.com/connect/articles/perils-deep-packet-inspection; (15.8.2016.)

[14] http://go.radisys.com/rs/radisys/images/paper-dpi-motivations.pdf; (12.8.2016.)

[15] Mochalski K, Schulze H. Deep packet inspection: Technology, applications & net neutrality. ipoque GmbH, White Paper. 2009.

[16] Bendrath R. Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection. InInternational Studies Annual Convention, February 2009 Feb 15 (pp. 15-18).

[17] http://www.digitalsociety.org/2009/10/understanding-deep-packet-inspection-technology/(19.8.2016.)

[18] Turow J. Niche Envy: Marketing discrimination in the digital age. MIT Press Books. 2008;1.

[19] Aspray W, Doty P. Privacy in America: interdisciplinary perspectives. Scarecrow Press; 2011.

[20] Fuchs C. Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society. PACT.

[21] Daly A. The legality of deep packet inspection. International Journal of Communications Law & Policy. 2011 Jun 17(14).

[22] Yemini M. Mandated network neutrality and the first amendment: lessons from Turner and a new approach. Va. JL & Tech.. 2008;13:1.

[23] Mochalski K, Schulze H. Deep packet inspection: Technology, applications & net neutrality. ipoque GmbH, White Paper. 2009.

[24] Daly A. The legality of deep packet inspection. International Journal of Communications Law & Policy. 2011 Jun 17(14).

[25] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570 (22.8.2016.)

[26] Wu T. Network neutrality, broadband discrimination. Journal of Telecommunications and high Technology law. 2003;2:141.

[27] Lessig L, McChesney RW. No tolls on the Internet. Washington Post. 2006 Jun;8.

[28] https://aws.amazon.com/gaming/pc-console/ (18.8.2016.)

[29] http://www.wired.com/2016/02/one-billion-people-now-use-whatsapp (18.8.2016.)

[30] https://www.youtube.com/yt/press/statistics.html (18.8.2016.)

[31] https://techcrunch.com/2016/02/01/gmail-now-has-more-than-1b-monthly-active-users/ (18.8.2016.)

[32] http://bgr.com/2012/10/23/apple-ipad-mini-event/ (18.8.2016.)

[33] https://www.ixiacom.com/sites/default/files/resources/whitepaper/policy_management.pdf (18.8.2016)

[34] http://www.ciscopress.com/articles/article.asp?p=471096&seqNum=6 (18.8.2016.)

[35] http://www-sop.inria.fr/members/Vincenzo.Mancuso/SatRM3.pdf (18.8.2016.)

POPIS AKRONIMA I KRATICA

Kratica ili akronim	Broj stranice	Prijevod ili opis kratice
DPI	3	Deep Packet Inspection
TAP	4	Test Access Point
SPAN	5	Switced Port Analyzer
NIC	6	Network Interface Card
IP	9	Internet Protocol
P2P	9	Peer-to-peer
ADSL	10	Asymmetric digital subscriber line
UDP	10	User Datagram Protocol
TCP	10	Trasmission Control Protocol
HTTP	10	Hypertext Transfer Protocol
SIP	10	Session Iniciation Protocol
FTP	10	File Transfer Protocol
SMTP	10	Simple Mail Transfer Protocol
RTMP	11	Real-Time Messaging Protocol
HD	11	High Definition
NNTP	12	Network News Transport Protocol
DNS	12	Domain Name System
ICMP	12	Internet Control Message Protocol
NTP	12	Network Time Protocol

SSL	12	Secure Sockets Layer
SSH	12	Secure Shell
L2TP	12	Layer 2 Tunneling Protocol
ODI	12	Open System Interconnection
TTL	13	Time to Live
SPI	14	Shallow Packet Inspection
MPI	14	Middle Packet Inspection
FPGA	17	Field-programmable gate array
DoS	20	Denial of Service
DDos	20	Dustrubuted Denial of Service
PCRF	31	Policy and Charging Rules Function
QCI	36	QoS Class Indicator
ARP	36	Allocation and Retention Priority
3GPP	36	The 3rd Generation Partnership Project

POPIS ILUSTRACIJA

Popis slika:

Popis tablica:

Popis dijagrama:

METAPODACI

Naslov rada: Analiza mogućnosti napredne metode za filtriranje paketa
Student: Sandro Brajković
Mentor: izv. prof. dr. sc. Štefica Mrvelj

Naslov na drugom jeziku (engleski): Analyses of Deep Packet Inspection Features
Povjerenstvo za obranu:

- Doc. dr. sc. Niko Jelušić predsjednik
- izv. prof. dr. sc. Štefica Mrvelj mentor
- Dr. sc. Marko Matulin član
- Prof. dr. sc. Zvonko Kavran zamjena

Ustanova koja je dodijelila akademski stupanj: Fakultet prometnih znanosti Sveučilišta u Zagrebu
Zavod: Zavod za informacijsko komunikacijski promet
Vrsta studija: diplomski studij
Studij: Informacijsko Komunikacijski Promet (npr. Promet, ITS i logistika, Aeronautika)
Datum obrane diplomskog rada: 27. rujna 2016.

Napomena: pod datum obrane diplomskog rada navodi se prvi definirani datum roka obrane.

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski 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 diplomskog rada pod naslovom **Analiza mogućnosti napredne metode za filtriranje paketa**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom

repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 04.09.2016.

(potpis)