ZAVOD ZA ELEKTRONIKU MIKROELEKTRONIKU, RAČUNALNE I INTELIGENTNE SUSTAVE
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA
SVEUČILIŠTE U ZAGREBU

DIPLOMSKI RAD br. 1879

Određivanje reputacije autonomnih sustava temeljeno na praćenju sustava DNS

Mislav Stublić

Zagreb, prosinac 2010.

Sažetak

Diplomski rad razmatra sigurnosne probleme DNS protokola te opisuje koncept reputacije primijenjen na razini autonomnih sustava kao mogući korak u ukupnom poboljšanju sigurnosti DNS protokola. Opisuju se detalji DNS protokola te mnogi sigurnosni propusti i pogreške DNS prometa. Predlažu se mnogi modeli kažnjavanja pogrešaka DNS prometa i opisuje njihova uporaba u reputacijskom sustavu.

Razvijen je reputacijski sustav koji različitim analizama utvrđuje pogreške u DNS paketima te nizom funkcija izračunava reputacije autonomnih sustava koji sudjeluju u komunikaciji. Detaljno se opisuju reputacijske funkcije i njihovo ponašanje s različitim ulaznim parametrima. Obavljeno je niz mjerenja na više mjernih točaka u različitim autonomnim sustavima te je prema dobivenim podatcima prezentirano ponašanje razvijenog reputacijskog sustava i autonomni sustavi s najlošijim rezultatima.

Abstract

Diploma thesis discusses domain name system security issues and describes the concept of reputation applied at the autonomous system level as a possible step towards raising protocol security. Domain name system is described in details as well as many security issues and errors of DNS traffic. Different models of DNS error penalization are suggested and also their use in the reputation system is described.

A reputation system is implemented which uses different analyses to identifies errors in DNS packets and by using several functions calculates reputation of autonomous systems which are communicating. Reputation functions and their behaviour using different parameter values are described in details. A number of measurements at several measurement points in different autonomous systems are performed and by using the acquired data behaviour of implemented reputation system and also autonomous system with worst scores are presented.

Sadržaj

1. Uvod

Sigurnost korisnika na Internetu jedan je od glavnih problema s kojim se susreće internetska zajednica. Brzi rast Interneta potaknut razvojem i dostupnosti tehnologije te nizom otvorenih protokola i standarda, donio je i niz problema i sigurnosnih prijetnji. Na nedostatak sigurnosti često utječe sukob ciljeva dizajna pojedinog protokola te tehničkih opterećenja koje dolaze uvođenjem sigurnosnih elemenata u protokol. Primjerice, protokoli na Internetu danas često kao glavni zahtjev imaju skalabilnost i robusnost, proizašao iz veličine cijelog sustava i njegova rasta, a zanemaruju sigurnost koja sa sobom nosi povećanje potrebnih resursa brzine prijenosa, memorije, procesorskog vremena itd. To se posebno očituje u vidu problema tajnosti i integriteta podataka, raznih napada poput DoS-a (uskraćivanje usluge, *denial of service*), prijevara poput *phisinga*, lažnih predstavljanja, krađe identiteta itd.

Specifičan su problem napadi koji iskorištavaju sigurnosne manjkavosti dizajna pojedinih protokola na Internetu. Za razliku od direktnih napada na pojedine korisnike, napadi koji eksploatiraju greške u protokolima ili implementacijama protokola imaju dalekosežnije posljedice i predstavljaju sigurnosni problem cijele zajednice. Korisnici često nisu niti svjesni takvih napada, jer se odvijaju u pozadini, na razini protokola, stvarajući privid normalnog funkcioniranja sustava. U ovom diplomskom radu se razmatraju sigurnosni propusti DNS protokola.

Sustav naziva domena (*domain name system, DNS*) služi klijentima pri utvrđivanju IP (*internet protocol*) adresa računala koje pokušavaju kontaktirati. Nizom upita i odgovora na temelju zadanog imena domene prema DNS protokolu klijenti mogu jednostavno pronaći IP adrese poslužitelja, ali i druge podatke vezane za danu domenu poput poslužitelja elektroničke pošte (*mail server*), ili naziv domene koja se nalazi na nekoj IP adresi itd.

DNS protokol u svojoj osnovnoj varijanti praktički ne podrazumijeva nikakve sigurnosne elemente te je time posebno pogodan za mnoge vrste napada i prijevara. S vremenom protokolu su dodavana razna sigurnosna proširenja međutim niti ta proširenja ne osiguravaju razinu sigurnosti koja bi bila zadovoljavajuća. Problem je što mnogi napadi tim proširenjima nisu zaustavljeni. Dodatan problem stvara i činjenica da se sigurnosna proširenja izrazito sporo implementiraju na poslužiteljima i klijentima na Internetu.

Razvoj sustava koji bi poboljšao sigurnost DNS protokola pokazuje se izrazito bitnim. Jedan od pristupa povećanju sigurnosti je koncept reputacije kojim se klijentima koji sudjeluju u komunikaciji nekim protokolom pridaju vrijednosti koje ukazuju kakav promet se može očekivati od tog klijenta. To pomaže u izbjegavanju komunikacije s klijentima za koje se utvrdi da nemaju kvalitetan promet, odnosno imaju lošu reputaciju.

Zadatak ovog diplomskog rada je razviti sustav koji primjenjuje koncept reputacije na autonomne sustave (AS), pri čemu se reputacija temelji na promatranju kvalitete DNS prometa. Kao klijente koji koriste DNS protokol i kojima se dodjeljuje reputacija nećemo gledati krajnje korisnike na Internetu, niti poslužitelje, već AS-ove. Postavljanjem reputacije AS-ovima želi se postići obrnut efekt – povećati pažnju AS-ova za promet koji generiraju njihovi korisnici, a onda posredno i za sigurnost tog prometa.

Ovaj diplomski rad sastoji se od sedam poglavlja. Drugo poglavlje razmatra sigurnosne probleme na Internetu vezane za autonomne sustave i njihove odnose, te uvodi koncept reputacije kao moguć doprinos povećanju sigurnosti.

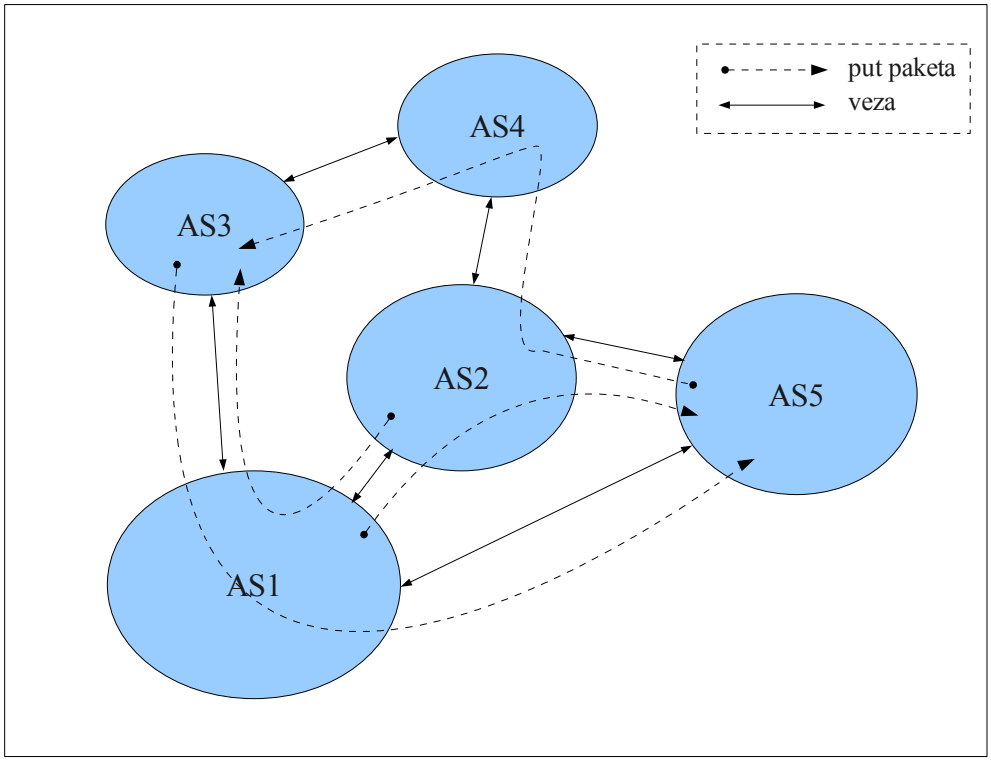
Treće poglavlje bavi se opisom DNS protokola, zatim razmatra najčešće pogreške i propuste koji se mogu uočiti u DNS protokolu, daje kratki prikaz srodnih radova i mjerenja te detaljnu razradu prijedloga modela ocjene kvalitete DNS prometa. Četvrto poglavlje opisuje arhitekturu sustav koji bi vršio potrebna mjerenja i postavljao reputacije autonomnim sustavima prema modelu predstavljenom u trećem poglavlju.

Peto poglavlje detaljno opisuje pretpostavke na kojima se temelji reputacijski sustav, korištene reputacijske funkcije te komponente implementiranog reputacijskog sustava. U šestom poglavlju analizirana su ponašanja reputacijskih funkcija i sustava u cjelini te prikazani rezultati mjerenje odnosno izračunate reputacije AS-ova. Rad završava zaključkom i popisom literature.

2. Problem ponašanja autonomnih sustava

Kada govorimo o sigurnosti protokola poput DNS-a, uzroke i moguća rješenja sigurnosnih problema možemo tražiti na različitim mjestima. Primjerice, možemo ispravljati pogreške programske opreme ili tražiti slabosti u specifikaciji samih protokola, ali možemo promatrati i autonomne sustave koji su zaduženi za prijenos podataka. Nama su najzanimljiviji upravo autonomni sustavi i njihov doprinos ukupnoj sigurnosti Interneta te moguća rješenja vezana za operacije koje obavljaju AS-ovi.

Autonomni sustav (AS) je skup međusobno vezanih mreža koje imaju zajedničke politike usmjeravanja prema Internetu bazirane na IP protokolu, a kojima često upravlja jedan entitet, u pravilu ISP (pružatelj usluge Interneta, *Internet service provider*). Zadatak AS-a je osigurati prijenos, odnosno usmjeravanje, podataka u komunikaciji s okolnim autonomnim sustavima. U tom smislu AS možemo smatrati kao odvojen entitet u globalnom Internetu koji osigurava protok informacija prema i od korisnika unutar mreže koju omeđuje te u određenim slučajevima prenosi promet okolnih autonomnih sustava na čijem putu se nalazi, slika 2.1. Autonomni sustavi imaju na razini Interneta definiran identifikacijski broj koji ih jedinstveno određuje i može se koristiti za utvrđivanje informacija vezanih za pojedini AS. Pojedini AS je samoodrživ i neovisan o vezama s ostatkom Interneta, ali ovisi o vezama s okolnim autonomnim sustavima za uspostavljanje krajnje komunikacije od korisnika do korisnika.



Slika 2.1. Općeniti prikaz mogućih veza autonomnih sustava

Takav položaj AS-ova dopušta nebrigu za promet koji sami generiraju, kao i manjak pažnje za kvalitetu prometa koji dolazi od ostalih AS-ova. Štoviše upravo je takva pozicija

osigurala da se svaki AS može ponašati na način koji mu najviše odgovara, a to u pravilu znači sebično gledanje svojih interesa. AS-u može biti u interesu osigurati sigurnost prometa svojih korisnika, tj. dostupnost usluge. S druge strane mnogo će manje pažnje posvetiti prometu koji potencijalno može štetiti svima izvan njegovog područja jer im se to vrlo teško može pokazati isplativim, a svakako bi bilo riječ o dodatnom trošku. Moguće su zapravo i suprotne situacije u kojima je određenom AS-u čak i u interesu propuštati štetan promet prema ostatku Interneta npr. AS koji održava poslužitelje neželjene pošte.

Distribuiranost Interneta pozitivno doprinosi razvoju i širenju te se uz robusnost pokazuje kao najveća snaga Interneta, ali kada govorimo o odgovornosti AS-ova distribuiranost predstavlja i stvaran problem kojem je posebno teško doskočiti. Jednostavno ne postoji određeni nadzor koji bi bio iznad razine AS-ova i koji bi osiguravao poštivanje "pravila igre". Štoviše razumno je tvrditi da bi takav nadzor bilo i praktički nemoguće izvesti zbog kompleksnosti sustava, sakupljanja podataka, njihove analize te utvrđivanja činjenica vezanih za ponašanje pojedinog AS-a, odnosno utvrđivanje odgovornosti za pojedini štetan promet.

Dakle, odgovornost za kontroliranje pogrešaka prometa je u potpunosti na svakom pojedinom AS-u. Pritom pojedini AS ne mora imati interes pratiti promet vlastitih korisnika, nego samo promet koji dolazi izvana da bi se, u slučaju da je neispravan, od njega mogao obraniti. Stoga sustav koji želi povećati sigurnost prometa na razini AS-ova mora na prvom mjestu AS-u omogućiti adekvatno praćenje pogrešaka. Drugi zahtjev je da posredno natjera AS da i sam pazi na svoj promet. To je moguće postići kroz koncept reputacije.

2.1. Reputacija

Koncept reputacije dolazi iz sociologije i podrazumijeva evaluaciju nekog entiteta prema određenim kriterijima. Određivanje reputacije AS-ova podrazumijeva aktivnu ulogu entiteta, u našem slučaju AS-a, u procjeni kvalitete prometa koji do njega dolazi. Ako AS-ovi nemaju interes paziti na vlastiti promet, ipak imaju interes od ostalih sudionika mreže dobivati ispravan promet. Kako ne mogu natjerati okolne AS-ove da paze na svoj promet i prosljeđuju samo ispravan promet, ostaje im opcija promjene politike prema susjednim AS-ovima. Politiku koji primjenjuju u odnosima s okolnim, ili udaljenim, autonomnim sustavima mogu određivati prema informacijama koje generira reputacijski sustav.

Unutar mreže koja implementira reputacijske sustave AS-ovi mogu, na temelju informacija o reputaciji, odrediti svoje ponašanje prema drugoj strani komunikacije. Reputacijske podatke mogu graditi na temelju svog iskustva komunikacije s pojedinim klijentima ili mogu podatke temeljiti na razmjeni reputacijskih podataka s poznatim izvorima kojima vjeruju.

Reputacijski sustav se sastoji od tri osnovna dijela:

1. praćenje prometa susjednih ili udaljenih autonomnih sustava
2. analiza i ocjena prometa, te određivanje reputacije promatranog autonomnog sustava na temelju te analize
3. promjena politike adekvatno dodijeljenoj reputaciji

Na razini autonomnih sustava korištenje sustava reputacije značilo bi promatranje prometa različitih protokola koje pojedini AS smatra ključnim za ukupno poboljšanje komunikacije s okolnim autonomnim sustavima. Posljedica je poboljšanje usluge korisnicima, smanjivanje vlastitih troškova ili problema koji nastaju radi neispravnog prometa te povećanje sigurnosti. Ako se reputacijski podatci mijenjaju s vremenom AS može prilagođavati svoje ponašanje prema drugim AS-ovima koje je na taj način ocijenio. Osnovna metoda prilagodbe je ograničavanje prometa susjednih AS-ova za koje se utvrdi da ne paze na vlastiti promet, odnosno, kojima je utvrđena loša reputacija. Ograničavanje prometa se može vršiti u slučajevima nužde npr. kada je mreža preopterećena, a AS treba procijeniti koji je promet koristan te ga treba propuštati, a kojeg treba blokirati. U radu pod normalnim opterećenjem AS na temelju reputacijskih podataka može razmatrati efikasnije dodjeljivanja mrežnih resursa ili politike usmjeravanja prometa.

Osnovni poticaj implemenatiranju reputacijskog sustava za AS je pokušaj utvrđivanja krivca za štetni promet te adekvatan odgovor. AS sa svojim strogo definiranim "granicama" može lako pratiti linije kojima dolazi promet i analizirati ga za potrebe utvrđivanja reputacije. Sustav može biti koristan i ako ga nitko drugi ne implementira jer daje važne informacije o prometu koji mu šalju susjedi. Ako pak reputacijske sustave implementira više autonomnih sustava, korisna posljedica je povećana pažnja autonomnih sustava na vlastiti promet upravo zbog reputacije koju prema njima postavljaju njihovi susjedi. Više im nije samo u interesu dobivati ispravan promet nego ga i slati ostalima kako ne bi dobili lošu reputaciju, a time i lošiji tretman.

Ovaj princip može biti i "tranzitivan". Ako se nedužni AS nalazi na putu lošeg prometa kojeg treba prosljeđivati dalje prema ostatku Interneta tada bi taj nedužni AS također dobio lošu reputaciju. Međutim, to onda znači da će se nedužni AS na putu neispravnog prometa morati pobrinuti za takav promet svojih susjeda – ograničavanjem, blokiranjem lošeg prometa, drugačijim politikama usmjeravanja itd. – kako bi popravio svoju reputaciju. Posljedica je opet, u ovom slučaju posredno, kažnjavanje krivca za neispravan promet.

Reputaciju je moguće mjeriti prema raznim vrstama prometa. Moguće je da neki AS koristi samo određeni protokol za određivanje reputacije okolnih autonomnih sustava. Međutim, za obuhvatniju analizu prometa bilo bi korisno primijeniti sustav reputacije na što veći broj protokola na Internetu, a posebno na one koji se češće koriste za napade ili druge vrste neželjenog prometa. Dobar primjer je elektronička pošta kojom se distribuira neželjena pošta, ili koja se koristi kao medij za prijenos virusa, trojanaca itd. Također, razumno je primijeniti reputacijski sustav na protokole koji inače u svojim standardima ne pretpostavljaju neke posebne sigurnosne mehanizme, pa su time ranjiviji za napade ili služe kao medij za napade, poput DNS protokola. Da bi sustav bio maksimalno efikasan idealno bi bilo promatrati što veći broj "problematičnih" protokola čijom se analizom onda mogu uočiti inače teže uočljive pojave štetnog prometa npr. distribuirane mreže zaraženih računala, a prema kojima se onda mogu poduzeti adekvatne mjere.

Prepoznavanje i ograničavanje zlonamjernog prometa poput DoS napada važan je cilj svakog sustava koji želi povećati sigurnost na Internetu, međutim, pažnju AS-ova treba usmjeriti također i prema prometu koji nije nužno neispravan, ali je zato neželjen. Neželjena pošta je dobar primjer, no to se odnosi i na sav promet koji nastaje zbog krivo podešene ili neispravne programske podrške i sklopovlja, nepoštivanja internetskih standarda i protokola itd. Riječ je velikoj količini "dobronamjernog" prometa koji zagušuje

mrežu i stvara probleme najčešće izvan AS-a iz kojeg dolazi, a za kojeg zato autonomni sustavi nemaju razloga brinuti.

Problem sigurnosti na Internetu se pokazuje kao posljedica sebičnog ponašanja AS-ova, a omogućavanje obrane pojedinom AS-u od lošeg prometa susjeda prvi je korak rješavanja tog problema. Time bi, s jedne strane, izbjegli pokušaj discipliniranja svakog pojedinog korisnika, što se svodi na ispravljanje grešaka programske opreme ili sklopovlja i namjernih napada. S druge strane, izbjegli bi pokušaj nadgledanja svog prometa AS-ova kako bi ih se pomoću neke vrste arbitra natjeralo da paze na promet svojih korisnika. Podjela odgovornosti svakom AS-u da nadgleda promet svojih korisnika je nasuprot ove dvije krajnosti realna mogućnost, posebno zato što AS-ovi imaju kontrolu nad linijama te zato što sami definiraju politike usmjeravanja. Tu podjelu odgovornosti na AS-ove moguće je postići primjenom reputacijskih sustava.

Prije daljnje analize nužno je navesti bitne pretpostavke promatranja prometa na razini AS-a, a koje u bitnom određuju daljnji dizajn sustava, mogućnost praćenja pogrešaka i njihovu analizu:

1. AS ima stroge granice koje se mogu apstrahirati linijama komunikacije koje ga vežu za okolne autonomne sustave
2. AS može slobodno promatrati sav promet koji prolazi preko graničnih linija i pritom zna susjedni AS s kojeg paket dolazi odnosno kojem se paket prosljeđuje
3. promet promatra niz senzora postavljenih na svaku komunikacijsku liniju AS-a
4. senzori mogu imati procesiranje i čuvati podatke neko vrijeme što im pomaže u prepoznavanju pogrešaka u prometu
5. mjerenja se prvenstveno vrše u realnom vremenu te se tako i ocjenjuje kvaliteta prometa, iako mjerenja mogu biti poduprta naknadnom analizom prikupljenog prometa.

3. Mjerenje reputacije na temelju DNS-a

Princip mjerenja reputacije na razini autonomnih sustava moguće je primijeniti na čitav niz protokola na Internetu. Posebno pogodan protokol za praćenje prometa i postavljanje reputacije je sustav naziva domena. Razlog je tome što je riječ o jednom od osnovnih protokola na Internetu, a koji je u originalnoj specifikaciji podrazumijevao vrlo malo sigurnosti te ga je moguće zloupotrijebiti. Manjak sigurnosti je prvenstveno bio uzrokovan nužnošću skalabilnosti i robusnosti protokola koji svoju strukturu bazira na strogo utvrđenoj hijerarhiji poslužitelja odnosno zadanih autoriteta za tražene DNS podatke. Mjerenjima je također utvrđeno da je velika većina DNS prometa po nekom kriteriju neispravna, krši protokol ili je jednostavno nepotrebna te time opterećuje sustav i zagušuje mrežu. Također, DNS je moguće koristiti i u DoS napadima. Iz navedenih razloga opravdano je u reputacijski sustav AS-a uključiti i promatranje DNS prometa.

3.1. Temelji protokola DNS

Sustav naziva domena je protokol kojim se nizom upita i odgovora naziv domene pretvara u IP adresu poslužitelja dotične domene. Osnovna definicija protokola nalazi se u dva RFC-a, 1034 i 1034 (*RFC – request for comment*, jedan od koraka u standardizaciji protokola na Internetu) [1], [2]. Klijenti i poslužitelji na Internetu komuniciraju poznavajući IP adrese druge strane. Kako je IP adrese teško pamtiti, razumljivo je uvođenje identifikacije putem naziva domena koje će, poput osobnih imena ili naziva organizacija biti trajno prepoznatljive. IP adrese mogu biti dodijeljene poslužiteljima na dulje vrijeme, ali kako u sustavu IPv4 adresa adrese nisu trajno dodijeljene pojedinim poslužiteljima ili klijentima, već je vrijeme na koje se dodjeljuju korisnicima ipak ograničeno, potrebna je metoda utvrđivanja trenutnih IP adresa koje se kriju iza "trajnih" naziva poslužitelja s kojima želimo komunicirati. Drugi razlog je što je zbog veličine nemoguće lokalno imati pohranjenu bazu svih adresa poslužitelja.

U osnovnom tipu DNS komunikacije klijent postavlja upit koji sadrži naziv domene čiju IP adresu želi saznati. Upit se postavlja poslužitelju koji posjeduje te podatke. DNS podatci su podijeljeni hijerarhijski, počevši od korijenskih poslužitelja (*root server*) koji sadrže podatke o poslužiteljima vršnih domena (*TLD, top-level domain*) pa niže po hijerarhiji do poslužitelja koji poslužuje traženu domenu i sadrži sve podatke vezane za nju. Utvrđivanje tražene IP adrese se dakle svodi na niz upita kojima se slijedno otkrivaju poslužitelji u DNS lancu do poslužitelja za traženu domenu koji daje odgovor na puno originalno pitanje. Nijedan poslužitelj u DNS hijerarhiji ne posjeduje sve podatke već su oni raspršeni na niz poslužitelja koji posjeduju samo djelić cjelokupnog prostora imena. To doprinosi otpornosti protokola na kvarove pojedinih poslužitelja i njegovoj skalabilnosti na globalnom Internetu.

Klijent koji postavlja upit na početku mora znati barem jednu adresu nekog korijenskog poslužitelja kako bi mu mogao postaviti pitanje za niže poslužitelje u hijerarhiji – poslužitelje vršnih domena, pa onih niže itd. U uobičajenom okruženju klijent će zapravo poznavati adresu lokalnog DNS poslužitelja od kojeg će dalje tražiti podatke. Može biti riječ o poslužitelju u lokalnoj mreži ili pak o poslužitelju ISP-a kojem se prosljeđuju svi

upiti. Pritom često klijent niti nije u stanju obaviti sam proces pretrage već to prepušta DNS poslužitelju, klijent je tada tzv. jednostavni rješavač (*stub resolver*).

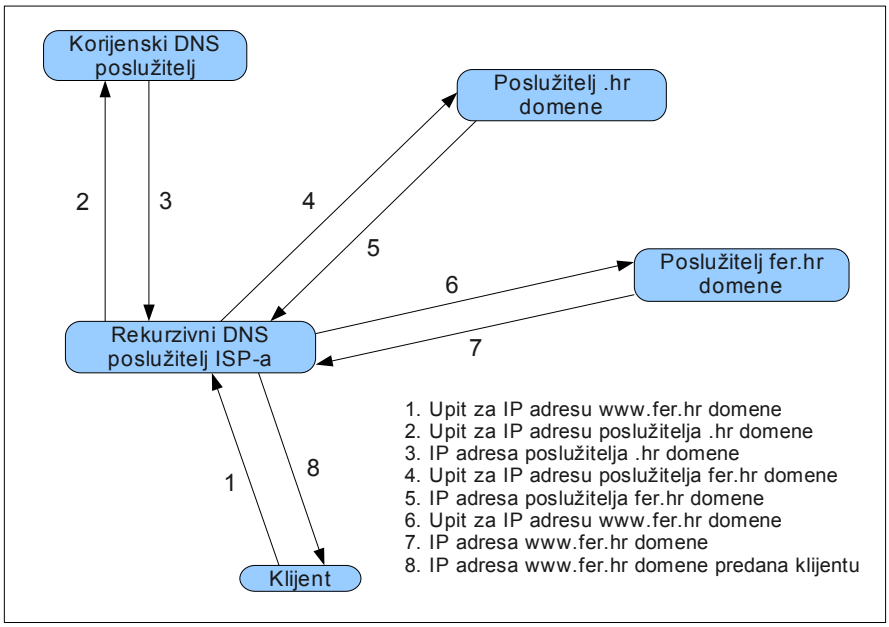
Rješavanje upita iz perspektive klijenta može biti:

1. iteritivno – klijent postavlja niz upita lancu poslužitelja, koji vraćaju djelomične odgovore, dok ne dobije konačan odgovor
2. rekurzivno – klijent postavlja upit DNS poslužitelju naznačujući da želi da upit riješi rekurzivno te time posao rješavanja prepušta poslužitelju, a kao odgovor dobiva puno rješenje originalnog pitanja, slika 3.1

Poslužitelj može biti:

1. autoritativan (*authoritative*)– sadrži autoritativne podatke za neku zonu, i odgovara samo na te upite
2. rekurzivan – obavlja rješavanje rekurzivnih upita za druge klijente
3. *caching* – privremeno pohranjuje zapise prikupljene iz raznih upita te u odgovorima koristi sadržaj privremene memorije kako bi ubrzao postupak pronalaska odgovora

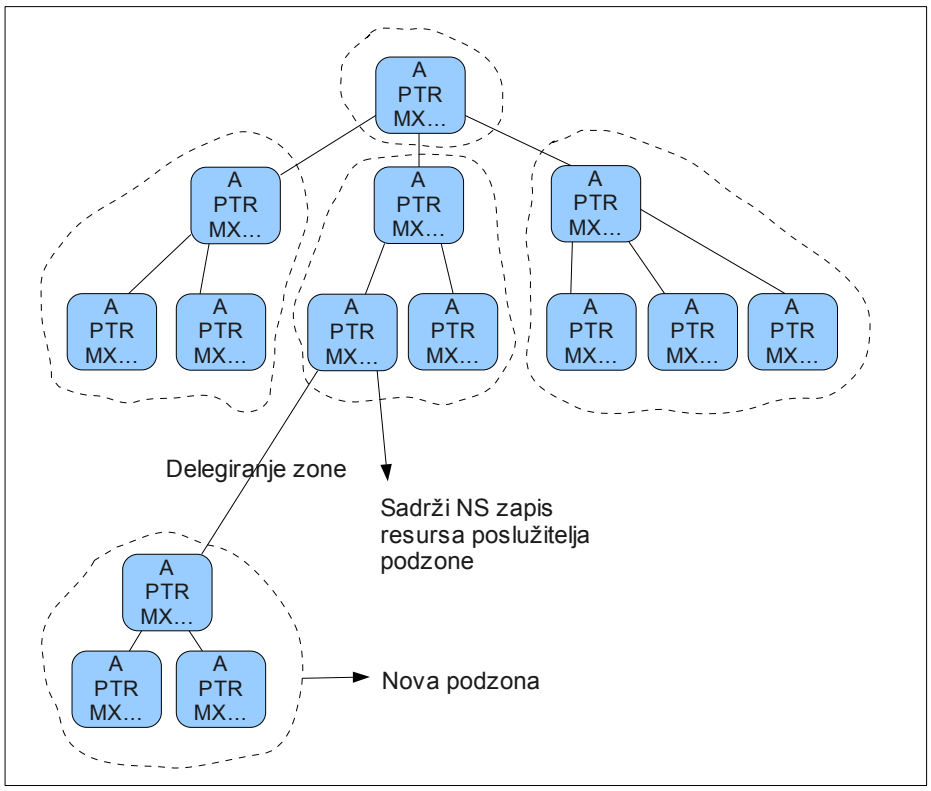
Funkcije poslužitelja nisu međusobno isključive već neki poslužitelj može podržavati više ili čak sve funkcije. To posebno vrijedi za privremeno pohranjivanje podataka koje se može smatrati poželjnom funkcijom svakog poslužitelja i klijenta, posebno kada je riječ o podatcima vezanim za vršne domene, čime se olakšava posao poslužitelja vršnih domena na kojima je najveći pritisak. Tada su takvi podatci neautoritativni.



