SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD BR. 1894

POBOLJŠANJE SIGURNOSTI ANONIMNE MREŽE TOR UPORABOM REPUTACIJSKOG SUSTAVA

Marko Salkić

Zagreb, rujan 2011.

Zahvaljujem se mentorima što su mi kroz ovaj rad omogućili i pomogli smisleno zaokružiti studij, potaknuti znatiželju, produbiti znanje i usvojiti životne lekcije.

Zahvaljujem se i svima koji su sa mnom prolazili ovaj put, davali konstruktivne kritike, bodrili me kad je nedostajalo snage i pridonijeli završetku mog studija.

SADRŽAJ

U ovom radu opisani su sustavi anonimnosti, zloupotrebe sustava anonimnosti i neka rješenja protiv zloupotrebe, a detaljno je opisan sustav anonimnosti Tor. Opisani su reputacijski sustavi i predloženo je rješenje problema zloupotrebe mreže Tor upotrebom reputacija. Predloženi reputacijski sustav, temeljen na beta reputacijskom sustavu, omogućava dobronamjernim korisnicima korištenje mreže Tor uz pružanje anonimnosti dok istovremeno obeshrabruje zlonamjerne korisnike smanjivanjem kvalitete usluge. Reputacijski sustav je simuliran u simulacijskom okruženju OMNeT++ na temelju scenarija koji opisuju funkcioniranje reputacijskog sustava u različitim topologijama, ponašanjima klijenata i napadima.

ABSTRACT

This diploma thesis gives an overview of anonymity systems, identifies attacks on anonymity systems and lists proposed solutions. Thorough insight is given into Tor anonymity network. Reputation systems are also a part of the thesis. The central part of the thesis is the reputation system for Tor network, based on the beta reputation system, which gives incentives to good users, and punishes misbehavior by degrading the quality of service, while preserving user anonymity. The proposed reputation system is simulated with the OMNeT++ simulation framework using various scenarios consisting of different network setups, user behaviors and attack vectors.

Sadržaj

1. Uvod

Društvo zahtijeva anonimnost iz raznih razloga, a budući da je korištenje Internet usluga u svakodnevnom poslovanju i dokolici sve prisutnije, zahtjev za anonimnošću se iz klasičnih društvenih oblika prenosi i na digitalni, a zajedno s tim, prenosi se i zloupotreba anonimnosti. Osoba koja odluči svjesno kršiti zakon može zloupotrijebiti anonimnost za skrivanje svog identiteta i izbjeći sankcije. Iako svaka država ima svoje zakone, društveno uređenje i pravila, ljudi se većinom slažu za koja ponašanja počinitelji ne bi trebali ostati anonimni. Prvenstveno je riječ o raznim računalnim napadima, skupljanju i slanju dječje pornografije, komunikaciji kriminalnih osoba i organizacija.

Na način kako je prvotno zamišljen, Internet ne jamči anonimnost. Postoji više različitih tehnologija kojima se pokušava zaštititi identitet korisnika, kao što su *remaileri* i anonimni posrednici, a Tor je prikladan jer je prilagođen najčešćim aktivnostima na Internetu, kao što je surfanje. Uspješnost mreže Tor, kao i drugih sustava anonimnosti, je direktno proporcionalna s brojem korisnika, pa se korisnike mora privući i održati u sustavu jednostavnošću, pouzdanošću i zadovoljavajućim performansama. Nažalost, efekti zloupotrebe odvraćaju dobronamjerne korisnike od korištenja sustava zbog legalnih implikacija ili nepoštenog omjera uloženog i dobivenog. Performanse mreže Tor su dodatno pogoršane sebičnim ponašanjem korisnika koji ne doprinose dio resursa (engl. freeriders), a to se pogotovo osjeća kod interaktivnog korištenja, primjerice surfanja Web-om. Loše performanse odvraćaju korisnike od korištenja sustava, smanjuje se stabilnost i anonimnost mreže koja ovisi o broju korisnika. To dodatno odvraća korisnike i tako se stvara začarani krug.

U decentraliziranim sustavima ne postoje jedinstvena pravila i autoritet koji ih provodi. Korisnici se u međusobnoj interakciji oslanjaju na povjerenje koje imaju jedni u druge i u sustav kao cjelinu. Reputacijski sustavi pokušavaju unijeti reda u sustave gdje je povjerenje bitno. Uvođenje reputacija u anonimne sustave, kao što je Tor, je na prvi je pogled problematično jer je reputacija vezana za identitet, a anonimni sustav štiti identitet. U ovom radu se predlaže rješenje tog problema.

Cilj reputacijskog sustava mreže Tor predloženog u ovom radu je nagrađivanje poželjnog ponašanja pružanjem dobre kvalitete usluge. Korisnicima s nepoželjnim ponašanjem preostaje koristiti mrežu Tor s minimalnim performansama, što će odvratiti dio korisnika od zloupotrebe. U ocjenjivanju ponašanja korisnika se ne koristi njegov identitet nego anonimni komunikacijski putovi koje je izgradio sâm korisnik. Predloženi reputacijski sustav je implementiran i simuliran u simulacijskom okruženju OMNeT++, a rezultati simulacija potvrđuju njegovu uspješnost u jednostavnim slučajevima i pojednostavljenoj okolini.

Rad je podijeljen u sedam poglavlja. Poglavlje 2 opisuje sustave anonimnosti, od kojih se detaljno opisuje mreža Tor. U poglavlju 3 se opisuju načini zloupotrebe mreže Tor i neka predložena rješenja. Poglavlje 4 opisuje reputacijske sustave kao jedno od rješenja protiv zloupotrebe u P2P mrežama. U poglavlju 5 se razrađuje reputacijski sustav za mrežu Tor. Implementacija reputacijskog sustava u simulacijskom okruženju OMNeT++ i rezultati simulacije opisani su u poglavlju 6. Rad je zaključen u poglavlju 7.

2. Sustavi anonimnosti

U modernom društvu, anonimnost i privatnost su važni u ostvarivanju osnovnih ljudskih prava kao što su sloboda govora, slobodan pristup informacijama i jednakost pred zakonom. To pogotovo dolazi do izražaja u represivnim političkim sustavima gdje svaka akcija, koju vladajuća politika proglasi nepoželjnom, može pojedinca dovesti u nevolju. Anonimna komunikacija motivira građane da govore o stvarima o kojima inače ne bi, od srama ili straha od odmazde, a od općeg su društvenog interesa. Motiviraju se zviždači na ukazivanje nepravdi, aktivisti na poticanje demokracije i civilnog društva, novinari na slobodno izvještavanje i slično. Također, anonimnost štiti pojedince od praćenja u političke i komercijalne svrhe, a gospodarske subjekte od poslovne špijunaže. U jednom istraživanju, SANS institut je računalnu špijunažu (engl. cyber espionage) naveo kao treće-rangiranu prijetnju na ljestvici deset najvećih računalnih opasnosti 2008. godine [1]. Određena doza anonimnosti je potrebna kada se radi o osobnim, medicinskim, pravnim ili vladinim informacijama.

Danas se problemi osiguranja anonimnosti sele i na Internet gdje dobivaju sve veću pozornost i važnost. Na suptilnoj razini, pojedinci svakodnevno u raznim situacijama ostavljaju elektronički trag. Otkrivanjem znanja[1] iz tih elektroničkih podataka ekstrahiraju se informacije o pojedincima, često bez njihovog znanja i pristanka. Ekstrahirane informacije mogu služiti za izgradnju profila koji mogu sadržavati podatke osobnog karaktera, a njihova primjena može biti neetična i diskriminatorna [2]. Google je trenutno najkorištenija tražilica na Internetu, a sve više je pod povećalom javnosti njihova kontroverzna politika pohranjivanja i prilagođavanja korisničkih upita. Bez obzira na Googleov neformalni moto "ne budi zao" (engl. don't be evil), količina podataka koje sakupljaju ima ogroman potencijal za zloupotrebu. Trendovi računarstva u oblacima (engl. cloud computing) također podrazumijevaju sve veću količinu korisničkih podataka koja se akumulira u udaljenim podatkovnim centrima na nepoznatim lokacijama. Većina korisnika Interneta nije svjesna skupljanja podataka o njima pa ne ulažu dodatne napore u osiguranje privatnosti i anonimnosti.

Arhitektura Interneta sama po sebi ne jamči anonimnost. Naime, zaglavlje IP paketa sadrži adresu pošiljatelja koja, s obzirom na blok IP adresa kojoj pripada, može odati pružatelja usluga Interneta (engl. Internet Service Provider), a samim time i geografsku lokaciju korisnika. Pružatelji Internet usluga su dužni uz sudski nalog na temelju IP adrese i vremena korištenja pružiti informacije o stvarnom pretplatničkom identitetu korisnika. Situacija je malo drugačija kod privatnih mreža. Zbog relativno malog broja IPv4 adresa, za korištenje u privatnim mrežama rezervirane su privatne IP adrese. U slučaju izlaska paketa iz privatne mreže na Internet, NAT uređaj (engl. Network Address Translation) privatne IP adrese multipleksira na javne IP adrese. NAT uređaj koji provodi pretvorbu adresa donekle čuva anonimnost korisnika s privatnom adresom jer više korisnika izlazi na Internet s jednom javnom adresom.

Hansen i Pfitzmann su definirali osnovne pojmove koji se pojavljuju u radovima na temu anonimnosti na Internetu [3].

---

[1] Otkrivanje znanja (engl. data mining) je ekstrakcija implicitnih, dotad nepoznatih i potencijalno korisnih informacija iz velikih baza podataka [91]

Subjekt je pošiljatelj ili primatelj poruke koja prolazi kroz komunikacijski kanal u komunikacijskoj mreži.

Anonimnost subjekta znači da se subjekt ne može identificirati u skupu subjekata, tzv. *anonimnom skupu*. Preciznije, subjekt je za napadača anoniman ako napadač na temelju svih informacija kojima raspolaže ne razlikuje subjekta od drugih subjekata u anonimnom skupu.

Anonimni skup je skup svih potencijalnih, odnosno mogućih subjekata. Skup svih mogućih subjekata ovisi o informacijama koje napadač posjeduje. Iz ovoga slijedi da je anonimnost relativna u odnosu na napadača.

Ovako definirana anonimnost podrazumijeva binarnu vrijednost: subjekt je anoniman ili nije. Subjekt je za napadača anoniman sve dok ga sa sigurnošću ne uspije identificirati. Napadač određuje koliko siguran mora biti da bi smatrao da subjekt više nije anoniman. U tom smislu anonimnost se može kvantificirati kao vjerojatnost.

Kada se anonimnost promatra na razini pojedinog subjekta, govorimo o *individualnoj anonimnosti*, dok za sustav u cjelini možemo reći da pruža *globalnu anonimnost* svojim korisnicima. Globalna anonimnost je veća što je veći anonimni skup i što je ravnomjernije raspodijeljeno slanje ili primanje poruka među subjektima u skupu. Za konstantni anonimni skup, globalna anonimnost je *maksimalna* ako i samo ako su svi subjekti iz anonimnog skupa jednako mogući subjekti.

Pseudonim je identifikator subjekta, a da nije njegovo stvarno ime. Identifikator je ime koje je neovisno o subjektu, odnosno ne sadrži informacije koje se s istim mogu dovesti u vezu. *Digitalni pseudonim* bi trebao biti jedinstven s velikom vjerojatnošću i prikladan za autentikaciju poruka poslanih pod pseudonimom. Pozivanje na digitalni pseudonimim (engl. accountability) se može pospješiti vezivanjem novčanih sredstava na njihovo korištenje ili preko nezavisnih entiteta koji su odgovorni za vezivanje pseudonima na stvarne identitete.

Anonimnost pošiljatelja (engl. sender anonymity) znači da je pošiljatelj poruke anoniman unutar skupa potencijalnih pošiljatelja. *Anonimnost primatelja* (engl. receiver/responder anonymity) znači da je primatelj anoniman unutar skupa potencijalnih primatelja. *Uzajamna anonimnost* (engl. mutual anonymity) znači da identiteti pošiljatelja i primatelja ostaju skriveni. *Anonimnost veze* (engl. connection anonymity) podrazumijeva anonimnost pošiljatelja, primatelja ili uzajamnu anonimnost.

Nepovezivost (engl. unlinkability) znači da napadač ne može utvrditi vezu pošiljatelja i primatelja. Čak i ako se identitet jednoga od sudionika veze otkrije, ne postoji način da se poveže s partnerom u komunikaciji.

Tehnologije anonimiziranja za osiguranje *potpune anonimnosti* [4] trebaju osim anonimnosti veze osigurati i *anonimnost podataka* (engl. data anonymity). Anonimnost podataka odnosi se na informacije izuzete iz razmijenjenih podataka koje mogu poslužiti identifikaciji [5]. Takve informacije se anonimiziranjem brišu ili kriptiraju.

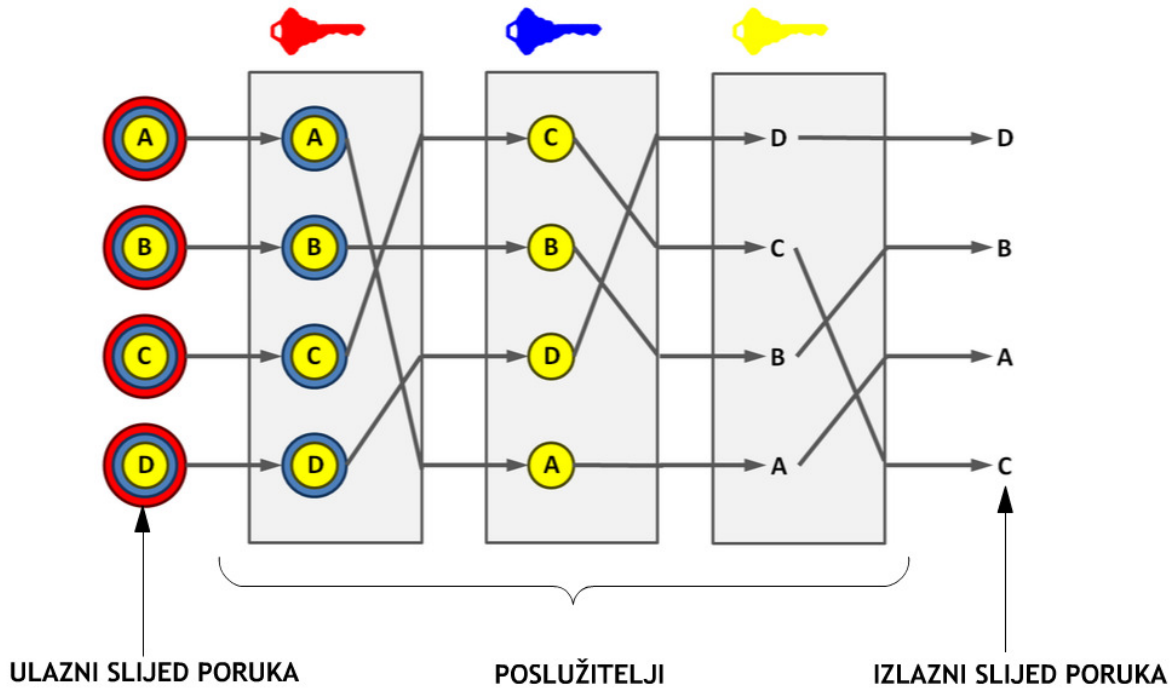
Sigurnosni sustavi većinom su usmjereni na sprječavanje prisluškivanja komunikacije (engl. eavesdropping), odnosno na zaštitu tajnosti poruke [6]. Tajnost poruke se relativno jednostavno štiti kriptografijom, ali informacija o tome tko komunicira s kim ostaje dostupna. IPsec protokol [7], primjerice, u transportnom načinu rada štiti (kriptira) samo podatke korisnog sadržaja IP paketa, a u tunelskom načinu rada enkapsulira cijeli kriptirani IP paket u novi IP paket. Pritom, zaglavlje paketa koji putuje Internetom sadrži IP adrese partnera u komunikaciji, što u tunelskom načinu rada mogu biti poveznici (engl. gateway) dviju korporacija u VPN vezi, a identiteti partnera *unutar* korporacije ostaju skriveni. U oba slučaja postoji dovoljno informacija za poslovnu špijunažu. Sâm obujam prometa, njegov intenzitet i

vremenska raspodjela mogu ukazati na određenu aktivnost unutar korporacije koja se želi sačuvati skrivenom. Prema tome, zaključujemo da je privatnost pošiljatelja i primatelja puno veći problem od tajnosti poruke, pogotovo u velikim otvorenim mrežama.

Bez obzira na potrebu za anonimnom komunikacijom, rijetke su uspješne komercijalne implementacije sustava anonimnosti. Razloga je puno, a jedan od njih je nevoljkost bilo koje organizacije da potpuno vjeruje sustavu anonimnosti koji ne kontrolira [8]. Za razliku od povjerljivosti (kriptiranju), subjekt ne može sam učiniti svoju komunikaciju anonimnom, nego mora vjerovati infrastrukturi. Na otvorenoj mreži, kao što je Internet, imati vlastiti sustav nije od koristi: sustav koji prenosi promet samo jedne organizacije ne može sakriti promet koji ulazi ili izlazi iz nje. Organizacija bi trebala prenositi tuđi promet koji služi kao zaklon (engl. cover traffic) i to u sustavu raspodijeljenog povjerenja u kojem svaki sudionik nalazi motivaciju dati resurse na raspolaganje. *U sustavima anonimnosti koriste se poruke kako bi sakrile poruke*: pošiljatelji su konzumenti anonimnosti, ali također i pružatelji anonimnosti jer porukama pružaju zaklon koji drugima omogućuje anonimnost. Što je veći promet, više je poruka koje služe kao zaklon i to pruža motivaciju sudionicima željnih anonimnosti da daju resurse na raspolaganje.

Pružanje anonimnosti uključuje velik broj različitih pretpostavki koje treba uzeti u obzir [9]. Kao i s drugim primjenama kriptografije, trebaju se odvagnuti mnogi kompromisi efikasnosti, praktičnosti i sigurnosti. Kada, primjerice, efikasnost i praktičnost ne bi bili bitni, mogli bismo difuzno poslati poruke (engl. broadcast) i tako čuvati anonimnost primatelja, kao u DC-net-u [10]. DC-net pruža jednostavno i elegantno rješenje, ali ima nekoliko ozbiljnih nedostataka: ako više korisnika šalje poruku u isto vrijeme dolazi do kolizije, komunikacija je previše kompleksna na mrežama koje nisu prstenaste topologije, količina ključeva koje korisnik mora dijeliti s drugima brzo raste, itd. Broj mogućih pošiljatelja i primatelja je ograničen, pa je u najboljem slučaju statistička vjerojatnost povezivanja pošiljatelja i primatelja za sve korisnike jednaka. Iz ovog proizlazi da je lakoća povezivanja pošiljatelja i primatelja obrnuto proporcionalna veličini anonimnog skupa.

Preteča modernih sustava anonimnosti je Chaumov sustav za miješanje poruka Mix-Net [11]. Sustav za miješanje poruka se sastoji od poslužitelja (engl. mixes) koji prosljeđuju poruke permutirajući njihov redoslijed na slučajan način. Poruke su kriptirane javnim ključevima poslužitelja. Slika 2.1 prikazuje ulazni slijed poruka A, B, C, D i tri poslužitelja u sustavu za miješanje poruka. Slijed poslužitelja kroz koji prolazi poruka tvori anonimni komunikacijski put, odnosno *kaskadu* (engl. mix cascade) kroz mrežu. Kaskadom se na izlazu iz mreže dodatno otežava sastavljanje originalnog redoslijeda poruke. Prije slanja, klijent višestruko kriptira poruke koristeći javne ključeve poslužitelja. Klijent, na primjer, poruku A na slici 2.1 prvo kriptira javnim ključem trećeg, zatim drugog i naposljetku prvog poslužitelja. U svakom poslužitelju se poruka prije prosljeđivanja dekriptira privatnim ključem i zadržava kako bi se promijenio originalni redoslijed poruka. Iz sustava poruke izlaze redoslijedom D, B, A, C. Budući da poslužitelji prenose poruke većeg broja klijenata, zbog premještanja redoslijeda je teško utvrditi pošiljatelja i primatelja pojedine poruke. Ideja "zamotavanja" poruke u slojeve kriptografije javnog ključa i "odmotavanja" je iskorištena u usmjeravanju temeljenom na slojevima (engl. onion routing).



Slika 2.1. Mix-net mreža anonimnosti: klijent višestruko kriptira poruke A,B,C,D i šalje ih kroz mrežu poslužitelja gdje se dekriptiraju, zadržavaju i šalju promijenjenim redoslijedom

Prije opisivanja daljnjeg razvoja sustava anonimnosti, definirana je terminologija narušavanja anonimnosti u poglavlju 2.1., a zatim se u poglavlju 2.2 daje povijesni pregled sustava anonimnosti. Analiza anonimnih sustava prema teoriji igara je razložena u poglavlju 2.3, a sustav anonimnosti Tor je opisan u poglavlju 2.4.

2.1. Narušavanje anonimnosti

2.1.1. Postupci narušavanja anonimnosti

Analiza prometa (engl. traffic analysis) je postupak prikupljanja podataka o mrežnom prometu uključujući vidljive mrežne adrese pošiljatelja i primatelja, ali i *vremenska obilježja prometa*: broj paketa, intenzitet i vremena prispijeća paketa [12]. U slučaju anonimne komunikacije, cilj analize prometa jest utvrditi identitet pošiljatelja i primatelja. Postupak analize prometa se može provoditi i u slučaju kada je promet kriptiran, primjerice kod IPsec-a. *Vremenskom analizom* (engl. timing analysis) napadač može korelirati vremena prispijeća poruka na različitim točkama u sustavu i s određenom vjerojatnoću utvrditi putove kojima prolazi poruka. Analiza prometa, a ne kriptoanaliza, je temelj praćenja i prikupljanja informacija u komunikacijama (engl. communication intelligence) [13].

Specifična vrsta analize prometa je *napad na krajnje točke*. Napad na krajnje točke (engl. attack on endpoints) podrazumijeva da napadač ima pristup krajevima komunikacijskog puta u mreži anonimnosti. Napadač može na krajnjim točkama provoditi vremensku analizu ili utjecati na vremenska obilježja prometa. Zaustavlja li napadač poruke na ulaznom kraju i utječe na njihova vremena pristizanja, onda stvara vremenska obilježja (markere) koje može prepoznati na izlaznom kraju. Vremenskom analizom na krajnjim točkama moguće je

povezati pošiljatelja i primatelja [14]. Napad na krajnje točke se još naziva i potvrda prometa (engl. traffic confirmation).

Napad na krajnje točke je teže izvesti nego analizu prometa jer zahtijeva kontrolu točno određenih poslužitelja, ali više narušava anonimnost. Naime, krajevi anonimnog komunikacijskog puta spajaju pošiljatelje i primatelje pa je jednostavnije narušavanje anonimnosti veze.

Analizu prometa i vremensku analizu može otežati prekrivajući promet (engl. cover traffic), odnosno nadopuna prometa (engl. padding). Prekrivajući promet ne prenosi korisne informacije već se dodaje korisnom prometu zbog osiguravanja konstantnih obilježja prometa poput broja i veličine paketa te intenziteta. Time se prikrivaju obilježja stvarnog, korisnog prometa. Što je promet manje karakterističan, to je korelacija neuspješnija.

2.1.2. Modeli napadača

Glavni cilj narušavanja anonimnosti je povezivanje pošiljatelja i primatelja. Drugi je cilj grupiranje poruka po pošiljateljima u slučaju da kroz isti poslužitelj prolaze poruke različitih pošiljatelja. Napadači se razlikuju po mogućnosti mijenjanja prometa, udjelu ukupnog prometa koji promatraju, poziciji u odnosu na anonimnu mrežu i prilagodljivosti [15]. S obzirom na mogućnost mijenjanja prometa, napadač može biti:

- *Pasivan*: samo prisluškuje promet
- *Aktivan*: prati, zaustavlja, mijenja i odbacuje poruke u sustavu

S obzirom na udio ukupnog prometa koji prati, napadač je:

- *Lokalni*: prati promet prema lokalnoj mreži i unutar nje
- *Globalni*: prati sav promet ili njegov veliki dio. Globalni napadač treba imati veliku količinu resursa za kontrolu cijele mreže, pa se smatra opasnim, ali malo vjerojatnim.

S obzirom na poziciju u odnosu na mrežu anonimnosti, napadač može biti:

- *Interni*: korisnik anonimne mreže, odnosno kompromitirani korisnik pod kontrolom napadača
- *Eksterni*: ne sudjeluje u protokolu anonimnog sustava, odnosno nije korisnik, ali ima pristup prometu u sustavu

S obzirom na prilagodljivost, napadač može biti:

- *Statičan*: ne koristi iskustva u svrhu mijenjanja taktike
- *Prilagodljiv*: bira mjesta gdje će pratiti mrežu s obzirom na prijašnja iskustva

Ove različite karakteristike napadača uzimaju se u obzir u teorijskim i empirijskim ispitivanjima otpornosti anonimnih sustava na napade.

2.2. Primjeri sustava anonimnosti

Babel [16], Mixmaster [17] i Mixminion [18] su primjeri sustava koji ciljaju na maksimalan stupanj anonimnosti uz cijenu relativno velikih i nepredvidivih latencija. Zadržavanje poruka te mijenjanje njihovog redoslijeda otežava napade jer se smanjuje korelacija vremenskog obilježja prometa koji ulazi u poslužitelj s onim koji iz njega izlazi. Takav sustav omogućuje zaštitu od globalnih napadača, ali zbog visoke latencije nije pogodan za interaktivne zadatke

poput pretraživanja Weba, Internet komunikaciju (engl. chat) ili udaljeni pristup (engl. secure shell).

Za interaktivne zadatke prikladni su sustavi anonimnosti s niskom latencijom. Niska latencija oslabljuje anonimnost jer olakšava pasivnom napadaču koji može pratiti promet na krajnjim točkama anonimne mreže da korelira vremena prispijeća i intenzitet ulaznog i izlaznog prometa. Ti su sustavi također ranjivi na aktivnog napadača koji uvodi vremenska obilježja u ulazni mrežni promet i korelira ga s izlaznim. Iako postoje napori da se ovakvi napadi otežaju, primarna zadaća dizajna s niskom latencijom je zaštita od analize prometa, a ne od napada na krajnjim točkama. Najjednostavniji primjeri sustava niske latencije su posrednici s jednim skokom (engl. single-hop proxies), kao što je Anonymizer [19]. Prije prosljeđivanja prometa, posrednik filtrira sve informacije o izvoru. Iako su jednostavnog dizajna i implementacije, zahtijevaju potpuno povjerenje korisnika u pružanju anonimnosti. Koncentracijom prometa u jednu točku povećava se anonimni skup, odnosno broj ljudi među kojima se skriva korisnik, što ujedno otežava identifikaciju pojedinog korisnika. S druge strane, napadač može koncentrirati svoje napore u snimanje prometa koji ulazi i izlazi iz posrednika i tako oslabiti anonimnost korisnika.

Složenije mreže anonimnosti uključuju raspodijeljeno povjerenje i bazirani su na izgradnji kruga. Krug je sastavljen od korisnika, tzv. usmjernika (engl. relay) koji daju svoje resurse na raspolaganje i prenose promet. U ovom kontekstu raspodijeljeno povjerenje znači da skup korisnika koji si međusobno ne vjeruju grade mrežu s ugrađenim mehanizmima sigurnosti kojoj vjeruju [20]. Korisnici grade jedan ili više privremenih krugova kroz koji tuneliraju promet u ćelijama stalne veličine. Uspostava krugova temelji se uglavnom na računski zahtjevnoj kriptografiji javnog ključa, a prosljeđivanje ćelija uglavnom na računski manje zahtjevnoj simetričnoj kriptografiji. Usmjernici u krugu poznaju samo svog prethodnika i sljedbenika tako da niti jedan usmjernik, osim prvog u krugu, ne može povezati promet koji prenosi s pošiljateljem. Primjeri dizajna s niskom latencijom uključuju: Tor [21], Java Anon Proxy [22], PipeNet [23], ISDN mixes [24], Tarzan [25], MorphMix [26], Crowds [27], Hordes [28], Herbivore [29], P^5 [30], Freedom [31], Cebolla [32], Anonimity Network [33].

Jedno od pitanja pri dizajniranju mreža anonimnosti baziranih na izgradnji kruga je koji sloj treba učiniti anonimnim. Mogu se direktno presretati IP paketi i prije prosljeđivanja u krug iz paketa maknuti izvorišnu adresu, kao što to rade Tarzan i Cebolla, ili, kao što je slučaj s Torom, prihvaćati TCP tôkove (engl. TCP streams). Postoje varijante sustava koji prihvaćaju aplikacijske protokole kao što je HTTP i prosljeđuju zahtjeve aplikacija. Odgovor na postavljeno pitanje dizajna svodi se na kompromis između fleksibilnosti i anonimnosti. Razumije li sustav HTTP, može ga ogoliti informacijama koje otkrivaju identitet korisnika, može koristiti međuspremnik za ograničavanje broja zahtjeva koji napuštaju mrežu, te optimizirati zahtjeve u minimalan broj veza. S druge strane, sustav koji anonimizira mrežni sloj može raditi s gotovo svim protokolima na višoj razini, čak i s predstojećim, još nepoznatim, protokolima. Na većini operacijskih sustava, anonimizacija mrežnog sloja zahtijeva modifikaciju na jezgri sustava (engl. kernel). Anonimne mreže koje rade na transportnom sloju, kao što je Tor, predstavljaju dobar kompromis: funkcioniraju bez modifikacija na jezgri operacijskog sustava, a podržavaju većinu aplikacijskih protokola. Važno je samo da aplikacija koristi TCP ili može tunelirati preko TCP-a, a tretirajući aplikacijske veze kao podatkovne tôkove, umjesto kao čiste TCP segmente (engl. raw packets), izbjegavaju se neefikasnosti TCP-preko-TCP tuneliranja.