Slika 3.1. Rekurzivno rješavanje DNS upita

Svaki DNS poslužitelj odgovara na dio za koji je on odgovoran unutar pojedinog upita, odnosno, za koji je on autoritativan te eventualno dodaje neke dodatne neautoritativne podatke, a koji bi mogli biti korisni za daljnju pretragu ili koje posjeduje u privremenoj memoriji. Korijenski poslužitelji su odgovorni za pitanja o poslužiteljima vršnih domena, a

poslužitelji vršnih domena su odgovorni za sve domene na toj razini hijerarhije itd. Time je DNS prostor imena podijeljen na tzv. zone autoriteta koje pojedini DNS poslužitelji održavaju. Svaka zona može imati podzone te sama u potpunosti upravlja dodijeljenim prostorom do ruba zone, a njen autoritet prestaje tamo gdje počinje autoritet podzone. Autoritativni poslužitelj može delegirati održavanje dijela zone drugim poslužiteljima te time stvoriti novu zonu ili podzonu, slika 3.2, pritom pojedini poslužitelj može biti autoritativan za više zona, odnosno, postojanje hijerarhije unutar zona ne diktira nužno postojanje i stroge hijerarhije među konkretnim poslužiteljima te je tako moguće da pojedini poslužitelji održavaju neku od zona i podzona određene domene. Delegiranih zona (odnosno podzona) može biti proizvoljno mnogo, do proizvoljne dubine stabla hijerarhije zona. Praktički jedino ograničenje predstavljaju granice dimenzija labela pojedine zone koje smiju biti duge maksimalno 63 znaka, dok cijela domena ne smije biti duža od 253 znaka.



Slika 3.2. Delegiranje podzone

Osnovni DNS upit može se podijeliti na labele počevši od vršne domene kojom završava npr. .com ili .hr, a nastavivši niže po upitu npr. "fer" i "www" u www.fer.hr domeni. Za primjer www.fer.hr domene, rješavanje (pod pretpostavkom da trenutno u privremenoj memoriji nije pohranjen nikakav relevantan podatak) će početi od korijenskog poslužitelja čiji IP treba biti unaprijed poznat, a kojeg će se pitati koji poslužitelj poslužuje hr vršnu domenu. Korijenski poslužitelji su unaprijed definirani i poznati, a sve vršne domene propisane na globalnoj razini. Poslužitelj će na to pitanje odgovoriti IP adresom poslužitelja hr domene. Taj pak poslužitelj posjeduje podatke o IP adresama svih domena unutar hr zone za koju je autoritativan pa tako i IP adresu poslužitelja fer.hr domena, a taj pak sadrži podatke o domeni www.fer.hr ili traženoj IP adresi, kako je prikazano na slici

3.1

DNS definira niz zapisa resursa (*resource record, RR*), a neki osnovni su:

1. A – vraća IPv4 adresu traženog poslužitelja
2. AAAA – vraća IPv6 adresu traženog poslužitelja
3. CNAME – definira kanonsko (primarno) ime nekog poslužitelja koji posjeduje alijase
4. MX – sadrži naziv poslužitelja elektroničke pošte
5. NS – definira autoritativnog DNS poslužitelja za određenu zonu
6. PTR – pokazivač na kanonsko ime poslužitelja, najčešće se koristi za tzv. obrnuta pretraživanja koja pronalaze nazive domena koje se skrivaju iza pojedinih IP adresa
7. SOA – početak autoriteta – sadrži autoritativne podatke vezane za zonu poput poslužitelja domene, elektroničke pošte administratora itd.
8. TXT – originalno zamišljen da prenosi čitljive podatke, danas također služi i za prijenos različitih dodatnih podataka za sigurnost i sl.

Zapisi resursa imaju standardni format koji sadrži podatke vezane za resurs, a sastoji se od polja:

1. NAME – ime upita (ili odgovora), varijabilne duljine, sastoji se od niza okteta koji govore koliko znakova ima labela koja slijedi pojedini oktet, a završava oktetom nula koji označava kraj imena
2. TYPE – sadrži dva okteta koji definiraju tip zapisa resursa koji se ovdje opisuje (poput A ili MX), a posredno opisuje značenje kasnijih polja
3. CLASS – dva okteta koji opisuju razred zapisa resursa (poput IN za Internet)
4. TTL (*time-to-live*, trajanje zapisa) – 32-bitni broj bez predznaka koji označuje vrijeme u sekundama koliko podatak može biti pohranjen prije nego ga se više ne smije koristiti, ako je TTL nula to znači da se podatak smije koristiti samo u trenutnoj transakciji i ne smije se pohranjivati
5. RDLENGTH – 16-bitni broj bez predznaka označava duljinu u oktetima sljedećeg RDATA polja
6. RDATA – polje koje sadrži tražene podatke, a čiji oblik ovisi o tipu i razredu zapisa resursa (npr. 32-bitni broj adrese kada je riječ o tipu A i razredu IN)

DNS upiti i odgovori su formirani kao poruke koje sadrže polja: zaglavlje (*header*), pitanje (*question*), odgovor (*answer*), autoritet (*authority*) i dodatno (*additional*). Zaglavlje poruke sadrži osnovne podatke o poruci:

1. ID – 16-bitni identifikator koji se prepisuje u odgovor, a koristi se kao pomoć kod uparivanja upita i odgovora
2. QR – jedan bit koji govori je li riječ o upitu ili odgovoru (0 upit, 1 odgovor)
3. Opcode – 4-bitno polje koje opisuje upit, a sadrži mogućnosti:

- QUERY – standardni upit
- IQUERY – zastarjeli tip "inverznih" upita, trebao služiti za preslikavanje zapisa resursa prema domenama koje ih posjeduju
- STATUS – upit za stanje poslužitelja
- NOTIFY – obavijest o promijeni sadržaja zone
- UPDATE – metoda posredne promijene sadržaja zone

4. AA – bit koji označava da je sadržaj odgovora autoritativan
5. TC – bit koji označava da je poruka zbog duljine bila skraćena
6. RD – bit označava da je rekurzivno rješavanje upita poželjno
7. RA – bit označava da je rekurzivno rješavanje upita dostupno na poslužitelju
8. Z – bit rezerviran za buduće primjene
9. AD – govori da su podatci u odgovoru autentificirani kod uporabe sigurnosnih proširenja
10. CD – govori poslužitelju da ne provjerava validnost podataka kod uporabe sigurnosnih proširenja
11. RCODE – dio odgovora koji može govorit:
    - *no error condition* – nema pogreške
    - *format error* – greška u formatu upita, poslužitelj ne može interpretirati upit
    - *server failure* – nemoguće procesirati upit zbog greške na poslužitelju
    - *name error* – nepostojeće ime domene, ima smisla samo za autoritativne odgovore
    - *not implemented* – poslužitelj ne podržava traženu vrstu upita
    - *refused* – poslužitelj odbija odgovoriti na upit, najčešće radi ograničenja politike poslužitelja
12. QDCOUNT – 16-bitni broj označava broj zapisa resursa u polju pitanja
13. ANCOUNT – 16-bitni broj označava broj zapisa resursa u polju odgovora
14. NSCOUNT – 16-bitni broj označava broj zapisa resursa u polju autoriteta
15. ARCOUNT – 16-bitni broj označava broj zapisa resursa u polju dodatno

Polja odgovor, autoritet i *dodatno* DNS poruke imaju oblik niza zapisa resursa čiji je broj definiran u zadnjih četiri polja zaglavlja poruke. Polje pitanje je nešto drugačije i sadrži samo ime, tip i razred upita koji zajedno nose sve potrebne podatke da bi se na upit odgovorilo.

DNS koristi pristup 53 (*port*), a najčešće se prenosi putem UDP protokola iako je moguć prijenos i TCP protokolom koji se koristi ponajviše kada se radi o većim DNS odgovorima koji bi zahtjevali više UDP paketa ili kada se radi o prijenosima zona.

S vremenom DNS je doživio mnoge promjene, proširenja protokola i funkcionalnosti, poput dinamičkog ažuriranja zapisa resursa, dodavanje novih zapisa resursa definiranih u nizu RFC-ova itd. Najvažnija proširenja su na području sigurnosti. DNS sigurnosna proširenja (*DNS security extensions, DNSSEC*) originalno definirana u RFC 2535, ali kasnije bitno izmijenjena u RFC 4033 [3], RFC 4034 [4], RFC 4035 [5], donose mogućnost autentifikacije izvora podataka, autentifikacije nepostojanja podataka i integritet podataka, međutim ne osiguravaju povjerljivost podataka.

3.2. Srodni radovi

Za razumijevanje DNS prometa i namjernih i nenamjernih propusta u DNS prometu osim referentnih dokumenata poput [1], [2], te njihovih kasnijih nadopuna korisno je pogledati članke u kojima se vrše mjerenja DNS prometa. Mjerenja DNS prometa mogu se ugrubo podijeliti na mjerenja:

1. latencije DNS upita i odgovora u pokušaju utvrđivanja opterećenja postojeće infrastrukture, posebno kada je riječ o korijenskim poslužiteljima, i posljedica na uslugu koji krajnji korisnici dobivaju
2. utvrđivanje problematičnih točaka i uskih grla postojeće mreže ili detalja dizajna protokola
3. analiza DNS prometa uzimajući u obzir ciljeve postavljene pri dizajniranju protokola i postignute rezultate, te nove elemente protokola i njihov utjecaj na cjelokupno ponašanje protokola i prometa
4. analiza opterećenje uzimajući u obzir najveće izvore prometa i najčešće tipove prometa
5. analiza i pokušaj utvrđivanja razloga čestih pogrešaka DNS prometa, te prepoznavanje najčešćih propusta
6. aktivna i pasivna analiza DNS prometa u potrazi za napadima, što na DNS infrastrukturu što korištenje DNS-a za druge tipove napada

Analize i mjerenja DNS-a mogu biti vršena na razini:

1. klijenta, pri čemu govorimo o manjoj količini prometa koju se može detaljno analizirati čuvajući veće količine informacija o pojedinim upitima i odgovorima. Ispitujući sigurnost, efikasnost, opterećenje itd. moguće je utvrditi konkretne uzroke problema i propusta koji se očituju DNS prometu
2. poveznika (*gateway*) koji usmjeravaju promet veće količine korisnika. Kako imamo više prometa, moguće je prepoznavanje čestih zajedničkih pogrešaka i problema, eventualnih napada i iskorištavanja DNS prometa. Koriste se statističke metode i baze podataka za uočavanje obrazaca ponašanja pojedinih korisnika ili grupa korisnika i korisničkih aplikacija te njihov utjecaj na ukupni promet. I dalje moguće pohranjivanja veće količine podataka o upitima i odgovorima iako su zahtjevi na infrastrukturu veći
3. pružatelja usluga Interneta, autonomnih sustava ili poslužitelja korijenskih ili vršnih domena. Velike količine prometa omogućuju promatranje "globalnih" trendova u

DNS prometu, posljedica izvedbe pojedine korisničke programske opreme i sklopovlja, suptilnih propusta koji imaju jak utjecaj na ukupan promet, izvore velikih količina neispravnog prometa, utjecaja određenih elemenata dizajna protokola na performanse, učestalost uporabe pojedinih funkcionalnosti itd. Moguće je pohranjivanje velike količine upita i odgovora za kasniju analizu, ali s mnogo većim ograničenjima koja postavlja infrastruktura, posebno kada je riječ o aktivnim mjerenjima i mjerenjima u stvarnom vremenu

Za razvoj reputacijskog sustava na razini autonomnog sustava korisna su mjerenja sigurnosti, propusta i nepoželjnog DNS prometa koja se vrše na razini korijenskih i vršnih poslužitelja, ISP-a i poveznika većih mreža. Srodni radovi koji sadrže takva mjerenja korišteni u ovom diplomskom radu:

1. [6] – mjerenje vršeno na poveznicima lokalnih mreža studentskih stambenih kompleksa, sveučilišnog kampusa, jezgre mreže sveučilišta i mreže ADSL korisnika uglavnom studenata. Prikupljen sav DNS promet, a promatra se samo promet koji se može odrediti kao neispravan prema RCODE zastavici zaglavlja DNS upita. Ovisno o tipu pogreške koja je definirana tom zastavicom analizira se promet te utvrđuju razlozi pojavljivanja pojedinih najčešćih pogrešaka DNS prometa toga tipa. Prikupljeni promet se prvo anonimizira kako bi se sačuvala privatnost korisnika i kako bi podatci kasnije mogli biti objavljeni te se izrađuju statistike latencije, broja propuštenih paketa, postotka u ukupnom prometu itd. Riječ je o pasivnom mjerenju, pa se sav promet snima i naknadno analizira
2. [7] – pasivno mjerenje vršeno na jednom od korijenskih poslužitelja (F korijenski poslužitelj) snimajući sav promet te ga analizira u potrazi za greškama. Utvrđuju da je većina prometa na razini korijenskih poslužitelja na neki način neispravna, pritom u neispravnosti ulaze različita kršenja DNS protokola, krivo oblikovani paketi, ponavljanja upita, DoS napadi, upiti za nepostojeće domene itd. Utvrđuju da se stanje prometa, unatoč saznanjima iz ranijih mjerenja (*Danzig, An analysis of wide-area name server traffic, 1992.*) o postojećim greškama i problemima, s vremenom pogoršalo. Nizom naknadnih aktivnih mjerenja pronalaze neke od razloga pojave neispravnog prometa i ponašanja pojedinih poslužitelja koji ga generiraju
3. [8] – autori razmatraju problem paralelnih puteva rješavanja DNS upita, odnosno paralelne "autoritete" DNS hijerarhije kao posljedicu sigurnosnih propusta ili napada. Paralelni putevi rješavanja DNS upita nastaju zlonamjernim promjenama puteva rješavanja pomoću različitih virusa, ili trovanjem međuspremnika, potpomognutim poslužiteljima koji lažu ili se lažno predstavljaju te navode klijente lažnim odgovorima. Utvrđuju veliki broj otvorenih rekurzivnih DNS poslužitelja od koji dobar dio lažno odgovara. Koriste različite aktivne tehnike, uključujući i pretraživanje IPv4 prostora adresa u potrazi za otvorenim rekurzivnim poslužiteljima, kako bi utvrdili razmjer ovog problema, metode navođenja klijenata i posljedice. Kao čestu pozadinu ovog tipa prijevare prepoznaju financijsku dobit kompanija koje održavaju takve poslužitelje
4. [9] – pasivno prikupljen DNS promet koji dolazi do F korijenskog DNS poslužitelja autori analiziraju u potrazi za greškama i uzročnicima tih grešaka. Procjenjuju da je

količina DNS prometa koja stiže do korijenskih poslužitelja oko dva reda veličine veća od očekivane što zahtjeva daljnje istraživanje. Pronalaze čitav niz pogrešaka poput ponavljanja upita, neispravnih A upita, upita koji sadrže adrese iz lokalnog prostora, upita s neispravnim vršnim domenama itd. te utvrđuju neke od većih generatora neispravnog prometa. Dobar dio nepotrebnog prometa u vidu ponavljanja se pridržava DNS protokola, ali uzrok tolike količine ponavljanja nije pronađen. Autori sumnjaju da odgovori nikada ne stignu do klijenata

5. [10] – autori pomoću *tcpdumpa* sakupljaju DNS promet na granici sveučilišne mreže te ga kasnije koristeći baze podataka analiziraju kako bi utvrdili neobične pojave u ponašanju DNS prometa. Prepoznaju utjecaje alata za zaštitu od neželjene pošte na DNS promet što se očituje na povećanom broju A upita, što vezuju za DNS crne liste (*DNS black list, DNSBL*). Razmatraju i negativne utjecaje brzog toka i zauzimanja tipfelera (*typosquatting*) na DNS promet (iako u osnovi takve pojave nemaju za cilj DNS), te kako se promatranjem i analizom DNS prometa može prepoznati takav promet. Predlažu i jednostavan način utvrđivanja reputacije pojedinih domena i IP adresa poznavajući određene DNS zapise resursa i uzevši u obzir prethodno poznato ponašanje vezano za te zapise resursa poglavito NS zapis resursa
6. [11], [12] – u dva članka (2003., 2006.) vršena detaljna analiza pojave RFC 1918 IP adresa u DNS prometu. Mjerenje je vršeno na autoritativnom poslužitelju za RFC 1918 adrese, te više korijenskih poslužitelja, sakupljanjem prometa u više navrata i kasnijom analizom. Cilj je utvrditi karakteristike tog prometa (količinu, obrasce pojavljivanja, vremenske razdiobe, IP adrese i pristupe izvora itd.) te eventualne uzročnike. Krivce prepoznaju u različitim verzijama Windows operacijskog sustava odnosno implementacijama protokola dinamičkog ažuriranja DNS-a (*dynamic DNS updates, RFC 2136*). Utvrđuju i razdiobu po najčešćim autonomnim sustavima i najvećim generatorima tog prometa i utjecaj krajnjih korisnika na mnoge pokušaje ažuriranja korijenskih zona
7. [13], [14] – u dva članka (2008., 2010.) obrađuju podatke vezane za DNS iz tri godišnja promatranja prometa na Internetu (*Day in the Life of the Internet, DITL*), 2006., 2007., 2008. Mjerenja su vršena na više korijenskih poslužitelja, te poslužitelja vršnih domena. Promatraju niz pogrešaka u DNS prometu, trendove u pogreškama temeljene na razlikama u mjerenjima pojedinih godina, te moguće i najčešće uzročnike neispravnog prometa. Utvrđuju da gotovo 90% DNS prometa na korijenskim poslužiteljima nije ispravan i da neispravan promet raste brže od ispravnog koji se tijekom tri godine ispitivanja udvostručio. Razmatraju i utjecaje, odnosno moguće buduće utjecaje DNSSEC-a i IPv6 adresa na DNS promet
8. [15] – diplomski rad bavi se izradom sustava aktivnog praćenja DNS prometa temeljenom na promatranju niza poznatih čestih pogrešaka i sigurnosnih propusta DNS-a. Mjerenja su obavljena na dva fakultetska DNS poslužitelja (FER, FSB) na kojima je testirana funkcionalnost implementiranog sustava, njegove karakteristike, te je analiziran promet koji je na taj način prikupljen

3.3. Analiza pogrešaka u sustavu DNS

Iz ranije navedenih članaka i mjerenja, te samog DNS protokola moguće je utvrditi vrste nepoželjnog, neispravnog ili zlonamjernog DNS prometa. Slijedi detaljan opis i analiza svih tipova propusta, mogućih i najvjerojatnijih uzročnika, ozbiljnosti pojave takvog prometa, te mogućnosti penalizacije za izvore nepoželjnog prometa uzevši u obzir autonomni sustav kao razinu na kojoj se promatra promet:

1. *Odgovori na upite s greškom*

   Ovaj odgovor poslužitelja je zapravo ispravan promet koji sadrži poruku klijentu da je u originalnom upitu bila greške u formatu. U njemu je sadržan originalni upit što se može iskoristiti za korelaciju s pohranjenim upitima (ako se upiti pohranjuju) ili analizu uzroka greške, iako bi takva analiza bila ograničena jer greška možda nije u odjeljaku pitanja (engl. *question section*) DNS upita, koji se prepisuje u odgovor, nego drugdje u cijelom upitu. Razlog za postojanje upita s greškom u formatu može biti neispravno podešen klijent, ali i neispravno podešen poslužitelj koji ne zna ispravno interpretirati upit, a onda "ispravno", prema DNS specifikaciji, odgovara da je riječ o upitu s greškom u formatu.

   U principu ovdje je riječ o grubim greškama u formatu upita koje bi morao biti u stanju prepoznati bilo tko na putu upita, a time i anticipirati eventualni odgovor ovog tipa. Kada posjedujemo upit koji ima grešku u formatu očekujemo i adekvatan odgovor (čak i ako ne prolazi promatranim AS-om) te je potrebno penalizirati klijenta koji takve upite generira, ali ostaviti poslužitelja nekažnjenog. Grešku na poslužitelju nije moguće predvidjeti, odnosno, ako samo primamo odgovore od poslužitelja koji ukazuju na grešku u formatu, zbog neispravnog poslužitelja, to ćemo vidjeti tek u samom odgovoru koji će sadržavati odgovarajući RCODE, te će to ukazivati na grešku na poslužitelju koji treba biti penaliziran, dok klijent treba ostati nekažnjen.

   Da bismo postavili takav promet, osim navedenog treba uzeti u obzir i slučaj kada imamo samo jedan smjer korespondencije. Ako primimo originalni neispravni upit penaliziranje klijenta nije upitno, pazeći dakako na mogućnost lažiranja IP adresa, a poslužitelja u manjoj mjeri prema odabranom modelu penaliziranja (model – obje strane se penaliziraju). Ako primimo samo negativan odgovor poslužitelja, ali ne posjedujemo originalni upit klijenta, tada penaliziramo:

   1. poslužitelja – u manjoj mjeri polazeći od pretpostavke da radi ispravan posao – ako ta pretpostavka nije točna to će se s vremenom akumulacijom pogrešaka (a time i loše reputacije), koje će dotični krivo podešeni poslužitelj generirati, ispraviti
   2. klijenta – kao da je on kriv – ako ta pretpostavka nije točna to će se odraziti na klijenta samo jednom ili manji broj puta, pretpostavljajući da klijent razumije odbijene upite. Ako klijent pretjeruje s istim upitom neovisno o odbijenom upitu onda ionako treba biti penaliziran

   Idealna je situacija kada posjedujemo i upit i odgovor jer tada točno znamo tko je kriv te krivca penaliziramo jako, a drugu stranu malo (zbog ograničenja privremene memorije ili čak njenog nepostojanja vjerojatnije je da nećemo posjedovati oba

paketa). U relevantnim mjerenjima nije nađen velik broj ovakvih upita [6].

2. *Upiti koje odbija DNS poslužitelj (REFUSED)*

   Riječ je o ispravom prometu koji najčešće nastaje kada klijent od poslužitelja traži podatke koje zbog ograničenja politike nema pravo dobiti. Ponekad može doći do ekscesa ovakvog prometa. Obično je riječ o krivo podešenom klijentu koji neispravno tretira negativne odgovore, iako je moguće da klijent traži podatke na koje ima pravo, ali poslužitelj zbog krive konfiguracije odbija odgovoriti. Nije utvrđen velika količina ovakvog prometa [6].

   Kod penaliziranja treba uzeti u obzir da ne možemo utvrditi stranu odgovornu za ovaj promet. Čak i u idealnom slučaju kada bi posjedovali i originalni upiti i odgovor poslužitelja to bi nam vrlo rijetko bilo dovoljno da utvrdimo koja strana je kriva. Utvrđivanje krivca je moguće, ali samo detaljnim aktivnim analizama. Dodatni problem stvara mogućnost lažiranja IP adresa klijenta. Penaliziranje obje strane je adekvatno, pritom poslužitelja manje, a klijenta više. Klijent mora biti sposoban prepoznati negativan odgovor te će, ako je ispravno podešen, biti ukupno minimalno penaliziran, ako to nije u stanju onda ionako treba biti penaliziran. Poslužitelj je prisiljen odgovarati na sve upite te je time penaliziran svaki put kad klijenti griješe, ali zato njega manje penaliziramo. U slučaju da je on krivac greške tog tipa će se akumulirati s vremenom.

3. *Upiti koji su propušteni zbog greške na poslužitelju (SERVFAIL)*

   Ovaj tip odgovora šalje poslužitelj kada nije u mogućnosti riješiti upit jer:

   1. je označen kao poslužitelj za zonu, ali nije podešen kao poslužitelj za zonu
   2. je podešen kao poslužitelj za zonu, ali ne može doći do podataka za zonu – podatci ne postoje, podatci imaju greške, drugi poslužitelj nije proslijedio zonu
   3. poslužitelj mora dobiti odgovor od drugog poslužitelja koji ne odgovara (zbog greške u mreži) ili odgovara sa SERVFAIL i sl.

   Dakle, tri su moguća krivca za ovaj promet:

   1. poslužitelj koji je nadređen poslužitelju koji javlja SERVFAIL
   2. poslužitelj koji javlja SERVFAIL
   3. poslužitelj koji je podređen (ili posjeduje podatke) poslužitelju koji javlja SERVFAIL

   Svaki klijent i poslužitelj bi morao biti u stanju razumjeti ovakav negativan odgovor. Razumno je očekivati ponovljeni upit nakon ovakvog odgovora pod pretpostavkom da je greška privremena. Svejedno ovakav promet treba penalizirati jer je riječ o nepotrebnom prometu. Obje strane mogu biti krive:

   1. neki od poslužitelja je kriv jer nije ispravno podešen ili je nedostupan
   2. klijent je kriv ako učestalo ponavlja upit na koji je dobio negativan odgovor

   S obzirom da je riječ o ispravnom prometu i da se pretpostavlja da je problem privremen obje strane treba minimalno penalizirati. U slučaju da problem postoji dulje vrijeme to će se značajnije odraziti na reputaciju sustava. Poslužitelj koji dulje

vrijeme vraća SERVFAIL će sakupiti puno negativnih ocjena prometa tijekom tog vremena. Klijent bi s druge strane morao moći razumjeti negativan odgovor pa ako, unatoč negativnom odgovoru, uporno postavlja isti upit, također će, s vremenom, biti značajnije penaliziran.

Utvrđivanje krivca na poslužiteljevoj strani nije trivijalno, odnosno često i nemoguće. Primjerice, u prvom slučaju nemoguće je utvrditi zašto je neki poslužitelj označen kao poslužitelj za zonu, a on se tako ipak ne ponaša, odnosno, je li grešaka u njegovoj krivoj konfiguraciji ili je za to ipak kriva neispravna konfiguracija nadređenog poslužitelja.

Dalje, problem ove analize potencijalno mogu biti poslužitelji na putu upita. Teoretski je moguće da je greška, zapravo, u poslužitelju koji šalje odgovor, a koji, zbog vlastite greške, neispravno tvrdi da nije moguće doći do odgovora jer traženi poslužitelj ne odgovara, što je moguće kod rekurzivnih pretraživanja. Aktivnim ispitivanjem trivijalno je utvrditi ovaj slučaj međutim to bi podrazumijevalo ispitivanje svakog ovakvog odgovora barem jednim upitom prema poslužitelju za kojeg se tvrdi da je nedostupan. Osim povećanja ukupnog DNS prometa koje bi to ispitivanje prouzročilo, neželjeni rezultat bi također bila i negativna reputacija koju bi sakupljao sustav koji radi takvo ispitivanje, a koja bi se asimptotski približavala ukupnoj negativnoj reputaciji koju sakupljaju svi klijent koji pozivaju tog poslužitelja, a čije odgovore sustav bilježi.

4. *Upiti na koje uopće nije odgovoreno*

   Nije poznat uzrok relativno velikog broja upita na koje uopće nije odgovoreno. Neovisno o sadržaju upita, svaki upit bi morao dobiti nekakav odgovor, makar to bilo da takva domena ne postoji ili da upit ima grešku. Najjednostavniji način utvrđivanja da na neke upite nije odgovoreno je da se mjeri postotak upita i odgovora na granici neke mreže pri čemu bi idealan omjer broja upita i odgovora morao biti 1, odnosno 50% svaki. Ta metoda ima više problema:

   1. moguće postojanje odgovora na upite koji nikad nisu poslani koji povećavaju postotak odgovora
   2. mogući upiti prema korisnicima koji nemaju poslužitelje i ne mogu odgovoriti na upite što povećava postotak upita (skeniranje IP prostora)
   3. podrazumijeva da postoji samo jedna granica mreže na kojoj se prati promet
   4. potvrđuje postojanje nesrazmjera, ali ne govori ništa o konkretnim paketima koji nedostaju
   5. lažiranje IP adresa izvora unutar promatrane mreže generira odgovor koji ne stiže natrag u mrežu

   Na razini autonomnog sustava teško je pratiti ovakav promet jer:

   1. u općenitom slučaju autonomni sustav ima više linija kojima prima i šalje promet
   2. odgovor ne mora prolaziti kroz autonomni sustav

   Ipak, kako je riječ o dosta grubim pogreškama, takve slučajeve bi ipak trebalo

kažnjavati kad je moguće. Reputacijski sustav ne može prepoznati takav promet za upite za koje je tranzitan, ali ga može utvrditi za upite korisnika unutar vlastitih granica na koje nije odgovoreno. Dodatni je problem što nije moguće utvrditi krivca jer ne znamo gdje je upit ili odgovor "zapeo". Može se penalizirati susjedne autonomne sustave jer s njih nam treba doći odgovor, te posebno autonomni sustav kojem smo poslali upit. Svejedno ako nije realno da će reputacijski sustav bilježiti sve upite svojih korisnika i čekati odgovore kako bi postavio reputaciju onda je *model penaliziranja svog DNS prometa* adekvatan odgovor (vidi poglavlje 3.4.).

5. *Upiti koji traže nepostojeće domene (NXDOMAIN)*

   Ovdje je riječ o ispravnom, ali nepoželjnom prometu koji predstavlja osnovnu pogrešku koju bi očekivali prilikom promatranja pogrešaka DNS protokola. Osim očekivanih tipfelera, veliki dio ovog prometa nastaje zbog drugih razloga:

   1. nepostojeće inverzno preslikavanje (*mapping*) adresa *in-addr.arpa* PTR upita
   2. korištenje DNS-a za pohranjivanje podataka crne liste neželjene pošte (*spam blacklist, DNSBL)* prema DNSBL specifikaciji

   Kao i sve druge negativne DNS odgovore, i ovaj možemo tretirati kao zapravo nepoželjan DNS promet, a pri tome ga minimalno kažnjavati. U najjednostavnijem slučaju kada je riječ o tipfelerima, krivac je klijent koji šalje takav promet; kako je za pretpostaviti da korisnik neće mnogo puta ponavljati istu grešku, to neće značajnije utjecati na ukupnu reputaciju. Kod nepostojećih inverznih preslikavanja opet treba kažnjavati klijenta te u manjoj mjeri i poslužitelja. Jednim dijelom ovo je krivnja poslužitelja, jer bi bilo i za očekivati da će vratiti odgovarajući inverzni odgovor, ali kako klijenti mogu postaviti inverzan PTR upit za bilo koju IP adresu, od kojih mnoge nemaju domenu, odgovornost je na njima, jer su poslužitelji dužni odgovoriti na svaki upit.