2.3. Ekonomika anonimnosti

Analiza sustava anonimnosti prema teoriji igara daje nam teorijski uvid u moguće motivacije subjekata za sudjelovanje u sustavu anonimnosti [8]. Polazište teorije igara je da svaki subjekt pokušava ostvariti svoj vlastiti cilj, a da sustav treba biti podešen tako da ostvarivanjem sebičnih ciljeva, sustav kao cjelina profitira. Pretpostavke koje vrijede u takvom ekonomskom sustavu su:

- Razina anonimnosti sustava je pozitivno korelirana s brojem korisnika sustava.
- Usmjernici povećavaju anonimnost vlastitih poruka jer ih mogu sakriti među poruke koje prosljeđuju. Čvor sljedbenik ne zna razaznati čije poruke prosljeđuje. Pošiljatelji koji nisu usmjernici su u lošijoj situaciji. Izaberu li zlonamjernog usmjernika za ulazni čvor, drastično im se smanjuje anonimnost.
- Relacija broja usmjernika i anonimnosti ne mora biti monotona. Pri konstantnoj količini prometa, usmjernicima kojima je anonimnost bitna je u interesu da u sustavu ima manje usmjernika kako bi kroz njih prolazilo više prometa, odnosno kako bi si povećali anonimni skup. Veći broj usmjernika znači veću vjerojatnost da će drugi biti izabrani za izgradnju kruga. Uz veći broj zlonamjernih usmjernika, korisnici će željeti više poštenih kako bi im povećali šanse odabira. Prema tome, pri konstantnom prometu, anonimnost je obrnuto proporcionalna s brojem usmjernika, ali pozitivno povezana s omjerom dobronamjernih i zlonamjernih usmjernika. Interes za manjim brojem usmjernika ne smije ići toliko daleko da olakša praćenje cijelog sustava, smanji njegovu zemljopisnu rasprostranjenost, neovisnost od autonomnih sustava i poveća osjetljivost na ispade, odnosno smanji pouzdanost.
- Motivacija za prenošenjem što više prometa kod usmjernika kojima je anonimnost bitna ih navodi da prihvaćaju određenu količinu sebičnog korištenja korisnika (engl. freeriding) koji služi kao šum. Prevelika količina besplatnog korištenja može stvarati prevelik trošak prometa.
- Usmjernik koji ima visoku reputaciju, to jest percipiraju ga dobronamjernim, privlači više prometa i povećava si anonimni skup.
- Postoje ekonomski razlozi za raspodijeljeno povjerenje ali decentralizirani sustav može uključivati velike troškove koordinacije. Centralizirani sustav koordinacije je praktičniji, ali može olakšati napade fokusiranjem na manji broj ciljeva napada.

Tablica 2.1 sažeto prikazuje utjecaj parametara mreže na anonimni skup. Opća reputacija, odnosno reputacija koju sustav kao cjelina ima među korisnicima, propusnost i niska zloupotreba su zapravo zahtjevi anonimnosti zato što utječu na broj korisnika, odnosno anonimni skup, što dalje utječe na stupanj anonimnosti koju je moguće pružiti.

Tablica 2.1. Odnos parametara mreže anonimnosti i anonimnog skupa

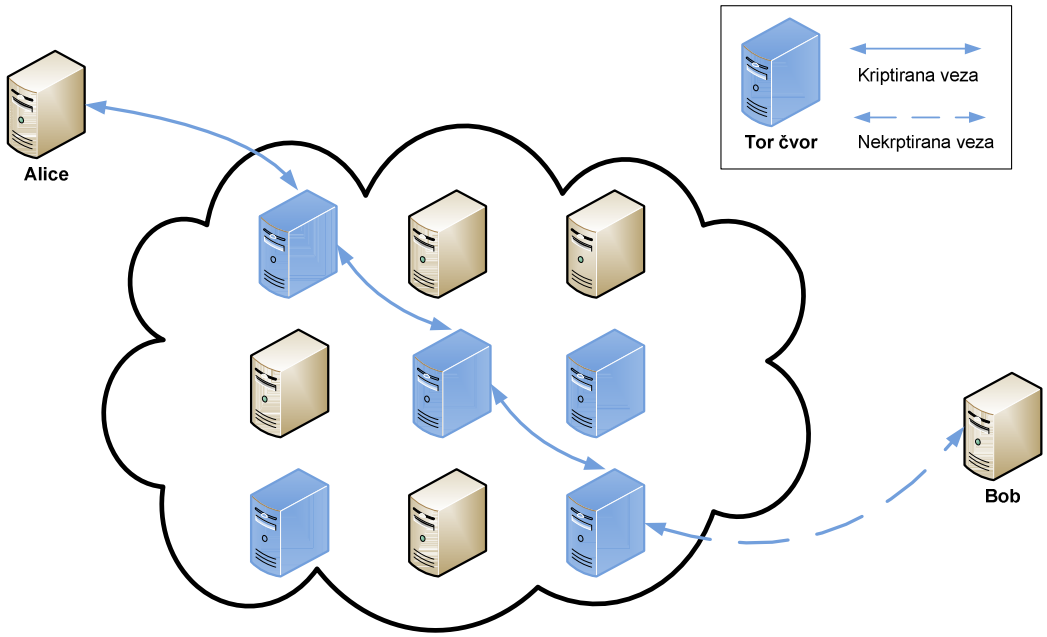
Parametar	*Proporcionalnost s anonimnim skupom*
opća reputacija mreže	proporcionalan
propusnost	proporcionalan
zloupotreba	obrnuto proporcionalan
anonimni skup	pozitivno povratan

Iz više razloga je bitno da protokoli praktičnih i iskoristivih sustava anonimnosti budu implementirani na Internetu i s adekvatnim performansama na računalima korisnika koji sudjeluju u sustavu [34]:

- *cijena infrastrukture*: zamjena infrastrukture Interneta je nedopustivo skupa.
- *cijena sklopovlja*: dodavanje sklopovske akceleracije (operacija kriptografije javnog ključa) korisnicima koji sudjeluju u sustavu (čvorovima) je skupo i predstavlja barijeru ulasku novim čvorovima. Ovo se ne odnosi na sustave s miješanjem poruka.
- *javna mogućnost provođenja revizije* (engl. public auditability): komponente sustava s raspodijeljenim povjerenjem trebaju se moći javno provjeriti. Puno je teže provjeravati sklopovlje nego javno dostupan izvorni kôd nekog sustava. Prema tome, programski pristup je poželjniji nego sklopovski.
- *prikladnost:* potencijalnim čvorovima mora biti omogućeno jednostavno sudjelovanje u sustavu. Instaliranje posebnog sklopovlja nije prikladno.

2.4. Sustav anonimnosti Tor

Uslojeno usmjeravanje (engl. onion routing) je mehanizam za anonimnu komunikaciju putem prekrivajuće (engl. overlay) mreže niske latencije. Za razliku od drugih sustava anonimnosti koji se koriste posebnim aplikacijama, uslojeno usmjeravanje mogu koristiti sve aplikacije koje koriste SOCKS sučelje [35] kao posrednik (engl. proxy). Uslojeno usmjeravanje provode čvorovi zvani slojni usmjernici (engl. onion routers), ili kraće "OR", preko kojih putuju poruke raznim, za promatrača nepoznatim, putovima. Klijent bira put kroz mrežu sačinjen od čvorova (engl. nodes) i stvara "krug" (engl. circuit), u kojem svaki čvor zna samo svog prethodnika i sljedbenika tako da niti jedan čvor u krugu ne poznaje čitav put. Promet klijenta putuje porukama koje se na izvorištu višestruko kriptiraju simetričnim ključem, dogovorenim sa svakim usmjernikom, te se šalju u krug. Višestruko uslojena struktura podataka koja enkapsulira promet namijenjen pojedinom čvoru se zove *uslojena poruka* (engl. onion). U svakom se čvoru kruga dekriptira jedan "sloj", slično ljuštenju slojeva luka, i "oljuštena" poruka se šalje sljedećem čvoru na putu. Postupak se ponavlja u sljedećem čvoru sve dok poruka ne stigne do zadnjeg čvora u krugu. Tamo se "ljušti" zadnji sloj kriptiranja i dobiva čisti tekst koji napušta krug do svog ciljnog odredišta. Slika 2.2 prikazuje skup računala spojenih na Internet, od kojih su neki Tor usmjernici. Alice izabire tri usmjernika, gradi krug te uspostavlja anonimni spoj s Bobom. Sva komunikacija do zadnjeg usmjernika u krugu je kriptirana, a iz mreže Tor izlazi kao čisti tekst.



Slika 2.2. Alice izabire usmjernike i uspostavlja krug za anonimnu komunikaciju s Bobom.

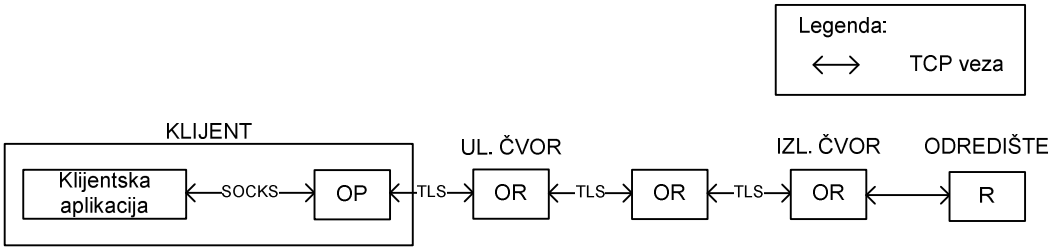
The Onion Router [21] (u daljnjem tekstu, "Tor") je implementacija druge generacije uslojenog usmjeravanja koja se oslanja na slobodnu, volontersku mrežu kako bi zaštitila privatnost korisnika na Internetu otežavajući analizu prometa. Tor je dostupan pod licencom otvorenog koda (engl. free software). Spada u sustave s niskom latencijom, koji pružaju anonimnost interaktivnog mrežnog prometa. Tor mogu koristiti sve aplikacije bazirane na TCP-u, kao što su preglednici Web-a, udaljeni pristup (engl. secure shell) i sustavi za slanje instant poruka (engl. instant messaging).

Osim anonimnosti klijenta, na primjer preglednika Interneta, Tor omogućuje anonimnost i davatelju usluge (primjerice web poslužitelju) kroz „skrivene usluge“ (engl. hidden services).

2.4.1. Struktura mreže Tor

Mreža Tor je prekrivajuća mreža čvorova na Internetu –Tor čvorovi su spojeni TLS vezom sa drugim Tor čvorovima. Svaki klijent može, ali ne mora, davati svoje resurse na raspolaganje mreži Tor, a izlaznom politikom (engl. exit policy) određuje koje protokole i pristupe (engl. ports) propušta. Na taj je način skup poslužiteljskih čvorova (engl. server node), odnosno usmjernika varijabilan, što napadaču otežava mogućnost da zagospodari cijelom mrežom. Za sigurnost mreže bitno je da je anonimni skup bude što veći, pa se korisnike potiče da daju svoje resurse na raspolaganje.

Većina programa koji koriste TCP može bez modifikacija koristiti Tor putem sučelja za SOCKS protokol. Svaki klijent ima Tor posrednik (engl. onion proxy), ili kraće "OP", koji je odgovoran za prihvaćanje TCP zahtjeva od klijentskih aplikacija, gradnju i održavanje kruga te multipleksiranje TCP veza kroz izgrađeni krug. Klijentska aplikacija se, kao što je vidljivo na slici 2.3, spaja TCP-om na SOCKS poslužitelj, odnosno OP i preko SOCKS protokola zahtijeva TCP vezu specificiranu odredišnom IP adresom i pristupom. Skup svih čvorova i TCP veza od OP-a do posljednjeg čvora tvori *virtualni kanal*. Zahtjev se prenosi virtualnim kanalom do zadnjeg čvora koji uspostavlja TCP vezu s odredištem. Time je uspostavljen *tôk* (engl. stream), odnosno anonimizirani spoj s odredištem. Nakon uspostave veze, aplikacija koristi TCP vezu s OP-om za slanje podataka.



Slika 2.3. TCP veze između aplikacije i odredišta *R*

Kako bi izgradio krug, OP inkrementalno gradi kriptiranu vezu sa svakim odabranim čvorom mreže na temelju algoritma za odabir čvorova. Popis aktivnih čvorova s *opisnicima* nalazi se na ovlaštenim imeničkim poslužiteljima (engl. authority directory server). Opisnik (engl. descriptor) sadrži informacije o usmjerniku kao što su javni ključ, deklarirana propusnost i izlazna politika. Tor program dolazi sa početnim popisom imeničkih poslužitelja i njihovim javnim ključevima jer je bitno da napadač ne usmjeri klijente na kompromitirane imeničke poslužitelje. Ovlašteni imenički poslužitelji su potencijalno usko grlo i laka meta napada, pa postoje poslužitelji koji djeluju kao predposlužitelji (engl. cash directories) koji dohvaćaju opisnike od ovlaštenih poslužitelja. Imenički poslužitelj je HTTP poslužitelj s kojeg OP povremeno dohvaća opisnike. Iz skupa aktivnih čvorova OP bira čvorove za izgradnju kruga. Krug se povećava za jedan segment (engl. hop) u svakom koraku, a svaki čvor na putu zna samo od kojeg čvora su mu proslijeđeni podaci i kojem čvoru mora proslijediti podatke. Sa svakim sljedećim segmentom, OP pregovara s čvorom nezavisan skup tajnih ključeva. U trenutnoj inačici Tora, OP gradi krug od tri čvora jer je to dobar kompromis sigurnosti i performansi[2]. Prvi čvor u krugu s klijentske strane se naziva *ulazni čvor* (engl. Entry node) i on jedini zna klijentsku IP adresu. Zadnji čvor u krugu se naziva *izlazni čvor* (engl. Exit node) i on dekriptira posljednju ljusku. Izlazni čvor ostvaruje vezu s odredištem i prosljeđuje klijentski promet. Sa stanovišta odredišnog poslužitelja, izlazni čvor je taj koji traži uslugu, a ne klijent kojeg skriva mreža Tor. Između ulaznog i izlaznog čvora je jedan ili više *srednjih čvorova* (engl. middle node). OP izabire izlazni čvor koji omogućuje vezu s odredištem. Hoće li određeni čvor biti odabran kao izlazni, ovisi o njegovoj izlaznoj politici. Otvorena izlazna politika dopušta slanje IP paketa na izlazu iz mreže Tor na bilo koju adresu i pristup. Restriktivnijom izlaznom politikom izlazni čvor zabranjuje pristupe i blokove IP adresa kako bi spriječio zloupotrebu kao što je slanje neželjene pošte. Izlazni čvor se restriktivnom izlaznom politikom štiti od mogućeg odgovaranja za zloupotrebu. Zatvorenom izlaznom politikom čvor osigurava da iz njega promet nikada neće napuštati mrežu Tor. Drugim riječima, takav čvor ne može biti izlazni.

Svi praktični sustavi niske latencije, uključujući Tor, se ne pokušavaju braniti od globalnog pasivnog napadača i napada na krajnjim točkama. Model prijetnje mreže Tor (engl. threat model) pretpostavlja napadača koji može pokrenuti Tor usmjernik ili kompromitirati dio Tor usmjernika. Napadač može pratiti, ali i mijenjati dio prometa.

Tor osigurava *savršenu unaprijednu sigurnost* (engl. perfect forward security). Savršena unaprijedna sigurnost je definirana svojstvom kriptografskog sustava da tajni ključ sjednice izveden iz skupa dugoročnih javnih i privatnih ključeva nije kompromitiran ako jedan od dugoročnih privatnih ključeva bude kompromitiran u budućnosti. U ranijim verzijama Tora,

[2] Krug s tri čvora je nešto ranjiviji na napad na krajnje točke u prisustvu DDoS napada od kruga s dva čvora dok krug s dva čvora trivijalno otkriva ulazni čvor izlaznom [92]. Krug s tri čvora pruža lošije performanse od kruga s dva čvora.

koji nije osiguravao savršenu unaprijednu sigurnost, bilo je moguće da neprijateljski čvor snima promet, kasnije kompromitira čvorove sljedbenike u krugu i dekriptira promet.

2.4.2. Protokol Tor

Tor koristi kriptografski algoritam tôka (engl. stream cipher), kriptografiju javnog ključa (engl. public key criptografy), Diffie-Hellman protokol i funkciju sažetka (engl. hash function) [36]. Kriptografski algoritam tôka koristi 128-bitno AES kriptiranje brojačem (engl. counter mode). Algoritam javnog ključa je RSA s 1024-bitnim ključem i fiksnim eksponentom. Za dopunjavanje prometa (engl. padding) se koristi OAEP-MGF1, sa SHA-1 kao funkcijom sažetka. Diffie-Hellman protokol razmjene ključeva koristi generator (g) 2, a modulo (p) je 1024-bitni sigurni prosti broj definiran s RFC2409. Za funkciju sažetka koristi se SHA-1.

Protokol Tor koristi ključeve za postizanje tri cilja:

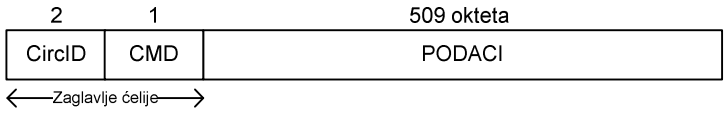
- *kriptiranje*: čuvanje tajnosti podataka u mreži Tor
- *autentikacija*: kako bi klijenti znali da komuniciraju s OR-ovima s kojima bi trebali komunicirati
- *potpis*: kako bi se osiguralo da svi sudionici imaju identične opisnike

Svaki OR ima višestruke parove javno-privatnih ključeva:

- *dugoročni ključ koji služi kao identitet* (engl. identity key) se koristi za potpisivanje dokumenata i certifikata te za potvrđivanje identiteta OR-a
- *srednjoročni ključ sloja* (engl. onion key) je privatni ključ kojim OR dekriptira sloj poruke prilikom proširenja kruga (time klijentu dokazuje poznavanje javnog ključa, odnosno identitet). Rotira se jednom tjedno.
- *kratkoročni ključ veze* (engl. connection key) koristi za pregovaranje TLS veze. Ključ se mora mijenjati barem jednom dnevno.

Svaka veza dva Tor usmjernika (OR-OR) ili klijenta i usmjernika (OP-OR) koristi TLS/SSLv3 za autentikaciju i kriptiranje. Nakon uspostavljanja TLS veze, strane razmjenjuju ćelije fiksne veličine.

Promet u mreži Tor putuje u ćelijama fiksne veličine od 512 okteta. Ćelija se sastoji od zaglavlja i korisnog sadržaja ćelije (slika 2.4). Zaglavlje sadrži identifikator kruga `CircID` (engl. circuit idenitifier) i naredbu (CMD) koja opisuje što treba uraditi sa sadržajem ćelije. Između dva OR-a mogu prolaziti ćelije različitih krugova, a `CircID` na relaciji OR-OR identificira krug. Identifikator kruga, prema tome, nije jedinstven za sve čvorove istog kruga, već svaki par OP-OR ili OR-OR dogovara vrijednost identifikatora kruga.



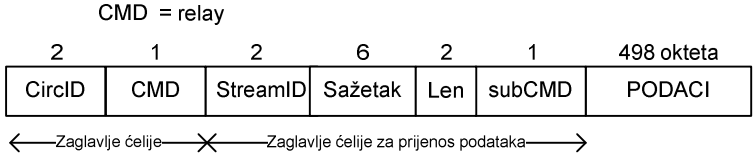
Slika 2.4 –Upravljačka ćelija mreže anonimnosti Tor

S obzirom na naredbu koju nose, ćelije mogu biti *upravljačke ćelije* (engl. control cell) ili *ćelije za prijenos podataka* (engl. relay cell). Upravljačku ćeliju uvijek tumači čvor koji ju prima, a moguće naredbe su popisane u tablici 2.2.

Tablica 2.2. Naredbe upravljačke ćelije

Naredba	*Funkcija*
padding	nadopuna (podaci se ne koriste)
create	stvaranje kruga (u podacima se nalazi prvi korak DH razmjene ključeva)
created	potvrda stvaranja kruga
destroy	zatvara krug

Ćelija za prijenos podataka, koja je prikazana na slici 2.5, prepoznaje se po naredbi *relay* u zaglavlju ćelije.



Slika 2.5 –Ćelija za prijenos podataka mreže anonimnosti Tor

Ćelija za prijenos podataka ima dodatno zaglavlje čija polja su popisana u tablici 2.3.

Tablica 2.3. Polja zaglavlja ćelije za prijenos podataka

Polje	*Funkcija*
streamID	identifikator tôka (jedan krug može multipleksirati više tôkova)
sažetak	kontrolna suma za osiguranje besprijekornosti podataka kroz cijeli krug
len	duljina ćelije
subCMD	naredba za prijenos podataka

Čitav sadržaj tijela i zaglavlja ćelije za prijenos podataka je kriptiran.

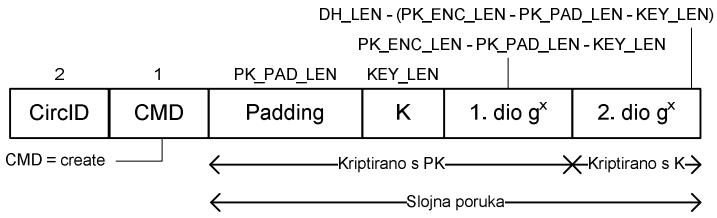
Naredbe ćelija za prijenos podataka i njihove funkcije su popisane u tablici 2.4.

Tablica 2.4. Naredbe ćelija za prijenos podataka

Naredba	*Funkcija*
relay data	za podatke koji putuju niz krug
relay begin	otvaranje tôka
relay end	uredno zatvaranje tôka
relay teardown	zatvaranje neispravnog tôka
relay connected	obavještavanje OP-a da je tôk uspješno otvoren
relay extend	produžuje krug za jedan segment
relay extended	potvrda produžetka kruga
relay truncate	zatvara dio kruga
relay truncated	potvrda zatvaranja dijela kruga
relay sendme	kontrola zagušenja
relay drop	dummy paket širokog dometa

OP može koristiti isti krug za ostvarivanje više anonimnih spojeva, odnosno tôkova. U prijašnjim verzijama Tora svaka je TCP veza zahtijevala izgradnju zasebnog kruga. To je oduzimalo dosta resursa zbog računske zahtjevnosti operacija kriptografije javnog ključa, pogotovo za aplikacije koje koriste više TCP veza, kao što je Web preglednik. Česte izgradnje krugova predstavljaju i sigurnosnu manjkavost zbog otkrivanja aktivnosti promatračima. Kako bi se povećala sigurnost, OP periodički otvara nove krugove, a zatvara stare krugove koji više nemaju otvorenih tôkova. Krugovi se grade unaprijed i time se izbjegava kašnjenje, a OP-ovi razmatraju stvaranje novog kruga svake minute. Zahtjevni korisnici tako ne troše puno vremena gradeći krugove, a na izlaznim čvorovima se zahtjevi teže međusobno mogu povezati.

OP krug gradi inkrementalno, pregovarajući simetrični ključ sa svakim OR-om, jedan po jedan segment. Kada želi izgraditi krug, OP (zvat ćemo ju Alice) šalje *create* ćeliju prvom čvoru (zvat ćemo ga Bob). Sadržaj ćelije je slojna poruka (slika 2.6), *hibridno* kriptirana Bobovim ključem sloja. Slojna poruka sadrži prvi korak Diffie-Hellman (DH) protokola razmjene ključeva. Alice izabire simetrični ključ `K` i privatni DH ključ `x` i šalje g^x, gdje je `g` generator. Na slici 2.6 može se vidjeti da je g^x rastavljen na dva dijela: prvi kriptiran s `PK`, a drugi s `K`. Oznake korištene na slici 2.6 i u algoritmu hibridnog kriptiranja popisane su u tablicama 2.5 i 2.6.



Slika 2.6. Struktura *create* ćelije mreže anonimnosti Tor

Hibridno kriptiranje slijeda okteta `M` u izlazni slijed `MK` javnim ključem `PK` obavlja se na sljedeći način:

```
Ako (duljina(M) < (PK_ENC_LEN – PK_PAD_LEN))
   MK = nadopuni_i_kriptiraj(M, PK)
Inače
   generiraj_nasumično(K, KEY_LEN)
   M1 = dio_od(M, 1, PK_ENC_LEN – PK_PAD_LEN – KEY_LEN)
   M2 = dio_od(M, PK_ENC_LEN – PK_PAD_LEN – KEY_LEN,
   duljina(M))
   MK1 = nadopuni_i_kriptiraj(K|M1,PK)
   MK2 = kriptiraj_kriptografskim_algoritmom_tôka(M2,K)
   MK = MK1|MK2
```

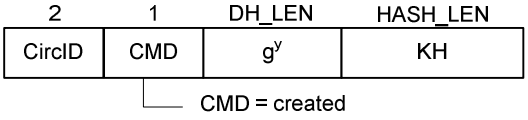
Tablica 2.5. Notacija u protokolu Tor

Kratica	*Značenje*
PK	javni ključ
SK	privatni ključ
K	simetrični ključ
H(m)	kriptografski sažetak od m
a|b	ulančavanje 'a' i 'b'

Tablica 2.6. Sigurnosni parametri u protokolu Tor

Kratica	*Značenje*
KEY_LEN	duljina ključa kriptografskog algoritma tôka u oktetima
PK_ENC_LEN	duljina poruke kriptirane javnim ključem u oktetima
PK_PAD_LEN	broj okteta kojima se nadopunjuje poruka kriptirana javnim ključem (padding). Najveći broj okteta koji mogu biti kriptirani u jednoj operaciji javnim ključem je, prema tome, PK_ENC_LEN – PK_PAD_LEN
DH_LEN	broj okteta kojima se prikazuje član Diffie-Hellman grupe
DH_SEC_LEN	broj okteta za Diffie-Hellman privatni ključ (x)
HASH_LEN	duljina izlaza funkcije sažimanja u oktetima
PAYLOAD_LEN	najveća dozvoljena duljina tijela ćelije u oktetima
CELL_LEN	duljina Tor ćelije u oktetima

Bob odgovara *created* ćelijom, prikazanom na slici 2.7, koja sadrži drugi korak DH protokola (g^y) i sažetak ključa KH o kojem se pregovara.



Slika 2.7. Struktura *created* ćelije mreže anonimnosti Tor

Nakon uspostave kruga, Alice i Bob mogu izračunati $K0 = g^{xy}$ i razmjenjivati ćelije za prijenos podataka kriptirane na temelju ključa K0. Iz K0 se izvode simetrični ključevi za oba smjera: Kf za smjer od OP prema OR i Kb za smjer od OR prema OP. Iz K0 se izvode i ključevi funkcije sažetka u oba smjera za očuvanje integriteta tôka podataka.

CircID *create* ćelije je nasumično izabran 16-bitni broj, izabran od čvora koji šalje *create* ćeliju. Alice, prema tome, bira $CircID = C_{AB}$ koji je trenutno neiskorišten.

Prije nego Alice počne stvarati krug, mora odabrati čvorove. Slijedi algoritam za stvaranje kruga:

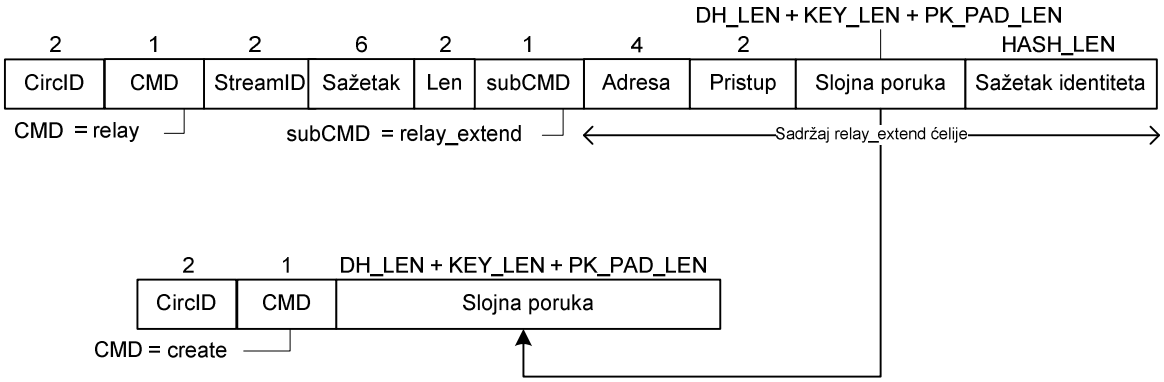
```
OR_N = pronađi_izlazni_čvor (izlazna_politika)
Za i = 1 do N-1
    OR_i = izaberi_OR_OR_1..i-1
Ako (veza(OR_1)!=otvorena)
      otvori_vezu(OR_1)
CircID = izaberi_neiskorišten_circID(OR_1)
pošalji_create_ćeliju(OR_1)
čekaj(primio_created_ćeliju)
završi_razmjenu_ključeva
izdvoji_ključ(Kf_1)
izdvoji_ključ(Kb_1)
Za i = 2 do N
    proširi_krug(OR_i)
```

Za proširenje kruga za neki OR_M, OP izvodi sljedeće korake:

```
M = stvori_sloj_poruke
kriptiraj(M, PK_OR_M)
pošalji_relay_extend_ćeliju(M,OR_M-1)
čekaj(primio_extended_ćeliju)
provjeri(KH)
izračunaj_ključeve
```

OR koji primi *relay extend* ćeliju šalje *create* ćeliju sljedećem OR-u, s uključenim slojem poruke u tijelu ćelije. Kada OR primi *created* ćeliju, pakira njen sadržaj u *relay extended* ćeliju. Kada OP primi *relay extended* ćeliju, može izračunati g^y.

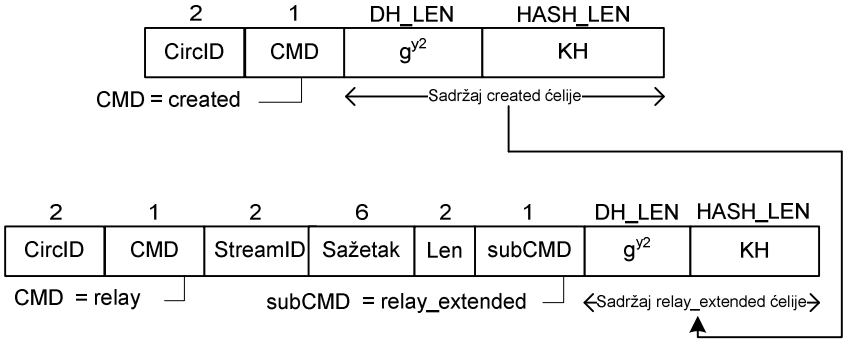
Na primjer, kako bi proširila krug za još jedan segment, Alice šalje *relay extend* ćeliju (slika 2.8) Bobu s adresom sljedećeg OR-a (zvat ćemo ju Carol) i kriptiranog g^{x2} u slojnoj poruci.



Slika 2.8. Struktura *relay_extend* ćelije mreže anonimnosti Tor

Polja `Adresa` i `Pristup` odnose se na IPv4 adresu i pristup sljedećeg OR-a u krugu; sažetak identiteta je sažetak javnog ključa sljedećeg OR-a. Sažetak služi OR-u koji proširuje krug da bude siguran u identitet sljedećeg OR-a i sprječava neke od napada s čovjeka u sredini (engl. man in the middle attack).

Bob bira `CircID` = C_{BC} koji je trenutno slobodan između njega i Carol. Vrijednost C_{AB} asocira s ulaznom vezom prema Alice, a C_{BC} s izlaznom vezom prema Carol. Bob kopira slojnu poruku od Alice (slika 2.8) s prvim korakom razmjene ključeva u *create* ćeliju i prosljeđuje ju Carol. Kada Carol odgovori s *created* ćelijom (slika 2.9), Bob ju umetne u *relay extended* ćeliju i vraća ju Alice. Sada Alice i Carol dijele zajednički ključ g^{x2y2}.



Slika 2.9. Struktura *created* odnosno *relay_extended* ćelije mreže anonimnosti Tor

Alice analogno proširuje krug na treći čvor ili dalje, uvijek nalažući zadnjem čvoru da proširi krug za jedan segment.

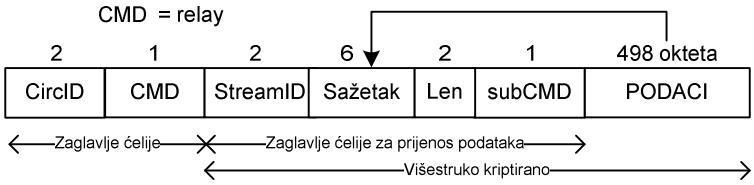
Protokol razmjene ključeva na razini kruga omogućuje jednosmjernu autentikaciju: Alice zna da se razmjenjuje ključeve s OR-om, ali OR-a ne zanima tko otvara krug. Alice ne posjeduje javni ključ i ostaje anonimna. Ključ je na sličan način jednosmjerno autenticiran: Alice i OR razmjenjuju ključ, ali Alice zna samo da ga OR zna. U drugom koraku, Bob dokazuje da je on taj koji je dobio g^x i tko je izabrao y.Također, osigurana je unaprijedna tajnost.

Formalno,

$$Alice \rightarrow Bob : E_{PK_{Bob}}(g^x) \quad (2.1)$$

$$Bob \rightarrow Alice : g^y, H(K) \quad (2.2)$$

Nakon što je Alice izgradila krug i dijeli ključ sa svakim pojedinim OR-om kruga, može slati ćelije za prijenos podataka. Ćelije za prijenos podataka služe OP-u i izlaznom čvoru da tuneliraju naredbe i tôkove kroz krug. Kada Alice želi poslati ćeliju za prijenos podataka (slika 2.10) određenom OR-u, ona izračunava sažetak sadržaja ćelije za prijenos podataka i onda slijedno kriptira zaglavlje ćelije za prijenos podataka i podatke simetričnim ključem svakog OR-a na putu do ciljnog OR-a.



Slika 2.10. Ćelija za prijenos podataka anonimne mreže Tor

Kada neki OR na putu primi prijenosnu ćeliju, na temelju pročitanog identifikatora kruga `CircID` i pripadnog simetričnog ključa dekriptira sadržaj ćelije. Kriptiranje i dekriptiranje tijela ćelije za prijenos podataka izvodi se kriptiranjem tôka podataka izvedenim ključevima `Kf` u smjeru *create* ćelije i `Kb` u smjeru suprotnom od *create* ćelije. Budući da je `Sažetak` višestruko kriptiran, tek će na odredištu, nakon posljednjeg dekriptiranja, odgovarati sažetku podataka. Polje `Prepoznato` duljine 2 okteta koje je na slici 2.10 skriveno u polju `Sažetak` prije kriptiranja ima vrijednost jednaku nuli. Kriptiranjem vrijednost nije više jednaka nuli, pa služi kao efikasan pokazatelj ciljnom OR-u. Ako je `Prepoznato` nula i sažetak odgovara, ćelija je došla na ciljni OR koji procesira *relay* naredbu i podatke. Ako `Prepoznato` nije nula ili sažetak ne odgovara, OR prosljeđuje ćeliju sljedećem čvoru u krugu. Prije toga zamjenjuje vrijednost `CircID` u zaglavlju odgovarajućom uparenom vrijednošću. Topologija kruga s višestrukim izlazima (engl. leaky pipe) omogućuje Alice da izabere bilo koji čvor u krugu za izlaz tôka. Alice može koristi višestruke izlaze zbog izlaznih politika ili da bi otežala OR-ovima saznavanje da su tôkovi od istog pošiljatelja.

Sličan proces se odvija i kod OP-a: tijelo ćelije se iterativno dekriptira s $\texttt{Kb}_i$ (gdje je *i* indeks OR-a u krugu). Sve ćelije za prijenos podataka koje se odnose na isti tunelirajući tôk imaju istu vrijednost streamID (koje nasumično bira OP).

Želi li zatvoriti krug, Alice šalje *destroy* ćeliju prvom čvoru u krugu koji želi zatvoriti. OR koji prima *destroy* ćeliju, oslobađa resurse vezane za taj krug te šalje *destroy* ćeliju dalje u krug. Krug se naposljetku zatvara zatvaranjem TCP veze izlaznog čvora s vanjskim odredištem. Alice može zatvoriti i dio kruga slanjem *relay truncate* ćelije ciljnom čvoru koji dalje šalje *destroy* ćeliju. Na taj način Alice može izgraditi upravo zatvoreni dio kruga bez znanja prethodnih čvorova.

Kada Alicina aplikacija želi ostvariti TCP vezu specificiranu adresom i pristupom, ona šalje zahtjev preko SOCKS-a OP-u da otvori vezu. OP bira najnovije otvoren krug i OR u tom krugu čija izlazna politika dopušta zatraženi spoj. OP zatim otvara novi tôk šaljući *relay begin*

ćeliju s nasumično odabranim `streamID`. Ćelija sadrži adresu i pristup odredišta, gdje adresa može biti ime računala (engl. DNS hostname), IPv4 ili IPv6 adresa. Pristup je broj od 0 do 65535. Neke aplikacije, poput Mozille i udaljenog pristupa (SSH), razrješavaju DNS imena prije slanja paketa i na taj način otkrivaju odredište DNS serveru (ili nekome tko vidi taj promet). Za Mozillu postoji rješenje u Privoxy posredniku, a za udaljeni pristup rješenje trenutno ne postoji. Za razrješenje imena koristeći mrežu Tor koristi se *relay resolve* ćelija.

Ako je potrebno, izlazni čvor razrješava ime u adresu, otvara TCP vezu s odredištem i vraća Alice *relay connected* ćeliju, a OP šalje SOCKS *reply* aplikaciji. OP sada prihvaća podatke iz aplikacije i pakira ih u *relay data* ćelije.

Zatvaranje tôka je analogno zatvaranju TCP veze: koriste se dva koraka za normalno zatvaranje i jedan korak kod neregularnog zatvaranja. Zatvori li se tôk preuranjeno, izlazni čvor šalje *relay teardown* ćeliju. Zatvori li se tôk normalno, izlazni čvor šalje *relay end* ćeliju u krug, a klijent odgovara još jednom *relay end* ćelijom. Dobije li izlazni čvor *relay end* ćeliju za bilo koji tôk, on će zatvoriti tu TCP vezu i neće poslati ništa nazad u krug (neregularno zatvaranje).

2.4.3. Skrivene usluge

Mreža Tor omogućava anonimnost primatelja kroz *skrivene usluge*. Skrivene usluge omogućavaju Bobu da pruža TCP uslugu (primjerice Web poslužitelj), bez otkrivanja njegove IP adrese klijentima. Time se uspješno brani od DoS (engl. denial of service) napada: napadač koji želi napasti Bobovu uslugu to može činiti samo napadom na mrežu Tor jer ne poznaje njegovu IP adresu.

Bob skriva svoju uslugu tako da odabire nekoliko OR-ova kao svoje *točke uvoda* (engl. introduction points), te ih obznanjuje u nekoj od *lookup* tablica, kao što je DHT (engl. distributed hash table), odnosno njegovoj implementaciji CFS [37]. Alice, klijent, izabire neki OR kao točku sastajanja (engl. rendezvous point), spaja se na Bobovu točku uvoda i obavještava je o točki sastajanja te čeka da se Bob javi.

Slijedi popis operacija koje za Alice i Bob izvršavaju njihovi lokalni OP-ovi:

1. Bob generira dugoročni javni ključ i upareni privatni ključ za identifikaciju usluge.
2. Bob izabire točke uvoda i objavljuje ih potpisane na *lookup* servisu (indeksirane sažetkom javnog ključa).
3. Bob gradi krug do svake točke uvoda, predaje im javni ključ koji identificira uslugu i ostavlja ih da čekaju zahtjeve.
4. Alice saznaje za Bobovu uslugu i prikuplja detalje usluge preko *lookup* servisa.
5. Alice izabire OR kao točku sastajanja, ili kraće RP, kako bi pristupila Bobovoj usluzi, gradi krug do RP i daje mu autorizacijski kolačić koji će služiti za prepoznavanje Boba.
6. Alice otvara anonimni tôk do jedne od Bobovih točaka uvoda, predaje poruku kriptiranu Bobovim javnim ključem gdje se predstavlja, informira o svojoj RP, predaje kolačić i prvu polovinu DH protokola razmjene ključeva. Alice predaje i sažetak Bobovog javnog ključa tako da točka uvoda može utvrditi da Alice zaista pristupa Bobovoj usluzi. Točka uvoda prosljeđuje poruku Bobu.
7. Odluči li Bob pružiti uslugu Alice, gradi krug do Alicinog RP-a gdje šalje kolačić i drugu polovinu DH razmjene ključeva. Alice zna da jedino Bob s njom dijeli ključ.
8. RP povezuje Alicin krug s Bobovim. RP ne poznaje ni Alice, ni Boba, kao niti promet koji razmjenjuju.

9. Alice šalje *relay begin* ćeliju niz krug koja pristiže Bobovom OP-u i spaja je s Bobovim Web poslužiteljem.
10. Anonimni tôk je ostvaren i dalje Alice i Bob normalno komuniciraju.

Iako je Bobov Web poslužitelj kroz skrivene usluge siguran od DoS napada, Bobove točke uvoda nisu. Kako bi smanjio rizik, Bob treba otvoriti veći broj točaka uvoda i oprezno raspolagati s informacijama o točkama uvoda. Na primjer, Bob može podijeliti još jedan tajni javni ključ odabranim korisnicima za pristup informacijama u *lookup* servisu.

Bobov Web poslužitelj i Alicina aplikacija koja mu pristupa se ne trebaju modificirati zbog skrivene uslugu. Bobov OP poznaje lokalnu IP adresu Web poslužitelja, strategiju autoriziranja klijenata i njegov javni ključ. Strategijom autoriziranja Bob može odrediti skup korisnika kojima pruža uslugu, primjerice, na način da moraju predati autorizacijski kolačić. Kada Alice traži pristup skrivenoj usluzi, kodira sve potrebne informacije u potpuno kvalificirani naziv domene (engl. fully qualified domain name, FQDN). Skrivene usluge koriste virtualnu *top level* domenu naziva `.onion`, a ime računala (engl. hostname) je oblika `x.y.onion`, gdje je `x` autorizacijski kolačić, a `y` kodira sažetak javnog ključa. Alicin OP provjerava adresu, ako je namijenjena skrivenoj usluzi, dekodira ključ i započinje protokol sastajanja.

Korištenje skrivenih usluga moguće je samo putem mreže Tor, što znači da je za korisnike Interneta bez korištenja mreže Tor Web stranica objavljena putem skrivenih usluga nedostupna.

Torova usluga točke sastanka omogućuje raznim sustavima anonimnosti uspostavu također anonimne veze. Eternity i Free Haven osiguravaju usluge anonimnosti putem servera koji se mogu sakriti kao Torova skrivena usluga.

2.4.4. Slabosti mreže Tor

Mreža Tor, kao sustav niske latencije, nije dizajnirana da bude otporna na napade na krajnje točke. To su napadi pasivnog napadača koji prateći promet može doznati razne informacije o korisniku, primjerice profiliranjem vremenskih uzoraka u tôku ili na krajevima kruga. Korisnik se od napada na krajnje točke može štititi sakrivajući vezu između sebe i ulaznog čvora tako da je i sam Tor usmjernik ili da bude iza sigurnosne stijene (engl. firewall). U tom slučaju napadač mora razdvojiti promet koji potječe od korisnika od onog koji samo prosljeđuje. Prečestom rotacijom krugova korisnik se stavlja u opasnost od napada koji se oslanjaju na nestalnost anonimnog skupa [38]. Tor usmjernici izlaze i ulaze u mrežu Tor te napadač može pratiti kako se anonimni skup mijenja u vremenu. Posumnja li napadač da u različitim krugovima prosljeđuje promet iste sjednice, primjerice ako pošiljatelj odaje neku informaciju o sjednici, a izlazni čvor ju identificira, može saznati moguće pošiljatelje korelacijom sa skupom aktivnih čvorova u određenom trenutku. Cilj je svesti moguće pošiljatelje na najmanji broj. Ovakav napad se zove *napad presjekom* (engl. intersection attack) [9]. Kada je služba za sigurnost sveučilišta Bowling Green State University posumnjala kako je netko sa sveučilišnog kampusa koristio Tor u neprimjerene svrhe, dovoljno je bilo ispitati dva stalna Tor korisnika i saznati identitet prijestupnika [39]. Sličan napad, odnosno podvrsta napada presjekom je *napad prethodnika* (engl. predecessor attacks). Posumnja li napadač da prosljeđuje promet iste sjednice, bilježi tko mu je prethodnik. Prethodnik koji je najviše puta zabilježen je najvjerojatnije pošiljatelj [40].

Aktivni napadač koji sazna TLS ključ može pročitati upravljačke ćelije, a s ključem sloja može i dekriptirati jedan sloj poruke i vidjeti *create* ćelije. Međutim, prozor ovog napada

ograničen je periodom izmjene ključeva. Slijednim kompromitiranjem OR-ova koji sačinjavaju jedan krug napadač može od klijenta doći do primatelja, ali samo za vrijeme trajanja kruga jer savršena unaprijedna sigurnost onemogućava naknadno dekriptiranje ćelija.

Budući da ništa ne sprječava napadače da pokrenu vlastiti OR, korisnik može izabrati kompromitirani OR na različitim mjestima u krugu. Vjerojatnost da korisnik izabere ulazni kompromitirani čvor je $P_1 = c/n$, gdje je c broj kompromitiranih čvorova, a n je ukupan broj čvorova u mreži. Kompromitirani čvor utvrđuje aktivnost pošiljatelja, ali ništa ne saznaje o sadržaju. Druga mogućnost je da kompromitirani čvor bude izlazni, uz vjerojatnost $P_2 = c/n$. U ovom slučaju je narušena anonimnost primatelja kao i sadržaj. Anonimnost primatelja i pošiljatelja, kao i sadržaj su narušeni ako su kompromitirani i ulazni i izlazni čvor, a to se može dogoditi s vjerojatnošću od $P_3 = \frac{c^2}{n^2}$ [14]. Uvođenjem zaštitnog ulaznog čvora (engl. entry guard), smanjuje se vjerojatnost kompromitiranja krajeva kruga, ali i napad prethodnika [38]. Status zaštitnog ulaznog čvora dodjeljuje ovlašteni imenički poslužitelj. Korisnik umjesto iz cijelog skupa Tor usmjernika ulazni čvor bira iz suženog skupa usmjernika i tako onemogućuje napad, pod uvjetom da nitko iz skupa zaštitnih ulaznih čvorova nije kompromitiran. Cilj je svesti rizik stalnog izabiranja ulaznog čvora među svim čvorovima pri izgradnji kruga na izabiranje skupa zaštitnih ulaznih čvorova [41]. U trenutnoj verziji, Tor klijent izabire skup od tri zaštitna ulazna čvora koji postaju ulazni čvorovi u svakom krugu [42]. Ograničavanjem skupa izlaznih čvorova također se smanjuje mogućnost napada, ali ne toliko kao kod ulaznih jer i pošteni izlazni čvor ne štiti od zlonamjernog resursa.

Vremenskom analizom napadač koji drži dva čvora M_1^K i M_h^L, gdje su K i L komunikacijski putovi, a indeks *1..h* označava redni broj čvora na putu, utvrđuje je li $K = L$, odnosno nalaze li se čvorovi na istom putu K između pošiljatelja I i primatelja R:

$$I \rightarrow M_1^K \rightarrow M_2^K \rightarrow \cdots \rightarrow M_h^K \rightarrow R \qquad (2.3)$$

Postoje dvije metode vremenske analize [43]:

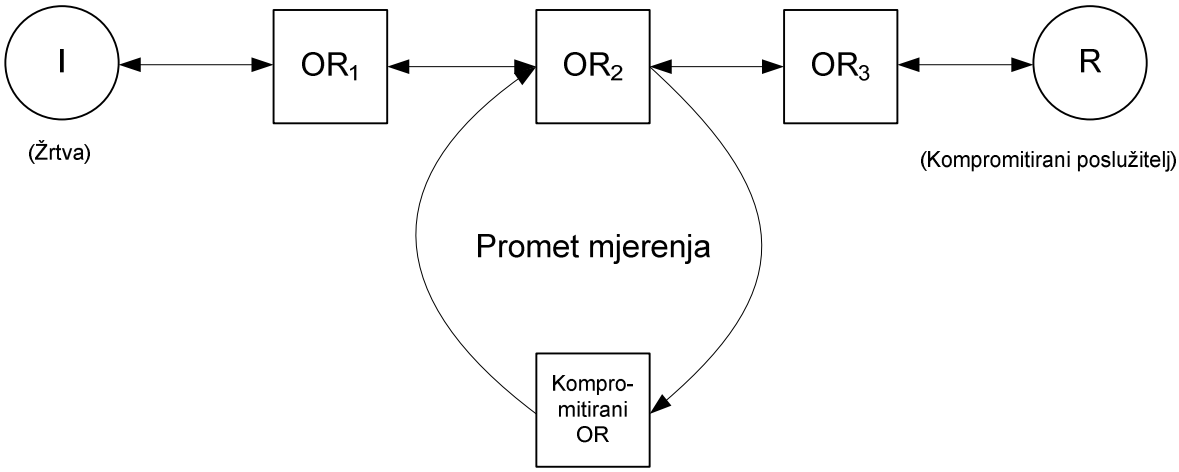
- Vremenska razlika između dolaska paketa *i* i njegovog prethodnika. Korelacija je veća za M_1^K i M_h^L, $K = L$ nego za M_1^K i M_h^L, $K \neq L$. Ako neki čvor ispusti paket, korelacija se drastično smanjuje.
- Brojanje paketa. Za razliku od vremenske razlike, ako čvor M_1^K ispusti paket, samo povećava korelaciju.

Napadač može dodatno modificirati vremena slanja paketa iz M_1^K ili može namjerno ispustiti paket što povećava vremensku korelaciju koju prate M_1^K i M_h^L. Što je veća korelacija, to je vjerojatnije da je $K = L$.

Za obranu se koristi prekrivajući promet jer smanjuje korelaciju vremenske razlike paketa ili obrambeno ispuštanje paketa, odnosno nalog jednom od čvorova M_m^K da namjerno ispusti paket.

Objavljeni su i napadi analizom prometa koji se oslanjaju na činjenicu da je latencija Tor usmjernika proporcionalna s količinom prometa koju prenosi [12] (engl. interference attack). Slika 2.11 prikazuje koncept napada. Želi li napadač utvrditi da je OR_2 dio nekog kruga, on gradi krug kroz OR_2 tako da ga zatvara u sebe i mjeri latenciju. Latencija se može analizom prometa korelirati s ukupnim prometom koji prolazi kroz OR_2, odnosno s nekim poznatim obilježjem prometa. Uključi li se u model napadača i kompromitirani Web poslužitelj koji

djeluje na vremenska obilježja prometa, tako da na primjer umetne izmjenu pauze i naleta prometa (engl. burst), koreliranje latencije i prometa od kompromitiranog poslužitelja će biti još učinkovitije. Binarnom pretragom mogu se identificirati svi čvorovi u krugu, ali ne i klijent pa napad nije potpun. Veličina i raznolikost mreže Tor utječe na efikasnost ovog napada jer binarna pretraga mora biti izvršena za trajanja kruga i na skupu od oko 2000 čvorova (napad je demonstriran na skupu od 50-tak čvorova). Sličan napad se oslanja na smanjenu propusnost kruga pri zagušivanju čvorova prometom (engl. clogging attack) [34].



Slika 2.11. Analiza prometa mjerenjem latencije kroz OR_2

3. Zloupotreba mreže Tor

Mreža Tor prvenstveno je namijenjena korisnicima kojima je anonimnost potrebna zbog slobode izražavanja, zaštite od opasnosti, neugode, marketinškog profiliranja ili zaštite poslovnih interesa. Zbog potrebe za što većim brojem korisnika, mreža Tor je otvorena za nove korisnike, jednostavna za korištenje i samim time česta meta zlonamjernika koji koriste anonimnost da sakriju svoju zloupotrebu. Anonimnost mreže Tor direktno ovisi o anonimnom skupu, odnosno količini korisnika, a zloupotreba mreže izlazne čvorove dovodi u opasnost od sankcija za proslijeđeni promet. Korištenje mreže Tor za neinteraktivan promet ima utjecaja na propusnost cijele mreže i općenito odvraća korisnike od korištenja mreže i tako umanjuje anonimni skup [44]. Smanjena anonimnost dodatno negativno utječe na ugled mreže i posljedično na daljnje smanjenje anonimnog skupa i tako u krug. Iz svih ovih razloga je jasno da je za opstojnost Tor usluge i njeno širenje ključno zadržati ugled, korisnike i spriječiti zloupotrebu što je više moguće. Anonimni skup treba biti raznolik jer je tako teže profilirati određene skupine, primjerice aktiviste, koji se skrivaju među ostalim korisnicima.

Analiza korištenja mreže Tor otkriva da je većina ostvarenih TCP veza korištena za interaktivan Web promet (HTTP), ali neinteraktivan promet, na primjer BitTorrent, zauzima puno veću količinu mrežne propusnosti u ukupnoj propusnosti s obzirom na udio veza [44]. Drugim riječima, manji broj korisnika ruši performanse i odvraća od mreže veći broj korisnika kojima je niska latencija bitna za interaktivno korištenje i tako utječe na anonimnost cijele mreže. Upravo iz tog razloga, dizajneri mreže Tor smatraju P2P promet štetnim pa je pretpostavljena izlazna politika zabrana TCP pristupa koji se koriste za dijeljenje datoteka (engl. file sharing). Daljnjom analizom strukture prometa u izlaznim čvorovima pokazano je da se relativno često koriste nezaštićeni protokoli, odnosno da su korisnička imena i šifre slani u čistom tekstu [44]. Udio nezaštićenih protokola, poput POP, IMAP, Telnet i FTP je u ukupnom prometu relativno mali, ali je njihovo korištenje opasno jer izlazni čvor može sakupiti korisničke informacije i time ugroziti anonimnost klijenta. Tuneliranjem nezaštićenih protokola preko mreže Tor, izlazni čvor je u stanju s klijentom asocirati različite tôkove koje idu preko istog kruga. Iz tog je razloga preporučljivo odvajanje nezaštićenih protokola u različite krugove kako otkrivanje identiteta u jednom protokolu ne bi uzrokovalo narušavanje anonimnosti u drugim. Ovdje je bitno spomenuti da i HTTP može sadržavati korisničke informacije koje Tor sam po sebi neće ukloniti. Za tu svrhu se koriste specijalizirani Web posrednici, kao što je Privoxy.

Prijetnje mreži Tor se obrađuju u poglavlju 3.1., a postojeća rješenja, preinake i dodaci Toru koji pokušavaju suzbiti zloupotrebe odnosno motivirati ispravno korištenje se obrađuju u poglavlju 3.2.

3.1. Prijetnje

Prijetnje mreži Tor mogu doći od zlonamjernih izlaznih i klijentskih čvorova.

3.1.1. Zlonamjerni izlazni čvorovi

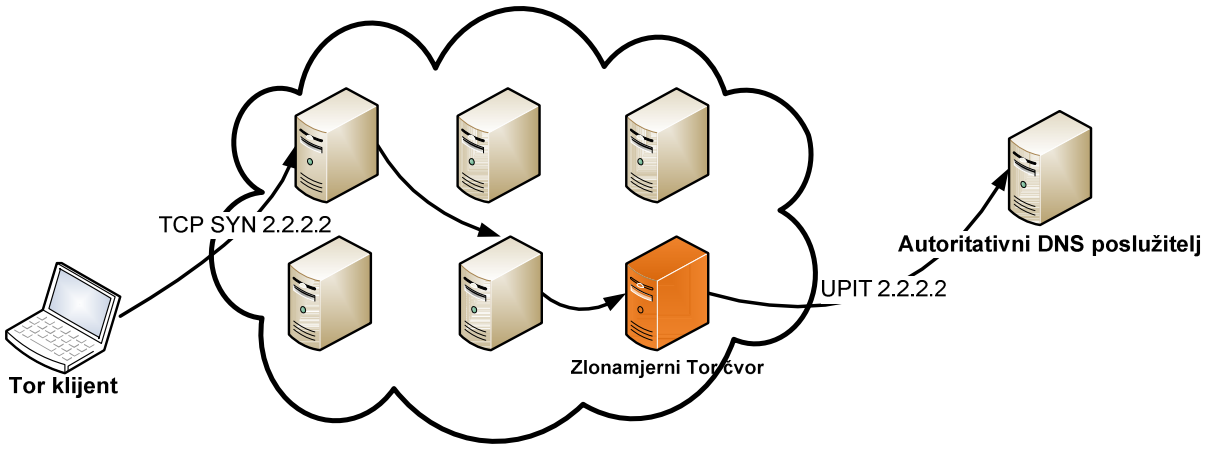
Jedino mjesto u krugu na kojem se pojavljuje promet klijenta u izvornom (nekriptiranom) obliku je izlazni čvor. Zbog relativno velike količine nezaštićenog prometa koji kroz njega prolazi, zlonamjerni izlazni čvorovi su motivirani da prate promet na izlazu iz mreže. Zabilježeni su slučajevi gdje se Tor koristio za pribavljanje korisničkih imena i šifri, nadalje

korištenih za upade u veleposlanstva i velike korporacije [45]. Izlazni Tor čvor također može mijenjati sadržaj koji izlazi na mrežu.

Za detekciju zlonamjernih izlaznih čvorova, mogu poslužiti Torflow skripte za skeniranje mreže Tor i prikupljanje statistika [46]. Torflow podržava skeniranje izlaznih čvorova u potrazi za modifikacijama na SSL-u, HTML-u, JavaScriptu i HTTP sadržaju. Nasumično odabrane stranice dobivene pretraživanjem ključnih riječi na Internet tražilicama se prvo učitaju bez Tora, a nakon toga preko njega. Ako su dohvaćene stranice iste, provjera je gotova, a ako nisu, ponovo se dohvaća stranica bez Tora, ali koristeći iste vjerodajnice (engl. credentials), primjerice kolačiće. Dodatno, sa svih dohvaćenih stranica se uklanjaju dozvoljene razlike između dva dohvaćanja bez Tora i potom se ponovo uspoređuju stranice dohvaćene Torom i bez njega. Postoje li i dalje razlike, utvrđuje se da je došlo do modifikacije. Skeniranje mreže Tor pokazalo je da se najčešće događa da izlaznim čvorovima istekne TCP tôk (engl. timeout) prije nego ga uspiju završiti ili ga odrežu u nekom trenutku. Dio njih ne može izvršiti DNS razlučivanje, a od zlonamjernih pokušaja primijećeno je i stvaranje vlastitog certifikata i zamjena s tuđim (engl. SSL spoofing), krađa sjednice udaljenog pristupa (napad čovjeka u sredini), ubacivanje Web sadržaja, itd. Torscanner je program sličan Torflowu, a namijenjen je otkrivanju zlonamjernih izlaznih čvorova [47].