   Promet koji nastaje zbog DNSBL-a je s jedne strane ispravan promet, a s druge strane čak može biti tretiran i kao poželjan. Upiti upućeni prema DNSBL poslužiteljima imaju sličnu strukturu kao i inverzni PTR upiti samo što za domenu ne koriste *in-addr.arpa* već domenu samog DNSBL poslužitelja na koju se dodaje obrnuta IP adresa za koju se traže podatci te je upit tipa A, a ne PTR. Kada neki DNSBL poslužitelj odgovara sa NXDOMAIN to znači da na traženoj IP adresi nema zabilježenog poslužitelja neželjene pošte, inače odgovara adresom. Iako bi inače kažnjavali NXDOMAIN odgovore jer je riječ o "nekorisnom" prometu, ovdje se radi o pokušaju utvrđivanja šalje li određeni poslužitelj elektroničke pošte neželjenu poštu, odnosno, ima li na nekoj IP adresi zabilježen poslužitelj neželjene pošte. Poželjno je nagrađivanje i klijenta i poslužitelja. Ipak reputacijski sustav onda mora biti u stanju raspoznati ovaj promet od uobičajenih NXDOMAIN negativnih odgovora.

   Dio NXDOMAIN odgovora nastaje zbog PTR upita za adrese iz RFC 1918 prostora, upita za nepostojeće vršne domene te A upiti koji već sadrže IP adresu (tzv. A za A), no oni su obrađeni kasnije.

6. *Upiti čija vrsta nije implementirana na DNS poslužitelju*

DNS protokol propisuje standardni odgovor na upite koji traže funkcionalnost koja nije implementirane na poslužitelju. Kako je dodavanje novih funkcionalnosti predviđeno protokolom, a neke osnovne funkcionalnosti su zajedničke svim poslužiteljima očekivano je postojanje poslužitelja koji nemaju sve funkcionalnosti implementirane. Primjerice, [2] je podrazumijevao postojanje IQUERY upita kao opcionalne funkcionalnosti za koji se kasnije pokazalo da nije doživjela širu implementaciju niti upotrebu. IQUERY je proglašen zastarjelim (RFC 3425) i za njega je potvrđen predviđen odgovor poslužitelja "nije implementiran".

Nisu poznati najčešći razlozi postojanja ovakvog prometa. Kako nije uočen veliki broj ovakvih upita ovo se može smatrati nepoželjnim prometom, ali koji ne treba pretjerano kažnjavati. Možemo kriviti poslužitelja jer nije ažuriran da podržava sve funkcionalnosti, međutim, kako je moguće i da klijent traži neku od funkcionalnosti koje su opcionalne ili čak zastarjele (a time se ne preporuča njihovo korištenje), krivnja može biti na bilo kojoj strani. Utvrđivanje krivca bi, dakle, zahtjevalo dublje analize upita što navodi na mogućnost jednakog penaliziranja obiju strana minimalnim kaznama.

7. *Upiti za lokalne adrese - RFC 1918*

   Ovdje je riječ o grubom pogreškama koje jednim svojim dijelom izlaze izvan definicije DNS protokola, ali su zato dobrim dijelom potencirani DNS prometom. IP adrese iz prostora definiranih RFC-om 1918 služe za korištenje unutar lokalnih mreža i ni u kom slučaju ne bi smjele izlaziti izvan lokalnih mreža na Internet. Kod DNS upita one se mogu pojaviti u dva oblika:

   1. izvor DNS upita je adresa iz RFC 1918 prostora
   2. sadržaj upita je PTR na adresu iz RFC 1918 prostora

   Prvo je kršenje RFC-a 1918 i nema direktno veze s DNS-om, iako se vrlo često pojavljuje na UDP paketima koji prenose DNS promet. Drugo predstavlja DNS upite na koje je nemoguće odgovoriti, odnosno odgovor je NXDOMAIN, jer traže ime domene prijavljene na IP adresi iz RFC 1918 prostora koje ne postoji. Pritom se ove dvije situacije međusobno ne isključuju već mogu dolaziti zajedno u upitu.

   Prema RFC 1918 zadatak je ISP-a da filtrira promet koji ima za izvorišnu adresu adresu iz RFC 1918 prostora. Ako takav promet nastavi do DNS poslužitelja on nije u mogućnosti odgovoriti jer ne zna kome. Krivci su dakle svi autonomni sustavi koji propuštaju taj promet i trebaju biti penalizirani.

   Za DNS su karakteristični pokušaji pronalaska imena domene prema poznatoj IP adresi koristeći PTR tip upit za preslikavanje, tzv. inverzni upit. Međutim kada je kao IP adresa predana adresa iz RFC 1918 prostora tada poslužitelji mogu samo odgovoriti sa NXDOMAIN jer to nije skup adresa na kojima može biti registrirana domena. Krivac je pritom isključivo krivo podešen klijent koji šalje upit i njega treba strože penalizirati. Ako taj upit ima i izvorišnu adresu iz RFC 1918 prostora adresa onda opet treba penalizirati sve autonomne sustave za koje znamo da je kroz njih prošao paket.

   Poseban slučaj ovog problema su dinamička ažuriranja (*dynamic updates*) DNS-a

koja su obrađena kasnije. Također mogući su i A upiti za IP adresu iz RFC 1918 prostora te oni potpadaju pod A za A pogrešku.

8. *Nepostojeće vršne domene (TLD)*

   Slično kao i kod upita koji traže nepostojeće domene i ovdje je ponekad riječ o tipfelerima. Međutim istraživanja [7], [13] pokazuju da se velika količina tog prometa ne može pripisati tipfelerima već neispravnim podešenjima u poslužiteljima i klijentima ili greškama u programskoj podršci. Česte tražene neispravne vršne domene su tipa: .localhost, .invalid, .local, .lan, .home, .domain, .localdomain i sl. što ukazuje na programsku podršku koja krivo tumači uobičajene nazive za "lokalne" (i *loopback*) domene. Također uočene su i greške na programskoj podršci koja neispravno "dopunjava" nepotpuno ili neispravno definirane domene lokalnih DNS podataka, kao i neispravno građenje imena domena na temelju pojedinih protokola (*web proxy auto discovery protocol, wpad*).

   Velika količina ovog prometa je problematična i zbog činjenice da nije riječ o povremenoj ljudskoj pogrešci već ugrađenim pogreškama programske podrške koje se dodatno potenciraju učestalim ponavljanjem istih upita, što je također uobičajeno za programe.

   Krivci su isključivo klijenti koji postavljaju takve upite. Druga strana komunikacije su korijenski poslužitelji koji su dužni odgovarati na svaki ovakav upit i koje se ne može penalizirati (ovdje ipak pretpostavljamo da korijenski poslužitelji imaju točan popis vršnih domena iako je teoretski moguće da je u njima pogreška). Kako je riječ o gruboj pogrešci koja opterećuje korijenske poslužitelje, krivce bi trebalo strože penalizirati. Sama činjenica da je nastanak takvih pogrešaka najčešće automatiziran, jer svoju osnovu imaju u programskoj podršci, navodi na zaključak da će klijenti koji će generirati veliki broj takvih upita brzo utjecati na reputaciju sustava, no svejedno moguća je i opcija da se dodatno kažnjava klijente za koje se utvrdi da proizvode zaista mnogo takvog prometa.

9. *A upiti za IP adresu (A za A)*

   Na razini korijenskih poslužitelja uočen je veliki broj upita koji kao ime upita već imaju zadanu IP adresu za koju se onda traži adresa – A za A. S obzirom da upit koji u imenu ima oblik IP adrese zapravo ne krši specifikaciji DNS protokola, jer su brojevi i točke uobičajeni (dopušteni) u DNS imenima, klijenti i poslužitelji prosljeđuju tako krivo oblikovane DNS upite do korijenskih poslužitelja. Korijenski poslužitelj tada pregledavajući zadnju oznaku (labelu) upita, prepoznaje broj u rasponu 0 – 255 kojeg nema na popisu vršnih domena i na upit odgovara sa NXDOMAIN, odnosno, nepostojeća domena. Pritom adresa ponekad može biti iz RFC1918 prostora što čini dvostruki propust.

   Najčešći uzroci ovog prometa su neispravno podešeni klijenti ili, općenito, propusti u programskoj podršci, DSL sklopovlje, vatrozid (sigurnosna stijena), ali i, što je najproblematičnije, neki virusi koji napadaju Windows sustave. Ponekad je riječ o klijentima koji ne prepoznaju IPv6 adrese nego ih smatraju imenima domena za koje treba tražiti adresu. Zbog velikog broja takvih upita na razini korijenskih poslužitelja, glavni razlozi su vjerojatno zaražena računala te neispravna

programska podrška, u pravilu Windows operacijskog sustava.

Krivac je klijent koji šalje takav promet te bi ga trebalo strogo penalizirati jer on može ukazivati da je riječ o zaraženom računalu. Također, kažnjavati bi se moglo i autonomne sustave na putu paketa jer su svi u stanju prepoznati ovaj neispravan promet koji opterećuje korijenske poslužitelje. Drugu stranu komunikacije, korijenske poslužitelje, ne može se penalizirati.

10. *Upotreba pristupa 0*

    Neke verzije BIND DNS poslužitelja dopuštaju da se pristup (*port*) izvora podesi na 0, što krši DNS specifikaciju koja predviđa da pristup bude "visoki" slučajni broj. Općenito pristup 0 je rezerviran i ne smije se koristiti ni za UDP niti za TCP promet te je tu zapravo riječ o administratorskoj pogrešci. Poslužitelji koji primaju takav promet, u pravilu odbijaju na njega odgovoriti (na razini korijenskog poslužitelja to su BIND poslužitelji), što može objasniti neke od upita na koje nikad nije odgovoreno.

    Penalizirati treba samo klijenta koji postavlja upit, a ako bi neki od poslužitelja odgovarao na takav upit penalizirati bi trebalo i njega, ali u manjoj mjeri.

11. *Dinamičko ažuriranje zapisa resursa na DNS poslužitelju*

    DNS je originalno zamišljen kao protokol koji koristi statički podešene podatke koji se rijetko mijenjaju. Razvojem tehnologije pojavila se potreba za mogućnošću dinamičke, odnosno automatske, promjene DNS zapisa, prvenstveno IP adresa. Primjer su poslužitelji koji često mijenjaju IP adrese koje im dodjeljuje ISP putem DHCP protokola, ili mobilni poslužitelji. Dinamičko ažuriranje DNS zapisa je nadogradnja DNS protokola koja to omogućuje.

    Zbog neispravnih DNS implementacija, dinamičko ažuriranja lokalnih DNS zapisa bježi na Internet i završava na korijenskim poslužiteljima. Greška je u pravilu u Windows DNS programskoj podršci koja periodički generira zahtjeve za ažuriranjem korijenskih zona, što je, obzirom na brojnost zahtjeva i njihovu razdiobu u vremenu, usporedivo s DDoS (distribuirani DoS) napadom [11]. Često takav promet sadrži RFC 1918 adrese u svojim zahtjevima i time doprinosi i tom problemu.

    Krivci su klijenti koje treba strože kažnjavati, ako je moguće i one na putu prometa.

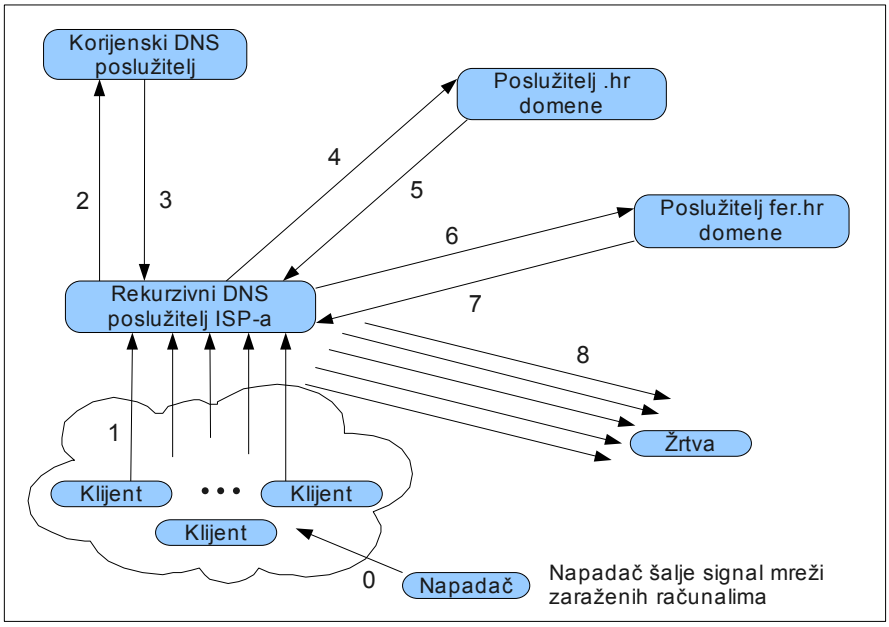
12. *DoS napadi*

    DNS protokol je moguće koristiti za DoS napade reflektirajući promet preko korijenskih poslužitelja prema žrtvi. Napad se ostvaruje lažiranjem IP adresa izvora DNS upita. Napadi mogu biti usmjereni i prema samom korijenskom poslužitelju, ali često tako nešto zapravo nije namjera nego posljedica DoS napada usmjerenog drugdje, a koji onda koristi korijenske poslužitelje kao dodatnu snagu.

    [7] uočava dvije vrste DoS napada. Prva je klasični napad lažiranjem IP adresa koji se reflektira preko korijenskih poslužitelja prikazanog na slici 3.3, a drugi je napad koji podsjeća na skeniranje prostora IP adresa.

    Drugi napad otkriven je naknadnom analizom prometa sortirajući ga po upitima

pojedinih poslužitelja, pri čemu je uočeno da određeni poslužitelji generiraju veliku količinu prometa naoko nikad ne ponavljajući upit. Upiti su sadržavali inverzne PTR upite koji su zbog neponavljanja IP adresa izgledali kao skeniranje IP prostora. Zadnji broj svake IP adrese uvijek je jednak i zapravo predstavlja napadačevu skriptu, iako bi se moglo čini kao da je riječ o neispravno okrenutoj IP adresi pri skeniranju IP prostora.



Slika 3.3. Reflektiranje DDoS napada koristeći DNS poslužitelje

DoS napade bi svakako trebalo najstrože penalizirati, no tu imamo dva problema:

1. često korištenje lažiranja IP adresa tijekom napada
2. ponekad zahtjevne analize potrebne za njihovo prepoznavanje

Zbog lažiranja IP adresa, otežano ili čak onemogućeno otkrivanje krivca za napad, te ponekad možemo samo načelno znati iz kojeg smjera, odnosno, kojeg susjednog autonomnog sustava napad dolazi.

Naknadnom analizom moguće je utvrdit postojanje DoS napada, ali pritom treba uzeti u obzir velike resurse koji bi za tako nešto bili potrebni i kompleksnost zadatka koji je time postavljen pred reputacijski sustav koji bi takvu analizu morao radit automatski. Specifični "potpisi" pojedinih napada obično postoje, ali je njihovo prepoznavanje kompliciran zadatak koji podrazumijeva i opasnost da se inače legitiman promet neispravnim tumačenjem okarakterizira kao DoS napad. Neka obilježja ipak mogu ukazivati na DoS napad, poput neobično velike količine prometa određenog poslužitelja koji sadrži iste ili slične upite, velika količina prometa usmjerena prema pojedinim poslužiteljima za koje se ne može utvrditi da su taj promet i prouzročili, puno upita različitog sadržaja s nekim zajedničkim karakteristikama koji dolazi od pojedinog poslužitelja i sl.

U slučajevima da se može utvrditi krivac, bilo da je riječ o jednom odnosno nekoliko poslužitelja, ili da je riječ o distribuiranoj mreži zaraženih računala, njega

se treba najstrože penalizirati. To vrijedi i za sve koji takav promet prosljeđuju.

13. Upiti s nepostojećim (nedopuštenim) znakovima

Prema RFC 1035 jedini dopušteni znakovi u DNS imenu su slova engleske abecede, brojevi i "-" (povlaka). Točka služi za razdvajanje labela. Međutim, u određenom broju upita u različitim mjerenjima primijećeno je pojavljivanje nedopuštenih znakova u DNS upitima. Iako nema sigurnog objašnjenja vjerojatno je riječ o tipfelerima i unosu specifičnih znakova abeceda ili pisama pojedinih zemalja. Poseban slučaj predstavljaju upiti koji sadrže "_" (donja crtica), jer je primijećen posebno velik udio upravo takvih upita u skupu upita koji koriste nedopuštene znakove, [13]. Ovdje se tretiraju kao ista greška.

Od 2009. uvođenjem IDNA (*internationalized domain name in applications*, međunarodni nazivi domena u aplikacijama), definiran je standard za prikazivanje specifičnih pisama unutar programske podrške, a da se istovremeno poštuje DNS protokol. Prve domene s takvim znakovima puštene su u promet 2010. godine. Može se pretpostaviti da će IDNA standard s vremenom smanjiti broj upita koji sadrže nedopuštene znakove, iako bi zapravo, barem u početku, mogao i povećati uzevši u obzir inicijalni period prilagodbe programske podrške novim standardima, te zastarjelu programsku podršku koja nije ažurirana.

Kriv je izvor kojeg ne treba pretjerano penalizirati.

14. Upit nepostojećeg razreda

DNS protokol predviđa pet dopuštenih razreda upita (*query class*) to su: IN (1), CH (3), HS (4), NONE (254), ANY (255). S druge strane, za polje razreda upita predviđeno je 16 bita, te su preostali bitovi slobodni za naknadna dodjeljivanja. Uzrok pojave upita koji sadrže nepostojeće razrede nije utvrđen, iako su takvi upiti primijećeni na razini korijenskih poslužitelja. Njihova brojka nije velika u usporedbi s količinom ostalih upita, odnosno, s količinom pogrešaka koje su primijećene na razini korijenskih poslužitelja [9]. Određeni raspon brojeva unutar polja razreda upita je definiran za privatnu uporabu (*private use*), što bi možda moglo objasniti neke od grešaka koje su uočene, tako što, teoretski, lokalno definirani razredi upita "bježe" ili su primijećeni na internetu gdje nisu definirani, međutim, ta hipoteza nije provjerena.

U konačnici, vjerojatno je riječ o neispravnoj programskoj podršci koja generira neispravne zahtjeve. Kriv je klijent s kojeg dolazi takav promet te ga ne bi trebalo prestrogo penalizirati.

15. Identični upiti

Velika količina prometa koji možemo smatrati neispravnim, spada u jednu od tri srodne kategorije: identični upiti, ponovljeni upiti, i nepohranjeni odgovori (zadnja dva su obrađena kasnije). Gledano izolirano, svaki pojedini ovakav paket predstavlja ispravan promet. Nepoznat je uzrok velike količine ovakvog prometa, ali se može pretpostaviti da se ponavljanje može pripisati uzrocima poput:

1. mreža koja ne osigurava dospijeće paketa
2. krivo podešeni klijenti

3. klijenti ili poslužitelji koji ne razumiju određeni odgovor (npr. SERVFAIL, [7])
4. klijenti koji ne pohranjuju odgovore ili negativne odgovore; često primijećeno na Microsoft programskoj podršci
5. upiti na koje uopće nije moguće odgovoriti, npr. upiti s RFC 1918 adresama u izvoru, a koji se onda uporno ponavljaju
6. neispravni poslužitelji
7. mrežna oprema i programska podrška koja neispravno ograničava (filtrira) dospijeće odgovora
8. prekratko čekanje na odgovor. Iako ovo vrijedi samo za manji broj slučajeva, [9]
9. pogreške podešenja zona

Nije isključena i mogućnost napada, npr. DoS, koji bi koristio ovakav "potpis".

Identični upiti imaju identičan razred (*class*), tip (*type*), ime (*name*) i ID polje upita. Protokolom nije propisano da ID polje mora biti u svakom upitu različito, ali se sugerira da se ID polje koristi za razlikovanje pojedinih upita, što bi ukazivalo na mogućnost i potrebu promjene ID polja svakog upita. Kod ponavljanja upita na koje nije odgovoreno, preporuka je da bi program morao biti u stanju prepoznati odgovor na bilo koji od upita koje je postavio.

Ponavljanja upita su nepotrebna, pa se promet ovog tipa se može smatrati neispravnim. Prihvatljivo i razumljivo bi bilo povremeno ponavljanje nekog upita na koji nije odgovoreno, međutim, u mjerenjima [9], [13] je utvrđeno veliko zagađenje DNS prometa upravo upitima koji se ponavljaju, bilo kao identični ili ponovljeni upiti. To navodi na potrebu penaliziranja klijenata koji generiraju ovakav promet.

Međutim, pred reputacijski sustav je postavljen problem prepoznavanja ovakvog prometa. Trivijalno je utvrditi ponavljanje naknadnom analizom sakupljenog prometa, međutim, kada govorimo o dodjeljivanju reputacije u trenutku dok promatramo promet, prepoznavanje ponavljanja postaje mnogo kompliciranije i podložnije parametrima samog promatranja. Privremena memorija je nužna kako bi se usporedbe pojedinih paketa uopće mogle vršiti. Na prepoznavanje ponavljanja će, prvenstveno, utjecati dva intervala:

1. vrijeme kojim definiramo donju granicu dopuštenu za ponavljanje
2. trajanje zadržavanja paketa u privremenoj memoriji

Ako je sustav u stanju prepoznati ponavljanje, treba ga strože penalizirati. Time bi se penaliziralo i opravdana ponavljanja, međutim, takva ponavljanja će se pojavljivati mnogo rjeđe i neće značajnije utjecati na konačnu reputaciju sustava. Klijenti koji generiraju puno identičnih upita jače će utjecati na reputaciju AS-a. Uz pretpostavku sustava koji neograničeno (ili vrlo dugo) pamti pakete, moguće je i postrožavanje kažnjavanja s vremenom i količinom paketa.

U slučaju da sustav nije tako izveden, nameće se drugi model kažnjavanja, tako što

bi se sav DNS promet, neovisno ispravan ili neispravan, kažnjavao u minimalnoj količini. Identični upiti, kao oblik zagađenja ispravnim DNS prometom, tako bi, zbog velike količine tog prometa, opet jače utjecali na reputaciju sustava.

16. Ponovljeni upiti

Kao ponovljeni upit možemo prepoznati svaki upit koji ima polja razreda, tipa i imena identična nekom ranijem upitu. Razlikuju se od identičnih upita po tome što nemaju jednako ID polje. Ponovljeni upiti također čine veliki dio DNS zagađenja ispravnim, a nepotrebnim prometom. Analize prometa identičnih upita potpuno se preslikavaju i na ponovljene upite. Protokolom je propisano čekanje na ponavljanje upita između 2 – 5 sekundi. Istraživanja su pokazala da se glavnina klijenata pridržava tog pravila te ponavlja upite u prosjeku svakih 4 sekunde, [9]. Razlog postojanja velike količine ponovljenih upita, jednako kao i kod identičnih upita, nije jasan, a to je potencirano činjenicom da se većina klijenata pridržava protokola kada su u pitanju ponavljanja upita.

Problemi bilježenja ponavljanja su identični kao kod identičnih upita.

Kriv je klijent koji generira ponovljene upite. Moguće metode penalizacije su identične kao i kod identičnih upita.

17. Nepohranjeni odgovori

Poseban slučaj ispravnih, a nepotrebnih upita su nepohranjeni odgovori (*referral not cached*). Kada neki klijent, pri iteritivnom pretraživanju, postavi upit za određenu domenu, on dobiva, osim adrese domene koju traži, i adrese autoritativnih poslužitelja za pojedine nadređene domene. Primjerice, ako klijent traži neku domenu unutar *com* zone, dobiva i adresu autoritativnog poslužitelja za *com* zonu. Kod nepohranjenih odgovora imamo slučaj da klijenti, nakon što su dobili podatke za neku zonu, nisu u stanju iskoristiti te podatke za sljedeći upit i time smanjiti broj upita.

Prepoznavanje ovakvih upita zahtjeva posjedovanje privremene memorije, te mogućnost analize tako pohranjenog prometa u kojem bi se tražili upiti za iste zone od strane istog klijenta, a koji bi bili upućeni u određenom kraćem vremenskom razdoblju za koje je razumno pretpostaviti da TTL (*time to live*) nije istekao. Posebno analizu komplicira činjenica da poslužitelj, koji je autoritativan za određenu zonu, može također biti autoritativan za podzone svoje zone što je slučaj kod korijenskih poslužitelja [9]. Komplikacije koje postoje kod uočavanja identičnih i ponovljenih upita postoje i kod nepohranjenih odgovora.

Razlog nepohranjivanja autoritativnih podataka nije poznat, ali vjerojatno je riječ ili o krivo podešenoj programskoj podršci ili programima koji se ne pridržavaju propisanog ponašanja kod pohranjivanja odgovora.

Klijent je krivac i trebalo bi ga strože penalizirati.

18. Neželjena pošta, alati protiv neželjene pošte, brzi tok

Sakupljanjem prometa i kasnijom analizom moguće je utvrditi utjecaj neželjene pošte, odnosno alata protiv neželjene pošte (*anti-spam*) na DNS promet. Mjerenja su pokazala [10] da veliki dio prometa koji sadrži A upite, ne pripadaju očekivanim

DNS aktivnostima, nego pripadaju alatima za borbu protiv neželjene pošte. Alati protiv neželjene pošte koriste A upite prema DNSBL poslužiteljima kako bi utvrdili dolazi li neka elektronička pošta s poznatih poslužitelja neželjene pošte (vidi poglavlje 3.3. - *5. NXDOMAIN*).

Ovaj porast A upita, kako je već ranije rečeno, može se smatrati poželjnim prometom jer se radi o pokušaju zaustavljanja neželjene pošte. S druge strane, ipak je riječ o povećanju DNS prometa ne direktno vezanog za uobičajene DNS uporabe. Takav promet možda ne treba direktno penalizirati kao neželjen promet, ali ako bi reputacijski sustav koristio penalizranje svog DNS prometa i taj promet bi sakupljao puno negativne reputacije s vremenom. To ponovno navodi na potrebu razlikovanja povećanja nastalog kao posljedica poželjnih aktivnosti (kojima bi se pritom mogla davati i pozitivna reputacija), te povećanja nastalog zbog nepoželjnih aktivnosti koje bi se pored uobičajenog penaliziranja svog prometa još dodavali posebni penali kada je sa sigurnošću moguće prepoznati takav promet.

Poseban su slučaj domene brzog toka (*fast flux domain*) koje se često koriste kao potpora generatorima neželjene pošte, pri skrivanju originalnih krivaca za napade ili neželjenu poštu te izbjegavanje registriranja na crnim listama (*blacklist*). Prijavljena domena stalno mijenja A zapise resursa te se time svaki put prijavljuje kao drugi poslužitelj, odnosno druga IP adresa. Brzi tok se može prepoznati po kratkim TTL-ovima A zapisa resursa (druga jednostavna metoda prepoznavanja brzog toka podrazumijeva sortiranje veće količine sakupljenog prometa prema broju A zapisa resursa po domeni pri čemu će domene brzog toka imati veliki broj A zapisa resursa, nedostatak je nemogućnost provođenja u realnom vremenu, vidi [8]). DNS je time pogođen jer izrazito kratki TTL-ovi zapisa tjeraju žrtve da učestalo šalju upite kako bi saznali nove adrese poslužitelja.

TTL je, dakle, moguće koristiti kao pokazatelj mogućih napada ili zlonamjernog prometa. Pristup bi pritom bio penalizirati DNS poslužitelje koji sadrže zapise s niskim TTL-om.

"Anomalije" DNS prometa koje su prouzrokovane zlonamjernim radnjama poput neželjene pošte ili domena brzog toka treba najstrože kažnjavati. S druge strane, pokušaje borbe protiv tih "napada" trebalo bi nagrađivati pozitivnom reputacijom.

19. Zastarjeli i eksperimentalni upiti

DNS protokol dopušta proširenja koja obično počinju kao eksperimentalni dodatci protokolu. Postojanje takvog prometa nije upitno, ali se ne može opravdati njegovo "bježanje" na Internet, niti se može smatrati poželjno izvan granica testnog okruženja.

Zastarjeli upiti predstavljaju funkcionalnosti koje se više ne koriste ili je s vremenom utvrđeno kako ta funkcionalnost nije postigla značajniji upotrebu ili implementaciju. Također, to se odnosi i na funkcionalnosti koje su zamijenjene novim poboljšanim ili promijenjenim verzijama.

Oba prometa možemo smatrati nepoželjnim: eksperimentalne upite zato što opterećuju sustav, a zastarjele jer ukazuju na programsku podršku koja nije ažurirana ili na potencijalne sigurnosne prijetnje ili propuste koje to može nositi.

Krivac je klijent koji postavlja upit, ali ne treba biti prestrogo kažnjen. Poslužitelj na takve upite treba odbiti odgovoriti (npr. u slučaju IQUERY koji je također zastario poslužitelj odgovara RCODE 4, "*not implemented*"), a ako to ne čini, treba biti kažnjen.

Postavljajući skalu ocjena od 1 do 10 možemo ocijeniti pojedini neispravni paketa, odnosno, utvrditi negativnu ocjenu koju paketu donosi pojedina pogreška. Tablica 3.1 u prvom stupcu sadrži vrstu pogreške, a u drugom i trećem stupcu negativne ocjene koje pojedina pogreška donosi klijentskoj i poslužiteljskoj strani. Ocjena 0 znači da se dotična strana ne penalizira.

Tablica 3.1. Ocjena pogrešaka klijenta i poslužitelja

Pogreška	Klijent	Poslužitelj
Odgovori na upite s greškom	- 4	- 1
Upiti koje odbija DNS poslužitelj (REFUSED)	- 4	- 1
Upiti koji su propušteni zbog greške na poslužitelju (SERVFAIL)	- 2	- 4
Upiti koji traže nepostojeće domene (NXDOMAIN)	- 3	- 1
Upiti čija vrsta nije implementirana na DNS poslužitelju	- 3	- 2
Upiti za lokalne adrese – RFC 1918	- 5	0
Nepostojeće vršne domene (TLD)	- 6	0
A upiti za IP adresu (A za A)	- 6	0
Uporaba pristupa 0	- 3	- 2[1]
Dinamičko ažuriranje zapisa resursa na DNS poslužitelju	- 5	0
DoS napadi	- 10	0
Upiti s nepostojećim (nedopuštenim) znakovima	- 3	0
Upiti nepostojećeg razreda	- 4	0
Identični upiti	- 6	0
Ponovljeni upiti	- 5	0
Nepohranjeni odgovori	- 5	0
Neželjena pošta, alati protiv neželjene pošte, brzi tok	- 2	- 9
Zastarjeli i eksperimentalni upiti	- 3, - 2	0, - 3[2]

Osim gore navedenih pogrešaka, literatura sadrži niz dodatnih mjerenja koja ne podrazumijevaju klasične neispravnosti u DNS prometu, ali koja mogu biti korisna za razumijevanje problema DNS protokola, ili načina na koji se DNS koristi kao potpora drugim sigurnosnim prijetnjama. Ta mjerenja prikazana su u dodatku, poglavlje

1 Klijenta kažnjavamo samo kada primijetimo upit s pristupom 0, a poslužitelja samo kada primijetimo takav odgovor. Kod primijećenog odgovora, klijenta ne treba penalizirati jer on nije kriv za odgovor. Poslužitelj ne smije odgovarati na takve upite, pa je to isključivo njegova krivica.

2 Kod zastarjelog ili eksperimentalnog upita penaliziramo klijenta, dok poslužitelja ne penaliziramo. Kod odgovora ovog tipa penaliziramo poslužitelja ako ne odgovori sa *not implemented*, a klijenta u manjoj mjeri jer je moguće već ranije bio penaliziran.

3.4. Dodjeljivanje ocjena DNS prometu

U daljnjem razmatranju, u svrhu razumljivosti, autonomni sustav koji implementira predloženi reputacijski sustav i na kojem se vrši mjerenje nazivati ćemo *AS0*, klijentov autonomni sustav nazivat ćemo *ASK*, a poslužiteljev *ASP*. Osim toga, analiza mogućih penalizacija prometa će biti općenita u odnosu na autonomne sustave, pa se podrazumijeva promatranje prometa AS0, kao i postavljanje reputacije AS0. U realnim izvedbama reputacijskog sustava, svaki AS bi mogao ignorirati pogreške prometa generiranog unutar vlastitih granica, ali mi ćemo ih u svrhu općenitosti ipak uzimati u obzir. Računanje reputacije AS0 može služiti samom AS0 kako bi približno procijenio koju reputaciju okolni AS-ovi njemu pridjeljuju.

DNS promet, promatran s razine AS-a, možemo dijeliti u dvije osnovne kategorije s obzirom na izvor, tj. odredište paketa:

1. promet kojem je AS0 izvor ili odredište
2. promet u kojem je AS0 tranzitan u odnosu na izvor i odredište.

Prvi problem na koji nailazimo kod promatranja DNS prometa je mogućnost lažiranja IP adresa. DNS promet se prvenstveno prenosi UDP protokolom na kojem je lažiranje IP adresa trivijalno. Zato treba prvo razmotriti probleme koje lažiranje IP adresa unosi u analizu. Promet koji je usmjeren korisnicima ili poslužiteljima unutar AS0 odnosno koji dolazi iz AS0, jednostavniji je za promatranje i ocjenjivanje. Idealan slučaj je promet koji generiraju klijenti unutar AS0. Za takav se promet gotovo sigurno može utvrditi i izvor i odredište, a prema tome i eventualne penalizacije, ako je takav promet neispravan. Kada su izvor vlastiti korisnici, postoji mogućnost lažiranja IP adresa:

1. lažirana IP adresa je također iz AS0 te je ponašanje reputacijskog sustava u krajnju ruku jednako jer je za reputaciju nebitno tko unutar AS0 šalje lažirani promet (pažnju ipak treba obratiti na ovakav promet jer je potencijalno riječ o nekoj vrsti napada, uključujući i DoS napad)
2. lažirana IP adresa je izvan AS0. Da bi se prepoznalo ovakvo lažiranje, potrebna je privremena memorija na svim granicama AS0 kako bi se moglo potvrditi da promatrani paket nije primijećen na nijednoj od ostalih ulaznih linija te da, dakle, nije došao izvana, već je nastao u AS0. Takav pristup bi stvarao velika opterećenja na memoriji i procesorskom vremenu senzora koji promatraju granice sustava, a zbog relativno složenog procesa ispitivanja postojanja traženog paketa, kod ostalih senzora bi se povećalo opterećenje prospusnog pojasa

Nesigurnost unosi i mogućnost napada čovjekom u sredini (*man-in-the-middle*). Promet koji nastaje izvan AS0, a usmjeren je poslužiteljima unutar AS0, ima sigurno samo odredište prometa te se također može utvrditi susjedni AS s kojeg je promet neposredno došao. Zbog mogućnosti lažiranja izvorišnih adresa ne može se sa sigurnošću utvrditi izvor prometa.

Kompliciraniji slučaj imamo kada se AS0 nalazi na putu nekog paketa, odnosno, kad je on samo tranzitni autonomni sustav između izvora i odredišta. Izvor takvog prometa, zbog mogućnosti lažiranja IP adresa, ne može biti sa sigurnošću utvrđen već samo odredište, a pritom još postoje i razlike između upita i odgovora:

1. ako je riječ o upitu, kako IP adrese mogu biti lažirane, ne možemo sigurno tvrditi tko je pošiljatelj, ali znamo koje je odredište
2. ako je pak riječ o odgovoru, i izvor i odredište su poznati iako zbog mogućnosti napada čovjekom u sredini izvor zapravo nije potpuno pouzdan (međutim, ovaj napad je manje vjerojatan, iz razloga što postoje jednostavniji napadi s jednakim mogućnostima). Dodatan problem postavlja otežano ili potpuno onemogućeno praćenje korelacije upita i odgovora koje je nužno kako bi se izbjeglo penaliziranje krivog klijenta ako je originalni upit sadržavao lažiranu IP adresu

Nakon problema lažiranja IP adresa, dodatno kompliciranje ocjenjivanja DNS paketa predstavlja tranzitni promet. Za tranzitni promet nije sigurno kojim će putem prolaziti upit, a kojim odgovor. Moguće su tri varijante, slika 3.4:

1. upit i odgovor prolaze kroz AS0 istim putem, odnosno prolaze istom komunikacijskom linijom obrnutim smjerovima
2. i upit i odgovor prolaze kroz AS0, ali različitim ulazima i/ili izlazima
3. samo pitanje ili samo odgovor prolazi AS0. Dio neispravnog ili namjerno štetnog prometa prikazuje kao nepostojanje odgovarajućeg odgovora na postavljeni upit ili postojanje odgovora na nepostavljeni upit, što se događa kod pokušaja trovanja DNS međuspremnika. Treba uzeti u obzir i tu činjenicu kako se ne bi ispravan promet neoprezno tretirao kao pokušaj napada, a neispravan promet kao nepostojanje korelacije upita i odgovora, uvjetovano topologijom mreža i politikama usmjeravanja na razini autonomnih sustava[3]

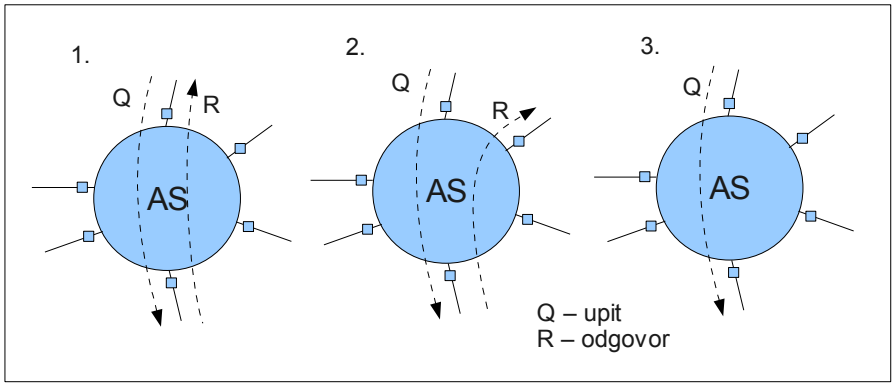
Zadnji bitan detalj jest dvostruko penaliziranje koje se javlja kod tranzitnog prometa. Kako tranzitni paketi nemaju ni izvor niti odredište u AS0, oni će se dva puta pojaviti na senzorima, prvi puta kad ulaze, a drugi puta kad izlaze iz AS-a. Tranzitni promet bi, dakle, bio dva puta penaliziran. To se može izbjeći na dva načina:

1. dvostruko penaliziramo sav promet koji za izvor ili odredište ima AS0, dok tranzitni promet penaliziramo jednostruko, ali onda i na ulazu i na izlazu. U tom slučaju kod izračunavanja reputacije treba paziti da su vrijednosti dvostruko veće od stvarnog stanja
2. penalizirati sav promet jednostruko, ali za promet koji nema za izvor niti za odredište AS0 ne penalizirati na izlazu iz AS-a već samo na ulazu, moguće je i obrnuto

Postavlja se pitanje na čiju sve reputaciju utječe pojedini neispravan DNS promet? Osnovno je kažnjavanje AS-ova za koje se sa sigurnošću može utvrditi da generiraju neispravan promet. Ovisno o razini sigurnosti u krivnju pojedinog AS-a, te ozbiljnosti prekršaja, možemo prilagođavati reputaciju pojedinih AS-ova. Drugo, važno je procijeniti kolika je odgovornost drugih tranzitnih AS-ova na putu pojedinih paketa. Kod grubih grešaka, kojih vrlo lako može biti svjestan bilo koji tranzitni AS, treba primjenjivati kažnjavanje svih AS-ova na putu. Za promet u kojem nismo potpuno sigurni tko je kriv

3 ovaj problem se zapravo pokazuje praktički nepremostivim na razini AS-a jer ne samo da je moguće da ne postoji jedan od smjerova komunikacije, nego čak i ako je postojao zabilježen na nekom od senzora, zbog nužnosti vremenskog ograničenja čuvanja uočenog upita, nije sigurno da će postojati u trenu kada neki od senzora primijeti odgovor

ostaju nam druge opcije, poput promjene reputacije samo susjednog AS-a s kojeg dolazi promet, ili, ako ne možemo odrediti put kojim promet dolazi, promjena reputacije AS-ova u stablu koje se nadovezuje na AS s kojeg dolazi promet, do proizvoljne dubine stabla.



Slika 3.4. Mogući putevi paketa tranzitnih upita i odgovora

Sada treba razmotriti modele penaliziranja koji su adekvatni za različite propuste DNS prometa:

Grube pogreške – na svaki promatrani paket primjenjuje se sve metode analize, niz filtera, kako bi se utvrdilo koje sve pogreške eventualno zadovoljava. Za početak, potrebno je kažnjavati sve pojave koje se odmah mogu prepoznati kao pogreška. Ovdje uglavnom pripadaju grube pogreške upita, poput upita za neispravne vršne domene, A upiti za IP adresu, upiti koji sadrže nedopuštene znakove, pogreške u formatu upita itd. Svaka prepoznata pogreška ima propisanu razinu negativne reputacije koju sa sobom nosi. Pritom se pogreške međusobno ne isključuju već se nadopunjavaju za svaku prepoznatu pogrešku. Ne postoji hijerarhija pogrešaka ili red ispitivanja za pogreške već samo razlika u razini loše reputacije koju nose. Dakle, ako je na nekom paketu prepoznato više pogrešaka, tada mu se uračunavaju utvrđene negativne ocjene svake od tih pogrešaka. U ovom skupu pogrešaka, kažnjava se samo strana koja šalje paket, ili susjedni AS s koje je paket došao kada nije moguće sa sigurnošću utvrditi tko šalje paket.

Odbijeni upiti – drugi slučaj su odbijeni upiti (negativni odgovori RCODE polja). Riječ je o ispravnom prometu koji može ukazivati na ekscese ponašanja neke od strana komunikacije. Utvrđivanje krivca za taj ispravan, ali nepotreban promet može biti vrlo komplicirano, ponekad i nemoguće, a kako takvog prometa može biti zaista mnogo potrebno je razviti pristup koji će maksimalno kažnjavati pravog krivca, a minimalno drugu stranu. Mogućnosti su:

1. kažnjavati samo ASK – ako je klijent zaista kriv za neispravan promet onda je prihvatljivo kažnjavati samo ASK; ako, pak, on šalje ispravan promet, ali poslužitelj zbog krive konfiguracije odbija upite, tada je opravdano kažnjavati ASK jer bi morao biti sposoban prepoznati negativan odgovor i ne pretjerivati s upitima, međutim, u tom slučaju pravi krivac za pogrešku, ASP, ostaje nekažnjen.
2. kažnjavati samo ASP – ako je on zaista kriv za odbijen promet to je opravdano, no ako on nije kriv za odbijen promet već krivo podešeni klijent, onda zapravo kažnjavamo samo krivu stranu, a koja još k tome nije u nemogućnosti izbjeći odgovoriti na upite.

3. kažnjavati ASK i ASP

Treba u ovom trenu uzeti i količinu tog prometa u obzir, odnosno, razmjere količina takvog prometa na pojedinim stranama komunikacije. Primjerice, ako je neki poslužitelj krivo podešen, on će zbog toga, u pravilu, krivo odgovarati većem broju klijenata iz različitih AS-ova. Jednako tako, krivo podešen klijent će krive upite slati većem broju poslužitelja u različitim AS-ovima. To navodi na treću mogućnost, a to je kažnjavanje i jedne i druge strane. Dakle, iako možda neka od strana zapravo nije kriva za odbijanje prometa, ta strana će biti samo kažnjena za taj konkretni incident, a to će se u skupu svih ocjena za sav promet tog AS-a minimalno odraziti. S druge strane, pravi krivac za taj promet će ponavljati istu grešku dulje vrijeme i to ponašanje će se kumulativno jače odraziti na reputaciju tog AS-a.

Moguć je i rubni slučaj, manifestacija neke greške samo u specifičnoj komunikaciji određenog para klijent – poslužitelj, a da je samo jedna od strana kriva za promet (prvenstveno klijent jer on može prekinuti postavljanje upita i nikada ne bi smio pretjerivati s istovjetnim upitima, dok poslužitelj ne može odbiti odgovoriti na upit). To bi kod kažnjavanja obiju strana navodilo na moguće značajno kažnjavanje strane koja ne bi trebala uopće biti kažnjena. Međutim, tu treba imati na umu da iako promatramo pojedinačne DNS pakete reputacija se postavlja AS-u, a ne pojedinim klijentima i poslužiteljima. Nadgledamo proizvoljne slučajeve komunikacije velikog broja klijenata i poslužitelja pojedinih AS-ova, pri čemu bilo koja od strana može biti neispravno podešena, te time i neusporedivo veću količinu ostalog prometa koja također utječe na konačnu reputaciju.

Kontrolni mehanizam za kažnjavanje ASP trebao bi imati oblik step funkcije. Pojedinom poslužitelju se dopušta određena količina negativnih odgovora i njih se minimalno kažnjava, međutim, ako broj negativnih odgovora prijeđe određenu "razumnu" granicu, drastično se poveća negativna ocjena po pojedinom odgovoru. Povećanje može biti brzo rastuće linearno do određene ciljane razine kazne ili jednostavno oblika step funkcije. Razumno je očekivati da će pojedini poslužitelj imati određeni broj negativnih odgovora proizašlih iz niza mogućih neprihvatljivih upita koje klijenti mogu generirati i samog broja klijenata koji svoje upite upućuju poslužitelju, ali ako je broj negativnih odgovora vrlo velik, to sugerira da je problem u krivom podešenom poslužitelja, a ne u klijentima. Za ovakvo mjerenje potrebna je jednostavna baza s popisom poslužitelja i količinama negativnih odgovora koje generiraju. Proširenje ove metode moguće je kod upita koji traže nepostojeće domene, odnosno, NXDOMAIN odgovora. Pritom jednako se dopuštaju NXDOMAIN odgovori koji nastaju kao posljedica upita malog broja klijenata. Međutim ako je broj klijenata koji traže nepostojeću domenu velik, penaliziramo više ASP pod pretpostavkom da bi takav zapis resursa trebao postojati i da je riječ o greški na poslužitelju. Zapravo, riječ je o kažnjavanju na osnovi neispravno ili neadekvatno formiranih zapisa resursa na DNS poslužitelju.

Automatsko penaliziranje svog DNS prometa – određene pogreške i propuste u DNS prometu razmatrane u ranijem poglavlju izrazito je teško prepoznati u reputacijskom sustavu koji radi u realnom vremenu. Prvenstveno, to su pogreške poput ponovljenih upita, nepohranjenih odgovora i sl., a do neke mjere i domene brzog toka i DoS napadi. Zbog te vrste neželjenog DNS prometa nameće se model kažnjavanja svog DNS prometa. Svaki

DNS paket, bio on ispravan ili ne, kažnjava se određenom minimalno kaznom. U normalnom funkcioniranju DNS-a, takva negativna ocjenjivanja neće se odražavati na ukupnu reputaciju AS-a, tj. ona će biti predviđena samim modelom kažnjavanja. Te minimalne kazne postaju korisne kada počinje dolaziti do pretjeranog prometa karakterističnog za ranije navedene pogreške. Anomalije u količini prometa, koje bi inače bilo teško uočiti, svojim količinama početi će utjecati na reputaciju AS iz kojeg dolazi. Pretpostavljeno je, ipak, da je poznata neka vrsta srednje vrijednost prometa pojedinih autonomnih sustava, odnosno uobičajene količine prometa bazirane na broju klijenata i poslužitelja te njihovoj popularnosti. Srednje vrijednosti je moguće utvrditi s vremenom promatranjem količina prometa. Funkcija negativne ocjene svog prometa mora biti modelirana tako da se u normalnom radu negativne ocjene prikupljene od svih paketa poništavaju s prosječnim količinama prometa (uzimajući u obzir ciljane srednje vrijednosti pojedinih AS-a, a ne neku opću srednju vrijednost svih autonomnih sustava). Korisna bi bila i funkcija koja bi uključivala i korekciju dopuštenih razina prometa pojedinih autonomnih sustava,odnosno srednjih vrijednosti, s tendencijom vrlo blagog pada. Time bi se korigirao stalni porast DNS prometa koji se dobrim dijelom može pripisati porastu neželjenog, a ne ispravnog DNS prometa.

Veličina TTL-a – dobrom praksom DNS-a možemo smatrati izdavanje zapisa resursa s visokim TTL-om. Trajnost podataka smanjuje potrebu za ponovnim postavljanjem istih DNS upita od strane istih klijenata i time smanjuje ukupan DNS promet, tj. opterećenje. Također, neke zlonamjerne prakse, poput brzog toka ovise o niskim vrijednostima TTL. Kako bi izbjegli prepoznavanje na crnim listama, napadači moraju stalno mijenjati zapise resursa koje izdaju svojim žrtvama, a izrazito niskim TTL-ovima postižu da ih žrtve stalno iznova pozivaju za nove vrijednosti. Osim što raste DNS promet, žrtve su u pravilu uvučene u neku vrstu prijevare. Preko TTL se može posumnjati u takvu praksu. Proširenje modela kažnjavanja svog DNS prometa bilo bi prilagođavanje funkcije penaliziranja dodavanjem TTL-a, koji zapis resursa nosi, kao parametra. Različit pristup treba primijeniti prema ASK i ASP:

1. ako je TTL zapisa resursa nizak kažnjavamo ASP više, a ASK manje – klijent je prisiljen postavljati upite zbog niskog TTL-a pa je ASK manje kažnjen, dok je poslužitelj koji postavlja TTL tako nisko, odnosno ASK, više kažnjen. ASK će sakupljati malo, a ASP puno negativne reputacije
2. ako je TTL zapisa resursa visok kažnjavamo ASP manje, a ASK više – poslužitelj ovdje postupa ispravno i zato je ASP manje penaliziran. Ako klijent poštuje TTL tada će ASK praktički biti zanemarivo penaliziran. S druge strane ako ga ignorira brzo će sakupiti negativnu reputaciju

Različito penaliziranje ASK i ASP – potrebno je pripaziti i na mogućnost lažiranja izvorišnih IP adresa upita. Kako je to vrsta napada koju je vrlo teško ili nemoguće primijetiti, a koja bi mogla negativno utjecati na performanse reputacijskog sustava, sustav bi trebao imati neki minimalni mehanizam otpora ovom napadu. Jedna od mogućnosti je i različito kažnjavanje upita i odgovora. Za pojedini upit ne možemo biti sigurni da je došao od deklariranog klijenta zbog mogućnosti lažiranja IP adrese izvora, te je siguran samo susjedni AS s kojeg je paket neposredno došao. Prihvatljivo bi bilo onda penalizirati samo susjedni AS jer on prosljeđuje neželjen promet. Očekivana posljedica je da susjedni AS

penalizira sebi susjedni AS s kojeg je sam dobio takav promet te tako u lancu sve do stvarnog izvora neželjenog prometa.

Kada govorimo o odgovorima poznati su i izvor i odredište paketa, međutim, zbog mogućnosti lažiranja IP adrese u originalnom upitu svejedno ne možemo biti sigurni da je odredište krivo za uočeni paket. Da bi penaliziranje i izvora i odredišta kod odgovora bilo opravdano, treba uzeti u obzir da se reputacija određuje autonomnim sustavima, a ne pojedinim korisnicima. Ako penaliziramo obje strane (neovisno što zapravo nismo sigurni u klijentovu stranu), zapravo penaliziramo AS-ove koji sigurno sudjeluju u razmjeni paketa te će imati interes poboljšanja svoje reputacije prema AS-ovima koji ih vide kao krivce. Ako bi ekvivalentno penalizirali deklarirani izvor kad je riječ o upitima, tada je moguće da penaliziramo AS koji uopće nije sudjelovao u razmjeni paketa.

Slaba strana ovog pristupa je da vjerojatno velika većina DNS prometa (bilo ispravnog, bilo neispravnog) zapravo ima ispravne adrese izvorišta te se ovim pristupom potencijalno oslabljuje efikasnost reputacijskog sustava. Kažnjavanje susjednog AS-a je, s druge strane, opravdano i kod upita i kod odgovora.

Aktivna mjerenja, DNS lanac i otvoreni rekurzivni poslužitelji – određena mjerenja koja bi bila korisna za utvrđivanje kvalitete prometa i ispravnosti ponašanja pojedinih klijenata i poslužitelja nije moguće provesti, a da se posredno ne ugrozi reputacija AS0. Ovaj tip mjerenja je utvrđivanje je li pojedini poslužitelj autoritativan za pojedinu domenu, odnosno utvrđivanje je li on "legalan" poslužitelj u DNS lancu. Klijenti u svojim upitima mogu biti proslijeđeni bilo kojem poslužitelju bez mogućnosti provjere je li taj poslužitelj zapravo dio DNS lanca (oni to nužno opravdano pretpostavljaju uz uvjet da su krenuli od vrha DNS hijerarhije ili da imaju pretpostavljenog rekurzivnog DNS poslužitelja poput ISP-a, što najčešće jest slučaj), npr. klijent koji je napadnut trovanjem DNS privremene memorije neće biti svjestan da je preusmjeren poslužiteljima s kojima inače ne bi komunicirao. Još gore, takav klijent nema izbora već vjerovati odgovorima koje takav poslužitelj daje. Utvrđivanje "ispravnosti" DNS poslužitelja bi iziskivalo postavljanje upita ili niza upita nadređenim poslužiteljima, a koji bi narušavali reputaciju AS0. Svejedno takva mjerenja bi se mogla raditi ako se ne bi primjenjivala na svaki primijećeni odgovor već na određenom statističkom uzorku. Tako pronađene DNS poslužitelje treba najstrože penalizirati.

Sličan tip mjerenja je i pretraživanje IP prostora u potrazi za otvorenim rekurzivnim poslužiteljima kakvo su proveli Dagon i ostali, [8]. Iz tog mjerenja očito je da je nužno strogo penalizirati AS-ove u kojima se nalaze otvoreni rekurzivni poslužitelji jer vrlo često je riječ o poslužiteljima koji namjerno daju krive informacije. Utvrđivanje je li neki poslužitelj otvoreni rekurzivni moglo bi se također raditi na statističkom uzorku promatranih odgovora (postavljanjem upita poslužiteljima čije odgovore primjećujemo na svojim granicama) te time smanjiti utjecaj na reputaciju AS0, vidi poglavlje

Crne i bijele liste – reputacijski sustav bi kao potporu mogao imati i crne, tj. bijele liste. Bijele liste bi se koristile kod uočenog DNSBL prometa. Na popisu bi se nalazili svi poznati DNSBL poslužitelji kako bi se izbjeglo penaliziranje prometa kada je riječ o NXDOMAIN odgovorima koji prema ranijem modelu dobivaju dodatne kazne, a koji se kod DNSBL odgovora koriste kao obavijest o nepostojanju poslužitelja neželjene pošte na adresi iz upita. Potrebna je crna lista otvorenih rekurzivnih poslužitelja. Nešto kompliciranije crne liste mogle bi se koristiti za bilježenje poznatih poslužitelja brzog toka,

odnosno neželjene pošte (preko domena za odbacivanje, *throwaway domains*) koje se može prepoznati po velikom broju A zapisa resursa za pojedinu domenu, ili za DNS poslužitelje takvih domena koje je moguće prepoznati pretraživanjem po zajedničkom NS zapisu resursa, više u poglavlju

Pozitivne prakse – reputacijski sustav bi morao imati i mogućnost dodjeljivanja pozitivnih ocjena baziranih na dobrim praksama uočenim u DNS prometu, poput korištenja DNSSEC-a.

Prema svemu ranije navedenom ocjena pojedinog paketa koje bilježe senzori postavlja se prema nizu parametara:

1. paket ima neku od grubih pogrešaka, nedopušteni znakovi, A za A upiti itd. – PU
2. paket je negativan odgovor, NXDOMAIN, SERVFAIL itd. – NO
3. automatsko penaliziranje svog prometa – A
4. reputacija prema TTL-u – T
5. različita reputacija ASK i ASP – KP
6. loše prakse uočenog prometa, otvoreni rekurzivni, izvan DNS lanca itd. – L
7. crne i bijele liste i svi dodatni pohranjeni podatci – CB
8. pozitivne prekse, DNSSEC i sl. – D

Ocjena pojedinog paketa je funkcija svih navedenih parametara. Svaki od parametara ima neku razinu loše ili dobre ocjene, a u konačnu funkciju se može dodavati izravno ili kao posebna funkcija. Opći oblik funkcije ocjene pojedinog paketa je:

$$R = f(pu(pkt), no(pkt), a(pkt), t(pkt), kp(pkt), l(pkt), cb(pkt), d(pkt))$$

Pojedine funkcije nisu fiksne već treba biti omogućena promjena funkcija, isto vrijedi i za opću funkciju, pritom će najčešće biti riječ o jednostavnom pribrajanju pozitivne ili negativne ocjene, iako su moguće i kompleksnije varijante pojedine funkcije ili više funkcija zajedno.

Izvan same funkcije ocjene pojedinih paketa u konačnom postavljanju reputacije AS-a čiji promet se promatra, moguće je i razmatranje ukupnog omjera količine ispravnog, nasuprot neispravnom prometu promatranog AS-a. Takav dodatak ne bi iziskivao velike intervencije u ostale dijelove sustava, niti bi ga dodatno opterećivao, ali bi zato mogao doprinijeti pouzdanosti reputacijskog sustava u cjelini.

4. Arhitektura sustava za mjerenje reputacije

Slijedi opis arhitekture sustava koji bi provodio mjerenja opisana u prošlom poglavlju i postavljao ocjene promatranom prometu.

Ranije smo rekli da se reputacijski sustav sastoji od tri osnovna dijela: dijela koji promatra promet, dijela koji analizira promet i određuje reputaciju AS-ova, i dijela koji mijenja politiku prema autonomnim sustavima prema određenim reputacijama. Ovdje su bitna prva dva dijela koja sadrže tehničku stranu promatranja prometa i određivanja reputacije, dok se promjenom politika prema promatranim AS-ovima ne bavimo.

Promatranje prometa i postavljanje reputacije izvodi se pomoću tri odvojena elementa, slika 4.1:

1. senzor – u pravilu će ih biti više, koliko i komunikacijskih linija
2. kolektor
3. reputacijski sustav – ovdje označava dio sustava koji izračunava konačne reputacije AS-ova na temelju svih prikupljenih podataka svih protokola

Na razini AS-a možemo očekivati velike količine DNS prometa. Prvi problem bi mogli biti senzori. Svaki senzor ima zadatak pratiti promet i analizirati ga tako da utvrdi osnovne pogreške koje se pojavljuju u pojedinim paketima. Zahtjev na senzore je da posao obavljaju u realnom vremenu, odnosno, da pakete obrađuju kako dolaze. Kada uoče pogrešku, oni prosljeđuju nužne podatke o paketu i pogreški kolektoru. Kako se kolektor u pravilu neće nalaziti na istom računalu kao i senzor to znači da će, zbog paketa koje će senzor slati kolektoru, doći do porasta prometa unutar AS-a za količinu uočenih grešaka DNS prometa, tj. za veličinu paketa informacija pomnoženih brojem grešaka. Poželjno je da paketi koji prenose podatke o pogreškama sadrže što više informacija, ali i da budu što manji jer će njihova količina i veličina opterećivati propusni pojas.

Senzori se trebaju postaviti na komunikacijskim linijama AS-a. Bitno je da promatranje prometa koji provode senzori ne opterećuje dodatno te linije ili DNS komunikaciju općenito. Senzori ne smiju utjecati na protok prometa i normalno funkcioniranje mreže.