Zlonamjerni čvorovi koji snimaju promet se mogu detektirati uz pretpostavku da imaju pokrenut snifer paketa (engl. packet sniffer) koji izvršava reverzne DNS upite [44]. Postupak je prikazan na slici 3.1 i izvodi se na sljedeći način:

1. Uspostavlja se autoritativni DNS poslužitelj za blok IP adresa koji je pod našom ingerencijom i rezerviran je samo za potrebe ovog postupka.
2. Kroz odabrani izlazni čvor se šalje zahtjev za otvaranjem TCP veze (TCP SYN segment) na neku od IP adresa iz bloka.
3. Prisluškuje li izlazni čvor promet, možda će izvršiti reverzni DNS upit za tom IP adresom što će zabilježiti naš DNS poslužitelj. Slanjem TCP SYN segmenata po svim pristupima možemo doznati koje pristupe prisluškuje izlazni čvor.



Slika 3.1. Postupak detekcije zlonamjernih izlaznih čvorova koji snimaju promet

Valja naglasiti da klijent šalje upit vlastitom DNS poslužitelju koji dalje rekurzivno vrši reverzno razlučivanje pa će naš DNS poslužitelj doznati samo IP adresu DNS poslužitelja izlaznog čvora. Provodi li se DNS razlučivanje u stvarnom vremenu, tada je moguće povezati upit s izlaznim čvorom. Alternativno se IP adresa iz bloka može mapirati na pojedini izlazni

čvor. Kada naš DNS poslužitelj primi upit za reverznim razlučivanjem, na temelju IP adrese iz upita možemo identificirati zlonamjerni izlazni čvor.

Ovim metodama adresiraju se neki od zloupotreba koje vrše izlazni čvorovi i mogu se iskoristiti za modifikaciju postojećih statusa izlaznog čvora koji održavaju ovlašteni imenički poslužitelji. Status izlaznog čvora određuje se konsenzusom među odabranim Tor usmjernicima i objavljuje se s opisnicima. Statusi izlaznog čvora [48] su popisani u tablici 3.1.

Tablica 3.1. Statusi izlaznog čvora

Status	*Značenje*
Exit	ispravan izlazni čvor
BadExit	nikada ne koristiti kao izlazni čvor jer je zlonamjeran (mijenja sadržaj)
Invalid/Valid	ako je "invalid" onda se ne koristi osim ako je uključen parametar `AllowInvalidNodes` (inače su dozvoljeni kao srednji čvorovi i za skrivene usluge)
Reject	izlazni čvor izbačen iz konsenzusa

3.1.2. Zlonamjerni klijenti

Ispravno podešeni, izlazni Tor čvorovi ne snimaju promet. Štoviše, lišenost zakonske odgovornosti zasniva se na nepoznavanju prometa koji potječe od mreže Tor [49]. Electronic Frontier Foundation uvjerava potencijalne Tor izlazne čvorove da nisu odgovorni za promet koji izlazi iz mreže Tor. S druge strane, pružatelji usluge Interneta ne razlikuju promet koji prosljeđuje izlazni čvor od prometa koji sâm stvara, pa često na adresu izlaznog čvora šalju prijave za zloupotrebu (engl. abuse), prijave za povredu autorskog prava i slično. Ista ta anonimnost koja se želi osigurati kod klijenata brani administratorima da pravilno adresiraju prijave i sankcioniraju prijestupnike, kako to inače čine.

Takav je bio slučaj i s izlaznim čvorom s otvorenom izlaznom politikom koji je postavljen na Fakultetu, kada je Carnet poslao upozorenje zbog generiranja neželjene pošte (engl. junk mail) [50]. Za daljnju analizu izlaznog prometa iskorištena je Honeynet [51] mrežna topologija i HoneyWall kao alat za prikupljanje i analizu mrežnog prometa. Postavljen na takav način, HoneyWall zapravo štiti Internet od prometa koji dolazi iz izlaznog čvora, što je princip reverznog vatrozida. Na žalost, HoneyWall je sustav za detekciju napada (engl. intrusion detection system, IDS) pokretan snortom i kao takav ne pruža aktivnu zaštitu već samo okidanje pravila prema karakterističnom potpisu napada (engl. signature).

Nekim pružateljima usluga, kao što je Wikipedia, zlonamjerni anonimni korisnici ponekad ne ostavljaju drugog izbora nego da blokiraju cijelu mrežu Tor, odnosno pristup Wikipediji s adresa javno popisanih izlaznih čvorova, što je iznimno nepovoljno za sve poštene korisnike. Izlazni čvorovi mogu utjecati na vrstu prometa restrikcijom pristupa, kao dijelu izlazne politike. Pretpostavljena izlazna politika, primjerice, blokira SMTP, to jest pristup 25. Tor prenosi samo ispravne TCP tôkove, za razliku od mnogih neispravnih IP paketa koje koriste razni alati za napade i snifanje, tako da je smanjena količina mogućih napada [41]. Ustanovljena raspodjela prometa pokazuje ipak kako je blokiranje pristupa relativno jednostavno zaobići, budući da neki protokoli mogu koristiti nestandardne pristupe [44].

Bez obzira na izlaznu politiku, izlazni čvor može za detekciju zloupotrebe koristiti IDS koji, primjerice, može prepoznati zlonamjeran HTTP promet prema karakterističnom potpisu. Za blokiranje neželjene pošte koja napušta mrežu Tor, može koristiti programe za filtriranje, poput SpamAssasina.

Iskorištavanje anonimnosti za zloupotrebu s klijentske strane demotivira čvorove da propuštaju izlazni promet. Čvorovi koji se odluče propuštati izlazni promet riskiraju isključenje od svog pružatelja Internet usluga. To direktno utječe na sigurnost mreže Tor jer njena opstojnost ovisi o volonterima koji su spremni dati svoje resurse na raspolaganje.

3.2. Postojeća rješenja motiviranja

Neka od postojećih sustava motiviranja su sustav Nymble, objašnjen u poglavlju 3.2.1, ugradnja motivacija u Tor pomoću prioriteta prometa, objašnjena u poglavlju 3.2.2 i plaćanje za anonimno usmjeravanje, objašnjeno u poglavlju 3.2.3.

3.2.1. Sustav Nymble

Sustav Nymble [52] omogućava pružateljima usluga, primjerice Web poslužiteljima, sprječavanje zlonamjernih anonimnih korisnika bez blokiranja cijele mreže. Sustav sačinjavaju dva nezavisna poslužitelja: Pseudonym Manager i Nymble Manager (slika 3.2). Tor klijent se registrira na Pseudonym Manager poslužitelj (1), ne koristeći mrežu Tor, i dobiva pseudonim koji je vezan za neki njegov resurs, na primjer IP adresu. Vezivanjem resursa i pseudonima se rješava problem višestrukog uzimanja pseudonima, takozvani Sybil napad. Klijent se potom spaja na Nymble Manager poslužitelj koristeći mrežu Tor, predočava pseudonim i zahtjev spajanja na određeni poslužitelj (2). Vremensko razdoblje određuje vrijeme u kojem je moguće blokirati klijenta ako bude zlonamjeran. Nymble Manager poslužitelj na temelju pseudonima i zahtjeva spajanja na poslužitelj stvara ključ za povezivanje (engl. linking tokens), a klijentu šalje privremeni identifikator – *nymble*. Klijent predočava *nymble* ciljnom poslužitelju (3). *Nymble* je vremenski ograničen, stoga će klijent pri sljedećem spajanju na poslužitelj zatražit drugi *nymble* i tako ostati anoniman. Počini li klijent neki prijestup, poslužitelj predočava klijentski *nymble* Nymble Manageru (4) i dobiva ključ za povezivanje s kojim može prepoznati i blokirati svako sljedeće spajanje klijenta unutar definiranog vremenskog razdoblja (engl. linkabiliy window).

Slika 3.2. Sustav Nymble se sastoji od Pseudonym Managera i Nymble Managera

Do tog trenutka svako prethodno spajanje klijenta unutar tog vremenskog razdoblja za poslužitelja ostaje anonimno, a to vrijedi i za novo vremensko razdoblje jer predstavlja novu šansu.

Ovu ideju je teško implementirati jer zahtijeva promjene na pružateljima usluga za komunikaciju s Nymble Managerima, a i voljnost klijenata da prihvate sustav Nymble kako bi došli do sadržaja.

Reputacijski sustav predložen u ovom radu rješava upravo opisane implementacijske probleme. Klijenti su voljni prihvatiti reputacijski sustav jer dobivaju bolju kvalitetu usluge, a ne uključuje dodatne entitete u sustav.

3.2.2. Ugradnja motivacija u Tor pomoću prioriteta prometa

Broj korisnika mreže Tor raste, a istovremeno se pojavljuje više faktora koji odvraćaju korisnike od postavljanja izlaznih čvorova što loše utječe na ukupne performanse mreže. Neki od načina kako doskočiti ovom problemu su:

1. stvaranje zajednice
2. olakšavanje pokretanja usmjernika
3. pružanje bolje kvalitete usluge volonterima koji se odluče biti usmjernici

Tor se koncentrirao na prva dva pristupa zbog pretpostavke kako praćenje performansi čvorova narušava anonimnost. Tor klijenti ne mogu izvještavati o svojim iskustvima jer bi time indirektno otkrivali krugove koje su koristili. Usmjernici također ne mogu izvještavati jer bi mogli strateški lagati o svojim iskustvima [53] ili otkrivati informacije o klijentima koje narušavaju njihovu anonimnost. Korištenje "rekla-kazala" informacija bez mogućnosti provjere je otvaranje puta za prevare, primjerice Sybil napad. U predloženom rješenju, mjerenja provode čvorovi od povjerenja i potom ih objavljuju.

Ugradnja motivacija u Tor pomoću prioriteta prometa je rješenje u kojem centralni Tor imenički poslužitelji mjere performanse svakog OR-a i sastavljaju listu reputacija [54]. OR-ovi ažuriraju liste reputacija prilikom redovnih ažuriranja. OR-ovi s dobrom reputacijom se nagrađuju tako da njihov promet dobiva prioritet kroz cijeli krug. Ugradnjom motivacija privlače se novi usmjernici jer bi njihov promet trebao dobiti veći prioritet. Međutim, saznanje o tome čiji promet putuje mrežom treba ostati tajan kako bi mreža mogla pružati uslugu očuvanja anonimnosti. Problem se rješava označivanjem visokog prioriteta sa "zlatnom zvjezdicom". Prioritet ne bi trebali označavati usmjernici zbog opasnosti da svoj promet uvijek označe visokim prioritetom, već imenički poslužitelji. Usmjernici daju prioritet onom prometu koji potječe od usmjernika koji ima "zlatnu zvjezdicu". Mjerenje latencije i propusnosti imenički poslužitelji mogu provoditi bez otkrivanja identiteta, koristeći sâmu mrežu Tor. Pristup je već iskorišten u [55], [56] i [57]. Alternativno, svaki usmjernik prenosi svoja zapažanja imeničkom poslužitelju koji izračunava medijan [58]. U simulaciji [54] je modelirano pet vrsta usmjernika:

- *Usmjernici koji surađuju*: pružaju maksimalnu propusnost (500 KB/s) i daju prioritet prometu sa "zlatnom zvjezdicom"
- *Sebični*: ne prenose promet, već koriste punu propusnost mreže Tor za sebe
- *Spori usmjernici koji surađuju*: slično kao usmjernici koji surađuju, samo pružaju 50 KB/s
- *Usmjernici koji umjereno surađuju*: imaju propusnost kao usmjernici koji surađuju (500 KB/s), ali prenose promet propusnošću od 50 KB/s, čuvajući ostatak propusnosti za sebe

- *Prilagodljivi*: ovi čvorovi će surađivati dok ne dobiju "zlatnu zvjezdicu". Nakon toga će biti sebični dok ne izgube "zlatnu zvjezdicu".

Eksperimenti pokazuju da sustav korektno prepoznaje korisnike s traženim svojstvima i prikladno ih nagrađuje. Poboljšanja u performansama su pogotovo očita u trenucima kada je mreža zagušena, kao što je trenutno slučaj u stvarnoj mreži [59]. Ovaj način rješavanja zagušenosti mreže Tor podrazumijeva određene prijetnje za anonimnost. Kada je broj korisnika sa "zlatnom zvjezdicom" još malen, svaki put kada čvor dobije ćeliju sa "zlatnom zvjezdicom", zna s apsolutnom pouzdanošću da je promet došao od nekog od usmjernika iz anonimnog skupa usmjernika sa "zlatnom zvjezdicom". Time je uvelike smanjen anonimni skup, a potraga za pošiljateljem olakšana (napad presjekom). Ipak, sustav motiviranja treba privući sve više korisnika, prvo onih kojima su važnije performanse od anonimnosti, a zatim i svih ostalih. Autori vjeruju da je određeni kompromis anonimnosti i performansi vrijedan ukupnog cilja: poboljšanja usluge i privlačenja novih korisnika.

3.2.3. Plaćanje za anonimno usmjeravanje

U PAR (engl. Payment for Anonymous Routing) shemi [60] korisnici se motiviraju na suradnju na bazi njihovog osobnog ekonomskog interesa. PAR je hibrid dva postojeća principa plaćanja:

- plaćanje vezano za identitet na temelju sheme mikroplaćanja [61]
- anonimno plaćanje na temelju sheme elektroničkog novca bazirane na slijepom potpisu [62]

Plaćanje vezano za identitet sadrži uplatu potpisanu od strane uplatitelja, kao u shemi mikroplaćanja (engl. micropayment). Primijenjeno na mrežu Tor, čvor koji plaća se drži odgovornim za to plaćanje. Čvor koji plaća mijenja stvarni novac (monetu) za mikronovac u entitetu zvanom Banka, a čvor kojemu se plaća može u Banci zamijeniti mikronovac za monetu. Banka, dakle, sakuplja podatke o svim transakcijama mikroplaćanja u mreži, te na taj može narušiti anonimnost svakog čvora koji plaća na ovaj način. Zbog toga se ovaj princip plaćanja koristi kad anonimnost ne može biti narušena, primjerice kad jedan Tor čvor plaća svom susjedu.

Anonimno plaćanje ne sadrži nikakve informacije o identitetu. Chaumov digitalni novac [63] je primjer ove kategorije. Korisnik povlači digitalni novac iz Banke i može ga potrošiti bez otkrivanja svog identiteta. Bez identiteta nema odgovornosti, pa korisnik može pokušati više puta potrošiti novac (engl. double spending). Kod Banke je moguće provjeriti je li novac više puta "potrošen" i, kod neanonimnih mreža, objaviti identitet varalice. Kod anonimnih mreža to se, naravno, ne može primijeniti.

U PAR shemi svaki Tor čvor plaća svog sljedbenika za prosljeđivanje poruka po nalogu pošiljatelja. Čvor enkapsulira plaćanje u poruke koje prosljeđuje. Pošiljatelj u slojnoj poruci obavještava svaki čvor na putu o predviđenom plaćanju koji se može usporediti s ostvarenim plaćanjem. Plaćanje se ostvaruje korištenjem potpisanog mikronovca i anonimnog novca.

Potpisani mikronovac (engl. S-coin, ili kraće SC) je oblika:

$$SC_{T_i \to T_j} = sig_{T_i}\{MC, H(r), T_j\} \quad (3.1)$$

Potpisani mikronovac je potpisan od čvora *Ti* koji ga stvara i potpisuje, a sadrži identitet onoga komu se plaća (*Tj*). Nasumični broj *r* (račun) je identifikator SC-a i vezan je za SC njegovim sažetkom *H(r)*. Sažetak čini mikronovac vjerodostojnim. Banka dozvoljava polaganje mikronovca tek uz predočenje odgovarajućeg računa *r* i sažetka *H(r)*. MC (engl. microcoin) je dio SC-a koji sadrži detalje transakcije, sa sekvencijalnim brojem za sprječavanje višestrukog trošenja i bez vremenskog biljega koji bi mogao narušiti anonimnost. MC je preuzet iz originalne sheme mikronovca [61].

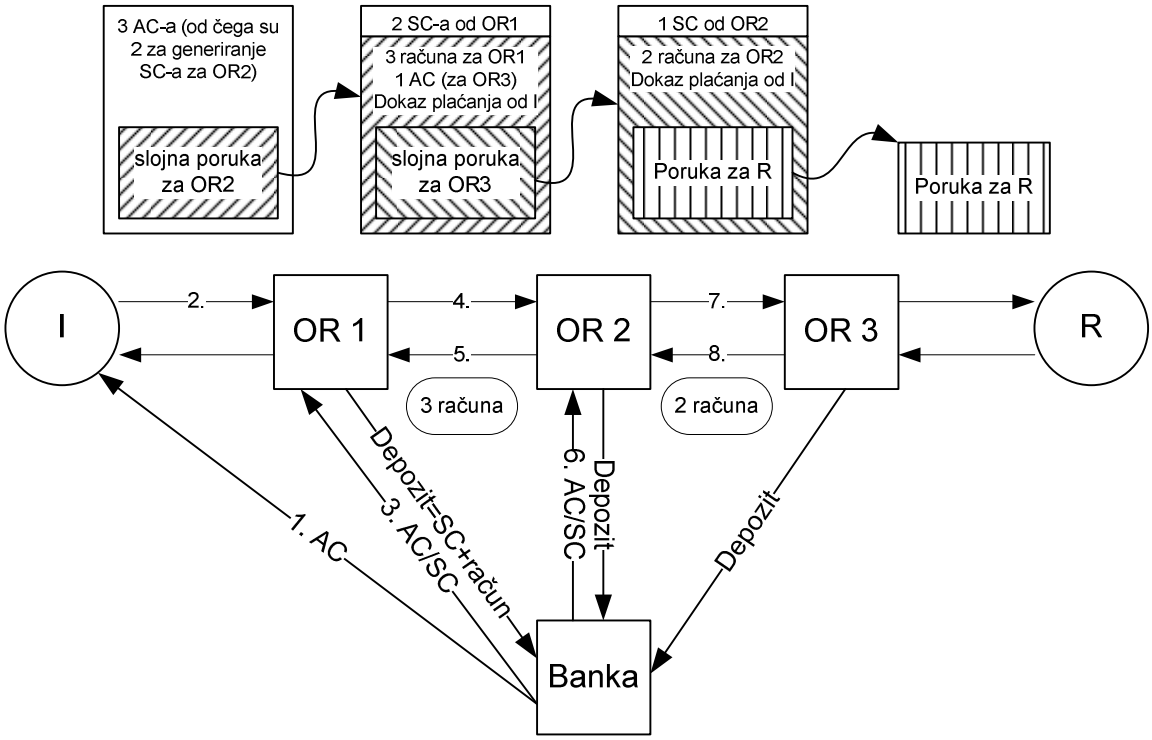
Anonimni novac (engl. A-coin, ili kraće AC) je oblika:

$$AC(r) = sig_B\{r\} \quad (3.2)$$

gdje je nasumični broj *r* (račun) identifikator AC-a koji generira korisnik, a $sig_B\{r\}$ je slijepo potpisani *r* od strane Banke.

Na slici 3.3 je ilustrirana upotreba PAR protokola. Pošiljatelj *I* dobavlja od Banke anonimni novac (AC) za plaćanje prvom čvoru (1). Klijentu treba ukupno 3 AC-a da plati svim čvorovima u krugu pa šalje 3 AC-a prvom čvoru OR_1 (2), od čega je za OR_1 namijenjen 1 AC . Prvi čvor tada koristi SC ili AC (3) da plati sljedećem (4). Kako bi pošiljatelj osigurao uslugu koju je platio usmjerniku OR_1, u slojevito kriptiranoj ćeliji za OR_2 šalje i 3 računa *r* (4). OR_2 šalje račun usmjerniku OR_1 tek nakon što je od njega primio poruku, za što je plaćen. OR_2 dobiva i dokaz plaćanja kojim pošiljatelj obvezuje OR_1 da izvrši mikroplaćanje prema OR_2. Ne bude li plaćen, OR_2 ima dokaz da je trebao biti. OR_2 šalje prema OR_1 3 računa (5) s kojima OR_1 može položiti mikronovac u Banku. OR_2 šalje 1 SC, 2 računa i dokaz plaćanja usmjerniku OR_3 (7) i dobiva 2 računa kao dokaz obavljene transakcije (8).

Autori tvrde da korištenjem predložene sheme nisu uvedene nove sigurnosne slabosti u postojeći sustav.



Slika 3.3. PAR protokol: za svaku poruku pošiljatelj plaća svim čvorovima u krugu prilažući AC i SC, dokaze plaćanja te račune u slojevito kriptirane poruke

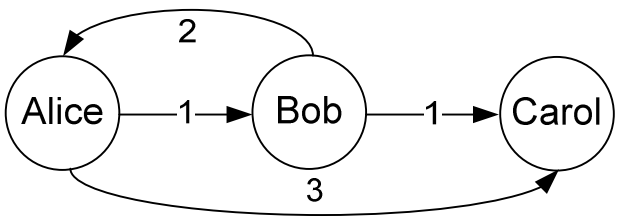
4. Povjerenje i reputacija

U stvarnom svijetu dajemo povjerenje poznanicima ili ustanovama na temelju iskustva s njima i očekujemo da izvrše zadatke koje smo im povjerili. Bez iskustva s nekim, nije racionalno imati očekivanja, pa rizik odnosa s osobom procjenjujemo na temelju glasina i potom donosimo odluku. Širenjem glasina o subjektu o njemu se stječe apstraktna generalna slika *povjerenja*, odnosno on gradi određenu *reputaciju*. Naglim porastom i razvojem elektroničkog trgovanja i P2P mreža, nastaje potreba za povjerenjem i u digitalnom obliku. Upravo su povjerenje i reputacijski sustavi prepoznati kao ključni faktori u uspješnom usvajanju elektroničke trgovine [64]. Najuspješniji i najpoznatiji primjeri uključuju eBay i Amazon.

P2P mreža se sastoji od partnera, ravnopravnih članova mreže, koji se najčešće međusobno ne poznaju i za koje postoji mala šansa ponovljenog susreta. Budući da članovi P2P mreže imaju jednaka prava i odgovornosti te ih ne kontrolira jedinstveni centralizirani entitet, ništa ih ne sprječava da iskorištavaju svoju ravnopravnu poziciju i izbjegavaju odgovornosti. Također, članovi mogu pronaći način kako iskoristiti dobru volju drugih članova i njihove resurse. Takvi sebični članovi zauzvrat daju malo ili ništa. Počne li količina nepoželjnog ponašanja utjecati na prosječnu kvalitetu usluge, cijeli koncept P2P usluge je u opasnosti zbog napuštanja dobronamjernih korisnika. Sustavi bazirani na reputacijama u P2P mrežama pomažu uspostavi povjerenja među članovima zajednice. Reputacijski sustavi mogu utjecati na prosječnog korisnika kako bi osim korištenja resursa zajednice ipak pridonio dio resursa. Partneri u P2P zajednici prije interakcije s drugim partnerima procjenjuju njihovu vjerodostojnost, odnosno količinu povjerenja koju zaslužuju [65]. Bez prijašnjeg znanja jednih o drugima, oslanjaju se na povratne informacije partnera koji posjeduju znanja i iskustva o drugima. Motiviranjem i sankcioniranjem može se smanjiti količina varanja ili nekog drugog ponašanja koje nije u interesu šire zajednice. Naravno, reputacijski sustav ne može u potpunosti iskorijeniti zlonamjerno ponašanje, već ga dovesti na neku ograničenu razinu.

Lik Mui definira *povjerenje* kao subjektivno očekivanje koje entitet ima o tuđem budućem ponašanju na temelju povijesti njihovih susreta [66]. Definirano na drugi način: *reputacija* entiteta *A* je prosječno povjerenje svih drugih entiteta prema *A* [67]. Iz toga je vidljivo da reputacija ima globalni aspekt, dok se na povjerenje gleda iz lokalnog i subjektivnog kuta. Povjerenje entiteta A prema entitetu B u određenoj kategoriji se utvrđuje iskustvom s tim entitetom u toj kategoriji.

Tranzitivno povjerenje podrazumijeva povjerenje u entitet s kojim postoji indirektna veza. Primjerice, Alice ima povjerenje u Boba, a Bob u Carol (1). Bob preporuča Carol s obzirom na svoje iskustvo (2), a Alice može izračunati mjeru povjerenja u Carol (3) kombinirajući povjerenje u Boba i informaciju koju je od njega dobila.



Slika 4.1. Tranzitivno povjerenje. Alice vjeruje Bobu, Bob vjeruje Carol, znači da i Alice vjeruje Carol

Reputacijski sustavi su klasificirani po različitim kriterijima u poglavlju 4.1, a poglavlje 4.2 sadrži pregled P2P reputacijskih sustava. U poglavlju 4.3 se opisuju napadi na reputacijske sustave.

4.1. Klasifikacijske dimenzije

Sabater i Sierra predlažu klasifikaciju reputacijskih sustava na temelju konceptualnog modela, izvora informacija, područja vidljivosti, konteksta, pretpostavkama o ponašanju entiteta, vrsti izmijenjenih informacija i vjerodostojnosti reputacije [64].

Prema konceptualnom modelu, reputacijski sustavi mogu biti bazirani na kognitivnom pristupu i teoriji igara. Modeli bazirani na *kognitivnom pristupu* pretpostavljaju da su povjerenje i reputacija sačinjeni od uvjerenja i funkcija su stupnja tih uvjerenja [68]. Povjerenje u drugog agenta i reputaciju proizvod su razmišljanja i emocija, odnosno mentalnih procesa. Na temelju *teorije igara*, povjerenje i reputacija su subjektivne procjene prema kojima entitet A očekuje da entitet B učini neku akciju za vlastito dobro [69]. Povjerenje i reputacija nisu rezultat mentalnih stanja agenta u kognitivnom smislu, već više pragmatična igra s funkcijom korisnosti i numeričkom agregacijom prošlih iskustava.

Izvori informacija koje se koriste za izračun povjerenja i reputacije mogu biti: direktno opažanje, informacije svjedoka, sociološke informacije i predrasude. Direktno opažanje i informacije svjedoka su "tradicionalni" izvori informacija kojima se odnedavna pridružuju i neki modeli koji se oslanjaju na sociološke aspekte ponašanja agenata. Vrsta informacija dostupna agentima ovisi o senzornim mogućnostima. Korištenje različitih izvora informacija, ako su uzeti u obzir na odgovarajući način, može uvelike povećati vjerodostojnost izračunatih vrijednosti povjerenja i reputacija, ali istovremeno povećavaju kompleksnost modela. *Direktno opažanje* je daleko najvažnija i najvjerodostojnija informacija za model povjerenja i reputacije. Postoji dva načina direktnog opažanja: opažanje partnera iz direktne međusobne interakcije ili opažanje drugih sudionika i njihove interakcije. Drugi način nije čest jer su rijetki slučajevi kada je to moguće ostvariti. Nedostatak ovog pristupa očituje se kod novih korisnika jer je njihovo znanje o okolini nikakvo i treba proteći neko vrijeme dok direktnim zapažanjem ne sakupe dovoljno iskustva za održavanje stabilnih performansi [70]. Za to vrijeme je novi korisnik izložen riziku loših iskustava s nepoznatim članovima sustava. *Informacije svjedoka*, ili indirektne informacije (trač), dolaze od drugih članova zajednice. Te informacije mogu opet biti prikupljene od trećih članova ili proizlaze iz direktnih opažanja. Jasno je da su najčešće ove informacije najobilnije, ali nisu tako jednostavne za korištenje jer je nejasno koliko su vjerodostojne. Postoje članovi zajednice koji se žele okoristiti ili namjerno napakostiti drugim članovima izdajući krive informacije o njima. Problematično je i nalaženje informacija o traženim članovima, a to je u nekim modelima riješeno centralnim prikupljanjem i pohranom svih informacija svjedoka ili implementiranjem procesa traženja svjedoka [70]. U pozadini *sociooloških informacija* leži sociološki odnos entiteta i uloge koju igra u društvu. U stvarnom svijetu, osobe zauzimaju različite uloge u odnosima u društvu. Osoba će nerijetko imati različite uloge u tom društvu i s obzirom na ulogu koju igra, njezino će se ponašanje mijenjati. Ovakvu vrstu znanja koristi vrlo malo modela, ali se pretpostavlja da će povećanjem kompleksnosti sustava jačati njihov značaj. *Predrasuda* je dodjeljivanje svojstava, u ovom slučaju reputacije, entitetu na temelju obilježja koji ga povezuju s određenom grupom. Ovakav mehanizam nema svoju klasičnu negativnu asocijaciju kao u stvarnom svijetu jer se ne temelji na rasnim i drugim obilježjima neke sociološke grupe.

Prema području vidljivosti reputacije mogu biti vidljive globalno i lokalno. *Globalno vidljive* reputacije su javno dostupne svim članovima, a izračunate su na temelju mišljenja onih koji su

imali interakciju s članom čija se reputacija računa. To pretpostavlja centralizirani entitet koji prikuplja i agregira pojedina mišljenja. Povjerenje i reputacija kao globalna svojstva česta su u *online* reputacijskim mehanizmima koji su zamišljeni za scenarije s tisućama ili milijunima korisnika. Zbog male vjerojatnosti ponovnog susretanja, članovi nemaju motivaciju graditi dugoročne dobre odnose s drugim članovima. Glavni nedostatak globalne reputacije je lišenost odražavanja osobnog stava o tome što je *loše* ili *dobro*. Postoji li konsenzus u zajednici o tome što je loše, a što dobro, ovaj pristup je primjenjiv. *Lokalno vidljive* reputacije subjektivno ocjenjuje svaki član za sebe na temelju iskustva s drugim članovima. Član može prikupljati informacije članova o drugim članovima, ali uzimajući u obzir vlastitu procjenu vjerodostojnosti tih podataka. U ovom slučaju ne možemo govoriti o općoj vrijednosti reputacije entiteta x, već o reputaciji koju entitet y ima o entitetu x. Ovaj model se češće primjenjuje u malim i srednje velikim zajednicama gdje postoji veća vjerojatnost od ponovnog susreta članova te samim time i uspostave dugotrajnog povjerenja.