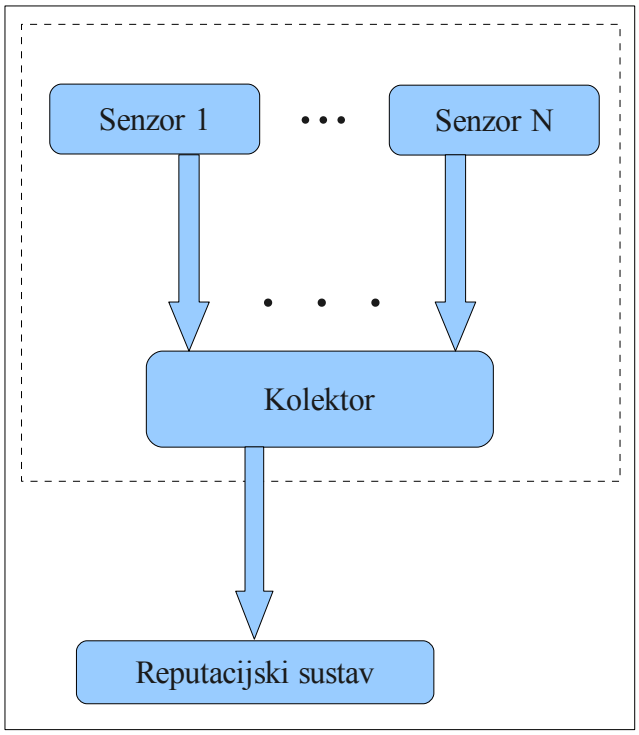
Zadatak je kolektora da sakupi sve DNS pogreške koje su primijećene i analizirane na granicama AS-a. Neispravnom DNS prometu se prvo pridjeljuje osnovna ocjena koja ovisi o utvrđenoj pogreški. Kolektor ima dodatni zadatak proanalizirati sve dobivene pakete kako bi eventualno prepoznao pogreške koje nije moguće uočiti senzorima. Uglavnom je riječ o pretraživanju crnih i bijelih lista poslužitelja u potrazi za generatorima neželjene pošte, brzim tokom, DNSBL poslužiteljima i sl. Kolektor sadrži i sve potrebne baze podataka o pojedinim poslužiteljima kako bi mogao ocijeniti odbijene odgovore te, po potrebi, može raditi aktivna mjerenja. Na kraju, nakon što sve analize uzme u obzir, koristi funkciju ocjene paketa da bi izračunao konačnu ocjenu pojedinog paketa. Rezultate tada prosljeđuje reputacijskom sustavu.

Kolektor je potencijalno drugo usko grlo. Prvenstveno će na njemu biti opterećenje na propusnom pojasu. Kako kolektoru stižu sve zabilježene pogreške na granicama AS-a, uzimajući u obzir uočene količine neispravnog prometa, razumno je očekivati promet reda veličine ispravnog DNS prometa na granicama AS-a. Opterećenje je i na procesoru koji

mora obraditi sve pristigle pogreške, obaviti dodatne analize i dodijeliti odgovarajuće ocjene.

Na kraju reputacijski sustav prikuplja sve dodijeljene ocjene i izračunava konačnu reputaciju svih AS-ova temeljenu na podatcima o DNS-u, ali i ostalim protokolima.

Prvi je cilj pokušati maksimalno rasteretiti kolektor, jer se njemu šalje sav neispravan promet koji dolazi na granice AS-a. Funkcionalnost se prebacuje u senzore koji imaju zadatak odraditi procesorski zahtjevniji zadatak pronalaska pogrešaka. Drugi je zahtjev osigurati nesmetan tok prometa na komunikacijskim vezama AS-a, a da istovremeno senzori analiziraju promet u realnom vremenu. U biti, imamo dva suprotstavljena zahtjeva – ovaj drugi pokušava smanjiti funkcionalnosti na senzorima, jer bi idealno bilo na njima samo promatrati promet.



Slika 4.1. Shematski prikaz arhitekture sustava

Prednost kompleksnih senzora jest što se posao raspodjeljuje, realno je za očekivati da mogu obraditi sve podatke te je time odluka premještanja utvrđivanja pogrešaka na senzore opravdana. Kompleksni senzori, s druge strane, usložnjavaju utvrđivanje određenih specifičnih pogrešaka (poput brzog toka) koje zahtijevaju posjedovanje trajnijih informacija o prometu s različitih granica AS-a, pa se taj dio prepušta kolektoru koji na jednom mjestu ima skupne podatke o poslužiteljima, i AS-ovima te koji može vršiti naknadna aktivna mjerenja da bi potvrdio postojanje nekih tipova neispravnog prometa. Za razliku od senzora, na kolektor se ne postavlja strogi zahtjev rada u realnom vremenu nego može, ovisno o opterećenju, pohranjivati upite za kasniju obradu, ili odrađivati pojedina aktivna mjerenja kada se za to oslobode resursi.

Podatke o pogreškama senzori šalju Internetom do kolektora. Zato je poželjno kriptiranje paketa koji prenose podatke o IP adresama i pogreškama od senzora do kolektora. Također

mora biti osigurano da svi privatni podatci, koji se možda u nekom obliku pohranjuju za kasniju analizu, budu nedostupni izvan sustava pojedincima ili kompanijama koje bi ih mogli zlouporabiti. Cilj je postići minimalno potrebno zadržavanje podataka o paketima u sustavu do izračunavanja reputacije. O poslužiteljima za koje se utvrdi da generiraju neželjen promet čuvaju se potrebni podatci.

5. Reputacijski sustav

Pretpostavke iznesene u potpoglavlju 3.4. i poglavlju 4. idealno bi bilo ispitati u stvarnom vremenu sa senzorima postavljenim na granicama AS i sa svim analizama na raspolaganju senzorima i centralnom reputacijskom sustavu. Određivanje reputacije AS-ova podrazumijeva postojanje reputacijskog sustava koji bi obuhvaćao više protokola preko kojih se određuje konačna reputacija, međutim, reputaciju možemo računati na temelju samo jednom protokolu. Za potrebe utvrđivanja reputacije, temeljene na promatranju DNS protokola, razvijen je reputacijski sustav koji se sastoji od modula za promatranje prometa i analizu te modula za izračunavanje reputacije na temelju utvrđenih pogrešaka. U daljnjem tekstu ukratko će biti opisana implementacija reputacijskog sustava.

5.1. Temelji reputacijskog sustava

Osnovni problem u izradi reputacijskog sustava bila je nemogućnost pristupa granicama nekog AS-a na kojem bi bila vršena mjerenja. Iz toga razloga, a kako bi se uspjela obaviti mjerenja, nužno je bilo izraditi reputacijski sustav koji reputaciju računa prema DNS prometu koji je prethodno zabilježen na odabranom mjestu promatranja prometa i pohranjen u datoteku. Reputacija tako nije rezultat podataka dobivenih s više različitih točaka na granici nekog AS-a već predstavlja reputaciju kako ju vidi određena točka, poput pojedinih poslužitelja unutar AS-a (više o točkama bilježenja prometa u poglavlju 6.).

Promet je pohranjen u *pcap* (hvatanje paketa, *packet capture*) datoteku koja sadrži cjelovite originalne pakete te vremenske oznake trenutka kada je pojedini paket primijećen. Prema tome, iako reputacijski sustav promet ne promatra u stvarnom vremenu, rekonstruirajući događaje zabilježene u pcap datoteci može postići identične rezultate onima postignutim mjerenjem u stvarnom vremenu. Ograničenje ostaje jedino činjenica da promet, pohranjen u pcap datoteci, predstavlja promet samo jedne točke, pa tako i izračunata reputacija samo reputaciju kako ju vidi jedna točka. U slučaju postojanja više pcap datoteka koje bi sadržavale podatke prikupljene s granica nekog AS-a u istom vremenskom razdoblju, gledano iz perspektive reputacijskog sustava, moguće je to ograničenje izbjeći jednostavnim spajanjem svih pcap datoteka u jednu datoteku. Pri tome treba pripaziti jedino da se prema vremenskim oznakama očuva ispravan redoslijed paketa u novonastaloj pcap datoteci. Tako vršeno mjerenje na implementiranom reputacijskom sustavu dalo bi iste rezultate kao cjelovit sustav opisan u poglavlju 4.

U svrhu dobivanja općenite slike o prometu koji dolazi na pojedine mjerne točke, odnosno o reputaciji kako ju vide pojedine mjerne točke, reputacijski sustav namjerno ignorira neke od potencijalnih prijetnji. Prvenstveno, ovdje je riječ o mogućem lažiranju IP adresa i detaljima vezanim za DNS pakete koji na putu prolaze AS-om. Iako bi realnom AS-u bilo u interesu reputaciju AS-ova podešavati i prema tim elementima analize, u našem slučaju korisnija je pretpostavka da velika većina prometa nije lažirana te da, prema tome, modeli kažnjavanja koji se preporučaju u slučaju tranzitivnog prometa i lažiranih IP adresa trebaju biti ignorirani. Reputacijski sustav iz tog razloga sve pakete tretira kao da su došli s zabilježenih IP adresa. Kada je riječ o paketima koji samo prolaze AS-om, realni reputacijski sustav bi kažnjavao samo susjedne AS-ove za koje je siguran da od njih dolazi

neispravan promet. Implementirani reputacijski sustav, s druge strane, reputaciju uvijek podešava AS-ovima izvora i odredišta, a susjede kažnjava samo ako su oni izvor ili odredište.

Reputacijski sustav također ne implementira pozitivno ocjenjivanje DNSSEC paketa, što je posljedica ograničenja sučelje za izradu aplikacija (*application programming interface, API*) Scapy modula na kojem su građeni određeni moduli sustava (novije verzije Scapy modula uključuju i DNSSEC, više u potpoglavlju 5.3.). S obzirom na relativno malu rasprostranjenost i uporabu DNSSEC-a, pretpostavka je da to neće bitnije utjecati na rezultate mjerenja. U budućnosti, može se očekivati sve veća uporaba DNSSEC-a, a za taj slučaj moguće je relativno jednostavno nadograditi postojeći reputacijski sustav funkcijom nagrađivanja takvog prometa jednako kao i bilo koji drugi pozitivan aspekt DNS prometa.

Reputacijski sustav ne provodi aktivna mjerenja niti posjeduje crne i bijele liste, koje sakupljaju informacije o prometu pojedinih poslužitelja, poput otvorenih rekurzivnih poslužitelja. Kako se pri izradi pazilo da bi i takve analize mogle biti dodane u budućnosti, njihovo dodavanje bi iziskivalo minimalne izmjene postojećeg koda i uglavnom bi se odnosile na samu funkcionalnost koju je potrebno implementirati. Jedina bijela lista koju reputacijski sustav posjeduje jest popis DNSBL poslužitelja koja je dio nagrađivanja pozitivnih aspekata DNS prometa. Tu listu je moguće proizvoljno nadograditi.

IPv6 adrese u odgovorima se ignoriraju i ne ulaze u daljnje analize. Kako je tijekom testiranja primijećeno svega nekoliko odgovora koji sadrže IPv6 adrese njihovo ignoriranje ne utječe na rezultate mjerenja. Implementacija funkcionalnosti IPv6 DNS upita je svakako prioritet u budućnosti.

Testiranjam su pronađene i dvije vrste pogrešaka koje se ne pojavljuju u literaturi. Prva je pogreška neispravnog RCODE-a 15 koju generiraju neke verzije BIND poslužitelja. Druga pogreška su paketi s nizom neispravnosti u strukturi. Uzrok ove pogreške nije poznat. Kako se obje pogreške pojavljuju u svega nekoliko paketa, one ne utječu bitnije na rezultate i reputacijski sustav ih ignorira. U budućnosti moguće je nadograditi sustav da i takve pogreške penalizira.

Podešavanje parametara rada reputacijskog sustava, moguće je kroz konfiguracijsku datoteku reputacijskog sustava. Konfiguracijska datoteka sadrži parametre podijeljene u pet skupina:

1. korištene datoteke i njihov sadržaj
2. analize koje želimo provesti
3. parametri analize i funkcija računanja reputacije
4. funkcije koje želimo uključiti u izračunavanju reputacije
5. težinski faktori pojedinih pogrešaka podijeljeni na klijentsku i poslužiteljsku stranu

Osnovna podešenja podrazumijevaju izbor pcap datoteke, popise DNSBL poslužitelja, baze translacije IP adresa u AS-ove te popise mreža koje pojedina mjerna točka ne uračunava u mjerenje.

U sekciji analiza moguće je odabrati koje analize želimo primijeniti na DNS promet. Osnovne analize predstavljaju potragu za grubim greškama u DNS prometu i, iako ih je

moguće isključiti, podrazumijeva se da su one temelj svakog promatranja DNS prometa. Na raspolaganju su još analize negativnih odgovora koje uključuju i potragu za DNSBL upitima, analize pozitivnih elemenata DNS prometa, penaliziranje svih DNS paketa te penaliziranje prema TTL-u.

U sekciji parametara, moguće je podešavati granične vrijednosti TTL-a i konstante funkcije reputacije. TTL-ovi DNS zapisa su podijeljena u tri veličine – kratki, srednji i dugi. Parametri TTL-a se odnose na granice između kratkog i srednjeg te srednjeg i dugog TTL-a. Različito trajanje TTL-a donosi i različite kazne na DNS promet.

Sekcija parametara sadrži konstante računanja reputacije nakon kojih ostatak konfiguracijske datoteke čine podešenja težina kazni pojedinih pogrešaka i metoda izračunavanja reputacije. U svrhu razumijevanja ostalih parametara, slijedi opis funkcije reputacije.

5.2. Reputacijska funkcija

Reputacijska funkcija definirana je rekurzivno 5.1:

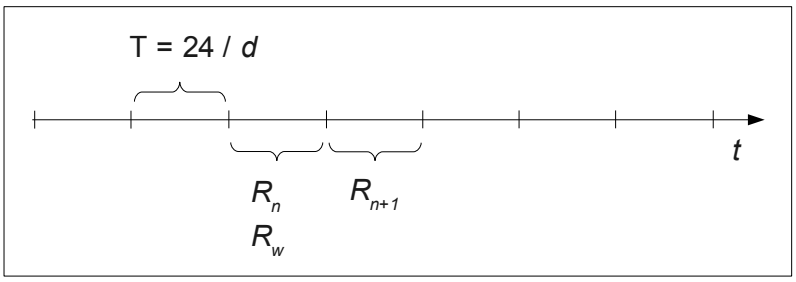
$$R_{n+1} = \alpha R_n + (1-\alpha) R_w$$

1. R_{n+1} je nova vrijednost reputacije pojedinog AS-a nakon perioda promatranja n
2. R_n je reputacija pojedinog AS-a u prethodnom periodu promatranja ($n - 1$)
3. α je faktor opadanja (*decay factor*)
4. R_w rezultat težinske funkcije za promatrani period n

Reputacija se računa periodički pri čemu je početni trenutak ponoć te se podrazumijeva da je početna reputacija, odnosno reputacija u nultom periodu, nula. Period se u konfiguracijskoj datoteci određuje vremenskim djeliteljem d koji razdoblje od 24 sata dijeli na 1, 2, 3, 4, 6, 8, 12 ili 24 dijela čime se određuje trajanje perioda u satima:

$$T = \frac{24}{d}, d = (1, 2, 3, 4, 6, 8, 12, 24)$$

Faktor opadanja α realan je broj u rasponu $\alpha = \langle 0,1 \rangle$ i predstavlja utjecaj reputacije perioda $n - 1$ na vrijednost reputacije u periodu n. Kako težinska funkcija R_w utječe upravo obrnuto, razlikom $1 - \alpha$, faktor opadanja zapravo određuje postotni udio R_n i nove vrijednosti R_w u konačnoj reputaciji.



Slika 5.1. Vremenska podjela reputacija

Reputacijski sustav podržava pet varijanti težinske funkcije R_w koje je moguće birati u konfiguracijskoj datoteci:

1. $R_{w1} = \sum r_i \beta_i$, osnovna težinska funkcija koja se ponavlja u svakoj funkciji

2. $R_{w2} = \frac{\sum r_i \beta_i}{A_n}$, normalizacija ukupnom količinom prometa. A_n označava ukupnu količinu prometa

3. $R_{w3} = \frac{\sum r_i \beta_i}{A_n + \sum r_i}$, normalizacija zbrojem pogrešaka i ukupne količine prometa

4. $R_{w4} = \frac{\sum r_i \beta_i}{\sum r_i}$, osnovna težinska funkcija normalizirana brojem pogrešaka

5. $R_{w5} = \frac{\sum r_i}{A_n} \sum r_i \beta_i$, normalizacija omjerom broja pogrešaka i ukupnog prometa

Parametar r_i predstavlja broj pojavljivanja pojedine vrste pogreške u danom periodu računanja, a parametar β_i predstavlja težinu koju nosi pojedina pogreška prikazane u tablici 3.1. Na taj način osnovna težinska funkcija je suma umnožaka broja pojavljivanja pojedine pogreške i njezine težinske vrijednosti. β_i je moguće podešavati u konfiguracijskoj datoteci za svaki tip pogreške, pri čemu vrijednosti težina mogu biti različite za klijentsku i poslužiteljsku stranu.

R_{w1} prikazuje reputaciju kao apsolutnu vrijednost. Prema toj funkciji, AS-ovi kojima veliki broj pogrešaka ima veliki težinski parametar, postizati će velike vrijednosti negativne reputacije. Nedostatak te funkcija jest da će AS-ovi, s kojih općenito dolazi puno prometa, a neovisno o kvaliteti njihova prometa, dobivati visoke razine negativne reputacije temeljene na činjenici da se u puno prometa može očekivati i razmjerno veći broj pogrešaka. To će se prvenstveno odnositi na susjedne ili "lokalne"[4] AS-ove. Problem te funkcije jest što ne prepoznaje omjer ukupne količine prometa i broja pogrešaka. U rubnom hipotetskom slučaju AS-a koji ne generira nikakve pogreške, ali ima jako puno prometa, može imati najlošiju reputaciju u odnosu na druge AS-ove. Također, moguć je i obrnut slučaj AS-a koji generira malo prometa, ali zato isključivo pogreške, a da bude prepoznat kao AS s prilično dobrom reputacijom.

Ostale težinske funkcije normaliziraju funkciju R_{w1}. Normalizacijom se apsolutne vrijednosti reputacije dobivene sumacijom broja pogrešaka i njihovih težina pretvaraju u relativne vrijednosti s obzirom na broj pogrešaka i ukupan broj paketa pojedinog AS-a u danom periodu.

R_{w2} normalizira R_{w1} ukupnom količinom prometa, odnosno brojem paketa pojedinog AS-a. AS-ovi koji generiraju mnogo prometa, ali pritom uglavnom ispravan promet, dijeljenjem

4 U Hrvatskoj se može očekivati puno komunikacije među lokalnim AS-ovima npr. T-HT-a, CARNET-a itd.

će, s ukupnom količinom svog prometa, općenito dobivati manje vrijednosti konačne negativne reputacije. U rubnom slučaju AS-a koji generira samo ispravan promet, uz pretpostavku da kažnjvamo sav promet i da je težina pojedinog paketa -1, njegova će ukupna reputacija iznositi -1. AS-ovi kojima je promet uglavnom neispravan, imat će visoke negativne vrijednosti reputacije:

$$\sum r_i \ll A_n$$
$$\frac{A_n(-1)+\sum r_i \beta_i}{A_n} = -1 + \frac{\sum r_i \beta_i}{A_n} \approx -1$$

Težinske funkcije R_{w3} i R_{w4} predstavljaju normaliziranje funkcije R_{w1} brojem pogrešaka, pri čemu R_{w3} u broj pogrešaka uključuje i ukupan promet dok R_{w4} ukupan promet ne smatra pogreškom. Obje funkcije zapravo teže prema srednjoj vrijednosti težine najučestalije pogreške koju pojedini AS čini, npr. ako AS uglavnom šalje pakete s pogreškom težine -30 funkcija će težiti -30. U općenitom slučaju, vrijednost funkcije će biti srednja vrijednost kvalitete ukupnog prometa:

$$r_p \approx \sum_{i=1}^{n} r_i$$
$$R_{w4} = \frac{r_1\beta_1 + \ldots + r_p\beta_p + \ldots + r_n\beta_n}{\sum_{i=1}^{n} r_i} \approx \beta_p$$

R_{w5} normalizira R_{w1} omjerom broja pogrešaka i ukupne količine prometa pojedinog AS-a. Taj omjer je postotni koeficijent neispravnog prometa u ukupnom prometu, odnosno, stopa pogrešaka. Što je više pogrešaka u odnosu na ukupni promet, koeficijent će biti veći, a time i ukupna negativna reputacija. U rubnom slučaju, kada je broj pogrešaka jednak količini prometa, R_{w5} daje isti rezultat kao i R_{w1}. S druge strane, ako AS ne čini nikakve pogreške, reputacija je 0:

$$\sum r_i = A_n$$
$$R_{w5} = \frac{\sum r_i}{A_n} \sum r_i \beta_i = \sum r_i \beta_i = R_{w1}$$

Računanje pojedine težinske funkcije moguće je isključiti u konfiguracijskoj datoteci, međutim, to se ne odnosi na osnovnu težinsku funkciju R_{w1} koja se koristi u svim ostalim funkcijama pa zato uvijek mora biti izračunata.

5.3. Implementacija reputacijskog sustava

Reputacijski sustav napisan je u programskom jeziku *python* i sastoji se od pet modula:

1. modul senzora DNS prometa – *sniff_senzor.py*
2. modul filtera osnovnih pogrešaka – *sniff_filters.py*
3. modul dodatnih analiza DNS prometa – *traffic_analysis.py*
4. modul računja reputacije AS-ova – *reputation_calculator.py*

5. startni modul – *reputation_system.py*

Modul senzora DNS prometa i modul filtera osnovnih pogrešaka preuzeti su iz [15]. Preuzeti kod ima funkcionalnost praćenja prometa u realnom vremenu, ali uz manje izmjene prilagođen je čitanju prometa iz pcap datoteka. Senzor se bazira na Scapy sučelju koje između ostalog pruža funkcionalnosti vezane za praćenje DNS prometa, manipulaciju i izgradnju DNS paketa. Scapy nije dio standardnih biblioteka pythona, ali je objavljen pod GPL licencom te je često dio repozitorija *Linux* distribucija.

Senzor preko *callback* funkcije preuzima uhvaćene pakete od Scapy sučelja i nakon rekonstrukcije sadržaja paketa u čitljivi oblik, korištenjem funkcija modula filtera, traži grube pogreške u paketima. Paketi se zatim prosljeđuju modulu dodatnih analiza. Senzor je izmijenjen na način da sve uočene pogreške DNS prometa šalje modulu za računanje reputacije AS-ova.

Modul filtera radi analize koje traže grube pogreške u paketima. U njemu su vršene manje izmjene dodavanjem analiza koje su nedostajale i izbacivanjem analiza koje su se pokazale neadekvatnima na razini promatranja prometa AS-a (više u poglavlju). Dodani su:

1. filter nepoznatog razreda upita
2. filter zastarjelih razreda upita
3. filter nedopuštenog pristupa 0

Izmijenjen je filter nepoznati OPCODE tako da traži samo zastarjele OPCODE-ove.

Modul dodatnih analiza DNS prometa implementira funkcionalnosti pretrage negativnih odgovora, penaliziranje TTL-a, penaliziranja svog prometa, i analize DNSBL negativnih odgovora. Moguće je proširiti ga funkcionalnostima potrage za DNSSEC paketima koje, zbog ograničenja verzije Scapy sučelja koje je na raspolaganju, nisu implementirana. Rezultate, jednako kao i modul senzora, prosljeđuje modulu računanja reputacije.

Modul za računanje reputacije prima pogreške koje mu prosljeđuju modul senzora i modul dodatnih analiza te, nakon utvrđivanja AS-ova pojedinih IP adresa, razvrstava pogreške odgovarajućim AS-ovima, brojeći svako pojavljivanje pojedine pogreške. Sakupljanje paketa traje sve dok vremenske oznake u pojedinim paketima ne prijeđu granicu novog perioda reputacije, što pokreće izračunavanje reputacije, pohranjivanje nove trenutne vrijednosti reputacije svih AS-ova, određivanje novog perioda i pokretanje novog ciklusa sakupljanja pogrešaka. Granice perioda novog računanja reputacije određuju se prema vrijednosti parametra vremenskog djelitelja. Određivanje AS-ova na temelju IP adresa preuzeto je iz [16] te je funkcionalnost donekle izmijenjena kako bi se postigla mogućnost usporedbe s mrežnim maskama. *Whois* poslužitelj koji se koristi za utvrđivanje AS-ova prema IP adresama ponekad nema odgovor za danu IP adresu. Paketi s takvim IP adresama se ignoriraju i ne ulaze u računanje reputacije.

Rezultati se ispisuju u dvije datoteke po AS-u, od kojih prva sadrži vremenske oznake perioda mjerenja i vrijednosti reputacija u danom mjerenju u *csv* (vrijednosti razdvojene zarezom, *comma separated values*) formatu, a druga sadrži popis pogrešaka i broj pojavljivanja pojedine pogreške podijeljene na klijentsku i poslužiteljsku stranu. Iz te datoteke moguće je detaljnije analizirati aktivnosti pojedinog AS-a za promatrano razdoblje.

Reputacijski sustav se pokreće startnim modulom. Posao reputacijskog sustava je podijeljen u tri dretve i zadatak je startnog modula da pokrene izvođenje dretvi pojedinog modula te pričeka završetak svake pojedine dretve prije gašenja programa.

6. Rezultati mjerenja

Za potrebe diplomskog rada opisanim reputacijskim sustavom izvršeno je niz računanja reputacija na prometu sakupljenom na više mjernih točaka:

1. ZEMRIS-ov poslužitelj, dio CARNET AS-a (AS2108) na kojem su odrađena dva snimanja prometa u razdobljima od 3.10.2010. do 12.10.2010. i 20.10.2010. do 30.10.2010. U prvom snimanju je prikupljeno 385 MB DNS prometa, a u drugom nepunih 560 MB. Iz računanja reputacije izbačene su IP adrese koje pripadaju CARNET-ovim mrežnim rasponima
2. poslužitelj u Metronet AS-u (AS35549) na kojem je izvršeno snimanje u razdoblju od 14.10.2010. do 27.10.2010. pri čemu je prikupljeno nepunih 160 MB DNS prometa
3. poslužitelj u AS49788 na kojem je izvršeno snimanje u razdoblju od 6.10.2010. do 16.10.2010. pri čemu je prikupljeno 17 MB prometa. To je manji AS kojem je jedina veza na Internet preko Metronet AS-a pa se može smatrati drugom mjernom točkom unutar Metroneta
4. poslužitelj u Keyweb AS-u (AS31103) na kojem je vršeno snimanje u razdoblju od 6.10.2010. do 22.10.2010. pri čemu je prikupljeno oko 200 MB prometa

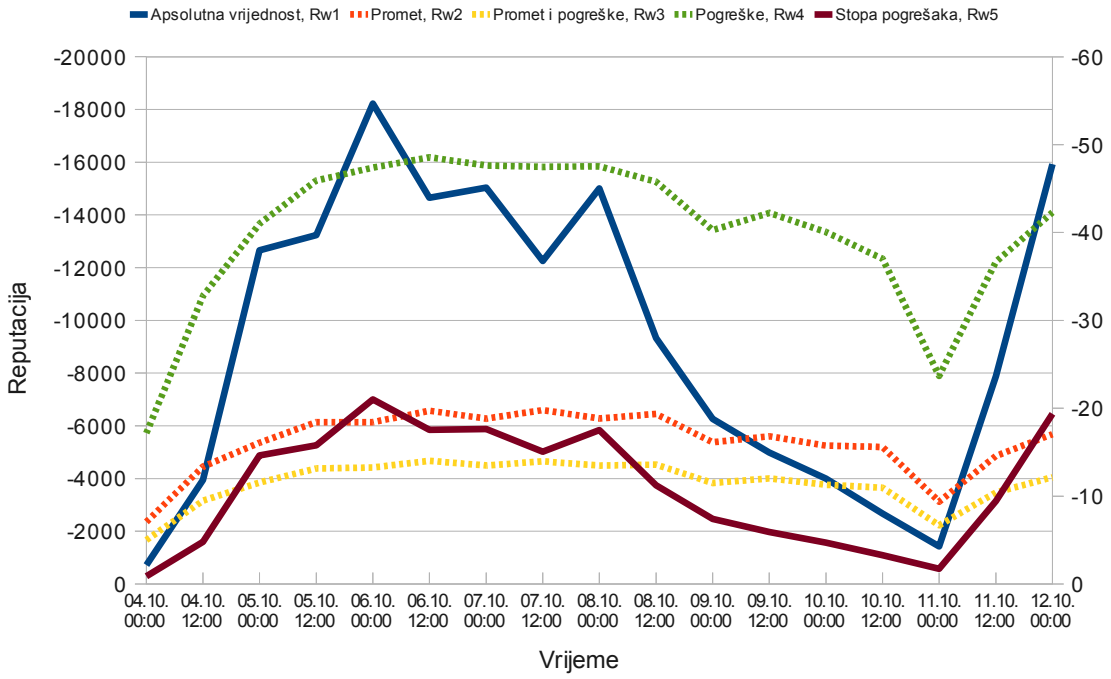
Na prometu svake mjerne točke izvršeno je devet računanja reputacija prema svim kombinacijama odabranih vrijednosti parametara α i vremenskog djelitelja d. Za α su korištene vrijednosti 0.3, 0.5 i 0.7, a za parametar d vrijednosti 1, 2 i 4 što čini periode računanja novih reputacija od 24, 12 i 6 sati. Parametri su odabrani kako bi što općenitije prikazali mogućnosti ja i utjecaja parametara na rezultate pritom uzimajući dvije razumne "rubne" vrijednosti ($\alpha = 0.3$, $\alpha = 0.7$ i $d = 1$, $d = 4$) i jednu srednju ($\alpha = 0.5$ i $d = 2$). Cilj je daljnjih razmatranja analizirati ponašanja pojedinih funkcija ovisno o podešenim parametrima te pokušati utvrditi koji parametri i koje funkcije daju najvjernije rezultate. Pri svakom računanju reputacije korišteno je svih pet funkcija reputacije.

Svako pojedino računanje ovisno o korištenim mjernim točkama rezultira izračunatim reputacijama za 4000 do 17000 AS-ova. Iz tih rezultata prikazani će biti AS-ovi s najgorim rezultatima ovisno o pojedinim funkcijama reputacije. Najgori AS-ovi utvrđeni su traženjem aritmetičke sredine reputacije za određenu mjernu točku te prema svakoj funkciji posebno.