U stvarnom svijetu, povjerenje ovisi o kontekstu. Ekspertiza pojedinca u određenom području daje mu vjerodostojnost unutar tog područja, ali ne nužno i na nekom drugom području. Međutim, dodavanjem više kontekstnih okvira reputacijama pojačava njihovu kompleksnost. U *modelu s jednostrukim kontekstom* svakom partneru dodjeljuje se jednostruka vrijednost povjerenja/reputacije bez obzira na kontekst. U *modelu s višestrukim kontekstom* partneru se pristupa ocjenjivanju u različitim kontekstima što proizvodi različite vrijednosti povjerenja/reputacije za svaki kontekst.

Ako je to moguće, neki će si entiteti nekorektnim ponašanjem (laganjem, varanjem, iskorištavanjem) priskrbiti nezasluženu korist ili će iz raznih motiva pokušati voditi negativnu kampanju prema odabranoj žrtvi. Različiti modeli rješavaju taj problem na različite načine:

- Varanje se ne uzima u obzir. Većina poštenih entiteta anulira potencijalne učinke neistinitih ocjena koje pružaju zlonamjerni entiteti.
- Model pretpostavlja da entiteti skrivaju informacije ili ih oblikuju prema svojoj predrasudi, ali nikada ne lažu.
- Model ima specifične mehanizme za obranu od laži.

S obzirom na vrstu informacija koje entiteti sakupljaju od svjedoka, postoje dvije grupe informacija: logička (engl. boolean) i realna vrijednost. *Logičke vrijednosti* najčešće koriste modeli koji računaju vjerojatnosti, a realne vrijednosti koriste modeli s agregacijskim mehanizmima.

Ponekad je uz vrijednost povjerenja i reputacije jednako važno znati kolika je ta informacija vjerodostojna. Najčešće se radi o još jednoj vrijednosti koja ide uz vrijednost povjerenja/reputacije. Modeli koji računaju vjerodostojnost, različito pristupaju izboru elemenata koji ulaze u izračun. Na primjer, mogu se uzeti u obzir: starost informacije, vjerodostojnost svjedoka (koliko je prije lagao ili govorio istinu), broj ostvarenih iskustava s entitetom.

4.2. Postojeći reputacijski sustavi u P2P mrežama

Problem zaobilaženja odgovornosti, besplatno iskorištavanje (engl. freeriding) i postavljanje zlonamjernog sadržaja u mrežu su boljke svih P2P mreža. Skupljanjem reputacija o partnerima, odnosno gradnjom povjerenja može se interakciju sa zlonamjernim partnerima svesti na minimum [71].

Preduvjeti za uspješan reputacijski sustav u P2P mrežama su:

- partner ima dugotrajni identitet
- mora postojati mogućnost stjecanja iskustava s partnerima i dijeljenje istih
- reputacijski sustav treba biti vjerodostojan, odnosno zadobiti povjerenje korisnika kako bi uopće funkcionirao

U većini P2P mreža ipak se koriste privremeni identiteti, odnosno, klijentima se pruža određena anonimnost. To rezultira gubitkom informacija o povijesti transakcija i utječe na slabu procjenu reputacije. Tomu se može doskočiti ako se izaberu slabe početne vrijednosti reputacije pa se klijentima isplati graditi reputaciju na dugotrajnom identitetu. Drugim riječima, neisplativo im je graditi reputaciju od početka. Time reputacijski sustav motivira klijente na korištenje dugotrajnih identiteta, a to je preduvjet za praktičnu primjenu reputacijskog sustava. Problem vjerodostojnosti reputacija je riješen na različite načine u različitim primjenama, ali princip je da količina istinitih povratnih vrijednosti mora nadmašiti količinu neistinitih. Vjerodostojan reputacijski sustav pomaže klijentima razlikovati "dobre" od "loših" partnera i bit će motivirani da sudjeluju. Što više korisnici sudjeluju, više korisnika daje svoje mišljenje o jednom partneru i povijest transakcija seže dulje u prošlost. Što je više različitih glasova o jednom partneru, teže je kovati zavjeru protiv sustava.

Još neki preduvjeti za dobar reputacijski sustav su [72]:

- *Visoka točnost*: izračunata vrijednost reputacije treba biti što je bliže moguće realnoj razini povjerenja.
- *Brza konvergencija*: izračunata vrijednost se treba brzo prilagođavati promjenljivom ponašanju partnera
- *Mali dodatni trošak*: sistem ne bi trebao zahtijevati puno dodatnih računalnih resursa (engl. overhead)
- *Prilagodljivost na dinamiku partnera*: partneri dolaze i odlaze iz mreže cijelo vrijeme. Sustav bi trebao tome biti prilagođen, umjesto da se oslanja na stalni skup partnera.
- *Otpornost na zlonamjerne partnere*: sustav bi trebao odoljeti različitim napadima individualnih partnera i grupe partnera.

Većina pouzdanih reputacijskih sustava danas zahtijeva centralno mjesto za skladištenje i računanje reputacija [73].

U nastavku teksta su opisani reputacijski sustavi Eigentrust, Powertrust, TrustMe, DCRC i CORC, Sporas, Histos i Beta reputacijski sustav.

Eigentrust [74] je raspodijeljeni reputacijski sustav u kojem je svakom partneru *i* dodijeljena jedinstvena globalna vrijednost reputacije koja reflektira iskustva svih partnera s partnerom *i*. Ne postoji centralna politika, već ju korisnici sami određuju, odnosno stvaraju zajednički pojam *dobrog* i *lošeg*. Novopridošli korisnici počinju s minimalnom reputacijom što ih ne motivira na često mijenjanje pseudonima. Svaki korisnik *i* lokalno čuva vrijednost reputacije s_{ij} o partneru *j* s kojim je imao interakciju. Kad poželi saznati globalnu reputaciju o drugima, raspituje se kod partnera o kojima ima dobro mišljenje i stvara normaliziranu vrijednost povjerenja u intervalu [0,1]. Ako partner kojeg pita nema informaciju, on se dalje raspituje kod svojih partnera, i tako dalje.. Normalizirane vrijednosti povjerenja c_{ij} se pohranjuju u matricu iz koje se iščitava vektor povjerenja. Partner *h* može za svakog partnera *j* izračunati globalnu vrijednost povjerenja t_{hj}:

$$t_{hj} = \sum_{i=0}^{n} c_{ij} \cdot s_{hi} \quad (4.1)$$

Zapis t_{hj} predstavlja povjerenje koje partner *h* ima u partnera *j*, prema onome što je saznao od drugih.

Za dovoljno velik broj raspitivanja, vektor povjerenja počinje za svakog partnera *i* konvergirati u jedinstveni vektor, globalni vektor povjerenja $\vec{t}$. Elementi globalnog vektora povjerenja, t_j, kvantificiraju koliko sustav kao cjelina ima povjerenja u člana *j*. Ovakvo indirektno stvaranje mišljenja bazira se na ideji tranzitivnog povjerenja. Kako u početku svi partneri ne bi imali vrijednost povjerenja 0, jer izračun ne bi bio moguć, u početnom sustavu postoji inicijalni skup partnera od povjerenja. Vrijednosti reputacija se drže kod menadžera ocjena (engl. score manager) u raspodijeljenoj tablici sažetaka (engl. distributed hashtable, ili kraće DHT), često korištenoj u P2P mrežama.

Powertrust sustav [72] se oslanja na zakon o potencijama (engl. power law) koji kaže da će u sustavu, gdje puno entiteta može slobodno birati neku uslugu, manji dio entiteta dobiti neproporcionalno veliku količinu prometa (ili pozornosti ili dobitka), čak i ako nitko iz sustava aktivno ne promiče takav rezultat [75]. Za razliku od Eigentrusta, ne postoji predefinirani skup partnera od povjerenja, već se na temelju zakona o potencijama izabiru superčvorovi (engl. power nodes) za agregaciju globalnih vrijednosti i brzo dohvaćanje reputacija. Prekrivajuća mreža TON (Trust Overlay Network) sadrži vezu između svaka dva partnera koji su imali interakciju. Nakon interakcije se izdaje povratna informacija i drži na strani primatelja usluge. Dođe li do ponovljene interakcije, ocjena se ažurira. U TON-u svaki čvor drži lokalne reputacijske ocjene s_{ij} o svojim susjedima pomoću kojih se normalizacijom gradi globalna vrijednost reputacije:

$$r_{ij} = s_{ij} / \sum_{j} s_{ij} \quad (4.2)$$

Sačuvamo li ovo u matrici $R = (r_{ij})$, dobit ćemo matricu u kojoj su sve vrijednosti između 0 i 1, a zbroj svakog retka je 1. Sada možemo izračunati globalnu vrijednost reputacije v_i za svaki čvor *i* i sačuvati ih u normalizirani vektor reputacije $V = (v_i)$, $\sum_i v_i = 1$, prema rekurzivnoj formuli:

$$V_{(t+1)} = R^T \cdot V_{(t)} \quad (4.3)$$

dok nije $\left|V_{(t+1)} - V_{(t)}\right| < \varepsilon$, gdje je ε proizvoljno malena tolerancija greške.

TrustMe [76] je anonimni, decentralizirani reputacijski sustav. Reference partnera se drže kod drugih, nasumično odabranih, partnera. Anonimnost je osigurana, kako za onoga koji se raspituje, tako i za onoga koji čuva vrijednost reputacije. Uz to su osigurane sigurnost i pouzdanost, odnosno dostavljanje pravih vrijednosti i odgovornost onih koji dostavljaju krive vrijednosti.

Svaki partner ima nekoliko parova javno-privatnih ključeva. Reputacijske vrijednosti partnera, recimo partnera *B*, su nasumično dodijeljene nekom drugom partneru (engl. Trust-

Holding Agent, ili kraće THA), a za to nitko, pa ni partner *B*, ne zna. Želi li partner *A* saznati reputaciju partnera *B*, odašilje upit u mrežu. THA partner odgovara i dokazuje poznavanje reputacijske vrijednosti partnera *B* specijalnim ključem. Partner *A* ocjenjuje transakciju uz dokaz interakcije, a THA ažurira vrijednost reputacije partnera *B*. Sigurnost, pouzdanost i odgovornost se osiguravaju mehanizmima kriptografije javnog ključa.

Ako je korisniku važna anonimnost, može se poslužiti P5 [30] ili APFS [77] protokolima koji omogućuju anonimno pretraživanje i preuzimanje podataka u P2P mreži (APFS je također baziran na uslojenom usmjeravanju). Posljedice povećanja anonimnosti su otežana autentikacija i očuvanje sigurnosti, pa je jasno da postoji balansiranje između povjerenja, koje se oslanja na identitet, i anonimnosti.

DCRC (engl. debit-credit reputation computation) i *CORC* (engl. credit-only reputation computation) [78] su djelomično raspodijeljena rješenja koja uključuju entitet za računanje reputacija (engl. reputation computation agent, ili kraće RCA). DCRC shema ocjenjuje korisnike na temelju njihove *online* prisutnosti, sudjelovanju u protokolu traženja resursa u P2P mreži (engl. query-response protocol), preuzimanju (engl. download debit), slanju (engl. upload credit) i dijeljenju (engl. sharing credit). CORC shema ne ocjenjuje preuzimanje, već koristi vremensko zastarijevanje kako bi suzbio monotoni rast reputacije. U povremenoj komunikaciji s RCA-om, klijenti dobivaju potpisanu reputaciju od RCA na temelju predstavljenih dokaza o sudjelovanju u protokolu traženja resursa, preuzimanju, slanju i dijeljenju. Dobivena reputacija sprema se lokalno i služi za predstavljanje sustavu.

Sporas reputacijski sustav daje globalnu vrijednost reputacije asociranu na identitet korisnika [79]. Koristi se u slabo povezanim *online* zajednicama. Baziran je na sljedećim principima:

1. Novi korisnici počinju s minimalnom reputacijom.
2. Vrijednost reputacije nikada ne pada ispod razine novih korisnika.
3. Nakon svakog ocjenjivanja, vrijednost reputacije ažurira se na temelju povratne informacije.
4. Dva korisnika mogu se ocijeniti samo jednom. Dođe li do ponovne interakcije, sustav čuva recentniju ocjenu. Tako se sprječava umjetna inflacija u suradnji dvaju korisnika.
5. Korisnicima s vrlo visokom reputacijom se ocjena manje mijenja nakon svakog ažuriranja.

Svaki korisnik ima vrijednost reputacije koja se ažurira rekurzivnom formulom:

$$R_i = R_{i-1} + \frac{1}{\theta}\Phi(R_{i-1})R_i^{drugi}(W_i - E_i) \quad (4.4)$$

$$\Phi(R_{i-1}) = 1 - \frac{1}{1+e^{\frac{-(R_{i-1}-D)}{\sigma}}} \quad \text{i} \quad E_i = \frac{R_{i-1}}{D} \quad (4.5)$$

gdje je R_i vrijednost reputacije u *i*-toj iteraciji, $\Phi(R)$ funkcija prigušivanja, a ostale korištene varijable popisane su u tablici 4.1.

Tablica 4.1. Popis korištenih varijabli u formuli Sporas reputacijskog sustava

Varijabla	*Značenje*
θ	konstanta, *pamćenje* sustava (cijeli broj veći od 1). 1/θ je *brzina učenja* i određuje brzinu kojom se reputacija mijenja nakon svake ocjene.
W_i	predstavlja ocjenu koju daje drugi korisnik
R^{drugi}	vrijednost reputacije koju ima korisnik koji daje ocjenu
D	raspon vrijednosti reputacije
σ	faktor akceleracije funkcije prigušivanja Φ. Što je manja vrijednost σ, to je strmiji faktor prigušivanja Φ(R).

Histos reputacijski sustav se oslanja na postojeće veze od povjerenja i na tranzitivno povjerenje [79]. Namijenjen je dobro povezanim *online* zajednicama. Uparene ocjene u sustavu mogu se prikazati kao usmjereni graf, gdje čvorovi predstavljaju posljednju ocjenu, a smjer pokazuje na ocjenjenog korisnika. Postoji li neprekinuti put između dva korisnika, od *A* do A_L, možemo izračunati vrijednost reputacije koju *A* ima o A_L. Tako izračunata vrijednost reputacije uključuje vlastite stavove od *A*. U suprotnom, Histos se svodi na jednostavniji Sporas mehanizam.

Beta reputacijski sustav [80] se temelji na beta funkciji gustoće vjerojatnosti koja može poslužiti za prikaz vjerojatnosti distribucije binarnih događaja. Kombiniranje povratnih informacija i izražavanje ocjena reputacija time dobiva čvrstu matematičku osnovu. Ocjena reputacije u intervalu [-1,1] izvodi se formulom:

$$Rep(p_T^X, n_T^X) = \frac{p_T^X - n_T^X}{p_T^X + n_T^X + 2} \quad (4.6)$$

gdje su p_T^X i n_T^X ukupan broj pozitivnih i negativnih povratnih ocjena o entitetu *T* od entiteta (ili skupine entiteta) *X*.

Uzme li se u obzir da novije povratne informacije odražavaju stvarno ponašanje, model se može promijeniti tako da starije informacije imaju manju težinu nego novije. Efektivno, to znači opraštati (zaboravljati) stare povratne informacije. S obzirom na očekivanu brzinu promjena, namješta se faktor pamćenja.

Neka je od entiteta sakupljen niz *Q* n-torki $(p_{T,i}^Q, n_{T,i}^Q)$ indeksiranih s *i* o entitetu *T*. Sumiranjem n-torki dobiva se:

$$p_T^Q = \sum_{i=1}^{n} p_{T,i}^Q \text{ i } n_T^Q = \sum_{i=1}^{n} n_{T,i}^Q \quad (4.7)$$

Uvođenjem faktora pamćenja dobiva se:

$$p_{T,\lambda}^Q = \sum_{i=1}^{n} p_{T,i}^Q \lambda^{(n-i)} \text{ i } n_{T,\lambda}^Q = \sum_{i=1}^{n} n_{T,i}^Q \lambda^{(n-i)}, \text{ gdje je } 0 \leq \lambda \leq 1 \quad (4.8)$$

Kada je λ = 1, ništa se ne zaboravlja, a kada je λ = 0, uzima se u obzir samo posljednja informacija. Nedostatak računanja pomoću niza je nužnost pamćenja cijelog niza *Q* zauvijek.

S rekurzivnom formulom ažuriraju se parametri ($p_{T,\lambda}^{Q(i)}, n_{T,\lambda}^{Q(i)}$) svakom iteracijom, odnosno sa svakom novom povratnom informacijom:

$$p_{T,\lambda}^{Q(i)} = p_{T,\lambda}^{Q(i-1)}\lambda + p_{T,i}^{Q} \text{ i } n_{T,\lambda}^{Q(i)} = n_{T,\lambda}^{Q(i-1)}\lambda + n_{T,i}^{Q}, \text{ gdje je } 0 \leq \lambda \leq 1 \quad (4.9)$$

Parametri ($p_{T,\lambda}^{Q}, n_{T,\lambda}^{Q}$) koji rezultiraju nizom Q od n povratnih informacija, s faktorom pamćenja λ se mogu izraziti kao:

$$p_{T,\lambda}^{Q} = p_{T,\lambda}^{Q(n)} \text{ i } n_{T,\lambda}^{Q} = n_{T,\lambda}^{Q(n)}, \text{ gdje je } 0 \leq \lambda \leq 1 \quad (4.10)$$

Nakon svake transakcije, partner može istovremeno slati i pozitivne i negativne primjedbe, u obliku $p \geq 1$ i $n \geq 0$. Davanje ocjena u paru (p, n) reflektira ideju da partnerovo ponašanje u transakciji može biti djelomično zadovoljavajuće. Informacija p, $n = 0.5$ koja ima težinu 1, nije ista informaciji p, $n = 0$, koja, kao da povratna informacija nije ni poslana, nema težinu. Iznos $p + n$ može se smatrati težinom povratne informacije. Težina može biti proizvoljno velika, ali minimalno jednaka nuli. Normalizacijom težine, na način da $p + n = w$, možemo predstaviti povratnu informaciju kao jednu vrijednost. Skaliranjem se može omogućiti da vrijednost bude definirana na bilo kojem rasponu, primjerice [-100,+100] ili [-1,+1]. Uzmimo da je vrijednost v definirana na [-1,+1]. Tada se par (p,n) može dobiti kao funkcija od w i v:

$$p = w(1 + v)/2 \text{ i } n = w(1 - v)/2 \quad (4.11)$$

Pseudo Trust je model koji omogućuje autentikaciju i povjerenje bez otkrivanja stvarnog identiteta korisnika i bez centralnog autoriteta [81]. Za potrebe protokola, korisnik uz pomoć jednosmjerne funkcije sažetka generira provjerljivi pseudonim *PI* (engl. pseudo identity). *PI* se ne može falsificirati i nad njim se gradi reputacija. Za dokazivanje identiteta, korisnik objavljuje i javno dostupan certifikat pseudonima *PIC* (engl. pseudo identity certificate). Jednosmjernom funkcijom sažimanja, modificiranim SHA-1, na temelju dva velika prosta broja i pravog identiteta stvara se korisnikov slijed za stvaranje pseudonima. Iz PI-a se dalje stvara PIC. Korištene su zamisli dokazivanja bez poznavanja (engl. Zero-Knowledge Proof) kod kojeg jedna strana treba uvjeriti ispitivača da poznaje tajnu, bez otkrivanja ikakvih informacija o toj tajni za vrijeme dokazivanja. Dokazivanje bez poznavanja se zasniva na pretpostavci da je faktoriziranje velikih brojeva računalno nemoguće ili traje neprihvatljivo dugo. Protokol dokazivanja traje nekoliko krugova koji se sastoje od pitanja ispitivača i odgovora. Budući da jedino nositelj identiteta može dokazati svoj PI, PI se ne može ukrasti, niti se nad njim može provesti napad čovjeka u sredini.

4.3. Napadi na reputacijski sustav

Reputacijski sustavi, osim što uvode reda u sustav, i sami su podložni stjecanju krivih zaključaka uvođenjem lažnih ili nepotpunih informacija u sustav. Može biti riječ o nevoljkosti korisnika da pruže povratnu informaciju ili o namjernoj neistini. Često je vektor napada višestruk jer će napadač u suradnji s drugim entitetima, koji mogu biti pod njegovom kontrolom, lakše uvjeriti sustav u falsificiranu reputaciju. Cilj napada može biti građenje reputacije (engl. ballot stuffing) nekog od entiteta koji napadač zastupa ili "tračanje" (engl. bad-mouthing) koji ima za cilj srušiti nečiju reputaciju [82]. Varanje oko reputacija može biti

i financijski isplativo, primjerice u elektroničkoj transakciji, nakon što je prethodno napuhana zloupotrebljavajući sustav. Identiteti u P2P mrežama nisu vezani za stvarni identitet ili neko fizičko obilježje, pa ništa ne sprječava partnere da koriste višestruke identitete. Partner može jednostavno i brzo stvoriti veliki broj identiteta i multiplicirati šanse da kod raspodijele nekog resursa bude više puta nasumično izabran u ono što je trebao biti skup različitih korisnika. Iz te pozicije može izvršiti *Sybil napad* [83]. Iako postoje različiti pokušaji obrane i smanjivanja mogućnosti Sybil napada, Doucer tvrdi da bez centralnog entiteta od povjerenja (engl. trusted entity) ne postoji praktičan i uspješan način uvjerljivog dokazivanja jedinstvenosti identiteta u raspodijeljenoj mrežnoj okolini [83].

Korištene metode za pokušaj obrane [84] od Sybil napada su:

1. Testiranje resursa

   Cilj ove metode jest utvrditi posjeduju li identificirani entiteti manje resursa nego se to očekuje kod neovisnih entiteta. Testovi uključuju računalnu moć (CPU), mogućnost skladištenja, mrežnu propusnost i limitiranost IP adresa. Zahtjev za heterogenim IP adresama sprječava neke napade, ali ne sprječava korištenje *zombi* računala koja imaju nelimitirane IP adrese. Doucer je dokazao neefikasnost ove metode [83], ali mnogi je priznaju kao minimalnu obranu od Sybil napada. U ovu skupinu spada i SybilGuard [85] koji se oslanja na prirodu prijateljskih veza u grafu zajednice.

2. Ponavljajuće testiranje

   Varijacijom testiranja resursa, identiteti se ponavljano preispituju koristeći testiranje resursa. Ovaj pristup ograničava broj Sybil napadača količinom resursa koji mogu, ili su spremni, pružiti u određenom vremenu.

3. Uređaji od povjerenja

   Entiteti mogu biti vezani na siguran način sa specifičnim uređajem. Kao i s kriptografskim certifikatima, ništa ne sprječava napadača da prikupi više takvih uređaja, osim možda cijene.

S obzirom na Sybil napad, reputacijski sustavi se dijele na simetrične i nesimetrične [86]. U simetričnim reputacijskim sustavima reputacija nekog entiteta ovisi samo o topologiji grafa povjerenja i vrijednostima na vezama povjerenja, a ne o identitetu čvora. Napadač može koristeći Sybil napad kopirati postojeći graf koji predstavlja veze povjerenja, a reputacijski sustav ne može razabrati originalni sustav od kopije. U nesimetričnim sustavima postoje specifični čvorovi od povjerenja od kojih se prenose sve reputacijske vrijednosti ili svaki entitet za sebe izračunava povjerenje drugih entiteta. Budući da se Sybil čvorovi ne mogu predstavljati za čvorove od povjerenja, ne može se izgraditi kopija grafa kao u slučaju simetričnog sustava. Nesimetrični reputacijski sustavi prisiljavaju napadača da prije napada prvo izgradi povjerenje, što traje određeno vrijeme, pa su efektivni u povećanju cijene Sybil napada.

5. Reputacijski model u mreži TOR

Reputacijskim sustavom u mreži Tor želi se privući više korisnika i kazniti nepoželjno, zlonamjerno i po univerzalnim, apolitičnim normama neprihvatljivo ponašanje, kao što su dječja pornografija i izvršavanje napada. Povećanje broja korisnika i smanjena zloupotreba utječu na poboljšanje anonimnosti. Reputacija motivira usmjernike, kojima je anonimnost bitna, na pružanje usluge bolje kvalitete. Usmjernik će dobrom reputacijom privući puno korisnika za prekrivajući promet i povećati anonimni skup [87]. Direktno sankcioniranje korisnika koji zloupotrebljavaju mrežu uskraćivanjem usluge sustava nije moguće bez jedinstvenog i globalnog identifikatora korisnika na razini mreže, a to je suprotno ideji i implementaciji anonimnih sustava. S druge strane, indirektno sankcioniranje uvođenjem reputacija u anonimne sustave problematično je iz tri razloga [87]:

1. Korisnici mogu vrlo jednostavno preuzeti novi pseudonim, ako je za stari vezana loša reputacija jer je njihova lokacija uvijek skrivena
2. Teško je detektirati i provjeravati korisnikovo ponašanje i istovremeno čuvati njegovu anonimnost
3. Napadač može koristiti informacije o reputacijama kako bi narušio anonimnost korisnika

Postojeći raspodijeljeni P2P reputacijski sustavi nisu prikladni za primjenu u mreži Tor jer pri stvaranju globalne reputacije o članovima razmjenjuju podatke o istim. Razmjenjivanje i pretraživanje podataka o reputacijama među čvorovima mreže odaju informacije koje narušavaju anonimnost korisnika.

Inverz sankcioniranja *lošeg* ponašanja je nagrađivanje *dobrog* ponašanja i tako dolazimo do modela reputacijskog sustava koji korisniku omogućuje da prihvati nagradu za svoje *dobro* ponašanje. Korisnike se nagrađuje boljom kvalitetom usluge. Kvaliteta usluge se može zasnivati na propusnosti, ali je za većinu klijenata važnija niska latencija. Kompromis anonimnosti i performansi je inherentan i ovom sustavu, ali se polazi od pretpostavke da će loše performanse otjerati barem dio zlonamjernih korisnika. Korisnicima kojima je anonimnost bitna ionako više cijene svoju anonimnost od performansi. Ključno je omogućiti klijentu, ako on to zahtijeva, anonimnost koju mu pruža Tor sustav bez reputacija, odnosno zaustaviti istjecanje bilo kakvih informacija o njemu.

Tor je otvoren sustav; entiteti – usmjernici i klijenti slobodno ulaze i izlaze iz mreže, te vrijede sljedeće pretpostavke [70]:

1. velika je vjerojatnost da su entiteti sebični i ne izvrše uvijek ono što se od njih traži ili očekuje
2. niti jedan entitet ne može imati ukupan uvid u cijelu okolinu
3. centralni autoritet ne može kontrolirati sve entitete

Direktno opažanje (poglavlje 4.1) nije dobar izbor jer treba dulje vrijeme da korisnik uz interakciju s drugim čvorovima sakupi dovoljno relevantnih saznanja za vjerodostojnu i korisnu sliku stanja mreže. S druge strane, informacije svjedoka su podložne sebičnim interesima i ovise o volji entiteta da iste dijele s drugima. Zbog toga, predloženi model u ovom radu koristi *certificiranu reputaciju* [70], koju pošiljatelj sâm pruža drugima na uvid i čuva lokalno, a ne na nekom centralnom mjestu, primjerice na imeničkom poslužitelju. Imenički poslužitelj nije dobro mjesto za čuvanje reputacija iz sljedećih razloga:

1. Ovlašteni imenički poslužitelji su u postojećem Tor sustavu osjetljiva točka, odnosno moguće usko grlo i meta napada. Dodavanjem nove funkcije držanja reputacija svih klijenata stavio bi se dodatni naglasak na imeničke poslužitelje kao centralne točke ispada (engl. single point of failure).
2. Imenički poslužitelji vjerojatno nemaju računalnih resursa za čuvanje i računanje svih reputacija i izvođenje operacija kriptografije javnog ključa za tu svrhu. Promet prema i od imeničkih poslužitelja bi se znatno povećao i postojeća infrastruktura ne bi zadovoljavala. Infrastruktura u trenutnim uvjetima ne skalira dobro ni uz povećanje broja Tor usmjernika [36].
3. Tor se ionako zasniva na raspodijeljenom povjerenju pa promjena težišta na centralni autoritet vjerojatno ne bi prošla kod korisnika s visokim zahtjevima anonimnosti.

Kao što je rečeno u poglavlju 4.2, reputacija mora biti vezana uz dugotrajni identitet korisnika, a za to u mreži Tor može poslužiti samopotpisani certifikat. Certificiranu reputaciju pošiljatelj predaje ulaznom čvoru pri uspostavi kruga. Korisnici koji nemaju ili ne žele predati svoju reputaciju se tretiraju kao da imaju najnižu reputaciju, a samim time imaju i najlošiju kvalitetu usluge. Kada bi kretali s nekom srednjom reputacijom, korisnici bi imali motivaciju odbaciti identitet s lošom reputacijom i krenuti s novim. Usmjernici također imaju reputaciju, a ona se čuva zajedno s potpisanim opisnikom na imeničkom poslužitelju. Vrijednost reputacije se, prema tome, izračunava na dva načina:

1. Promet koji stvaraju pošiljatelji vide samo izlazni čvorovi te ga oni i ocjenjuju. Ocjena prometa se prenosi unazad do ulaznog čvora, a ulazni čvor, shodno ocjeni, prilagođava propusnost kruga. Na taj se način pošiljatelja nagrađuje ili kažnjava u realnom vremenu. Pri zatvaranju kruga pošiljatelj dobiva potpisanu certificiranu reputaciju.
2. Imenički poslužitelji u Tor opisnicima već sada objavljuju neke informacije o usmjernicima koji klijentima služe pri izboru kruga, kao što su: vrijeme rada čvora (engl. uptime), verzija Tora, deklarirana propusnost, statusi (Fast Server, Guard Server, Stable Server, Exit Server). Pouzdanost i stvarnu propusnost usmjernika, nasuprot deklariranim vrijednostima, imenički poslužitelji mogu provjeravati alatima kao što su Torflow [46] i Torscanner [47]. Algoritam za izbor čvorova kruga pokušava maksimizirati kvalitetu usluge i minimizirati vjerojatnost zloupotrebe na temelju reputacije usmjernika.