Promijene reputacije bit će prikazane grafikonom koji će općenito izgledati poput grafikona 6.1 (prikazana je reputacija AS-a Optima telekoma kako ju u jednom od mjerenja vidi poslužitelj na ZEMRIS-u). Pritom y os ima dvije skale, obje negativne. Lijeva skala odnosi se na vrijednosti u grafikonu označene punom crtom, dok se desna odnosi na vrijednosti označene crtkano. Na x osi je označeno vrijeme u danima, a ponekad i satima.

Slijede analize razlika među funkcijama te analize ponašanja, s obzirom na promjene parametara računanja reputacije. Za to su korištene dvije python skripte: prva za traženje najgorih AS-ova prema pojedinim funkcijama, i druga koja na temelju zabilježenog broja pogrešaka po pojedinom AS-u omogućuje ponovno izračunavanje reputacije s promijenjenim parametrima. Tom skriptom moguće je mijenjati vrijednosti težina

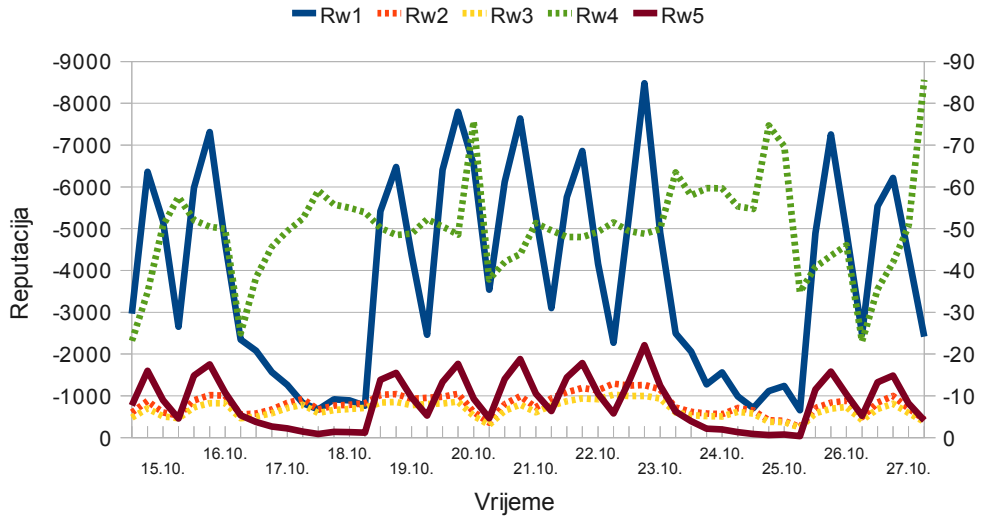
pogrešaka β_i te parametar α.



Grafikon 6.1. Reputacija autonomnog sustava AS34594 mjereno iz AS2108

6.1. Analiza razlika reputacijskih funkcija

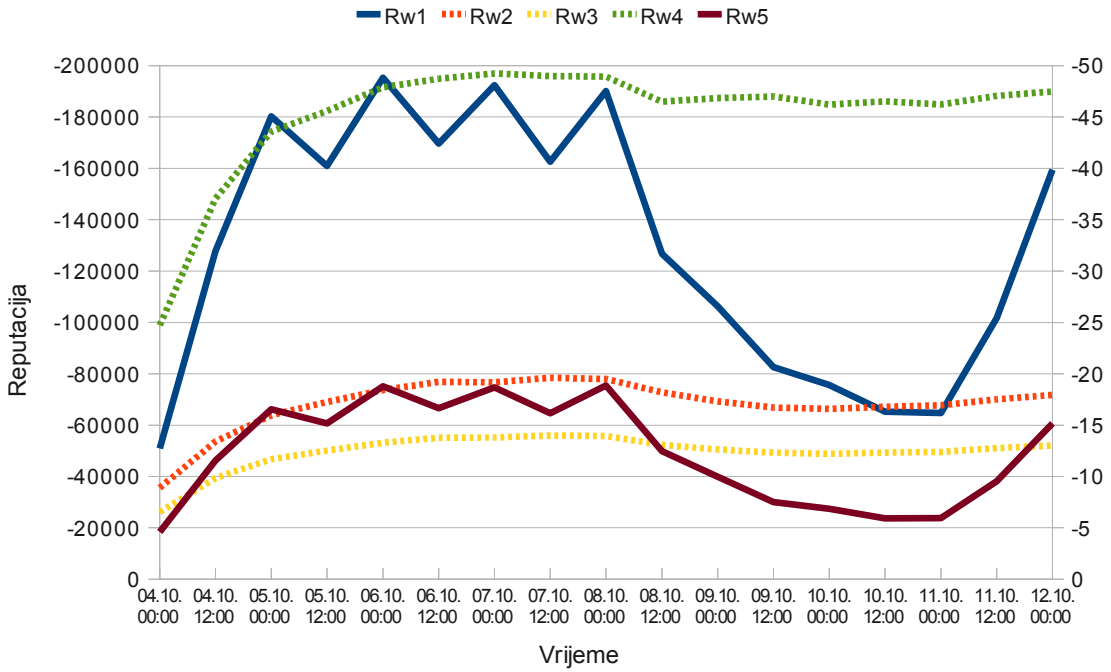
Analizu funkcija počinjemo prikazom reputacija za AS5391 (T-HT) s periodom računanja reputacije od 6 sati i parametrom $\alpha = 0.5$, gledano s mjerene točke Metronet (AS35549) u razdoblju od 14.10.2010. do 27.10.2010. za koju najgori rezultat funkcije R_{w1} daje upravo AS5391, grafikon 6.2.



Grafikon 6.2. Reputcija autonomnog sustava AS5391 mjereno iz AS35549

Funkcija R_{w1} prikazuje apsolutne vrijednosti reputacije temeljene samo na težinama pojedinih pogrešaka, ne uzimajući u obzir količinu prometa u kojem su se uočene pogreške pojavile. Nedostatak ovakvog pristupa vidljiv je i u ovom slučaju, jer je očekivano da će najviše pogrešaka u apsolutnim vrijednostima dolaziti upravo od AS-ova s kojima mjerna točka najviše komunicira, a taj problem postaje gori što je apsolutna razlika u količini prometa određenog AS veća od prometa svih ostalih AS-ova. Iako, moguće je da je količina DNS prometa upravo posljedica neželjenog DNS (DoS napadi, brzi tok i sl.).

Funkcija R_{w1} daje slične očekivane rezultate i gledano sa ZEMRIS-ova poslužitelja unutar CARNET-a (AS2108), s periodom 12 sati i parametrom $\alpha = 0.5$. U tom mjerenju najgori AS je Google Inc. (AS15169), na drugom mjestu je upravo Metronet (AS35549), a na trećem spomenuti T-HT, grafikon 6.3.



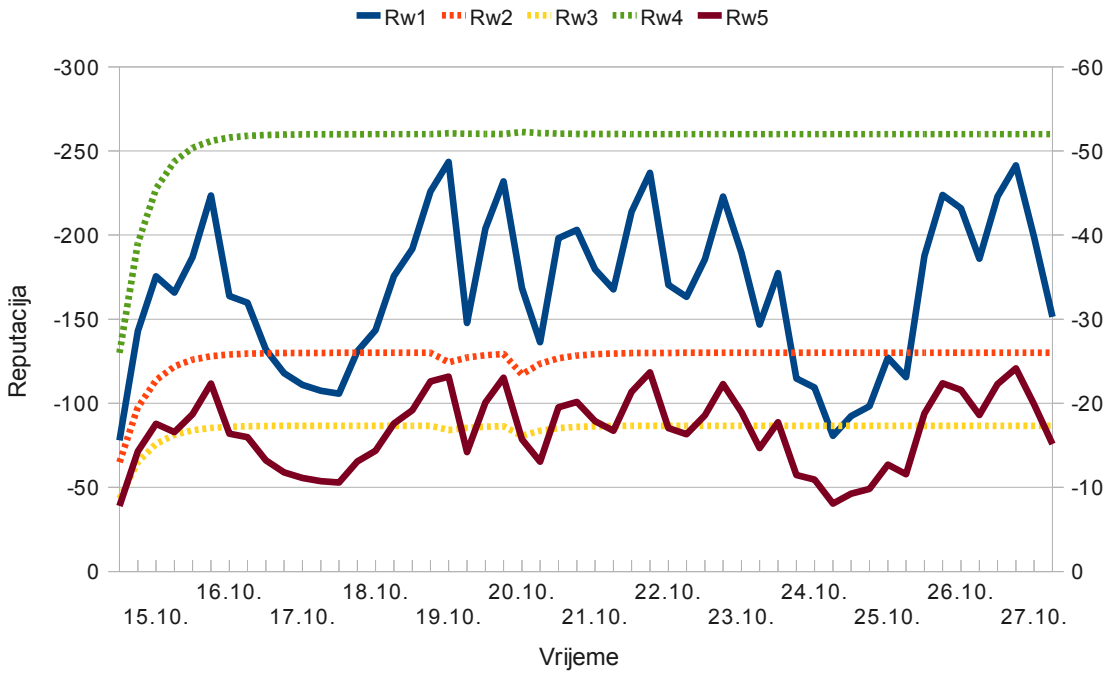
Grafikon 6.3. Reputacija autonomnog sustava AS15169 mjereno iz AS2108

Drugi problem funkcije R_{w1} su veliki skokovi i padovi u vrijednostima reputacije. Općenito, za funkciju reputacije poželjno je da bude što glađa i manje osjetljiva na varijacije u količini prometa. Na grafikonu 6.2 su lijepo vidljivi skokovi i padovi reputacije, ovisno o razdoblju mjerenja. Tijekom dana reputacije dostižu najviše vrijednosti, a tijekom noći najniže. Također, veliki periodi niske negativne reputacije odgovaraju vikendima, kada je količina prometa općenito najmanja. Mjerenje prikazano na grafikonu 6.3 pokazuje mnogo manje skokove što je posljedica promijene parametra d sa 6 na 12 sati (utjecaj parametara na ponašanje funkcija opisan je u poglavlju 6.2.). Ti skokovi su podjednaki u apsolutnim brojkama, ali to je posljedica ukupne veće količine prometa; varijacije su u relativnim odnosima najviših i najnižih vrijednosti mnogo manje. Opet je jasno vidljivo drastično smanjenje negativne reputacije preko vikenda.

Ako gledamo ponašanje ostalih težinskih funkcija na grafovima 6.1, 6.2 i 6.3 uočljivo je nekoliko trendova:

1. funkcije R_{w2} i R_{w3} imaju međusobno vrlo slično ponašanje
2. funkcija R_{w5} prati ponašanje funkcije R_{w1}
3. funkcija R_{w4} u pravilu prati funkcije R_{w2} i R_{w3} iako u određenim slučajevima može imati značajnija odstupanja

Ako za referentnu funkciju uzmemo R_{w2} ili R_{w3} iz mjerenja obavljenih u AS35549 najgori je AS104 (*University of Colorado Boulder*), grafikon 6.4.



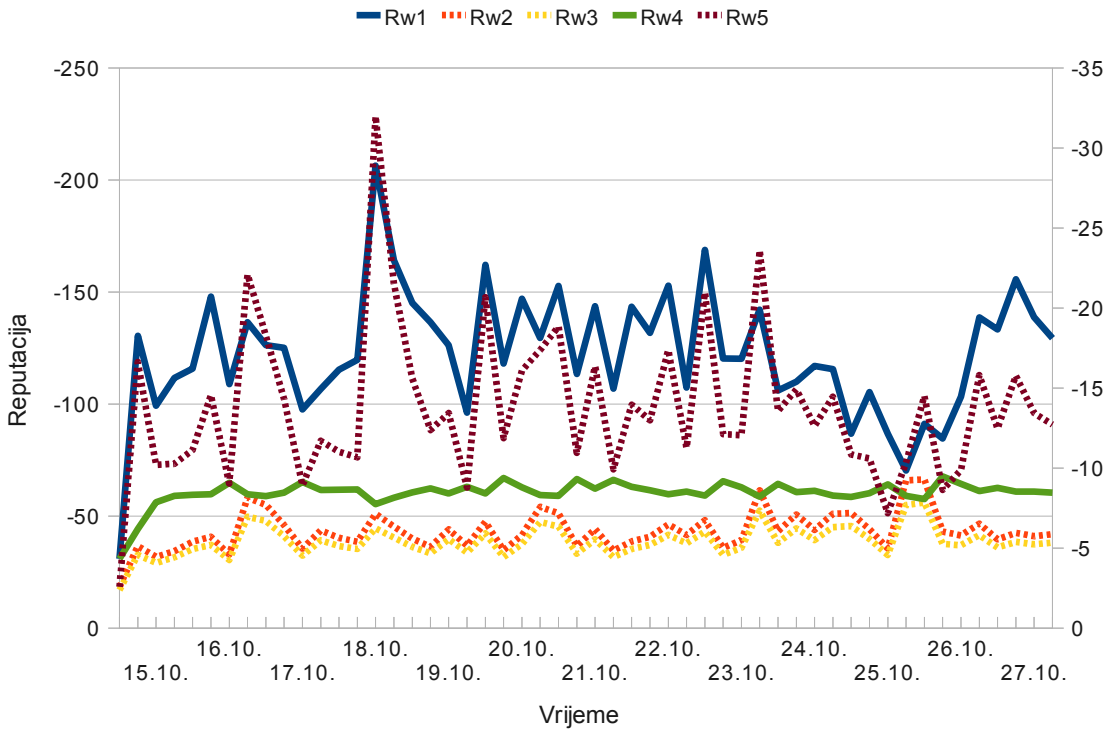
Grafikon 6.4. Reputacija autonomnog sustava AS104 mjereno iz AS35549

Trendovi u ponašanjima funkcija uočljivi su i u ovom slučaju pri čemu se posebno ističe čak previše ustaljena vrijednost reputacije za funkcije R_{w2}, R_{w3} i R_{w4}. I bez analiziranja samog prometa iz grafikona, odnosno lijeve y skale, moguće je naslutiti uzrok takvih rezultata. Riječ je o AS-u male količine ukupnog prometa relativno stalnog dotoka paketa. Kada se pogleda sam promet, odnosno uočene pogreške, otkriva se slabost funkcija R_{w2}, R_{w3} i R_{w4}. Te će funkcije općenito težiti "uglađivanju" grafa, međutim, bit će vrlo ovisne o parametrima mjerenja, odnosno rubnim slučajevima (ovdje je riječ o TTL-u i broju pogrešaka, detaljnije o problemima penaliziranja TTL-a u poglavlju 6.2.).

Pozitivna osobina funkcija R_{w2} i R_{w3} da normaliziraju reputaciju s obzirom na ukupni promet pokazuje se i kao nedostatak. Te funkcije ne mogu razlikovati lošu reputaciju AS-ova malog ukupnog prometa od loše reputacije AS-ova velike količine ukupnog prometa. Tako se u inicijalnim mjerenjima, kao najgori AS-ovi prema funkcijama R_{w2} i R_{w3} redom pojavljuju AS-ovi male količine prometa koji imaju dosta pogrešaka (najčešće je riječ o TTL-u što se, u tom slučaju, ne može smatrati ozbiljnom pogreškom). Tako je moguće, primjerice, da AS104 koji prosječno nema više od 10 paketa u 6 sati promatranja pri čemu ih pola ima pogrešku tipa TTL, postiže gore rezultate od AS-ova koji se ističu u apsolutnim negativnim reputacijama sa stotinama pogrešaka u istom periodu. Prema tome, rezultati

ovih funkcija također ne mogu služiti kao siguran pokazatelj reputacije.

Grafikon 6.5 prikazuje *Advanced Internet Technologies* (AS10843) koji u mjerenjima unutar Metroneta (AS35549) za funkciju R_{w4} daje najgore rezultate. Potrebno je zamijetiti dva detalja na ovom grafu. Lijeva *y* skala otkriva da je riječ o AS-u manje količine prometa. Drugi detalj jest da su funkcije R_{w4} i R_{w5} zamijenile strane grafa (R_{w4} pokazuje veće vrijednosti nego R_{w5}) u odnosu na dosadašnje ponašanje na ranijim grafovima. Razlika je u ponašanju funkcije R_{w4}, dok funkcija R_{w5}, zbog niskih vrijednosti apsolutnih reputacija funkcije R_{w1}, daje također niske vrijednosti. Uočene pogreške za AS10843 otkrivaju da je riječ o AS-u prilično dobrog prometa čija reputacija, zbog ujednačenog ponavljanja istih pogrešaka, izrazito ovisi o vrijednostima parametara. Iz grafova 6.2 i 6.5 mogu se uočiti slabosti funkcije R_{w4}. Grafikon 6.2 pokazuje veliku ovisnost o periodu mjerenja, dok grafikon 6.5 prikazuje ovisnost o količini prometa odnosno parametrima. Istovremeno, funkcije R_{w2} i R_{w3} daju stabilne rezultate i niske vrijednosti, što je u skladu s ukupnim ponašanjem promatranog AS-a.



Grafikon 6.5. Reputacija autonomnog sustava AS10843 mjereno iz AS35549

Funkcija R_{w4} ima još jednu vrlo neugodnu osobinu koja se lako primijeti u popisu najgorih AS-ova prema rezultatima te funkcije. Sve su redom AS-ovi s mnogo prometa i malo ili ništa pogrešaka. Razlog tome je što funkcija nagrađuje samo nepostojanje nijedne pogreške u kojem slučaju je reputacija 0 (to je i nužno jer bi u suprotnom došlo do dijeljenja s nulom). Međutim, ako AS ima makar jednu pogrešku i mnogo ispravnog prometa, njegova će reputacija biti nesrazmjerno negativna. Kriva procjena o količini neispravnog prometa po AS-u i njegovog relativnog odnosa prema ukupnom prometu te penaliziranje svog prometa, čine funkciju R_{w4} vrlo nepouzdanom, barem dok se njeno ponašanje ne korigira

neuračunavanjem kazni za sav promet.

Kako je bilo ranije rečeno, ponašanje funkcije R_{w5} na svim prikazanim grafovima umanjenim vrijednostima slijedi funkciju R_{w1}. Ukupni rezultati najgorih AS-ova ipak nisu identični. To je posljedica činjenice da kroz koeficijent stope pogrešaka funkcija R_{w5} naglašava svaku pogrešku koja nije običan promet. Istovremeno, količinom prometa ruši vrijednost, a težina pojedine pogreške generira rast negativne reputacije.

Sve funkcije pokazuju jaku ovisnost o parametrima i pretpostavkama mjerenja u kojima se koriste. Pažljivim odabirom vrijednosti parametara i usporedbom rezultata pojedinih funkcija moguće je donijeti pouzdanije zaključke o reputacijama i najgorim AS-ovima.

6.2. Analiza ponašanja funkcija prema parametrima

U poglavlju 6.1. uočena su neželjena ponašanja korištenih težinskih funkcija u konačnim rezultatima reputacija i kasnijem traženju ukupno najgorih AS-ova. Ona su jednim dijelom posljedica neispravnih pretpostavki o ponašanju DNS prometa gledano na razini AS-a, odnosno, vrijednostima pojedinih parametara s jedne strane te ograničenjima koje parametri postavljaju na mjerenje s druge strane. Analizom primijećenih pogrešaka AS-ova, koji su u inicijalnim mjerenjima pokazivali najgore rezultate, utvrđeno je da će na kvalitetu procjene reputacije pojedinog AS-a i ponašanje funkcija izrazito utjecati nekoliko parametara:

1. granice podjela veličine TTL-a
2. vrijednost težina pogrešaka TTL-a
3. vrijednost težina pojedinih pogrešaka s posebnim naglaskom na NXDOMAIN
4. duljina perioda računanja reputacija d
5. parametar α
6. metoda računanja najgorih AS-ova

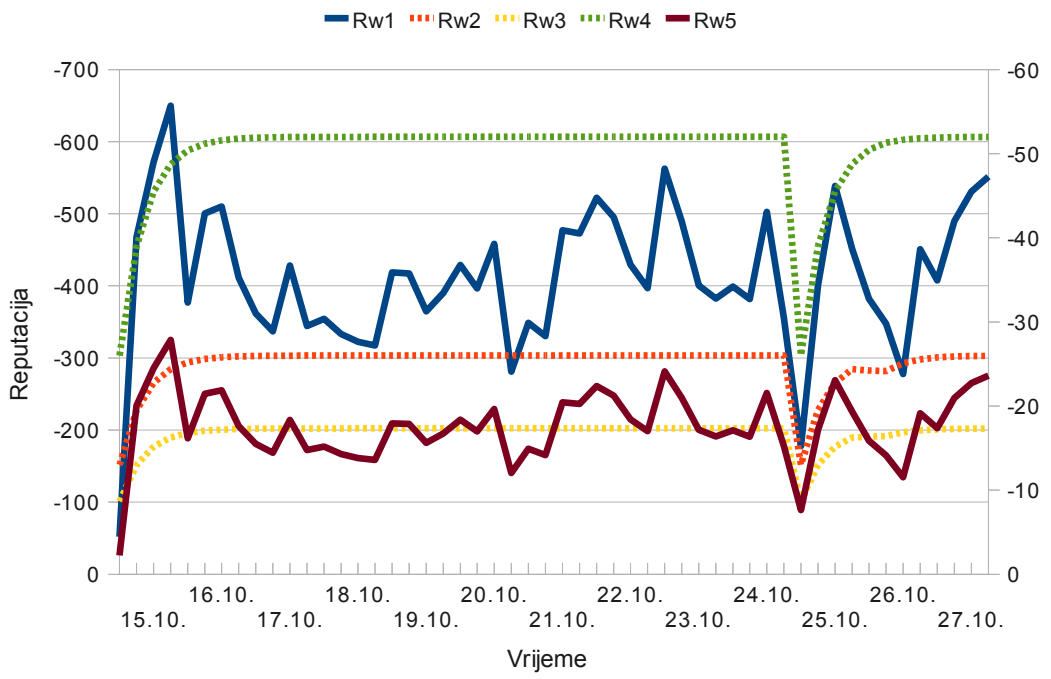
Prvo ograničenje koje je postavljeno na mjerenja jesu granice podjele veličina TTL-a i one imaju identičan utjecaj na sve težinske funkcije. Odabrane su vrijednosti od jednog dana za TTL koji smatramo kratkim (86400 sekundi), tjedan dana koji smatramo srednjim (604800 sekundi), a sve vrijednosti TTL-a veće od toga dugim. Analiza prikupljenog prometa pokazuje da granica od jednog dana za kratki TTL uvjetuje da će velika većina prometa koju penaliziramo zbog TTL-a dobivati kazne za kratki TTL. Sama granica od 86400 sekundi je zapravo vrlo česta osnovna vrijednost trajanja DNS zapisa. U usporedbi s ovako odabranim kratkim TTL-om, srednji TTL se pojavljuje mnogo rjeđe, a dugi gotovo nikada. Posljedice su donekle umanjene implementacijom reputacijskog sustava koji penalizira samo TTL u odgovorima dok ignorira TTL u ostalim zapisima. U slučaju kada bi se penalizirao TTL u svakom DNS zapisu resursa svakog DNS paketa, TTL bi još mnogo drastičnije utjecao na konačne rezultate te bi bio dominantna vrsta pogreške.

Najosjetljivija jest upravo granica kratkog TTL-a od 86400 sekundi. Kada bi se ona smanjila za samo jednu sekundu, veliki broj pogrešaka TTL-a dobio bi oznaku srednjeg TTL-a, npr. na ZEMRIS-ovom poslužitelju takva promjena uvjetuje da praktički svi odgovori dobivaju oznaku srednjeg TTL-a. Ista stvar ne mora vrijedi za velike AS-ove

poput Google Inc., ali to ukazuje da su njihovi odgovori uglavnom zaista kratkog TTL, što ne možemo smatrati dobrim, pa ih je opravdano penalizirati.

Ključan faktor je brojnost TTL pogrešaka. Reputacijski sustav kažnjava samo TTL pogreške u *polju odgovora* DNS odgovora te je na taj način broj TTL pogrešaka reda veličine ukupnog broja DNS paketa i varira od trećine do polovine ukupne količine paketa. To ukazuje da ako koristimo penaliziranje TTL-a kako god postavili granice vremenskog raspona TTL-a on će uvijek imati značajan utjecaj na ponašanje težinskih funkcija odnosno konačnu reputaciju.

Drugi važan faktor koji direktnije utječe na ponašanje težinskih funkcija jest težina pogrešaka tipa TTL. U inicijalnim mjerenjima neispravno je pretpostavljen razmjer ukupnog broja DNS paketa, broja pogreška te vrste tih pogrešaka. Naknadno je utvrđeno da će dobar dio pogrešaka biti upravo tipa TTL pa time i težina takvih pogrešaka ima značajan utjecaj. Visoke kazne za pogreške tipa TTL su zato dominirale rezultatima inicijalnih mjerenja. Grafikon 6.6 pokazuje reputaciji Ripple web AS-a (AS36053) prema inicijalnim mjerenjima unutar AS35549:



Grafikon 6.6. Reputacija autonomnog sustava AS36053 mjereno iz AS35549

AS36053 je prema funkcijama R_{w2} i R_{w3} AS s drugom najgorom reputacijom. Njegova reputacija se temeljila na stalnom prometu obilježenom isključivo TTL pogreškama. Uzimajući u obzir dominantnost TTL-a znatnim smanjivanjem težina TTL pogrešaka za AS36053 postižu se bitno drugačiji rezultati. Rezultati težinskih funkcija su očekivano smanjeni, iako njihovo ponašanje ostaje skoro identično. Posljedica je da AS36053, koji je inicijalno bio prepoznat kao izrazito loš, a koji nije radio druge pogreške osim TTL-a, sada svojim vrijednostima je daleko bolji od najgorih AS-ova. Prosječne vrijednosti najgorih AS-ova prema funkciji R_{w2} kreću se oko 5.8, dok je reputacija AS36053 u novom računanju prosječno oko 2.5. Izračunata reputacija s novim vrijednostima TTL-a prikazala je nove

najgore AS-ove prema funkcijama R_{w2} i R_{w3}, *University of Iowa* (Sveučilište u Iowi, AS3676) i Infolink (AS15083). Zanimljiva posljedica promijene težina pogrešaka TTL-a su i rezultati koje pokazuju funkcije R_{w1} i R_{w5}. Google Inc. koji je dosad uvijek držao mjesto najgoreg AS-a ili bio među najgorima, prema tim funkcijama, sada pada tek na jedanaesto mjesto. Na prvom mjestu se pojavljuju Columbus network access point (AS10297), a na drugom Amazon (AS14618). Sveučilište u Iowi, Infolink, Columbus network access point i Amazon pokazuju vrlo veliku količinu NXDOMAIN odgovora što navodi na drugu najutjecajniju pogrešku DNS prometa.

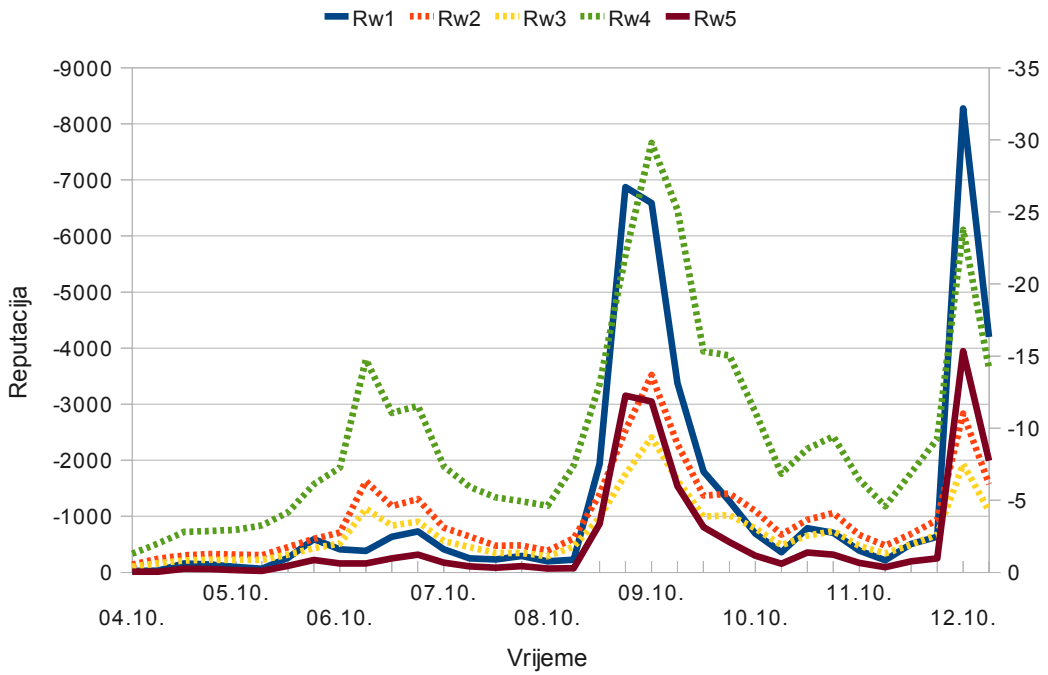
Na reputaciju osim TTL-a ponajviše utječu pogreške tipa NXDOMAIN. Većina najgorih AS-ova u popisu zabilježenih pogrešaka ima veliki broj NXDOMAIN pogrešaka, TTL pogrešaka ili oboje. Promjenom težine NXDOMAIN pogreške može se mijenjati utjecaj tog tipa pogreške na konačnu reputaciju. Međutim, smanjivanjem težine te pogreške na pola inicijalne vrijednosti postignut je relativno malen učinak. Popis najgorih AS-ova, gledano s mjerne točke ZEMRIS-ova poslužitelja za funkcije R_{w1} i R_{w5}, ne mijenja se značajnije, a razlike su zapravo samo u rasporedu istih AS-ova, npr. Amazon (AS14618) pada sa šestog na dvanaesto mjesto. Razlog tome je što se popis njegovih pogrešaka uglavnom sastoji od NXDOMAIN pogrešaka. S druge strane primjerice Metronet (AS35549) skače sa sedmog na četvrto mjesto, što je očekivano, s obzirom da se njegove pogreške uglavnom ne sastoje od NXDOMAIN pogrešaka.