Klijent ulaznom čvoru predočava potpisanu reputaciju dobivenu od ulaznog čvora iz nekog prethodnog kruga. Za vrijeme trajanja kruga, izlazni čvor ocjenjuje promet i vraća ocjenu ulaznom čvoru koji lokalno ažurira reputaciju klijenta. Prije zatvaranja kruga, ulazni čvor šalje ažuriranu reputaciju imeničkom poslužitelju na potpisivanje i vraća potpisanu reputaciju klijentu. Jasno je da vrijednost reputacije ocijenjene od samo jednog ulaznog čvora neće biti toliko relevantna kao kad bi se čuvala cijela povijest, kao na primjer u modelu decentraliziranih lanaca preporuka [88]. Ali s točnošću raste i gubitak anonimnosti. Budući da klijenti čuvaju vlastite reputacije, očekuje se da će klijent odbaciti novu reputaciju ako je ona slabija od prethodne i nastaviti koristiti staru. Kako bi se doskočilo tom problemu, uvodi se vremenska eksponencijalna funkcija. Kako vrijeme prolazi, klijentska reputacija slabi pa klijent ima motivaciju prihvatiti novopotpisanu reputaciju. Međutim, vremensku funkciju treba optimizirati tako da se balansiraju dva suprotna učinka:

1. Tjeranje korisnika koji nisu često prijavljeni. Povremeni korisnici bili bi odvraćani od korištenja usluge mreže Tor jer bi svako sljedeće spajanje podrazumijevalo znatan gubitak vrijednosti reputacije, a samim time i performansi. Važnost povremenih korisnika je u šumu koji, kao korisnici s malim zahtjevima anonimnosti, stvaraju korisnicima s većim zahtjevima anonimnosti.

2. Klijent neko vrijeme gradi reputaciju i nakon toga koristi dobrobit dobre reputacije za zloupotrebu. Korisnik bi mogao naučiti kako vremenski tempirati zloupotrebu tijekom koje zadržava maksimalne performanse. Nakon toga ne treba prihvatiti reputaciju smanjenu zbog svog ponašanja, već se može zadovoljiti vrijednošću koju je oslabila vremenska funkcija.

Klijenti mogu promijeniti pseudonim, odnosno osigurati veću anonimnost uz zadržavanje vrijednosti reputacije. Imenički poslužitelj, koji u ovom modelu uživa potpuno povjerenje, potpisuje reputaciju uz novi identitet, a pamti sažetak starog identiteta koji postaje nevažeći. Posebno osjetljivi klijenti mogu time umanjiti mogućnost praćenja od zlonamjernih ulaznih čvorova. Kada klijent preda reputaciju, ulazni čvor provjerava ispravnost korištenog identiteta kod imeničkog poslužitelja.

Reputacijski sustav je opisan protokolom i politikom. Protokolom, odnosno mehanizmom, reputacijskog sustava se omogućuje razmjena informacija potrebnih za funkcioniranje sustava, a politikom se određuje na koji način se informacije koriste za svrhu reputacijskog sustava – sprečavanje zloupotrebe. Politikom se također odgovara na pokušaje zloupotrebe samog reputacijskog sustava. Protokol reputacijskog sustava je objašnjen u poglavlju 5.1, a politika u poglavlju 0. Ispitivanje djelovanja reputacijskog sustava opisano je scenarijima u poglavlju 5.3, a poglavlje 5.4 navodi moguće smjerove razvoja reputacijskog sustava.

5.1. Protokol reputacijskog sustava

Za potrebe reputacijskog protokola, upravljačke ćelije proširene su za dva tipa (tablica 5.1).

Tablica 5.1. Proširenje upravljačkih ćelija

Naredba	*Funkcija*
REP_RELAY_CERT	predaja certificirane reputacije
REP_RELAY_EXIT	prijenos ocjene od izlaznog prema ulaznom čvoru

Upravljačke ćelije namijenjene su onome tko ih prima, a to vrijedi i za `REP_RELAY_EXIT` ćeliju. Za razliku od ćelija za prijenos podataka, upravljačke ćelije se u čvorovima na putu do ulaznog čvora ne kriptiraju inkrementalno. To znači da sadržaj `REP_RELAY_EXIT` ćelije nije zaštićen od promjene. To se regulira ponderiranjem ocjene prometa reputacijom usmjernika koji tu ocjenu, odnosno ćeliju, prenosi.

Certificirana reputacija *CR* pošiljatelja *I* je oblika:

$$CR_I = \{r, t, CERT_I, CERT_S, sig_S\{r, t, CERT_I\}\}$$

Korištene oznake popisane su u tablici 5.2.

Tablica 5.2. Struktura certificirane reputacije

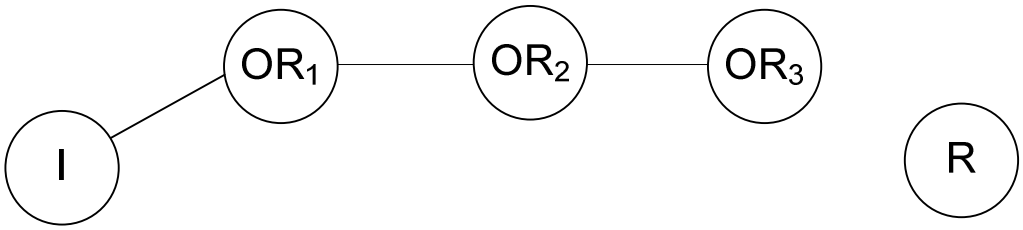
Varijabla	*Značenje*
r	vrijednost reputacije
t	vremenska oznaka (engl. timestamp) trenutka kada je reputacija potpisana
$CERT_I$	digitalni certifikat pošiljatelja *I*

$CERT_S$	digitalni certifikat potpisnika *S*
$sig_S\{m\}$	digitalni potpis poruke *m* privatnim ključem potpisnika *S*

Protokol izmjene i računanja reputacije odvija se u tri faze:

1. Predočavanje certificirane reputacije ulaznom čvoru
2. Slanje ocjene izlaznog prometa od izlaznog prema ulaznom čvoru
3. Potpisivanje nove reputacije klijenta i zatvaranje kruga

Protokol će biti objašnjen na primjeru kruga s tri usmjernika. Slika 5.1 prikazuje pošiljatelja *I* i krug s usmjernicima OR_1, OR_2, OR_3, gdje je OR_1 ulazni, a OR_3 izlazni čvor. *R* je primatelj, primjerice Web poslužitelj.

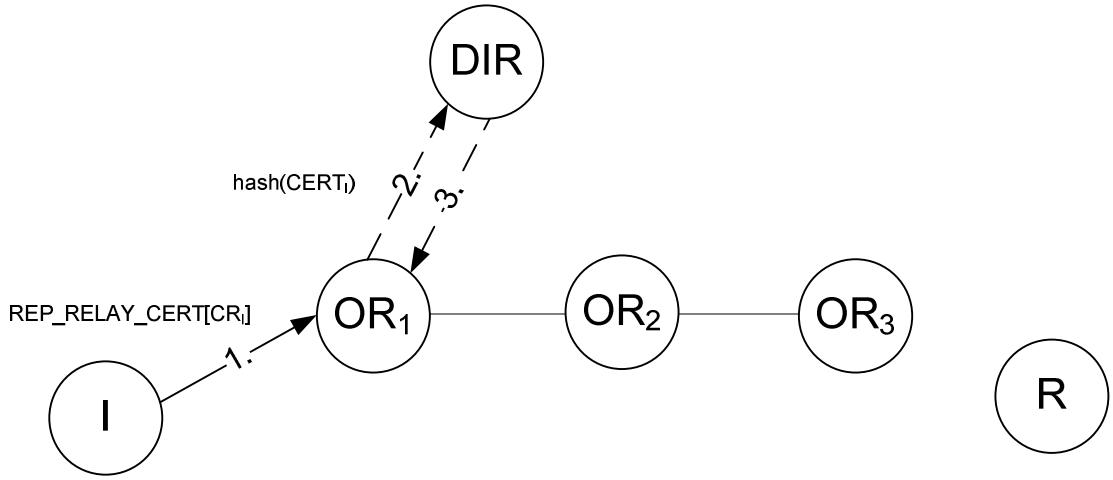


Slika 5.1. Pošiljatelj *I* i krug s usmjernicima OR_1, OR_2, OR_3

Odmah nakon faze izgradnje kruga slijede faze reputacijskog protokola:

1. Predočavanje certificirane reputacije ulaznom čvoru (slika 5.2)

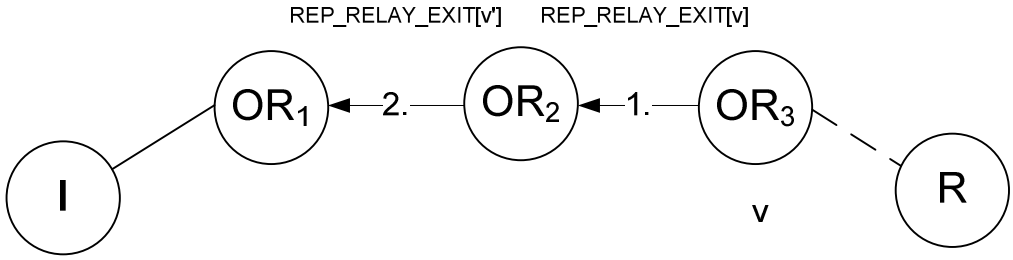
   Pošiljatelj predaje certificiranu reputaciju CR_1 ulaznom čvoru (1). Ulazni čvor provjerava ispravnost reputacije kod imeničkog poslužitelja tako da šalje sažetak certifikata vlasnika $h(CERT_1)$ certificirane reputacije (2). Imenički poslužitelj vraća odgovor (3).



Slika 5.2. Pošiljatelj predočuje svoju certificiranu reputaciju

2. Ocjena prometa na izlaznom čvoru i slanje ocjene prema ulaznom čvoru (slika 5.3)

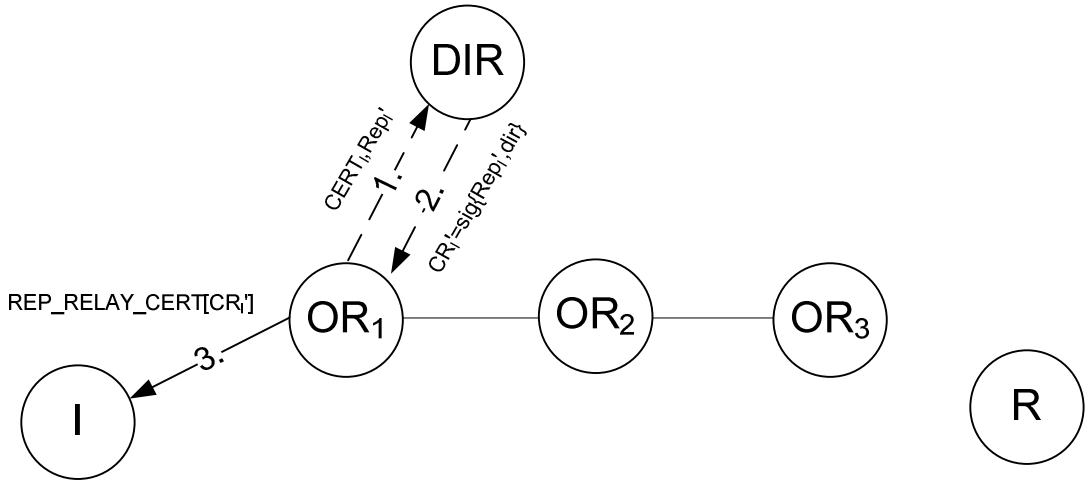
   Izlazni čvor (OR_3) šalje ocjenu prometa v u ćeliji `REP_RELAY_EXIT` (1). OR_3 ponderira ocjenu i prosljeđuje ćeliju ulaznom čvoru (2). Ova faza se odvija kroz čitavo vrijeme postojanja kruga.



Slika 5.3. Ocjena putuje prema ulaznom čvoru

3. Zatvaranje kruga i predaja nove reputacije pošiljatelja od ulaznog čvora (slika 5.4)

   Pošiljatelj šalje `DESTROY` ćeliju za zatvaranje kruga. Ulazni čvor šalje ažuriranu vrijednost reputacije Rep_I' i certifikat klijenta imeničkom poslužitelju (1). Imenički poslužitelj šalje nazad potpisanu reputaciju (2) koju ulazni čvor prosljeđuje pošiljatelju (3).



Slika 5.4. Pošiljatelj zatvara krug, imenički poslužitelj potpisuje novu reputaciju

5.2. Politika reputacijskog sustava

Politika reputacijskog sustava je objašnjenja kroz tri faze koje odgovaraju fazama protokola:

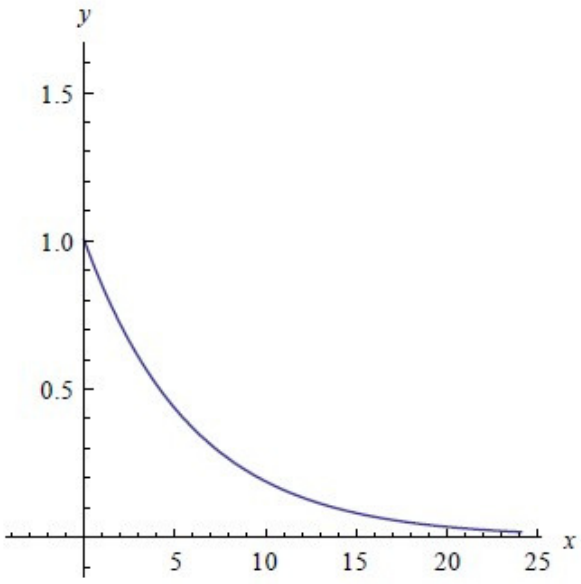
1. Dodjela prioriteta propusnosti u čvorovima kruga s obzirom na reputacije

   Ulazni čvor šalje sažetak certificirane reputacije imeničkom poslužitelju na provjeru (korak 2 na slici 5.2). Imenički poslužitelj dodaje sažetak certifikata listi trenutno korištenih certifikata i vraća broj (korak 3 na slici 5.2) u intervalu [0,1] koji je obrnuto proporcionalan broju krugova u kojem se trenutno taj certifikat koristi. Ako je klijent zamjenjivao identitet i predao ulaznom čvoru reputaciju s nekim od zamijenjenih identiteta, imenički poslužitelj će dojaviti neispravnost korištenog certifikata.

   Nakon toga, ulazni čvor ponderira vrijednost reputacije *r* koristeći vremensku eksponencijalnu funkciju (funkcija zastarijevanja):

$$\omega_{\mathrm{Re}}(CR_I) = \mathrm{e}^{-\frac{\Delta \mathrm{t}(CR_I)}{\lambda}} \qquad (5.1)$$

   gdje je $\Delta \mathrm{t}(\mathrm{CR_I})$ vremenska razlika sadašnjeg trenutka i trenutka potpisivanja reputacije *t*, a λ je faktor zastarijevanja kojim se skalira $\Delta \mathrm{t}(\mathrm{CR_I})$. Podešavanjem faktora zastarijevanja mogu se anulirati dva suprotna efekta – tjeranja povremenih korisnika i umjetnog građenja reputacije. Eksponencijalna funkcija za $\lambda = 6$ je prikazana na slici 5.5.



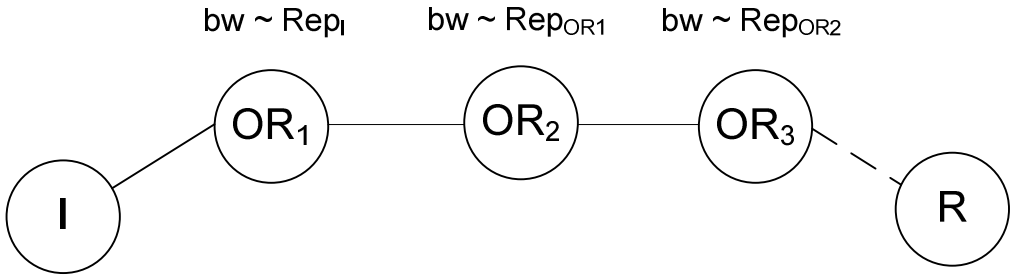
Slika 5.5. Funkcija zastarijevanja, $\lambda = 6$

   Graf pokazuje da reputacija stara 4 sata uz $\lambda = 6$ oslabi otprilike na pola svoje početne vrijednosti.

Ponderirana vrijednost reputacije je onda:

$$Rep_I = r \cdot \omega_{\mathrm{Re}}(CR_I) \quad (5.2)$$

Čvorovi kruga računaju propusnost koju pružaju krugu kao udio maksimalne propusnosti (slika 5.6). Udio propusnosti se računa s obzirom na reputaciju susjednih čvorova. Tako će OR_1 dati udio propusnosti krugu koji otvara pošiljatelj razmjeran reputaciji pošiljatelja s obzirom na reputacije eventualnih drugih čvorova prethodnika od OR_1. OR_2 i OR_3 daju krugovima propusnost razmjernu reputacijama OR_1, odnosno OR_2 s obzirom na reputacije eventualnih drugih čvorova prethodnika.



Slika 5.6. Dodijeljena propusnost u svakom čvoru proporcionalna je reputacijama prethodnika

Udio propusnosti $bw_I^{OR_1}$ koju će OR_1 dati pošiljatelju I jednaka je omjeru njegove reputacije i sume reputacija svih n čvorova prethodnika, ali ne prelazeći ponderiranu vrijednost reputacije CR_I:

$$bw_I^{OR_1} = \min\left(\frac{Rep_I}{\sum_i^n Rep_{OR_i}}, Rep_I\right) \quad (5.3)$$

Neki ne-ulazni čvor OR_{x+1} će dati udio propusnosti svom čvoru prethodniku OR_x računajući omjer njegove reputacije i sume reputacija svih n čvorova prethodnika, ali ne prelazeći vrijednost reputacije OR_x:

$$bw_{OR_x}^{OR_{x+1}} = \min\left(\frac{Rep_{OR_x}}{\sum_i^n Rep_{OR_i}}, Rep_{OR_x}\right) \quad (5.4)$$

OR-ovi čitaju reputacije susjednih čvorova u opisnicima dostupnim kod imeničkog poslužitelja.

2. Ocjena prometa na izlaznom čvoru i slanje ocjene unazad, ažuriranje reputacije i propusnosti

Izlazni čvor donosi ocjenu prometa (v) u intervalu [0,1] i šalje ju unazad u `RELAY_REP_EXIT` ćeliji (1) prema ulaznom čvoru (slika 5.3). Svaki OR na dobiveni v primjenjuje težinsku funkciju kredibilnosti ω_{Cr} za ponderiranje ocjene prometa (2) (4):

$$\mathrm{v}' = \omega_{\mathrm{Cr}}(\mathrm{Rep}_{\mathrm{OR}_3}) \cdot \mathrm{v} \quad (5.5)$$

$$v'' = \omega_{Cr}(Rep_{OR_2}) \cdot v' \quad (5.6)$$

Kredibilnost je mjera vjerodostojnosti usmjernika u prenošenju ocjene. U ovom modelu, kredibilnost se izjednačuje s reputacijom usmjernika.

Za ažuriranje reputacije u ulaznom čvoru se koristi formula 4.11 beta reputacijskog sustava skalirana na interval [0,1]. Prvo se vrijednost *v* rastavi na par (*p,n*):

$$p = v \cdot w \ \text{ i } \ n = (1 - v) \cdot w \quad (5.7)$$

Uz faktor pamćenja λ i niz *Q* od *n* povratnih informacija, računaju se ($p_{I,\lambda}^{Q(i)}, n_{I,\lambda}^{Q(i)}$) rekurzivnom formulom 4.10.

U nultoj iteraciji, $p_{I,\lambda}^{Q(0)}$ i $n_{I,\lambda}^{Q(0)}$ se računaju iz vrijednosti $v = Rep_I$ dobivene u 2. fazi.

Reputacija u *i*-toj iteraciji skalirano na vrijednost u intervalu [0,1] iznosi:

$$Rep_I = Rep_I^{OR_1(i)} = \frac{p_I^{(i)} + 1}{p_I^{(i)} + n_I^{(i)} + 2} \quad (5.8)$$

S ažuriranom reputacijom treba ažurirati i trenutnu propusnost (5):

$$bw_I^{OR_1} = bw_I^{OR_1(i)} = \min\left(\frac{Rep_I}{\sum_i^n Rep_{OR_i}}, Rep_I\right) \quad (5.9)$$

Interval između slanja ocjene je parametar reputacijskog sustava.

3. Potpisivanje nove reputacije klijenta i zatvaranje kruga

Ulazni čvor šalje trenutnu vrijednost reputacije Rep_I' i certifikat pošiljatelja $CERT_I$ imeničkom poslužitelju (slika 5.4). Na vrijednost reputacije imenički poslužitelj primjenjuje funkciju kredibilnosti, odnosno ponderira reputacijom ulaznog čvora:

$$r' = Rep_I'' = \omega_{Cr}(Rep_{OR_3}) \cdot Rep_I' \quad (5.10)$$

Nova reputacija sada izgleda ovako:

$$CR_I' = \{r', CERT_I, CERT_{DIR}, t'\}$$

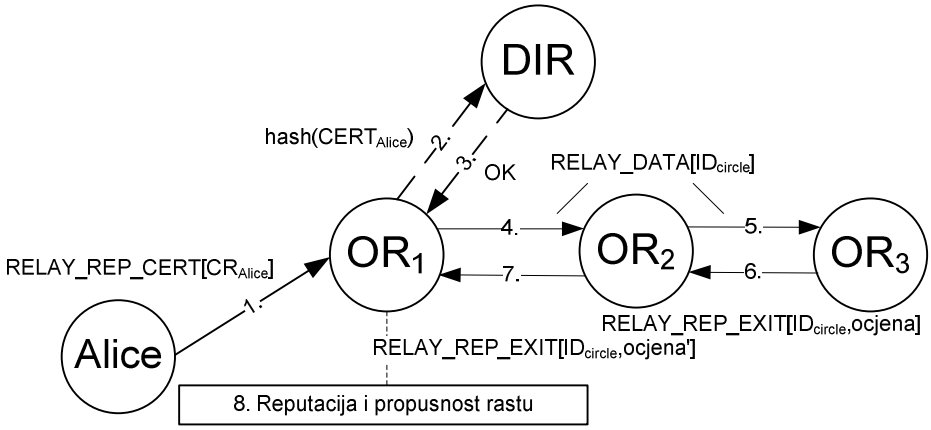
gdje je *t'* je vremenska oznaka sadašnjeg trenutka, a $CERT_{DIR}$ je certifikat imeničkog poslužitelja.

5.3. Scenariji za ispitivanje reputacijskog sustava

Scenariji opisuju ponašanje reputacijskog sustava i njegovu efikasnost u suzbijanju neželjenog ponašanja. Scenarij je definiran topologijom čvorova i njihovim svojstvima, kao što su reputacija i ponašanje. Za svaki scenarij se daje očekivani rezultat djelovanja reputacijskog sustava.

1. scenarij: nagrađivanje dobrog ponašanja pošiljatelja (slika 5.7)

   opis: Alice izabire tri usmjernika s dobrom reputacijom koristeći algoritam za biranje čvorova, gradi krug i predaje reputaciju ulaznom čvoru (1). Ulazni čvor šalje sažetak Alicinog certifikata na provjeru kod imeničkog poslužitelja (2). Imenički poslužitelj pretražuje listu nevažećih i trenutno korištenih certifikata i vraća rezultat nazad ulaznom čvoru (3). Alice koristi mrežu Tor bez zlonamjernog ponašanja (4) (5).

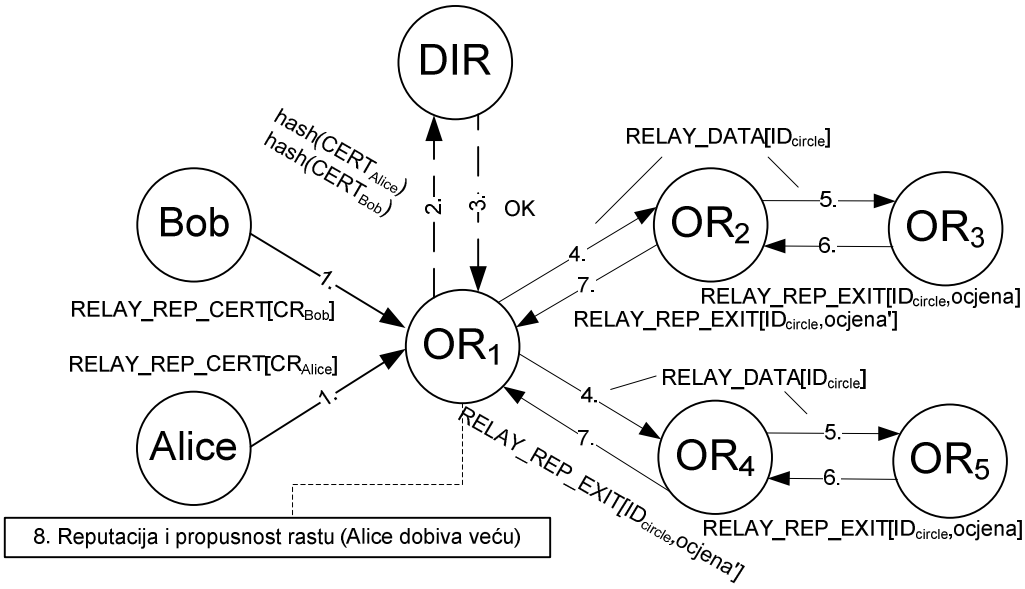


Slika 5.7. Nagrađivanje dobrog ponašanja pošiljatelja

   očekivani rezultat: Izlazni čvor ocjenjuje promet visokim ocjenama (6). Srednji čvor ponderira ocjenu s obzirom na reputaciju izlaznog čvora (7), a ulazni s obzirom na reputaciju srednjeg. Sa stanovišta ulaznog čvora, Alice asimptotski raste reputacija (8). Usporedo s ažuriranjem reputacije u ulaznom čvoru, povećana je propusnost za Alicin promet.

2. scenarij: nagrađivanje dobrog ponašanja pošiljatelja gdje ulazni čvor ima više čvorova prethodnika (slika 5.8)

   opis: Alice i Bob izabiru tri usmjernika s dobrom reputacijom, a ulazni čvor im je zajednički. Grade krug i predaju reputaciju ulaznom čvoru (1). Ulazni čvor provjerava sažetke certifikata kod imeničkog poslužitelja (2) (3). Alice i Bob počinju s istom reputacijom, ali Alice ima malo bolje ponašanje od Boba (4) (5).



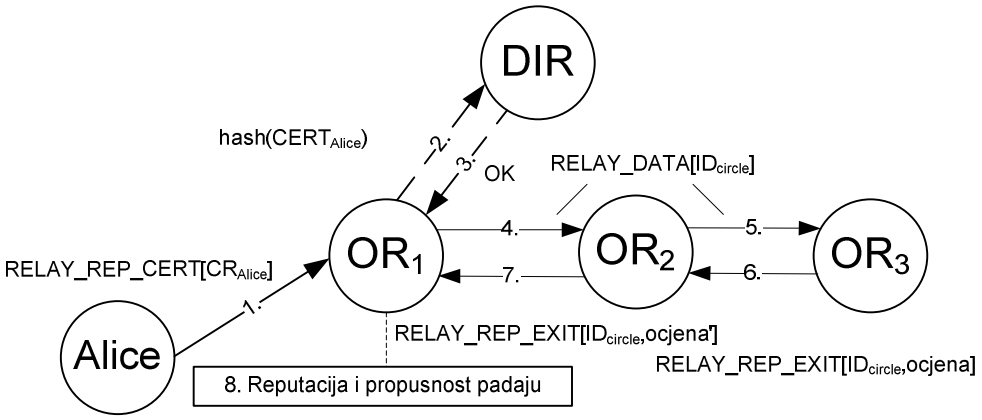
Slika 5.8. Raspodjela propusnosti u ulaznom čvoru za dva "dobra" pošiljatelja

očekivani rezultat: izlazni čvorovi ocjenjuju promet (6), ocjena se prenosi do ulaznog čvora (7) i pošiljateljima asimptotski raste reputacija (8). Usporedo s ažuriranjem reputacija u ulaznom čvoru, povećana je relativna propusnost u ulaznom čvoru za Alicin promet s obzirom na Bobov.

komentar: Budući da Alice i Bob počinju s istim reputacijama, ulazni čvor im dodjeljuje istu propusnost. Kako vrijeme teče, Alice dobiva bolju propusnost na razlici dobivene reputacije. To će trajati do zasićenja, kada će se reputacije Alice i Bob izjednačiti, a samim time i dodijeljene im propusnosti.

3. scenarij: kažnjavanje lošeg ponašanja pošiljatelja (slika 5.9)

opis: Alice izabire tri usmjernika s dobrom reputacijom koristeći algoritam za biranje čvorova, gradi krug i predaje reputaciju ulaznom čvoru (1). Ulazni čvor provjerava sažetak certifikata kod imeničkog poslužitelja (2) (3). Alice koristi mrežu Tor za zlonamjerno ponašanje (4) (5).



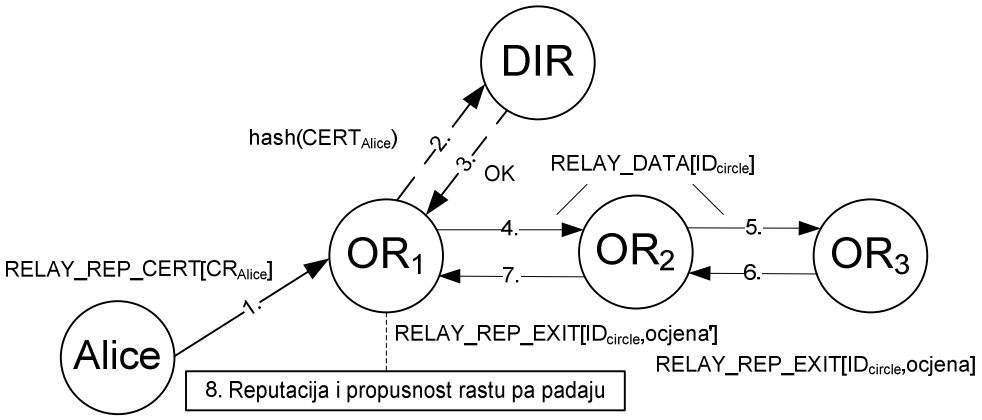
Slika 5.9. Kažnjavanje lošeg ponašanja pošiljatelja

očekivani rezultat: izlazni čvorovi ocjenjuju promet (6), ocjena se prenosi do ulaznog čvora (7) i Alice asimptotski pada reputacija (8). Usporedo s ažuriranjem reputacije u ulaznom čvoru, smanjena je relativna propusnost u ulaznom čvoru.

komentar: nije za očekivati da će pošiljatelj prihvatiti ovakvu reputaciju već će sljedećem ulaznom čvoru predati zadnju (dobru) reputaciju, sada oslabljenu vremenskom funkcijom. Neprihvaćanje reputacije obeshrabruje i regulira faktor zastarijevanja vremenske eksponencijalne funkcije.

4. scenarij: prilagodljivo ponašanje pošiljatelja u istom krugu (slika 5.10)

opis: Alice izabire tri usmjernika s dobrom reputacijom koristeći algoritam za biranje čvorova, gradi krug i predaje reputaciju ulaznom čvoru (1). Ulazni čvor provjerava sažetak certifikata kod imeničkog poslužitelja (2) (3). Alice koristi mrežu Tor za dobro ponašanje (4) (5), gradi reputaciju i zatim iskorištava visoku reputaciju odnosno propusnost za zlonamjerno ponašanje (8).

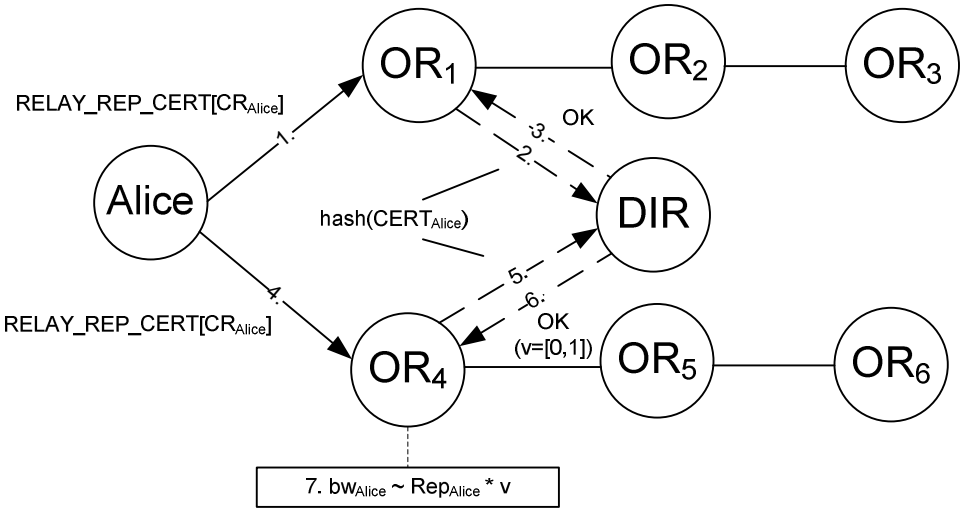


Slika 5.10. Prilagodljivo ponašanje pošiljatelja

očekivani rezultat: Nakon rasta, reputacijski sustav će reagirati na zlonamjerno ponašanje i sniziti reputaciju, a samim time i propusnost. Brzina reagiranja ovisi o reputacijskim parametrima, na primjer faktoru pamćenja. Ovisno o faktoru pamćenja, novije informacije imaju veću ili manju težinu. Što je ponašanje gore, propusnost će biti manja, a to će obeshrabriti Alice i otežati joj daljnju zloupotrebu.

5. scenarij: prilagodljivo ponašanje pošiljatelja u dva kruga (slika 5.11)

opis: Alice gradi dva kruga: u jednom gradi reputaciju, a u drugi koristi za zlonamjerna djela



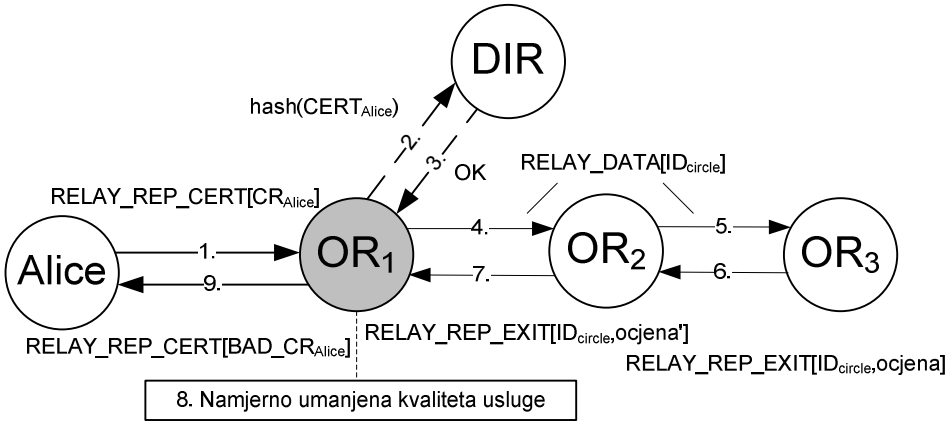
Slika 5.11. Alice koristi dva kruga za dvojako ponašanje

očekivani rezultat: Nakon predaje certificirane reputacije prvom ulaznom čvoru (1), u imeničkom poslužitelju zapisuje se sažetak certifikata u listu trenutno korištenih certifikata (2) (3). Alice potom predaje certificiranu reputaciju drugom ulaznom čvoru (4), a provjerom kod imeničkog poslužitelja (5) dobiva broj u intervalu [0,1] koji je obrnuto proporcionalan broju krugova u kojem se isti certifikat koristi (6). Brojem koji dobije, OR_4 ponderira reputaciju (7) kako bi se spriječili, odnosno obeshrabrili opisani slučaj zloupotrebe.

komentar: OP u svakom trenutku pokušava imati nekoliko krugova u pripravnosti kako bi prelazak na novi krug zbog sigurnosne rotacije ili zatvaranja kruga bio brz i učinkovit. Nakon zatvaranja kruga, ulazni čvor šalje imeničkom poslužitelju sažetak certifikata koju treba obrisati iz liste trenutno korištenih certifikata i ažuriranu reputaciju. Poslužitelj briše sažetak iz liste, ponderira reputaciju reputacijom ulaznog čvora, potpisuje i vraća ulaznom čvoru. Prije aktivnog korištenja drugog kruga, Alice šalje novu certificiranu reputaciju.

6. scenarij: zlonamjerni ulazni ili izlazni čvor (slika 5.12)

   opis: Alice izabire tri usmjernika s dobrom reputacijom, od kojih je ulazni čvor zlonamjeran, koristeći algoritam za biranje čvorova, gradi krug i predaje reputaciju ulaznom čvoru (1). Ulazni čvor provjerava sažetak certifikata kod imeničkog poslužitelja (2) (3). Alice koristi mrežu Tor za dobro ponašanje (4) (5). Izlazni čvor ocjenjuje promet (6), ocjena se prenosi do ulaznog čvora (7) koji namjerno smanjuje propusnost (8) ili šalje reputaciju umanjene vrijednosti (9). Uz to, ulazni čvor može uskratiti predaju reputacije pri zatvaranju kruga. Sa stanovišta pošiljatelja, scenarij je istovjetan manipulaciji ocjenama izlaznog čvora.



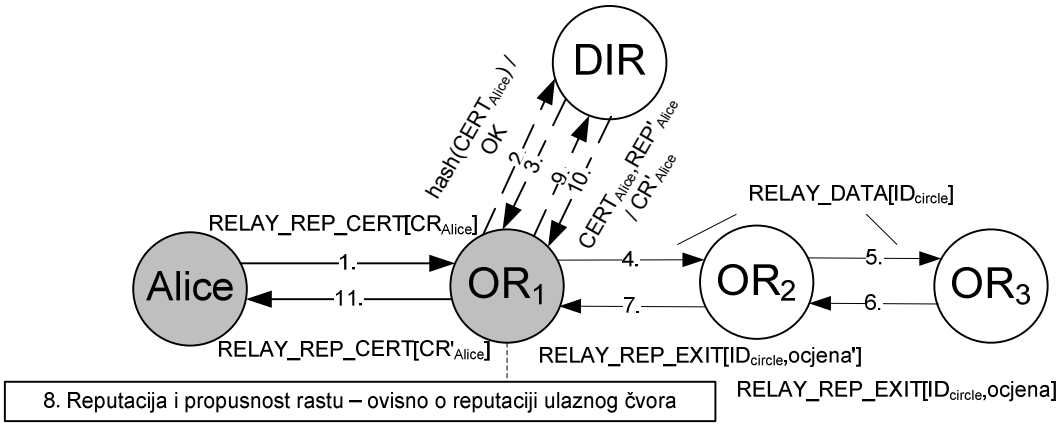
Slika 5.12. Zlonamjerni ulazni čvor namjerno umanjuje propusnost ili vraća umanjenu certificiranu reputaciju

   očekivani rezultat: pošiljatelj odbacuje reputaciju

   komentar: pošiljatelj ne zna tko je zlonamjeran: ulazni ili izlazni čvor. Pošiljatelj može prijaviti imeničkom poslužitelju zlonamjernost ulaznog i izlaznog čvora kako bi bili jednako kažnjeni. Za to mu treba dokaz transakcije koji se može dobiti potpisivanjem "ugovora" odmah nakon stvaranja kruga. Ugovor sadrži vremensku oznaku i sažetke certifikata ulaznog, odnosno izlaznog čvora i pošiljatelja, potpisanog od ulaznog, odnosno izlaznog čvora. Ova mjera se može zloupotrijebiti kao napad na ulazni i izlazni čvor. Zaredaju li se optužbe na nekog usmjernika, poslužitelj može sagraditi krug s usmjernikom i provjeriti. Ustanovi li da su optužbe neutemeljene ili pretjerane, ignorirat će pritužbe na neko određeno vrijeme.

7. scenarij: suradnja ulaznog čvora i pošiljatelja (slika 5.13)

   opis: Alice ima ulazni čvor pod kontrolom i koristi ga kako bi sagradila dobru reputaciju. Predaja reputacije ulaznom čvoru nije potrebna ukoliko Alice kontrolira ulazni čvor (1). Ulazni čvor šalje sažetak certifikata imeničkom poslužitelju (2) (3). Bez obzira na proslijeđeni promet (4) (5) i ocjene izlaznog (6) i srednjeg čvora (7), ulazni čvor povećava reputaciju Alice (10). Zapravo je nebitno koristi li Alice mrežu Tor za prosljeđivanje prometa jer ulazni čvor, nakon zatvaranja kruga, daje dobru ocjenu imeničkom poslužitelju na potpis (9) (10). Ulazni čvor šalje Alice umjetno izgrađenu reputaciju (11).

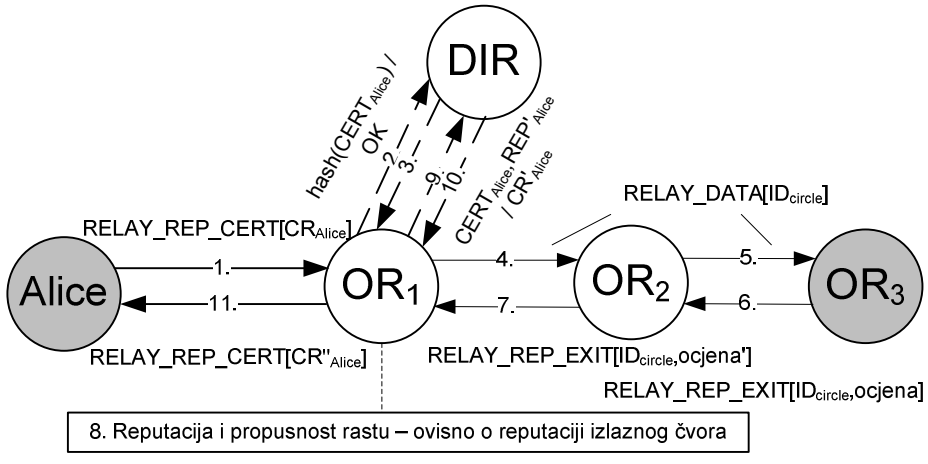


Slika 5.13. Alice i ulazni čvor surađuju

očekivani rezultat: ovisi o reputaciji ulaznog čvora. Ukoliko se radi o dva nova čvora, potpisana reputacija neće imati veliku vrijednost zbog slabe reputacije ulaznog čvora kojom se reputacija pošiljatelja ponderira. Kao mjera zaštite, imenički poslužitelj neće prihvatiti ažuriranje reputacije `MAX_REP_ENTRY_NODE` (3) puta za redom od istog ulaznog čvora. Skupo je ulagati resurse na dizanje reputacije ulaznog čvora za ovu svrhu jer se reputacije usmjernika sporije razvijaju.

8. scenarij: suradnja izlaznog čvora i pošiljatelja (slika 5.14)

opis: Alice izabire ulazni i srednji čvor s visokom reputacijom i suradnika za izlazni čvor. Alice predaje reputaciju ulaznom čvoru (1). Ulazni čvor provjerava sažetak certifikata kod imeničkog poslužitelja (2) (3). Nebitno je koristi li Alice mrežu Tor za prosljeđivanje prometa (4) (5) jer izlazni čvor šalje dobre ocjene bez obzira na promet (6). Srednji čvor prosljeđuje ponderiranu ocjenu (7). Shodno dobrim ocjenama, ulazni čvor povećava reputaciju i propusnost (8). Nakon zatvaranja kruga, ulazni čvor daje ocjenu imeničkom poslužitelju na potpis (9) (10) i nakon toga Alice dobiva umjetno izgrađenu reputaciju (11).



Slika 5.14. Alice i izlazni čvor surađuju na umjetnom građenju reputacije

očekivani rezultat: Slično kao i u prethodnom scenariju, ažurirana reputacija ovisi o reputacijama čvorova u krugu i vjerojatnosti da bi izlazni čvor dugo gradio reputaciju za ovaj napad.

5.4. Dodatna razmatranja

Manja skupina OR-ova s visokom reputacijom je primamljiv cilj napada zbog visoke vjerojatnosti izbora u krugu i posljedično velikog prometa. To je i sada slučaj u postojećoj mreži Tor gdje manji dio izlaznih čvorova s visokom propusnošću prenosi velik udio prometa [58]. U modifikaciji Tora, "Tunable Tor" [58], predlaže se da korisnici sami izabiru točku kompromisa između dva međusobno isključiva ekstrema: visokih performansi i visokog stupnja anonimnosti. Veća anonimnost ostvaruje se izborom čvorova s malom oglašenom propusnošću (manja koncentracija prometa), a veće performanse odabirom čvorova s velikom oglašenom propusnošću. Treba uzeti u obzir mogućnost particionirajućeg napada gdje se koristi činjenica da korisnici željni visoke anonimnosti izabiru čvorove isključivo niske propusnosti. Algoritam za odabir čvorova treba oblikovati tako da postoji vjerojatnost da budu izabrani i čvorovi manje reputacije. To će im ujedno pomoći da se kao novi čvorovi etabliraju u mreži ako su dobrog ponašanja.

Zbog ocjenjivanja prometa u realnom vremenu, izlazni čvor ne može uvijek na vrijeme reagirati na promet koji prenosi. Za neke napade može saznati tek putem prijave za zloupotrebu od ISP-a ili represivnog sustava. Ulazni čvor je za to vrijeme već sagradio novi krug, obrisao svoj trag i ne može ga se više kazniti.

Samo pošiljatelj zna prolaze li poruke do odredišta i nazad. Ne prolaze li poruke, pošiljatelj zatvara krug i gradi novi. Ostaje neistraženo odražava li trajanje kruga činjenicu da usmjernici dobro rade svoj posao ili sigurnosnu politiku rotacije krugova. Duljina trajanja kruga eventualno se može iskoristiti za reputaciju ulaznog čvora jer imenički poslužitelj ne zna za ostale članove kruga.

Dva su moguća načina postupanja ukoliko klijent želi eksplicitno kazniti čvorove kruga za neprosljeđivanje poruka:

1. Može javiti svima u krugu, nakon čega će svaki čvor dati svojim prethodnicima i sljedbenicima loše ocjene. Za ovo je potreban mehanizam sakupljanja reputacija usmjernika od drugih usmjernika kod imeničkog poslužitelja
2. Klijent dojavljuje imeničkom poslužitelju problem prosljeđivanja poruka i članove kruga. Imenički poslužitelj gradi takav krug da ispituje jednog po jednog člana kruga i ažurira reputaciju zlonamjernog usmjernika.

Zamišljena je koegzistencija usmjernika i klijenata s različitim verzijama protokola Tor jer je jedino takva implementacija i moguća pa se ne smiju raditi infrastrukturne i protokolne izmjene koje će onemogućiti sudjelovanje klijenata i usmjernika bez reputacijskog sustava. Pretpostavlja se da će aktivni usmjernici prije preuzeti verziju s reputacijskim sustavom što će natjerati klijente željne boljih performansi da ažuriraju svoju programsku podršku. U suprotnom će biti tretirani kao da imaju minimalnu reputaciju. Sve dok postoji i jedan čvor sa starijom verzijom, treba se osigurati mogućnost obostranog rada (engl. backward compatibility). Najvažniji dio uporabljivosti programske podrške tiče se Tor usmjernika, jer o njima ovisi cijela mreža, pa tako i usluga korisnicima.

6. Implementacija

Ponašanje reputacijskog sustava u modelu mreže Tor simulirano je simulacijskim okruženjem OMNeT++ [89]. Cilj simulacije je bio ustanoviti kako se reputacije entiteta u mreži Tor mijenjaju u vremenu s obzirom na njihova ponašanja. Model mreže Tor je apstrahiran do razine koji je nužan za ostvarivanje cilja ispitivanja. Simuliran je i utjecaj parametara reputacijskog sustava na njegovo funkcioniranje. Odabirom parametara namješta se brzina reakcije i efikasnost reputacijskog sustava u kažnjavanju neželjenog ponašanja i motiviranju željenog. Prema teoriji igara, svi entiteti žele najbolje za sebe, a sustav mora osigurati ravnotežu u kojoj većina dobiva zadovoljavajuću uslugu. Naglasak reputacijskog sustava je na sprečavanju zloupotrebe od strane klijenata koji mogu imati različite strategije za ostvarivanje svojih ciljeva. Strategija, odnosno ponašanje klijenta može biti:

- isključivo loše
- isključivo dobro
- vremenski promjenjivo
- ovisno o trenutnoj vrijednosti reputacije, odnosno propusnosti

Detektiranje ponašanja klijenata u okviru ovih simulacija je svedeno na crnu kutiju (engl. black box). Drugim riječima, idealizira se sposobnost izlaznog čvora da na temelju prometa koji kroz njega prolazi može dati točnu procjenu namjere ulaznog čvora i prepoznati zloupotrebu. Kao što je ranije predloženo, može se koristiti sustav za detekciju napada, primjerice snort. U postojećim simulacijama mreže Tor koriste se mjerenja stvarnog prometa mreže Tor, Tor metrics [90]. U ovoj simulaciji ne simulira se promet karakterističan za mrežu Tor, već samo dio protokola za uspostavu kruga i zatvaranje kruga, predaju i provjeru certificirane reputacije i ažuriranje reputacije preko ocjene izlaznog čvora.

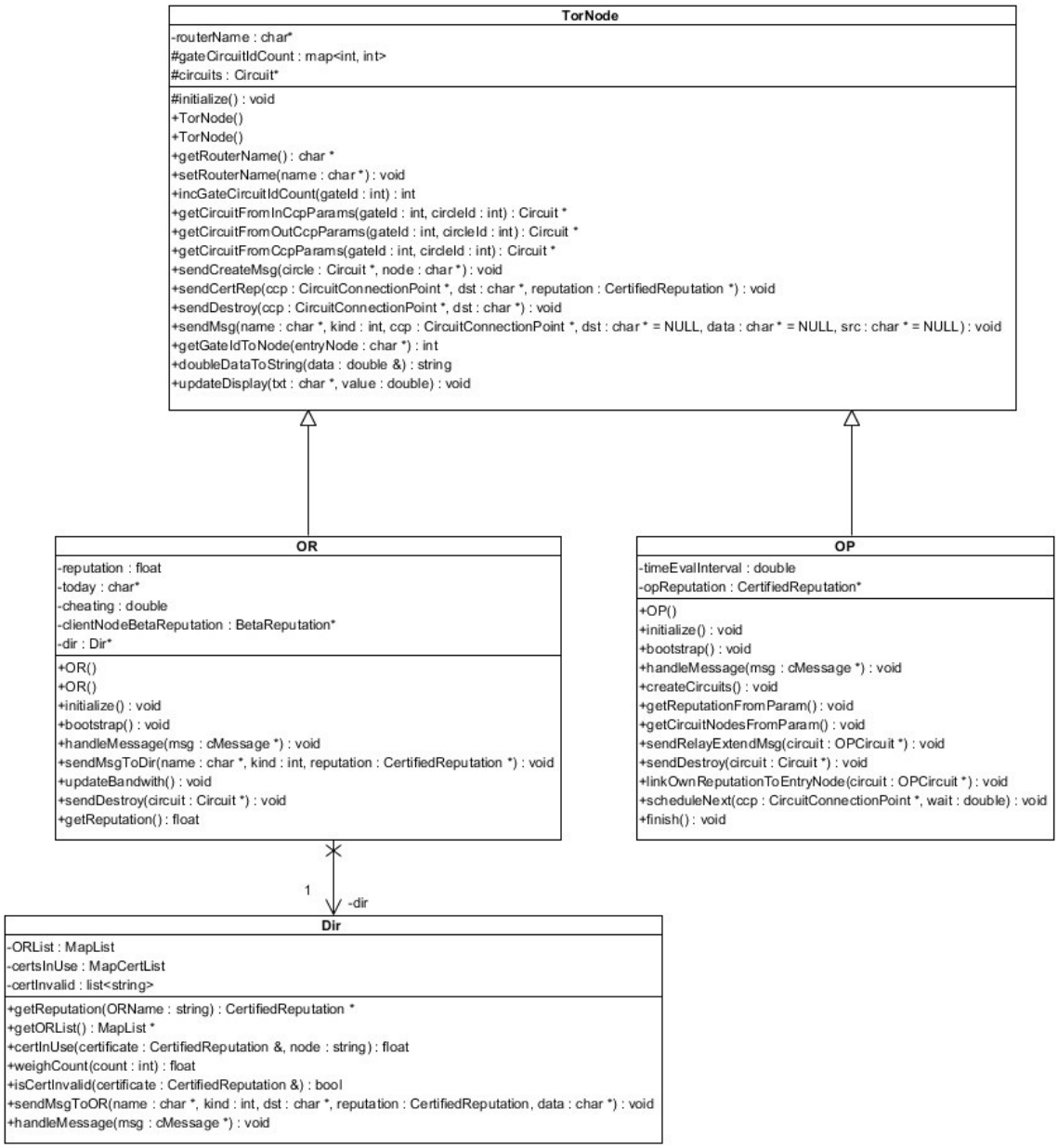
6.1. Opis simulacijskog modela

Osnovni razredi su popisani u tablici 6.1.

Tablica 6.1. Popis osnovnih razreda

Ime razreda	*Implementira*
TorNode	čvor mreže
OP	Tor posrednik
OR	Tor usmjernik
Dir	imenički poslužitelj
Circuit	krug mreže
TorCell	poruka (ćelija)

Na slici 6.1 se nalazi dijagram razreda `OP`, `OR`, `TorNode`, i `Dir`. `OP` i `OR` nasljeđuju `TorNode`, a `OR` sadrži pokazivač na `Dir`.



Slika 6.1. Razredi OR i OP nasljeđuju razred TorNode

U `ned` konfiguracijskoj datoteci se definira broj klijenata i usmjernika u simulaciji i topologija simulacije. Topologija mreže je statička i unaprijed su definirane TLS veze između čvorova. Svaki OR pri inicijalizaciji pronalazi `Dir` modul (slika 6.1) i njegova nespojena ulazna vrata (`directIn`). Komunikacija sa imeničkim poslužiteljem se simulira preko nespojenih vrata kako bi simulacija bila vizualno pregledna.

Parametri reputacijskog sustava i entiteta su definirani u konfiguracijskoj datoteci `omnetpp.ini`, a sve informacije koje klijent treba za izgradnju kruga, uključivo i certificiranu reputaciju, definirane su u xml datoteci `clients.xml`.

Na slici 6.2 je primjer konfiguracijske datoteke. Varijabla `today` označava lokalno vrijeme usmjernika potrebno za izračunavanje zastarjelosti reputacija. Reputacija klijenta `alice` usmjerena je na xml datoteku i *tag* unutar nje. Za reputacije svih usmjernika može se postaviti konstantna vrijednost ili se može koristi neki od omnetovih generatora slučajnih brojeva. U

stvarnoj mreži, izlazni bi čvor u definiranom intervalu ocjenjivao promet i slao ocjenu prema ulaznom čvoru. Budući da karakteristika prometa proizlazi iz ponašanja klijenta, logično je da u simulaciji, na temelju definiranog ponašanja, klijent sâm stvara ocjenu prometa. Ocjena se šalje u `RELAY_DATA` ćeliji do izlaznog čvora. Parametar `timeEvalInterval` definira koliko će često klijent slati poruku u kojoj je zapisana karakteristika prometa, odnosno ponašanje.

```
network = tor_rep.Tc1
Tc1.or[*].today = "10.1.2011 18:30:39"
Tc1.alice.reputation = xmldoc("clients.xml",
"//*[@name='alice']/reputation")
Tc1.alice.circuits = xmldoc("clients.xml",
"//*[@name='alice']/circuits")
Tc1.or[*].reputation = 0.9
Tc1.**.timeEvalInterval = 8s
Tc1.or[*].lambda = 6h
Tc1.or[*].betaLambda = 0.9
```

Slika 6.2. Izgled omnetpp.ini konfiguracijske datoteke

Slika 6.3 prikazuje dijagram razreda `Circuit`, `OPCircuit`, `CircuitConnectionPoint`, `CertifiedReputation` i `Behavior`. Svaki čvor u krugu sadrži instancu razreda `Circuit`. U njemu se drži status kruga, dodijeljena propusnost, korištene vrijednosti `circID-a` i informacije o čvorovima sljedbenicima i prethodnicima. Klijent sadrži instancu razreda `OPCircuit` koji nasljeđuje razred `Circuit`. `OPCircuit` još sadrži reputaciju klijenta koju implemetira razred `CertifiedReputation` i ponašanje klijenta koje implementira razred `Behavior`. Ponašanje klijenta se inicijalizira se iz xml datoteke koja je prikazana na slici 6.4. Datoteka sadrži certificiranu reputaciju definiranu vrijednostima popisanim u tablici 6.2. Certificiranu reputaciju implementira razred `CertifiedReputation`.

Tablica 6.2. Popis vrijednosti certificirane reputacije u simulaciji mreže Tor

Vrijednost	*Funkcija*
value	vrijednost reputacije
owner-id	vlasnik reputacije
signer-id	potpisnik reputacije
timestamp	vrijeme potpisivanja

Slika 6.3. Razred OPCircuit nasljeđuje razred Circuit, a sadrži instancu razreda Behavior i CertifiedReputation

U xml datoteci se nalazi popis svih krugova koje klijent treba izgraditi, svi čvorovi pojedinog kruga i skup ponašanja u krugu. Skupom ponašanja omogućuje se izmjena različitih ponašanja u istom krugu kako bi se simulirale naprednije strategije klijenata. Ponašanje je u xml datoteci definirano vrijednostima: `mean`, `stddev`, `time-limit`, `target-reputation`. `mean` i `stddev` definiraju aritmetičku sredinu i standardnu devijaciju normalne razdiobe, a `time-limit` i `target-reputation` definiraju uvjete završetka ponašanja. Kada je zadovoljen neki od ta dva uvjeta, klijent u krugu prelazi na novo ponašanje ili zatvara krug ako su sva ponašanja završila.