Opisano ponašanje ne vrijedi za funkcije R_{w2} i R_{w3} čiji rezultati ostaju praktički nepromijenjeni. Popis najgorih AS-ova prema tim funkcijama se sastoji od AS-ova s većom količinom SERVFAIL pogrešaka ili kombinacijama s drugim pogreškama s većim težinama od NXDOMAIN pogreške. To pokazuje da će funkcije R_{w2} i R_{w3} uvijek isticati AS-ove koji imaju najgoru kombinaciju najveće količine najtežih pogrešaka u što manjem prometu, što se može smatrati obrnutim ponašanje od funkcija R_{w1} i R_{w5} koje će isticati AS-ove s najvećom ukupnom količinom pogrešaka i njihovih težina.

Eventualno daljnje smanjivanje težine NXDOMAIN pogreške bi moglo značajnije mijenjati rezultate, ali takav postupak nema opravdanja. NXDOMAIN već sada ima prilično niske vrijednosti težina, a učestalost pojavljivanja te pogreške je vrlo velika što ne sugerira potrebu daljnjeg smanjivanja (osim u smislu da je ta pogreška očekivana i treba biti malo kažnjena). Drugi razlog protiv je i uočena *homogenost* pogrešaka po AS-ovima. Tendencija je da AS-ovi imaju izraženije pojavljivanje neke od pogrešaka, pa bi dodatnim smanjivanjem težine NXDOMAIN bilo postignuto svojevrsno favoriziranje AS-ova u kojima je NXDOMAIN dominantna pogreška, odnosno favoriziranje same NXDOMAIN pogreške.

Opisani parametri će zbog relativne homogenosti pogreška po AS-ovima pretežno utjecati na konačnu vrijednost funkcije, a u manjoj mjeri na njeno ponašanje. Parametri d i α s druge strane bitnije će utjecati na ponašanje funkcija.

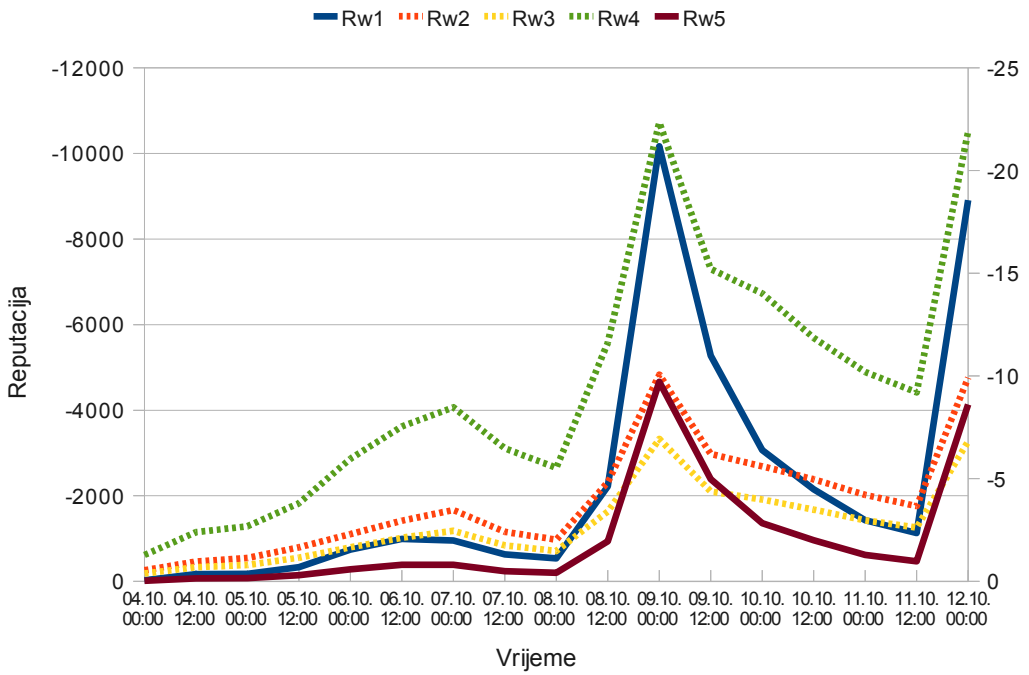
Analizu ponašanja funkcija prema parametrima d i α ćemo prikazati na reputaciji indijske nacionalne okosnice (*National Internet Backbone*, AS9829). Grafikon 6.7. prikazuje reputaciju kako ju vidi ZEMRIS-ov poslužitelj pri čemu je $d = 4$ (period 6 sati) i $\alpha = 0.5$. AS9829 ispočetka ima relativno malo prometa, no u dva razdoblja mjerenja postiže vrlo velike šiljke, što ukazuje na drastično povećanje prometa u tim razdobljima. Među uočenim pogreškama prevladavaju REFUSED, kratki i srednji TTL te NXDOMAIN.



Grafikon 6.7. Reputacija AS9829, d = 4, α = 0.5, mjereno iz AS2108

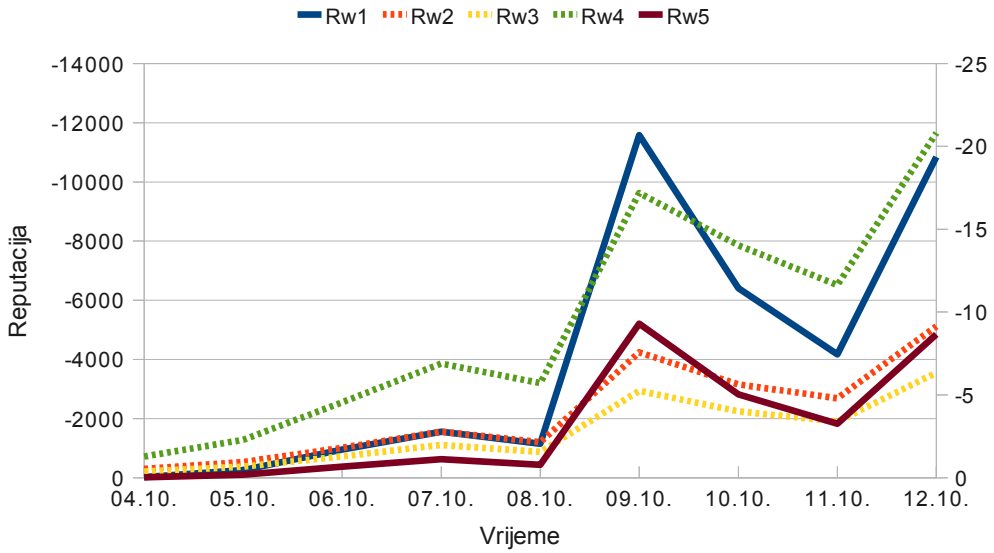
Skokovi funkcijskih vrijednosti mogu služiti za analizu stabilnost pojedine funkcije. R_{w1} u najvećem skoku ima omjer najviše i najniže vrijednosti veći od 70, dok je vrijednost tog istog omjera kod funkcije R_{w3} svega 10. Grafovi prikazuju sitnije promjene reputacije, što je posljedica kraćeg perioda mjerenja od 6 sati. S druge strane, to funkcije čini manje stabilnima, tj. skokove većima. Funkcija R_{w4} u razdobljima skokova prometa približava se vrijednosti najčešće pogreške, u ovom slučaju REFUSED s težinom 40.

Grafikon 6.8. prikazuje također reputaciju AS9829 samo što je djelitelj smanjen na d = 2 (period 12 sati). Očekivano graf prikazuje mnogo manje detalja što je posljedica grupiranja prometa u većim periodima računanja reputacije. Skokovi u vrijednostima funkcija su i dalje prisutni jer je riječ o izrazito velikim porastima prometa tijekom dva dana, ali su omjeri najvećih i najmanjih vrijednosti bitno smanjene pa je time i ponašanje funkcija stabilnije. Funkcija R_{w1} sada ima omjer najvećih i najmanjih vrijednosti oko 20 dok za funkciju R_{w3} taj omjer pada prema 3. Zbog duljeg perioda apsolutne vrijednosti funkcije R_{w1} su značajno veće dok će na funkcije R_{w2} i R_{w3} povećanje perioda djelovati kao smanjenje vrijednosti zbog dijeljenja s većom sumom ukupnog prometa.



Grafikon 6.8. Reputacija AS9829, d = 2, α = 0.5, mjereno iz AS2108

Na grafikonu 6.9. prikazana je zadnja promjena parametra d = 1 dok su ostali parametri ostali isti. Kako je period sada 24 sata, grupirane su još već količine prometa te se time dodatno gubi na detaljnosti grafa. Funkcije zato pokazuju veću stabilnost. Skokovi u prometu i dalje su jasno vidljivi, ali su razlike u najnižim i najvišim vrijednostima još manje. Tako je za funkciju R_{w1} omjer najvećih i najmanjih vrijednosti oko 11, a za funkciju R_{w3} pada prema 2.5. Rast funkcije R_{w5} se s povećanjem perioda računanja stabilizira i njene maksimalne vrijednosti više ne rastu iznad ranije postignutih maksimuma.



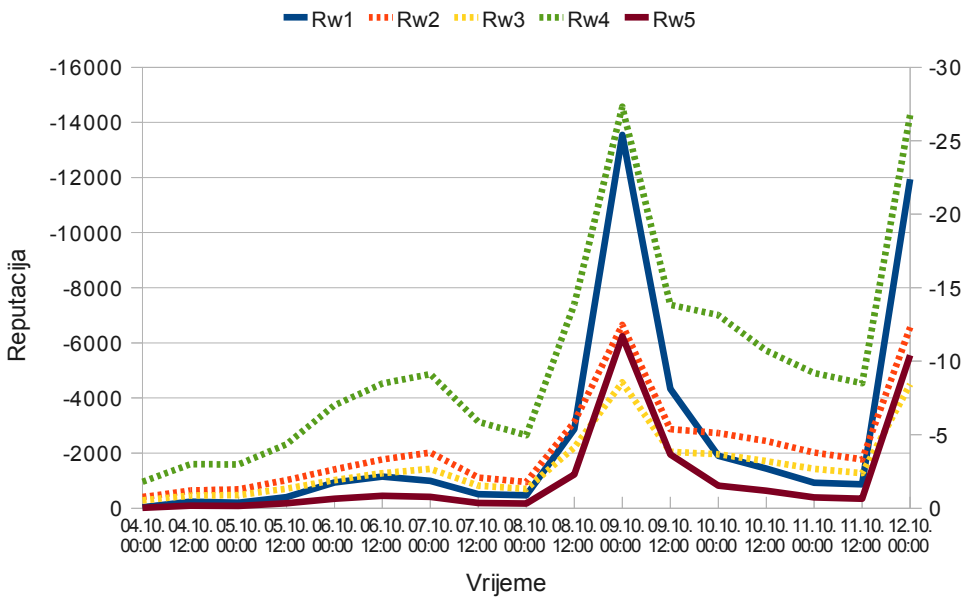
Grafikon 6.9. Reputacija AS9829 d = 1, α = 0.5, mjereno iz AS2108

Na ovim primjerima pokazano je ponašanje funkcija prema parametru *d*, i može se sažeti tako da, ako se želi postići veća detaljnost rezultata, to se može postići povećanjem parametra *d* odnosno smanjivanjem perioda računanja reputacije. To će za posljedicu imati smanjenje stabilnosti funkcije. Ako je cilj imati stabilniju funkciju otporniju na brze promijene reputacije, potrebno je smanjiti parametar *d*, odnosno, povećati period računanja. Pritom treba paziti da će smanjenje parametra *d* imati za posljedicu rast vrijednosti funkcija R_{w1} i R_{w5} i pad vrijednosti funkcija R_{w2} i R_{w3}. Vrijedi i obrnuto.

Kod analize rezultata treba paziti i na nejednakost vremenskih zona i njihovom vezom s parametrom *d*. Ponašanja reputacija AS-ova mogu se jednim dijelom dovesti u vezu s razdobljima u danu ili tjednu. Očekivano, promet je veći i više je pogrešaka tijekom radnih dana i preko dana, a manji noću i vikendima. Periodi računanja reputacije se poravnavaju prema uvijek istom početnom trenu, ponoći, a vremenske oznake pojedinih paketa dodjeljuju se prema trenutku kada stižu na mjernu točku, međutim, ignorira se vremenska zona iz koje paket dolazi.

Iz tog razloga, očekivan je vremenski pomak maksimalnog prometa pojedinih AS-ova, ovisno kada u njihovim originalnim vremenskim zonama dolazi do maksimalnog prometa. Tako je kod kraćih perioda računanja, odnosno većih djelitelja *d*, moguća veća osjetljivost rezultata na vremenske zone odnosno radna vremena u pojedinim vremenskim zonama. Kod duljih perioda računanja, poput jednog dana, utjecaj vremenskih zona će biti manji, iako se može pokazati kao vremensko "kašnjenje" rezultata ili dijeljenje skupina pogrešaka na više mjernih razdoblja.

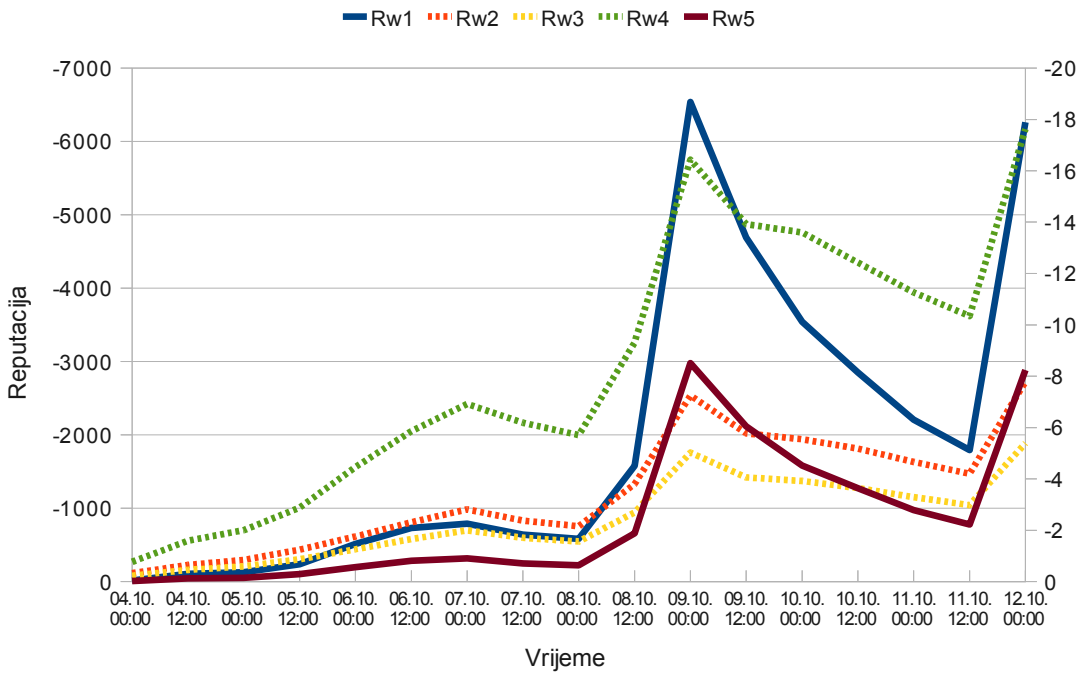
Zadnji parametar čiji utjecaj ćemo promotriti je α. Promjene ponašanja funkcija ovisno o parametru α prikazat ćemo također na AS9829. α predstavlja faktor opadanja, pri čemu manje vrijednosti daju prednost novim reputacijama, a veće starim. Grafikon 6.10. prikazuje reputaciju s parametrom $\alpha = 0.3$, grafikon 6.8. reputaciju s parametrom $\alpha = 0.5$, a grafikon 6.11. reputaciju s parametrom $\alpha = 0.7$. U sva tri slučaja parametar $d = 2$.



Grafikon 6.10. Reputacija AS9829, $d = 2$, $\alpha = 0.3$, AS2108

Grafikon 6.10. pokazuje da manje vrijednosti parametra α znače brže mijenjanje reputacije funkcije, odnosno da će funkcije biti nestabilnije. Također, funkcije će davati veće vrijednoti i skokovi između najvećih i najmanjih vrijednosti će biti veći. Povećanjem faktora α smanjuju se vrijednosti pojedinih reputacija i skokovi su manji, tj. funkcije su stabilnije.

Grafikon 6.11. pokazuje i efekt zadržavanja postignute razine reputacije kod većih vrijednosti faktora α kako nakon većeg skoka u reputaciji pad na niže vrijednosti je mnogo blaži. Općenito se može reći da, ako se želi postići stabilniju funkciju, treba koristiti veći α, a ako želimo brže promijene, što bi odgovarala potrebi više detalja u grafu, odnosno kraćih vremena računanja, treba koristiti manji α.



Grafikon 6.11. Reputacija AS9829, d = 2, α = 0.7, mjereno iz AS2108

Osim navedenih parametara koji se odražavaju na rezultate pojedinih funkcija, pri traženju najgorih AS-ova dodatno će utjecati i metoda računanja najgorih AS-ova traženjem aritmetičke sredine reputacija pojedinog AS-a. Moguće je da se pojedini AS pojavi samo u zadnjem periodu mjerenja s relativno visokim negativnim reputacijama, pa da takav AS bude prepoznat kao vrlo loš. To se posebno odnosi na najgore AS-ove prema rezultatima funkcija R_{w2} i R_{w3}. S druge strane, funkcije R_{w1} i R_{w5} neće pokazivati taj problem jer, ako bi se u zadnjem periodu pojavio AS s dovoljno lošom reputacijom da po apsolutnim vrijednostima dostigne ostale najgore AS-ove, prepoznavanje tog AS-a kao lošeg bi svakako bilo opravdano.

Metoda računanja najgorih AS-ova bi se mogla prilagoditi tako da se suma reputacija ne dijeli s brojem izračunatih reputacija pojedinog AS već s ukupnim brojem računanja reputacija za to mjerenje. Takav pristup bi riješio ranije opisan problem, ali uz cijenu favoriziranja mjernog razdoblja. To znači da bi svi AS-ovi čiji se promet pojavio kasnije u mjernom razdoblju nužno imali bolje rezultate, iako je zabilježen promet možda tek

početak lošeg ponašanja tog AS-a. Također, moguće je da neki AS ima kratak period vrlo lošeg prometa poput DoS napada čije bi značenje onda bilo umanjeno.

S obzirom na ranije analize moguće je odrediti optimalne parametre za određene namjene. Ako nam je potrebno postići stabilnije funkcije ili nije ključno imati česte promjene reputacije, potrebno je birati manje vrijednosti parametra d i veće vrijednosti parametra α. Također, s obzirom na utjecaj pogrešaka tipa TTL i NXDOMAIN, poželjne su manje vrijednosti težina za te pogreške.

6.3. Najgori AS-ovi

Na temelju prethodnih analiza ponašanja funkcija i rezultata koje prikazuju, moguće je odrediti najgore AS-ove. Popis najgorih AS-ova gradi se prema rezultatima pet mjernih točaka (dva mjerenja su napravljena na istom poslužitelju, ali u dva odvojena razdoblja) tako da svaka mjerna točka daje odvojenu listu najgorih AS-ova.

Kao optimalni parametri za računanje reputacije uzeti su $\alpha = 0.7$ i $d = 1$, jer osiguravaju najstabilnije ponašanje funkcija, što je u računanju kumulativnih rezultata poput najgorih AS-ova na nekom vremenskom rasponu mnogo bitnije od detaljnosti promjena reputacije. Prema analizama iz prethodnog poglavlja promijenjene su i težine pojedinih pogrešaka, tablica 6.1.

Tablica 6.1. Ocjena pogrešaka klijenta i poslužitelja

Pogreška	Klijent	Poslužitelj
Odgovori na upite s greškom	- 40	- 10
Upiti koje odbija DNS poslužitelj (REFUSED)	- 20	- 5
Upiti koji su propušteni zbog greške na poslužitelju (SERVFAIL)	- 10	- 20
Upiti koji traže nepostojeće domene (NXDOMAIN)	- 15	- 5
Upiti čija vrsta nije implementirana na DNS poslužitelju	- 30	- 20
Upiti za lokalne adrese – RFC 1918	- 50	0
Nepostojeće vršne domene (TLD)	- 60	0
A upiti za IP adresu (A za A)	- 60	0
Uporaba pristupa 0	- 30	- 20
Upiti s nepostojećim (nedopuštenim) znakovima	- 30	0
Upiti nepostojećeg razreda	- 40	0
Zastarjeli i eksperimentalni upiti	- 30	- 30

Prvi korak je računanje najgorih AS-ova kako ih na mjernim točkama vide pojedine težinske funkcije. To se postiže računanjem aritmetičke sredine vrijednosti reputacije za promatranu težinsku funkciju na cijelom rasponu vremena promatranja. Djelitelj sume aritmetičke sredine je broj dana mjerenja i razlikuje se od točke do točke.

Drugi korak je koreliranje rezultata najgorih AS-ova prema pojedinim težinskim funkcijama kako bi se utvrdili AS-ovi koji daju najgore rezultate u više funkcija istovremeno. Da bi AS bio loš, odnosno najgori, mora biti što više pozicioniran na svim

popisima najgorih AS-ova prema težinskim funkcijama. Funkcije R_{w1} i R_{w5} će isticati AS-ove s puno prometa i puno pogrešaka, a funkcije R_{w2} i R_{w3} AS-ove s najgorim omjerom pogrešaka i prometa. Metoda korelacije rezultata za različite funkcije služi izbjegavanju neželjenih ponašanja pojedinih funkcija, npr. za R_{w1} da kao najgore prepoznaje AS-ove s mnogo prometa, a za R_{w2} da ističe AS-ove s malom količinom prometa s puno grešaka. AS koji je visoko pozicioniran na obje funkcije će zato imati i mnogo prometa i mnogo grešaka po prometu.

Tablica 6.2. prikazuje dvadeset najgorih AS-ova podijeljenih po mjernim točkama. Prva dva stupca prikazuju mjerenje na ZEMRIS-ovom poslužitelju u dva različita razdoblja (CARNET), treće je mjerenje u Keyweb AS-u, četvrto mjerenje u Metronet AS-u, a peto AS47988 kao druga manja mjerna točka Metroneta. Prvi redak tablice sadrži brojeve AS-ova mjernih točaka, pri čemu prva dva još imaju i oznaku dana završetka mjerenja(12, 30), a stupaci ispod oznaka MT poredak najgorih AS-ova od prvog do dvadesetog.

Tablica 6.2. Reputacija dvadeset najgorih AS-ova za pet mjernih točaka

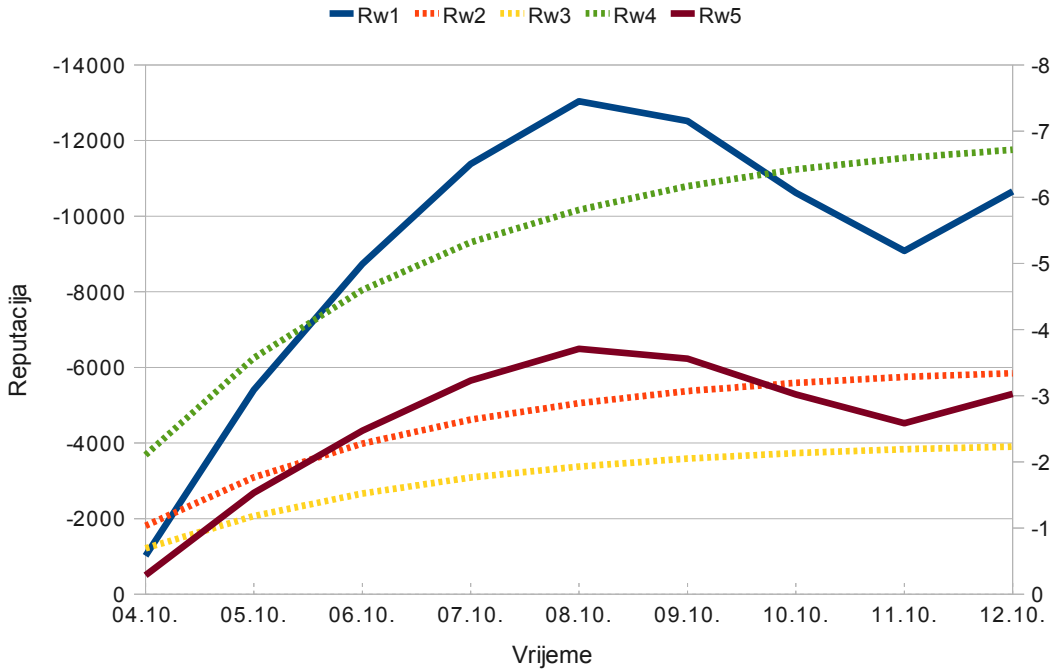
MT	2108 12	2108 30	31103	35549	47988	MT	2108 12	2108 30	31103	35549	49788
#						#					
1.	10297	10297	36692	15083	6939	**11.**	3265	3599	5391	39326	3676
2.	15083	45899	4134	29550	14618	**12.**	7011	12705	45839	6730	33517
3.	45899	15083	4608	3676	47955	**13.**	33	6849	18366	24940	17370
4.	29550	29550	3356	10297	112	**14.**	10451	7011	680	5078	26496
5.	14618	22927	15169	3599	15083	**15.**	4837	5384	36629	5430	4608
6.	3599	8358	24940	5388	10297	**16.**	24863	22576	4837	7545	786
7.	5391	14618	3462	7754	3599	**17.**	18403	33	3333	12392	3265
8.	17974	17974	4777	17370	22576	**18.**	22927	24863	36619	13238	6730
9.	6478	45595	2108	8069	4323	**19.**	7754	18403	1853	19104	174
10.	9829	4134	2914	21788	29550	**20.**	33517	17908	1653	10451	7754

Kao najgori AS, gledano iz mjerene točke ZEMRIS-ova poslužitelja, pokazuje se *The Columbus network access point* (AS10297), što je web hosting kompanija iz Ohia, SAD. Prvo mjesto zaslužio je izrazito velikom količinom NXDOMAIN odgovora u usporedbi s ukupnim prometom. Brojka je velika i kao omjer i u apsolutnim razmjerima. Također, greške su ponekad i kratki TTL. Na prvom mjestu kao najgori AS je u oba mjerenja na ZEMRIS-ovom poslužitelju, a pregledavanjem strukture pogrešaka jasno je da ima isto ponašanje u oba mjerenja. Zanimljivo je da se isti AS pojavljuje kao četvrti najgori u mjerenju na Metronetu pri čemu mu je ponašanje identično onom na ZEMRIS-u. Običan upit na *www.google.com* za drugi rezultat daje blog *blog.stopbadware.org* [17] koji *Columbus network access point* spominje kao nositelja IP adrese jednog od deset najzaraženijih poslužitelja za ožujak 2008. godine. Stranica *hostexploit.com* [18] prepoznaje AS10297 kao osamnaestu najzaraženiju mrežu za prvi kvartal 2010. godine (napad phising). Grafikon 6.12 prikazuje reputaciju za AS10297 u prvom mjerenju od 4.10.2010. do 12.10.2010. na ZEMRIS-ovom poslužitelju.

Kako se reputacija prvenstveno sastoji od NXDOMAIN pogrešaka, koje čine prosječno oko polovice ukupnog prometa u bilo kojem razdoblju, funkcije R_{w2} i R_{w3} su vrlo stabilne. Funkcije R_{w1} i R_{w5} otkrivaju promjene u količini prometa po razdobljima. Težina NXDOMAIN pogreške na strani poslužitelja je -5, pa se funkcija R_{w4} kreće oko te vrijednosti.

Dva mjerenja na ZEMRIS-ovom poslužitelju pokazuju slične rezultate pri čemu se samo manje mijenja raspored najgorih AS-ova. Među najgorima su još i:

1. *Infolink* (AS15083) IT kompanija iz Miamia, SAD-a
2. *Vietnam network information center* (AS45899) odnosno *VNPT Corp*. vijetnamske pošte i telekomunikacije,
3. *Simply transit* (AS29550) pružatelj mrežnih usluga iz Velike Britanije
4. *Amazon web services* (AS14618), dio Amazon.com, Inc.



Grafikon 6.12. Reputacija The Columbus network access pointa AS10297, mjereno iz AS2108

Od prvih pet najzanimljiviji je još AS45899 vijetnamskih pošta i telekomunikacija koji se također pojavljuje na popisu 50 najgorih stranice hostexploit.com [18]. Nalazi se na 28. mjestu zbog slanja neželjene pošte. Ispis pogrešaka pokazuje da se neispravan promet svodi na REFUSED pogreške tijekom cijelog razdoblja mjerenja.

Zanimljivo je da je jedan od najgorih i Amazon web services (AS14618). Razlog tome su velike količine NXDOMAIN odgovora i manja količina kratkog TTL-a, a broj pogrešaka je velik u usporedbi s ukupnim prometom. Općenito, veći internetski servisi i kompanije s puno prometa lakše će dolaziti na listu najgorih. To je prvenstveno posljedica kažnjavanja negativnih odgovora koje smo uključili kao neželjen DNS promet. Dijelom je riječ o slabosti sustava, ali isto tako dio krivnje je na samim kompanija. Ranije je spomenuto da

npr. Google izdaje odgovore kratkog TTL, i iako ponekad može biti za to potrebe, tako velike količine ipak nemaju opravdanja. Slično vrijedi i za slučaj Amazona. Nemoguće je bez detaljne analize paketa utvrditi razloge velikog broja NXDOMAIN odgovora, ali činjenica da praktički svaki drugi odgovor ima NXDOMAIN oznaku ne može biti prihvatljiva. Osim toga, jasno je da veliko ime ne garantira i ispravnost prometa, npr. Google se nalazi na 37. mjestu hostexploit.com [18] popisa najgorih zbog slanja neželjene pošte.

Visoko na popisu najgorih prema mjernoj točki ZEMRIS-ova poslužitelja je i T-HT (AS5391). Ispis pokazuje različite vrste pogrešaka, međutim, s izrazitom dominacijom kratkog TTL-a, u ulozi AS-a poslužitelja. Mnogo je i negativnih odgovora tipa REFUSED, u ulozi AS-a klijenta. Donekle je bilo očekivano da će T-HT zbog ukupne velike količine prometa lakše izbiti visoko na listi najgorih, ali činjenica da poslužitelji unutar T-HT AS-a izdaju gotovo sve uhvaćene kratke TTL-ov, te da klijenti unutar T-HT-a izazivaju sve REFUSED odgovore ZEMRIS-ova poslužitelja, nije ohrabrujuća. Slučaj T-HT svakako zahtjeva detaljnije analize te ukazuje da bi u stvarnom okruženju reputacijski sustav trebao posebnu pažnju kod određivanja reputacija posvećivati AS-ovima s kojima razmjenjuje mnogo prometa.

Od ostalih najgorih AS-ova dva se ističu po velikoj količini različitih pogrešaka, kratki TTL, NXDOMAIN, REFUSED, SERVFAIL, *format error*. To su AS17974 *PT Telekomunikasi Indonesia* indonezijski telekomunikacijski operater i AS4134 *CHINANET-BACKBONE* koji je dvadeseti na popisu najgorih prema hostexploit.com [18] zbog održavanja poslužitelja malicioznih programa (*malware server*).

Treba spomenuti i AS22576 *Layered Technologies* iz SAD-a. Pogreške se uglavnom svode na NXDOMAIN i niski TTL. Kako taj AS stvara velike količine neispravnog prometa vjerojatno bi bio i više na popisu najgorih, ali istovremeno dobar dio upita je tipa DNSBL što mu popravlja ukupnu reputaciju.

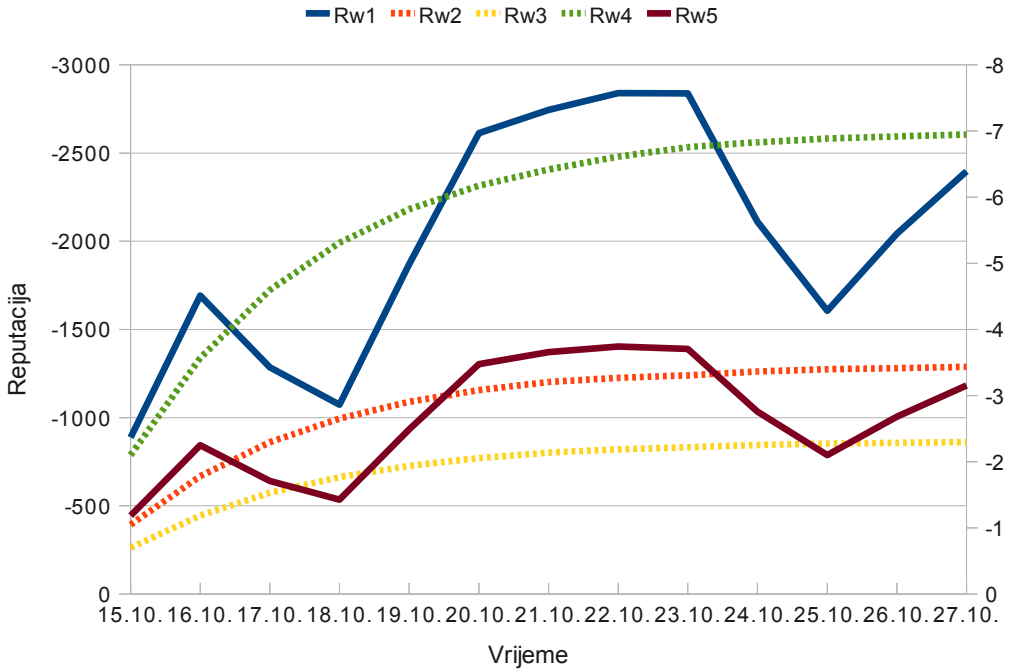
Ako uspoređujemo popis najgorih AS-ova s popisom iz Friščić 2010. [16] on se podudara u više rezultata. To mjerenje se temeljilo na promatranju količine neželjene pošte prikupljeno na FER-ovom poslužitelju u razdoblju od srpnja do prosinca 2009. godine. Najgori AS u tom mjerenju je AS45899 VNPT koji je već ranije spomenut kao drugi najgori AS u drugom mjerenju na ZEMRIS-ovom poslužitelju te kao 28. najgori prema hostexploit.com [18]. Osim VNPT-a zajednički su još i AS4837 *China169-backbone*, AS4134 CHINANET-BACKBONE dvadeseti na hostexploit.com, AS9829 *National Internet Backbone Bharat Sanchar Nigam Limited* iz Indije te AS18403 *FPT Telecom* iz Vijetnama.

Analiza dvadeset najgorih AS-ova, kako ih vidi mjerna točka Metronet (AS35549) pokazuje mnoga podudaranja s rezultatima dva mjerenja na mjernoj točki ZEMRIS, odnosno CARNET AS-a. Pet najgorih su:

1. Infolink (AS15083), grafikon 6.13
2. Simply transit (AS29550)
3. *University of Iowa* (AS3676)
4. The Columbus network access point (AS10297)

5. *Berbee Information Networks Corporation CDW Technologies* (AS3599)

Od pet najgorih na Metronetu, četiri se podudaraju s rezultatima mjerenja na ZEMRIS-u, a od toga su tri u prvih pet najgorih na ZEMRIS-u, Infolink, Simply transit i The Columbus network access point, a četvrti je šesti po redu najgori na ZEMRIS-u, Berbee Information Networks Corporation CDW Technologies. Jedini kojeg nema na popisu najgorih na ZEMRIS-u je University of Iowa (AS3676).



Grafikon 6.13. Reputacija Infolinka, AS15083, mjereno iz AS35549

Iako poslužitelj u Metronet AS-u po apsolutnim vrijednostima ima mnogo manje prometa od ZEMRIS-ova poslužitelja kada se usporede pogreške zajedničkih najgorih AS-ova, vidljivo je da nema značajne razlike niti u vrsti pogrešaka, niti u količini pogrešaka po ukupnom prometu.

Najzanimljivije je ponovno pojavljivanje The Columbus network access pointa kao jednog od najgorih, no on nije jedini AS koji je naveden na hostexploit.com, a koji se pojavljuje na popisu najgorih. Na desetom mjestu mjerenja na Metronetu je *BurstNET Technologies, Inc.,* također ponekad naveden kao *Network Operations Center Inc.* (AS21788) koji je na hostexploit.com rangiran kao 37. najgori AS zbog održavanja Zeus distribuirane mreže zaraženih računala (*Zeus botnet*).

AS49788 možemo smatrati drugom mjernom točkom unutar Metronet AS-a. Iz tog razloga je zanimljivo usporediti rezultate mjerenja s rezultatima na Metronetu. Pet najgorih AS-ova prema AS49778 je:

1. *Hurricane electric*, pružatelj mrežnih usluga iz SAD-a (AS6939)
2. Amazon Web Services, Elastic Compute Cloud, EC2 (AS14618)
3. *Citycom*, pružatelj mrežnih usluga iz Rusije (AS47955)

4. poslužitelj inverznih upita RFC1918 adresa (AS112)
5. Infolink (AS15083)

Gotovo svi AS-ovi s popisa najgorih se podudaraju s mjerenjima na drugim mjernim točkama, a gotovo pola s mjerenjem u Metronet AS-u. Posebno treba istaknuti ponovno pojavljivanje Infolinka, The Columbus network access pointa na šestom mjestu, Simply trasita na desetom mjestu i Berbee Information Networks Corporation CDW Technologies na sedmom mjestu.

Na četrnaestom mjestu se nalazi *www.godaddy.com* koji na hostexploit.com zauzima 48 mjesto radi održavanja poslužitelja malicioznih programa [18].

Popis najgorih sadržava i dva *McAfee Inc.* autonomna sustava, AS17370 i AS7754. McAfee se pojavljuje i u mjerenjima na ZEMRIS-u i na Metronetu. Razlog su u svim slučajevima NXDOMAIN odgovori.

Treći najgori prema mjerenjima na AS49788 je AS112. Riječ je o korijenskom poslužitelju koji poslužuje neispravne inverzne upite koji sadrže RFC1918 adrese. Razlog tome je što poslužitelj na kojem je sniman promet postavlja mnogo neispravnih RFC1918 upita te od AS112 poslužitelja dobiva negativne odgovore. Riječ je o manjkavosti reputacijskog sustava koji nije u stanju prepoznati da RFC1918 odgovore daje za to nadležni poslužitelj, a ne da je riječ o neispravnom uhvaćenom tranzitnom prometu.

AS49788 je mjerna točka s mnogo manje prometa od ostalih mjernih točaka, a kako količina prometa u apsolutnim vrijednostima nije velika može se očekivati da to donekle utječe na rezultate. Ipak, uporno pojavljivanje istih AS-ova na popisima najgorih AS-ova sugerira da su rezultati dobrim dijelom ispravni.

Zadnje mjerenje je izvedeno na prometu snimljenom u Keyweb AS-u (AS31103). Promet je sniman u razdoblju od 6.10.2010. do 22.10.2010. Poslužitelj na kojem je obavljeno snimanje, u uobičajenom radu ne prima mnogo DNS upita što se vidi iz prometa tijekom dva tjedna snimanja, međutim, zadnjeg dana snimanja poslužitelj je bio pod opterećenjem ogromnog broja upita na koje nije mogao odgovoriti. Upiti su dolazili u razmacima u mikrosekundama i sastoje se od nekoliko istih upita koji se neprestano ponavljaju tijekom cijelog dana. Analiza najgorih AS-ova pokazuje da u prvih dvadeset uglavnom iskaču registri poput APNIC-a (*Asia-pacific network information center*), ili *Verisigna*. Iako nije potpuno sigurno, vjerojatno je riječ o DoS napadu. Pojavljivanje APNIC-a i Verisigna sugerira lažiranje IP adresa izvora ili korištenje njihovih poslužitelja kao reflektora za napad. Kako reputacijski sustav nema mogućnost utvrđivanja lažiranih IP adresa, rezultati ovog mjerenja ne mogu biti pouzdani. Ovaj slučaj zahtjeva dodatne analize koje ne ulaze u okvir diplomskog rada.

7. Zaključak

Tema ovog diplomskog rada bila je razvoj reputacijskog sustava autonomnih sustava temeljen na promatranju prometa DNS sustava. Cilj je bio analizirati modele kažnjavanja neispravnog DNS prometa, modele izračunavanja reputacije autonomnih sustava, izraditi reputacijski sustav te na eksperimentalnim podatcima pokazati ponašanje razvijenog sustava.

Diplomski rad razmatra veliki broj posve različitih propusta i zlouporaba DNS prometa uočenih u nizu radova različitih autora. Cilj analize svakog pojedinog propusta je utvrditi razloge radi kojih se on pojavljuje i način na koji je moguće prepoznati pojedini propust promatranjem sadržaja paketa DNS prometa. Dodatno, važno je utvrditi eventualne veze između pojedinih propusta te na kraju probati što preciznije utvrditi krivce i ozbiljnost pojedinog propusta. Svaki propust ili zlouporaba se analizira gledajući promet na razini AS-ova. Detaljno se razmatraju mnogi modeli penaliziranja prometa te se pokušava pronaći adekvatan model, ili kombinacija modela koja bi obuhvatila sve razmatrane propuste ili namjerne pogreške u DNS prometu.

Prema utvrđenim pogreškama DNS prometa i modelima njihova kažnjavanja, razvijen je reputacijski sustav koji promatranjem DNS prometa utvrđuje pogreške i računa reputacije AS-ova koji sudjeluju u uočenoj komunikaciji. Reputacijski sustav implementira funkcionalnosti promatranja DNS paketa, analizu svakog pojedinog paketa u potrazi za pogreškama, utvrđivanje odgovornih AS-ova i periodičko računanje reputacije svih sustavu poznatih AS-ova na temelju prikupljenih podataka.

Tijekom izrade diplomskog rada, na prikupljenom prometu s više mjernih točaka, obavljeno je niz mjerenja reputacija u svrhu utvrđivanja ispravnosti rada implementiranog reputacijskog sustava i dobivanja reputacijskih rezultata kao osnove daljnje analize. Prema obavljenim mjerenjima, detaljno se analizira ponašanje korištenih težinskih funkcija i reputacijske funkcije u cjelini. Opisuje se ponašanje pojedine težinske funkcije, uspoređuju kvalitete rezultata pojedinih funkcija na uobičajenom prometu i različitim rubnim slučajevima. Također, funkcije se testiraju promjenama niza parametara sa svrhom utvrđivanja optimalnih vrijednosti parametara za računanje reputacije u danim uvjetima. Slabosti pojedinih težinskih funkcija umanjuju se istovremenim korištenjem više funkcija, odnosno informacija, koje pojedine funkcije daju o promatranom prometu i reputaciji.

S optimalno podešenim parametrima rada reputacijskog sustava izračunavaju se promjene reputacija AS-ova, a iz tih rezultata utvrđuje se AS-ove s najgorim reputacijama na mjernim razdobljima. Analizom pogrešaka utvrđuju se razlozi lošeg ponašanja najgorih AS-ova. Zadnji korak je pronalaženje međusobnog podudaranja popisa najgorih AS-ova različitih mjernih točaka i podudaranja s vanjskim izvorima, tj. popisima AS-ova loše reputacije.

Rezultati mjerenja, odnosno popisi najgorih AS-ova, pokazuju da implementirani reputacijski sustav ostvaruje očekivanja u vidu prepoznavanja neispravnih DNS paketa te točnosti utvrđivanja reputacije pojedinih AS-ova.

Prostor za daljnji razvoj reputacijskog sustava postoji u mnogim dijelovima sustava. Prvenstveno, moguće su nadopune vrsta DNS pogrešaka, nadogradnje sustava aktivnim

mjerenjima u potrazi za otvorenim rekurzivnim poslužiteljima i drugim aktivnim pretragama, dodavanjem analiza pozitivnih praksi u DNS prometu prvenstveno u vidu DNSSEC-a, proširenjem popisa korištenih težinskih i reputacijskih funkcija itd. Jedan od ciljeva daljnjeg razvoja sustava bi svakako trebalo biti prilagodba potrebama realnog AS-a i testiranje na radu u realnom vremenu.

8. Literatura

[1] P. Mockapetris, *Domain names - concepts and facilities*, The Internet Engineering Task Force, RFC 1034, http://www.ietf.org/rfc/rfc1034.txt, 1987.

[2] P. Mockapetris, *Domain names - implementation and specification*, The Internet Engineering Task Force, RFC 1035, http://www.ietf.org/rfc/rfc1035.txt, 1987.

[3] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, *DNS Security Introduction and Requirements*, The Internet Enbineering Task Force, RFC 4033, http://www.ietf.org/rfc/rfc4033.txt, 2005.

[4] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, *Resource Records for the DNS Security Extensions*, The Internet Engineering Task Force, RFC 4034, http://www.ietf.org/rfc/rfc4034.txt, 2005.

[5] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, *Protocol Modifications for the DNS Security Extensions*, The Internet Engineering Task Force, RFC 4035, http://www.ietf.org/rfc/rfc4035.txt, 2005.

[6] Brandhorst, C.J. and Pras, A., DNS: a statistical analysis of name server traffic at local network-to-Internet connections, *Eunice 2005: Networks And Applications Towards a Ubiquitously Connected World: IFIP International Workshop on Networked Applications*, 2006.

[7] Brownlee, N. and Claffy, KC and Nemeth, E., DNS measurements at a root server, *IEEE Global Telecommunications Conference, 2001. GLOBECOM'01*, 2001.

[8] Dagon, D. and Provos, N. and Lee, C.P. and Lee, W., Corrupted dns resolution paths: The rise of a malicious resolution authority, *Proceedings of Network and Distributed System Security Symposium (NDSS'08)*, 2008.

[9] Wessels, D. and Fomenkov, M., Wow, that's a lot of packets, *Proceedings of Passive and Active Measurement Workshop (PAM)*, 2003.

[10] Zdrnja, Bojan and Brownlee, Nevil and Wessels, Duane, Passive Monitoring of DNS Anomalies, *DIMVA '07: Proceedings of the 4th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 2007.

[11] Broido, Andre and Nemeth, Evi and Claffy, KC, Spectroscopy of Private DNS Update Sources, *WIAPP '03: Proceedings of the The Third IEEE Workshop on Internet Applications*, 2003.

[12] Broido, Andre and Hyun, Young and Fomenkov, Marina and Claffy, KC, The windows of pivate DNS updates, *SIGCOMM Comput. Commun. Rev.*, 36, 93 - 98, 2006.

[13] Castro, Sebastian and Wessels, Duane and Fomenkov, Marina and Claffy, Kimberly, A day at the root of the internet, *SIGCOMM Comput. Commun. Rev.*, 38, 41 - 46, 2008.

[14] Castro, Sebastian and Zhang, Min and John, Wolfgang and Wessels, Duane and Claffy, KC, Understanding and Preparing for DNS Evolution, *sourceTMA'10: 2nd International Workshop on Traffic Monitoring and Analysis*, 2010.

[15] Korunić, Dinko, *Analiza i prikupljanje DNS paketa*, ZEMRIS, Fakultet elektrotehnike i računarstva, diplomski rad br. 1784, 2009.

[16] Friščić, Tomislav, *Određivanje reputacije autonomnih sustava zasnovano na praćenju neželjene pošte*, ZEMRIS, Fakultet elektrotehnike i računarstva, diplomski rad br. 1857, 2010.

[17] J. Zittrain, J. Palfrey, Top Infected IP Addresses for March 2008, http://blog.stopbadware.org/2008/04/05/infections-stats-for-march-2008, (27.11.2010.)
[18] J. Armin, Top 50 Bad Hosts & Networks - 2010 Q1, http://hostexploit.com/tools/statistics/3509.html, (27.11.2010.)

Dodatak A: Dodatna razmatranja DNS pogrešaka

Osim navedenih pogrešaka koje su razrađene u poglavlju 3.3., u srodnim radovima nalaze se neka dodatna mjerenja koja nisu ušla u osnovni skup mjerenih pogrešaka (zbog kompleksnosti provedbe, neizvedivosti u zamišljenom reputacijskom sustavu, odbačena zbog pronađenih manjkavosti itd.), ali su zanimljiva za dodatna razmatranja pojava u DNS prometu i nekim sigurnosnim prijetnjama, a koja mogu poslužiti u osmišljavanju adekvatnijeg modela penaliziranja unutar reputacijskog sustava:

1. [15] – u svom sustavu praćenja DNS-a uvrštava pogrešku *nepoznati OPCODE*. Iako je teoretski moguće da neki neispravno podešeni klijent generira upite koji sadrže nepoznati OPCODE, u ostalim srodnim radovima takva pogreška nije uočena. Također, u tom radu implementirani sustav za praćenje DNS-a ne prepoznaje DNS specifikacijom naknadno dozvoljene kodove UPDATE i NOTIFY. U samom radu se spominje da mjerenjima primijećeni paketi nepoznatog OPCODE predstavljaju uglavnom UPDATE kod. Mjerenje je iz tih razloga odbačeno pod zaključkom da takvi propusti ili ne postoje ili su izrazito rijetki, pa ih tako ostali autori ne razmatraju.

   [15] razmatra i tri dodatna, međusobno slična, mjerenja:

   1. *više od tri odgovora s istima ID-em* – prepoznaje kao mogući pokušaj trovanja privremene memorije. Ovo mjerenje je neadekvatno za razinu AS-a iz razloga što bi senzori morali imati vrlo kompleksnu privremenu memoriju preko koje bi bili u stanju prepoznati ovu pojavu te metode međusobne komunikacije da utvrde postojanje takvih paketa na drugim linijama, odnosno senzorima. Potrebna bi bila i privremena memorija koja prati sve upite kako bi se utvrdilo jesu li primijećeni odgovori opravdani. Također, sasvim je razumljivo na razini AS-a pojavljivanje jako puno odgovora koji sadrže isti ID, posebno ako se uzme u obzir da nije nužno propisana promjena ID kod svakog novog upita
   2. *odgovor na nepoznati upit* – također prepoznaje kao mogući pokušaj trovanja privremene memorije. Za prepoznavanje ovakvog ponašanja potrebno je posjedovati sve upite kako bi se napravilo pretraživanje i utvrdilo nepostojanje ekvivalentnog upita za promatrani odgovor. Kako je na razini AS-a nemoguće očekivati da pojedini senzori imaju dovoljno veliku privremenu memoriju da mogu utvrditi postojanje odgovora na upit koji nije poslan, ovo mjerenje nije moguće koristiti. Osim toga, promatrani AS može biti tranzitan na putu upita i odgovora pa je normalno uočavanje odgovora na upite koji nikada nisu zabilježeni jer ne prolaze promatranim AS-om
   3. *odgovor na lažni upit* – slično kao i ranija dva mjerenja prepoznaje se kao pokušaj trovanja privremene memorije. Provjerava se sadrži li odgovor ispravan upit u polju upita. Ovo mjerenje je nemoguće iskoristiti iz istovjetnih razloga kao i kod *odgovora na nepoznati upit*

   Jedno od mjerenja koje Korunić provodi je i potraga za MS06-041 ranjivosti Microsoftove DNS programske podrške. Ranjivost je dopuštala izvođenje proizvoljnog programskog koda na računalu žrtve koji se prenosio krivo

oblikovanim DNS paketima koji bi zbog propusta programskoj podršci prepisivali memoriju računala žrtve. Problem s ovim mjerenjem je što takvih propusta ima mnogo te se oni s vremenom ispravljaju, a istovremeno pronalaze novi, posebno ako se uzme u obzir nadogradnja ili potpuno nova programska podrška koja proizvođači nude. Uočavanje ovakvih napad bilo bi poželjno, ali bi predstavljalo dosta veliko opterećenje na sustav praćenja DNS prometa, a ponekad bi imali i konkretan problem kako sa sigurnošću utvrditi ovakvo ponašanje napadača, s obzirom na ponekad nepostojeću dokumentaciju ranjivosti. Adekvatnijim se čini pristup u kojem se provjerava ispravnost formata svih DNS paketa te kažnjava uočene nepravilnosti u formatu paketa. Time bi se posredno kaznio i MS06-041 napad, kao i svi napadi sličnog tipa

2. [7] – zanimljiv slučaj zagađenja DNS prometa primijećen je tijekom istraživanja koje su na korijenskim poslužiteljima proveli Brownlee i ostali. Problem se javio zbog krivo podešenih usmjernika iza kojeg su se nalazili svi Microsoftovi DNS poslužitelji (kršeći jedno od pravila robusnosti DNS sustava imajući sve poslužitelje iza istog usmjernika, odnosno na istom mjestu). Usmjernik nije propuštao promet do poslužitelja čineći ih nedostupnima. TTL-ovi za Microsoftove adrese podešeni su na svega 2 sata, s vremenom je kako su TTL-ovi istjecali, sve više upita, ne mogavši dobiti odgovor od Microsoftovih poslužitelja, stizalo do korijenskih poslužitelja. Problem je bio potenciran činjenicom da Windows DNS poslužitelji ne pohranjuju negativne odgovore već uporno ponavljaju upite dok ne dobiju odgovor. Taj splet okolnosti doveo je do povećanja opterećenja korijenskih poslužitelja Microsoftovim prometom s početnih skoro 0% na 25% ukupnog opterećenja.

   Ovaj slučaj dokazuje neočekivanu osjetljivost DNS sustava na lokalne administratorske pogreške popularnih DNS poslužiteljima, a snagom je razmjeran DDoS napadu. Sposobnost reputacijskog sustava da prepozna anomalije u količini DNS prometa pojedinih klijenata ili poslužitelja, time se boreći protiv DoS napada, ali i ovakvih propusta, pokazuje se kao bitna komponenta

3. [8] – polazeći od pretpostavke da otvoreni rekurzivni DNS poslužitelji potencijalno predstavljaju namjerne pokušaje prijevare korisnika u rješavanju DNS upita, autori koriste mnoge aktivne i pasivne tehnike pronalaženja poslužitelja koji lažiraju odgovore. Aktivna mjerenja između ostalog podrazumijevaju pretraživanje prostora IP adresa za otvorenim rekurzivnim DNS poslužiteljima korištenjem unikatnih zahtjeva baziranih na IP adresama pojedinih poslužitelja kojima traže vlastitu domenom koju kontroliraju, te ispitivanje njihova ponašanja prema poznatim domenama često korištenim za prijevare poput banaka ili antivirusnih kompanija.

   Pretraživanje cijelog prostora IP adresa ili ekvivalentna aktivna potraga za otvorenim rekurzivnim DNS poslužiteljima je moguća, ali tu treba uzeti u obzir da bi takve aktivnosti narušile reputaciju promatranog autonomnog sustava. Međutim, na temelju mjerenja provedenih u ovom istraživanju, očita je potreba dodatnog penaliziranja otvorenih rekurzivnih DNS poslužitelja jer su rezultati pokazali ogroman broj takvih poslužitelja koji daju lažne podatke. Također, ovo istraživanje ukazuje da je unutar reputacijskog sustava potreban mehanizam provjere jesu li upiti usmjereni "legalnim" DNS poslužiteljima, ili su na neki način preusmjereni

izvan autoritativnog lanca DNS-a. Pretraživanje bi se moglo vršiti na statističkom uzorku i na poslužiteljima prepoznatima u promatranom prometu.

4. [10] – generatori neželjene pošte često koriste domene koje registriraju samo na kratko kako bi im poslužile za slanje neželjene pošte, a kasnije ih prestaju koristiti (domene za odbacivanje, *throwaway domains*). Prepoznavanje tih stalno prijavljivanih novih domena je moguće DNS NS upitima koji će u pravilu davati uvijek istog DNS poslužitelja za svaku takvu novoprijavljenu domenu. Poznavajući "reputaciju" poslužitelja, za koje se analizom utvrdi da u pravilu rješavaju upite za generatore neželjene pošte, lako je odmah utvrditi potencijalnu opasnost s novoprijavljene domene.

   Autori razmatraju i zauzimanje tipfelera. Zauzimanje tipfelera je tehnika varanja korisnika bazirana na tipfelerima pri unosu imena stranica koje korisnik poziva. Napadač registrira uobičajene tipfelere na domene popularnih stranica kako bi uhvatio korisnike koji zabunom otvaraju te stranice, a da toga često nisu niti svjesni. Protiv ovakvog napada se jako teško boriti jer je u pravilu jedini siguran pokazatelj sama krivo upisana adresa, a koju je često vrlo teško uočiti (jednostavna metoda koju primijenjuju autori je abecedno sortiranje upita iz kojeg je lako uočiti zauzimanje tipfelera, iako i tu postoji dodatna potreba automatizacije tog prepoznavanja, a problem je metoda koja podrazumijeva naknadnu analizu veće količine uhvaćenih paketa te se ne može provoditi u realnom vremenu). Iako se ne radi o napadu na DNS ili putem DNS-a, analizom DNS prometa moguće je prepoznati potencijalno zauzimanje tipfelera. Domene tog tipa često će biti prijavljene na jednom poslužitelju, a poslužitelj u pravilu rješava sve domene istom adresom, pa se uočavanjem velikog broja različitih A upita koji se rješavaju istom IP adresom može posumnjati u ovakav napad (neke IP adrese tako mogu rješavati i preko tisuću različitih domena). Ova istraživanja ukazuju na potrebu posjedovanja DNS crnih lista baziranih na NS i A zapisima resursa

Dodatak B: Uputa za korištenje

Na CD-u se nalazi zip datoteka s cjelokupnim implementacijom reputacijskog sustava i pratećim konfiguracijskim datotekama.

Za korištenje reputacijskog sustava potrebno je imati instaliran Python 2.6 interpreter (nije moguće koristiti Python 3.0) sa standardnim modulim. Dodatno potrebno je instalirati dva modula koji nisu dio Python standardnih modula:

1. Scapy modul za snimanje prometa i obradu DNS paketa koji obično dolazi u službenim repozitorijima Linux distribucija
2. IPy modul koji omogućuje manipulaciju IP adresama i mrežnim maskama koji se također nalazi u standardnim repozitorijima

U */data* direktoriju nalaze se:

1. *dnsbllist* datoteka u koju je moguće unijeti poznate DNSBL poslužitelje
2. *known_tlds.txt* datoteka s popisom poznatih vršnih domena koje se može nadopunjavati
3. *my_networks* datoteka u koju je potrebno upisati sve mreže kojima upravlja AS na kojem se vrši mjerenje
4. *ip_to_as* datoteka s preslikanim vrijednostima IP adresa u AS-ove

Konfiguracijska datoteka se nalazi u početnom direktoriju. U njoj je moguće mijenjati sve parametre mjerenja opisane u ranijim poglavljima te je moguće podešavati nazive datoteka koje se koriste prilikom rada a koje se moraju nalaziti u */data* direktoriju.

Pcap datoteka s prikupljenim DNS prometom se mora nalaziti u početnom direktoriji i njen naziv mora biti upisan u konfiguracijskoj datoteci. Nakon što su podešeni parametri mjerenja prema željenim vrijednostima reputacijski sustav se pokreće naredbom *python reputation_system.py*. Drugi način pokretanja je podešavanje izvršnih ovlasti na *reputation_system.py* koju se onda može izravno pokrenuti. Potrebno je imati vezu na internet.

Program stvara direktorij za svaku težinsku funkciju koju se želi koristiti. U slučaju da se koriste sve težinske funkcije rezultati se upisuju u zajednički direktorij. Rezultati su zapisani za svaki SA odvojeno u dvije datoteke pri čemu prva sadrži vremenske oznake računanja reputacija i promijene reputacija, a druga vremenske oznake i pogreške podijeljene na klijentsku i poslužiteljsku stranu. Ponovno pokretanje mjerenja ne može nastaviti raniji rad pa je potrebno sačuvati i ručno ukloniti stvorene direktorije kako se podatci ne bi miješali.

Program samostalno završava nakon što obradi sve podatake iz predane pcap datoteke, a moguće ga je prekinuti CTRL+C naredbom pri čemu je potrebno pričekati neko vrijeme dok se dotad učitani podatci očiste i pohrane pronađena preslikavanja IP u AS-ove (u pravilu ne više od 20 sekundi).