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
    <client name="alice">
          <reputation>
                <value>0.5</value>
                <owner-id>alice</owner-id>
                <signer-id>dir</signer-id>
                <timestamp>10.1.2011 14:00:00</timestamp>
          </reputation>
          <circuits>
                <circuit>
                      <node>or[0]</node>
                      <node>or[1]</node>
                      <node>or[2]</node>
                      <behavior>
                            <mean>0.75</mean>
                            <stddev>0.05</stddev>
                            <time-limit>5 min</time-limit>
                       <target-reputation>0.7</target-reputation>
                      </behavior>
                </circuit>
          </circuits>
    </client>
</root>
```

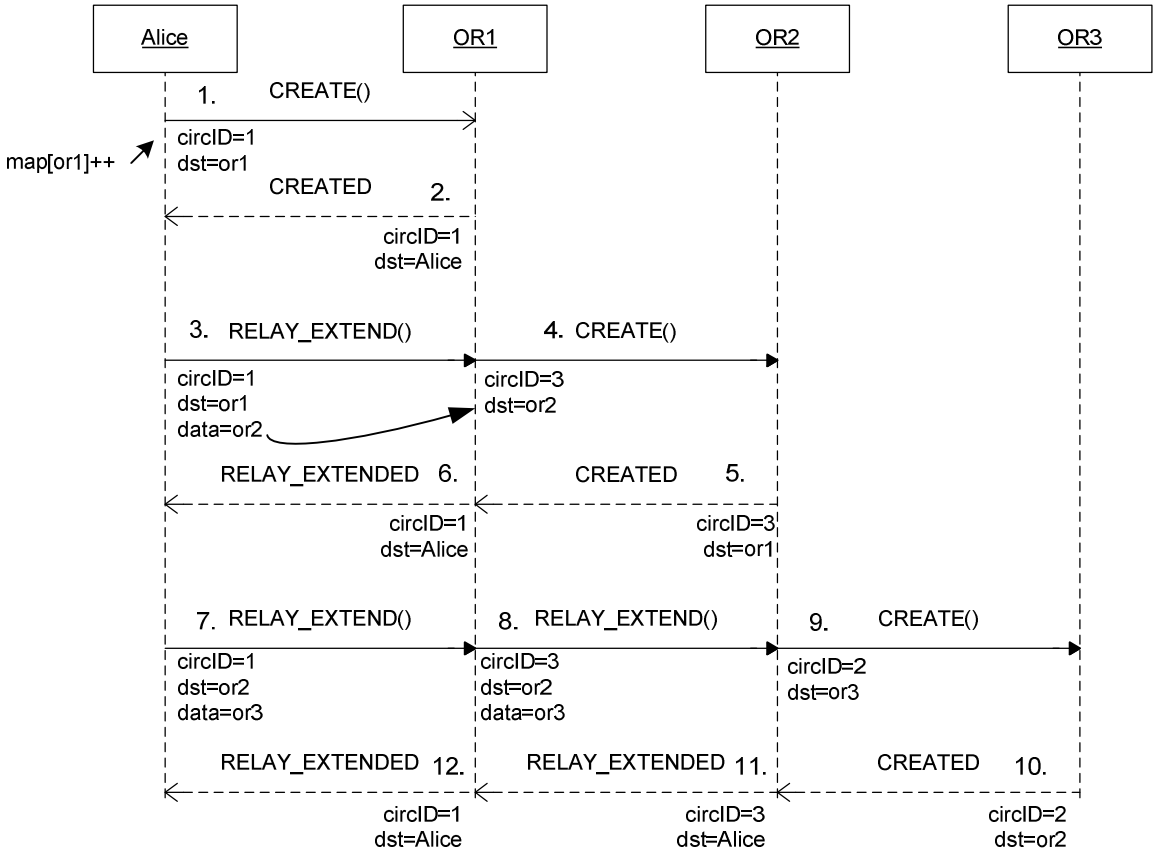
Slika 6.4. Izgled xml konfiguracijske datoteke

Protokol izgradnje kruga, prikazan slijednim dijagramom na slici 6.5, pojednostavljen je za potrebe simulacije. Sve funkcije kriptiranja i uslojavanja su izostavljene što znači da je sadržaj poruke dostupan svim čvorovima koji je primaju. Polje `dst` u poruci (razred `TorCell`) označava odredište, odnosno čvor koji bi nakon dekriptiranja u stvarnoj mreži Tor dobio čisti tekst. Konkretno, u stvarnoj mreži Tor usmjernik prepoznaje da je ćelija namijenjena njemu ako nakon dekripcije dobije nulu u polju `Prepoznato`. Krug se u simulaciji gradi čvor po čvor. Svaki klijent čita topologiju krugova iz konfiguracijske datoteke na početku simulacije i nakon toga inicira algoritam za izgradnju jednog ili više krugova. Kao i u stvarnom protokolu, `CircID` nije konstanta u cijelom krugu, već jedinstveni slijedni cijeli broj koji bira čvor prilikom slanja `create` ćelije. Svaka OP-OR ili OR-OR veza ima vlastitu vrijednost `CircID` za isti logički krug. Srednji i ulazni čvorovi mogu imati više prethodnika i više sljedbenika pa dvostranim mapiranjem u razredu `CircuitConnectionPoint` (slika 6.3) vežu ulazni par (`circId`, `gateId`) sa izlaznim parom (`circId`, `gateId`). Klijent ima samo izlazne parove, a izlazni čvor samo ulazne parove.

Slijedni dijagram na slici 6.5 opisan je u koracima:

1. Alice za `CircID` odabire prvi sljedeći cijeli broj vezan za sljedbenika, odnosno izlazna vrata.
2. OR1 dobiva `CREATE` ćeliju i odgovara sa `CREATED`
3. Alice proširuje krug sa OR2 ćelijom `RELAY_EXTEND` gdje u `data` polju naznačuje koji čvor treba dodati krugu.

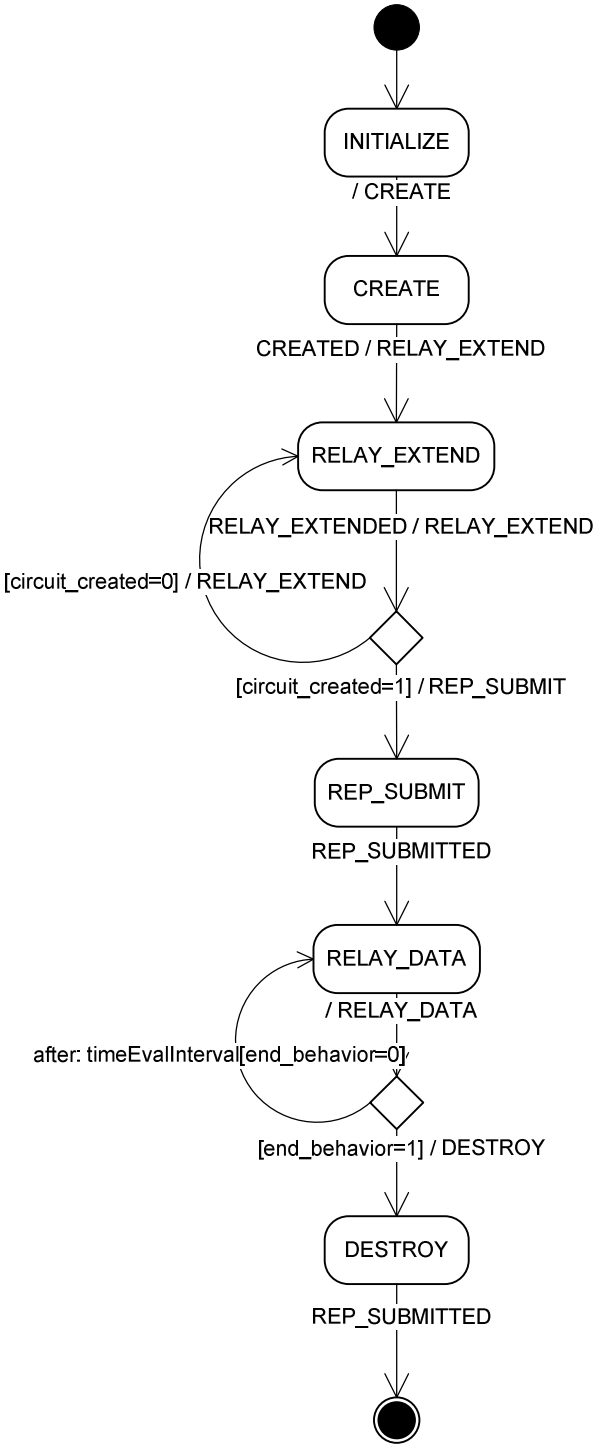
4. OR1 čita u polju `dst` da je `RELAY_EXTEND` ćelija za njega te sastavlja ćeliju `CREATE`, tako da promijeni `CircID` na vrijednost koju OR1 i OR2 trenutno ne koriste.
5. OR2 dobiva `CREATE` ćeliju i odgovara OR1 sa `CREATED`
6. OR1 na temelju `CREATED` ćelije šalje Alice `RELAY_EXTENDED`, uz promjenu `CircID`
7. Alice proširuje krug za jedan čvor ćelijom `RELAY_EXTEND`, gdje u `data` polju naznačuje koji čvor treba dodati krugu.
8. OR1 vidi da ćelija nije namijenjena (`dst=OR2`) njemu te je prosljeđuje dalje uz promjenu `CircID`
9. OR2 čita u polju `dst` da je `RELAY_EXTEND` ćelija za njega te sastavlja ćeliju `CREATE`, tako da promijeni `CircID` na vrijednost koju OR2 i OR3 trenutno ne koriste.
10. OR3 dobiva `CREATE` ćeliju i odgovara OR2 sa `CREATED`
11. OR2 na temelju `CREATED` ćelije šalje Alice `RELAY_EXTENDED` (promjena `CircID`)
12. OR1 prosljeđuje `RELAY_EXTENDED` uz promjenu `CircID`.
    Time je završeno stvaranje kruga.



Slika 6.5. Slijedni dijagram izgradnje kruga simulacije mreže Tor

Tijek simulacije definiran je automatima Tor posrednika i usmjernika. Automat Tor posrednika (OP) prikazan je na slici 6.6. Nakon inicijalizacije, Tor posrednik gradi krugove definirane u konfiguracijskoj datoteci. Slijedni dijagram izgradnje kruga može se vidjeti na slici 6.5. OP započinje stanjem `INITIALZIE` i šalje `CREATE` ćeliju. Prijelazi u `CREATE` stanje

i nakon primitka `CREATED` ćelije, proširuje krug slanjem `RELAY_EXTEND` ćelije. Prelazi u stanje `RELAY_EXTEND` u koje se ponovno vraća dok potpuno ne izgradi krug (`circuit_created = 1`). Nakon što je krug proširen na sve čvorove, OP šalje certificiranu reputaciju ulaznom čvoru (`REP_SUBMIT` stanje). U stanju `RELAY_DATA` šalje `RELAY_DATA` ćelije sa vrijednostima karakteristike prometa definirane trenutnim ponašanjem. Kada su sva ponašanja završila, OP šalje `DESTROY` ćeliju i čeka potpisanu ažuriranu reputaciju (`DESTROY` stanje).



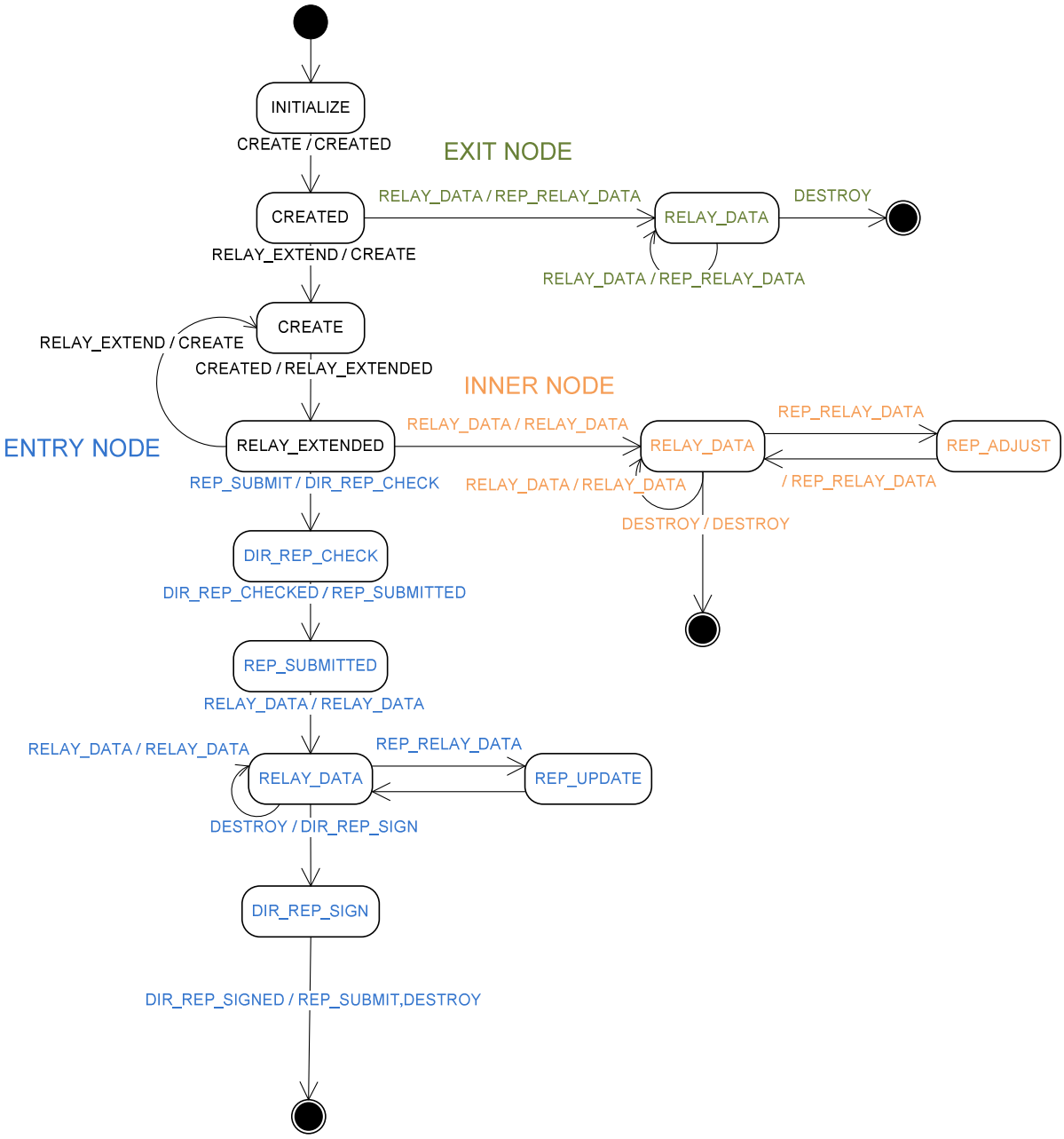
Slika 6.6. Automat Tor posrednika (OP) simulacije mreže Tor

Iako je usmjernik (OR) implementiran jednim razredom, tijekom simulacije može odrediti vlastiti položaj u krugu. Zato automat stanja na slici 6.7 pokazuje tri grananja: za ulazni, unutarnji i izlazni čvor.

Izlazni čvor prima `CREATE` ćeliju i odgovara sa `CREATED` ćelijom. Nakon toga, prima `RELAY_DATA` ćelije i odgovara prepisujući ocjenu u `REP_RELAY_DATA` ćeliju.

Unutarnji čvor dobiva jednu ili više `RELAY_EXTEND` ćelija, odnosno šalje jednu ili više `CREATE` ćelija. Nakon toga, prosljeđuje `RELAY_DATA` ćelije u `RELAY_DATA` stanju. Po primitku `REP_RELAY_DATA` ćelije, mijenja sadržaj ćelije ponderirajući vrijednost ocjene reputacijom čvora od kojeg prima poruku (stanje `REP_ADJUST`).

Ulazni čvor dobiva jednu ili više `RELAY_EXTEND` ćelija, odnosno šalje jednu ili više `CREATE` ćelija. Od klijenta potom prima `REP_SUBMIT` ćeliju koja sadrži certificiranu reputaciju. Ulazni čvor šalje sažetak certificirane reputacije imeničkom poslužitelju zbog provjere ispravnosti i trenutnog korištenja (stanje `DIR_REP_CHECK`). Po primitku `DIR_REP_CHECKED` ćelije, odgovara klijentu s `REP_SUBMITTED` ćelijom i ulazi u `RELAY_DATA` stanje. Ulazni čvor je sada spreman prosljeđivati `RELAY_DATA` ćelije, a primitkom `REP_RELAY_DATA` ažurira trenutnu reputaciju i na temelju nje propusnost (stanje `REP_UPDATE`).



Slika 6.7. Automat Tor usmjernika (OR) simulacije mreže Tor

6.2. Rezultati

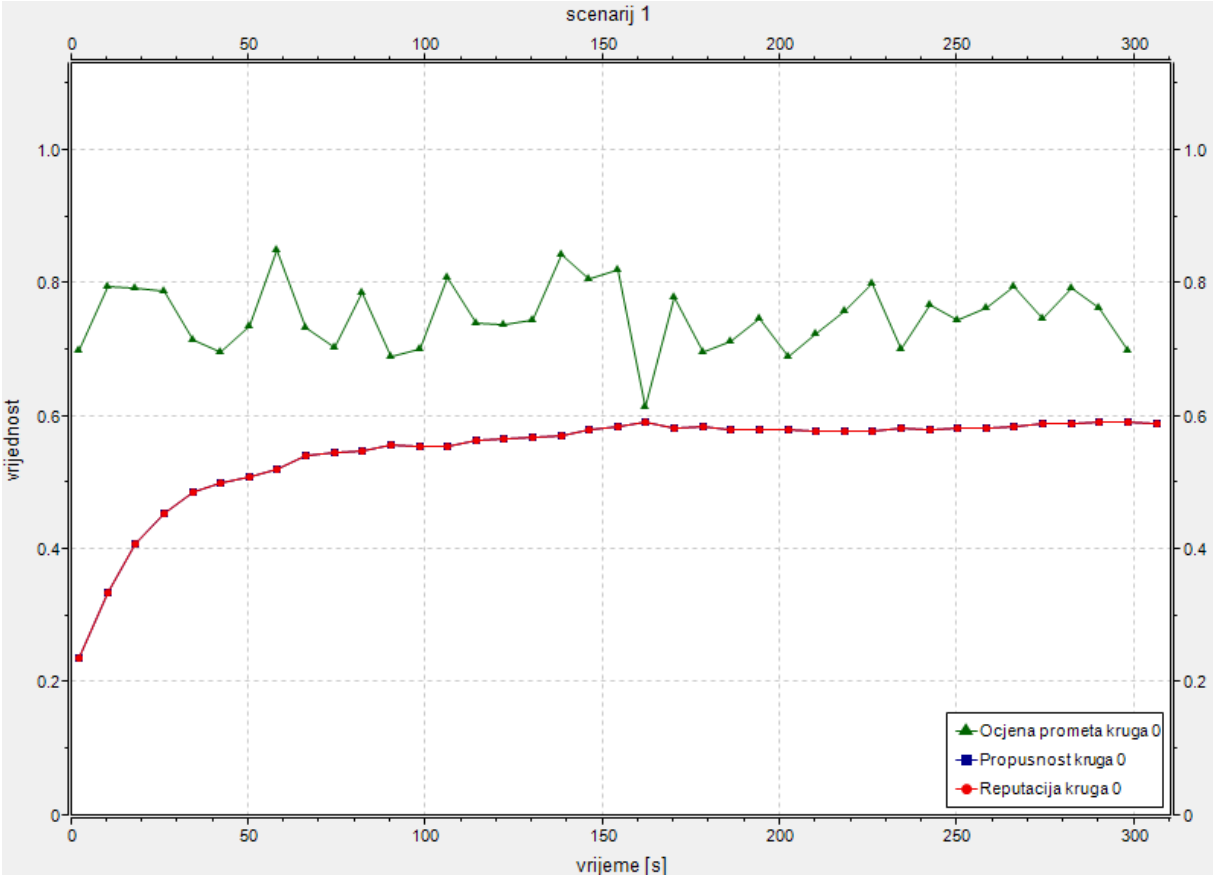
Rezultati simulacija svih 8 scenarija, opisanih u poglavlju 5.3, prikazani su na grafovima s ocjenom prometa, raspodjelom propusnosti po krugovima i reputacijom klijenta. Topologija i ponašanje klijenata u svakoj simulaciji odgovara definiranom scenariju pod istim rednim brojem. Budući da se trajanje kruga u mreži Tor mjeri u minutama, u simulaciji je prosječno vrijeme trajanja kruga 5 minuta. Vrijeme Svaki klijent ima definiran uvjet prestanka trajanja kruga. Trajanje se može ograničiti vremenski ili dostizanjem ciljne reputacije. Za to vrijeme, klijent može iskazivati različita ponašanja. Reputacije svih usmjernika, osim kada je drugačije navedeno, su visoke, kako ne bi previše negativno utjecale na ocjenu prometa u `REP_RELAY_DATA` ćeliji i propusnost. Releji s visokom reputacijom odražavaju potrebu klijenta za visokom propusnošću i povjerenje u vjerno ažuriranje reputacije klijenta. Svi

klijenti kreću sa srednjom reputacijom. Faktor zastarijevanja (λ) je 6 sati, što prema formuli 5.1 za certificiranu reputaciju *CR* staru 4.5 sati daje koeficijent $\omega_{\mathrm{Re}} = 0.47$.

U nastavku teksta su razloženi rezultati simulacija scenarija.

1. simulacija

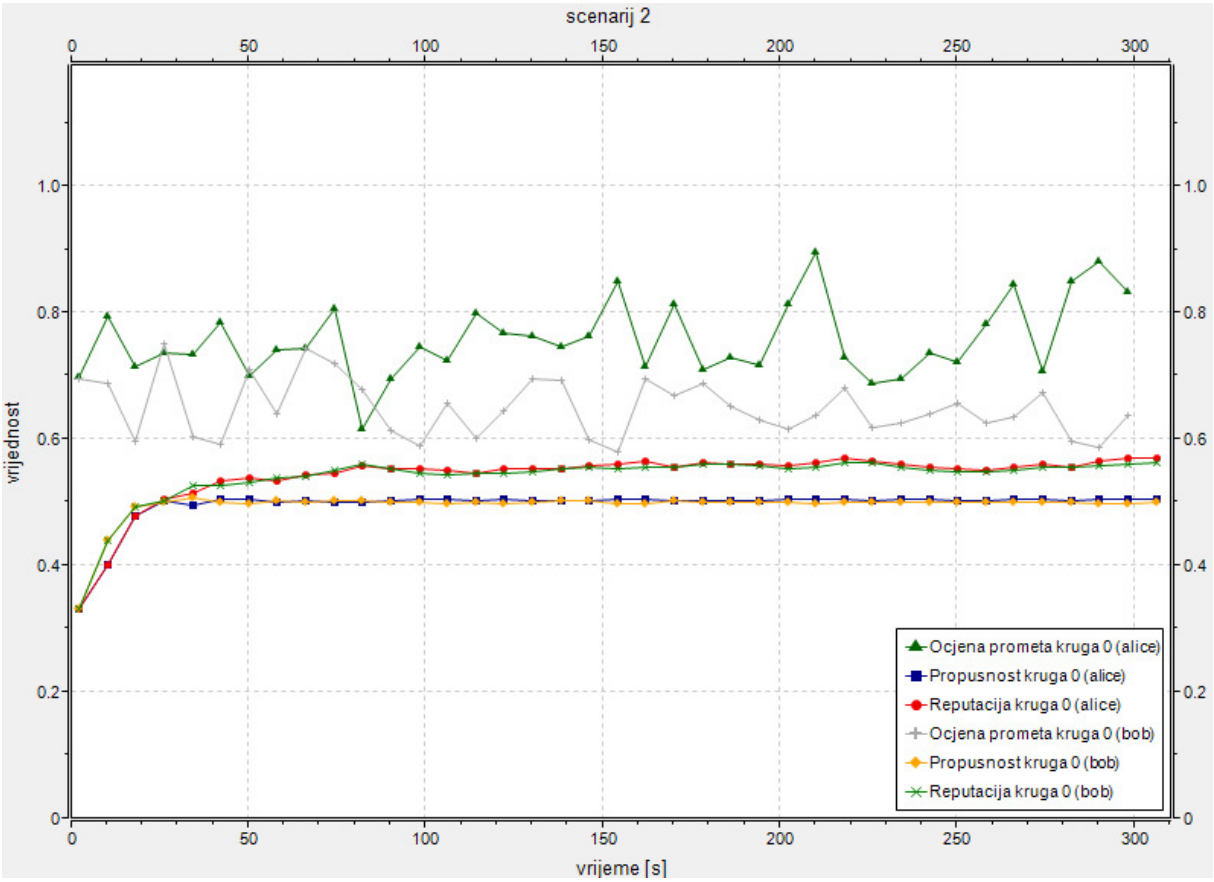
   Rezultat simulacije 1. scenarija u kojem se nagrađuje dobro ponašanje pošiljatelja je prikazan grafom na slici 6.8. Graf prikazuje reputaciju klijenta i propusnost u ovisnosti o ocjeni prometa, odnosno u ovisnosti o ponašanju. Reputacija i propusnost klijenta rastu do zasićenja određenog reputacijama čvorova koji prenose ocjenu. Krivulja propusnosti nije vidljiva jer se poklapa s krivuljom reputacije. Naime, ulazni čvor u ovom krugu ima samo jednog prethodnika pa je omjer reputacije klijenta prema sumi reputacija čvorova prethodnika jednak 1. To bi značilo da je propusnost maksimalna i zato je gornja granica propusnosti prema formuli 5.3 jednaka reputaciji.



Slika 6.8. Nagrađivanje dobrog ponašanja klijenta

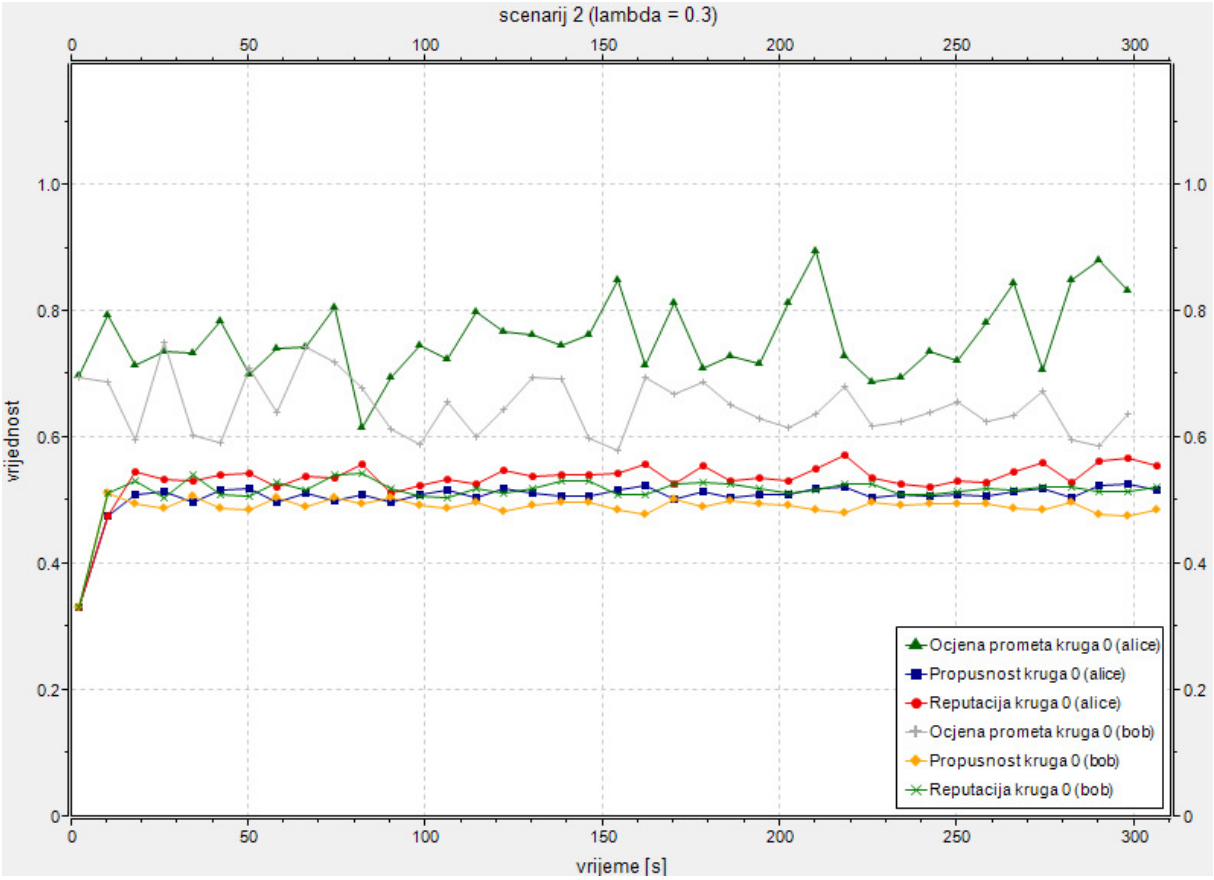
2. simulacija

Slika 6.9 prikazuje ocjene prometa klijenata Alice i Bob, njihove pripadne reputacije i propusnost. Iako je srednja vrijednost ocjene Bobovog prometa manja, reputacije im se, kao i propusnost, poklapaju. To se dogodilo jer relativno velik faktor pamćenja (lambda=0.9) umanjuje reagiranje na trenutne promjene ponašanja.



Slika 6.9. Nagrađivanje dobrog ponašanja klijenta. Ulazni čvor ima više prethodnika

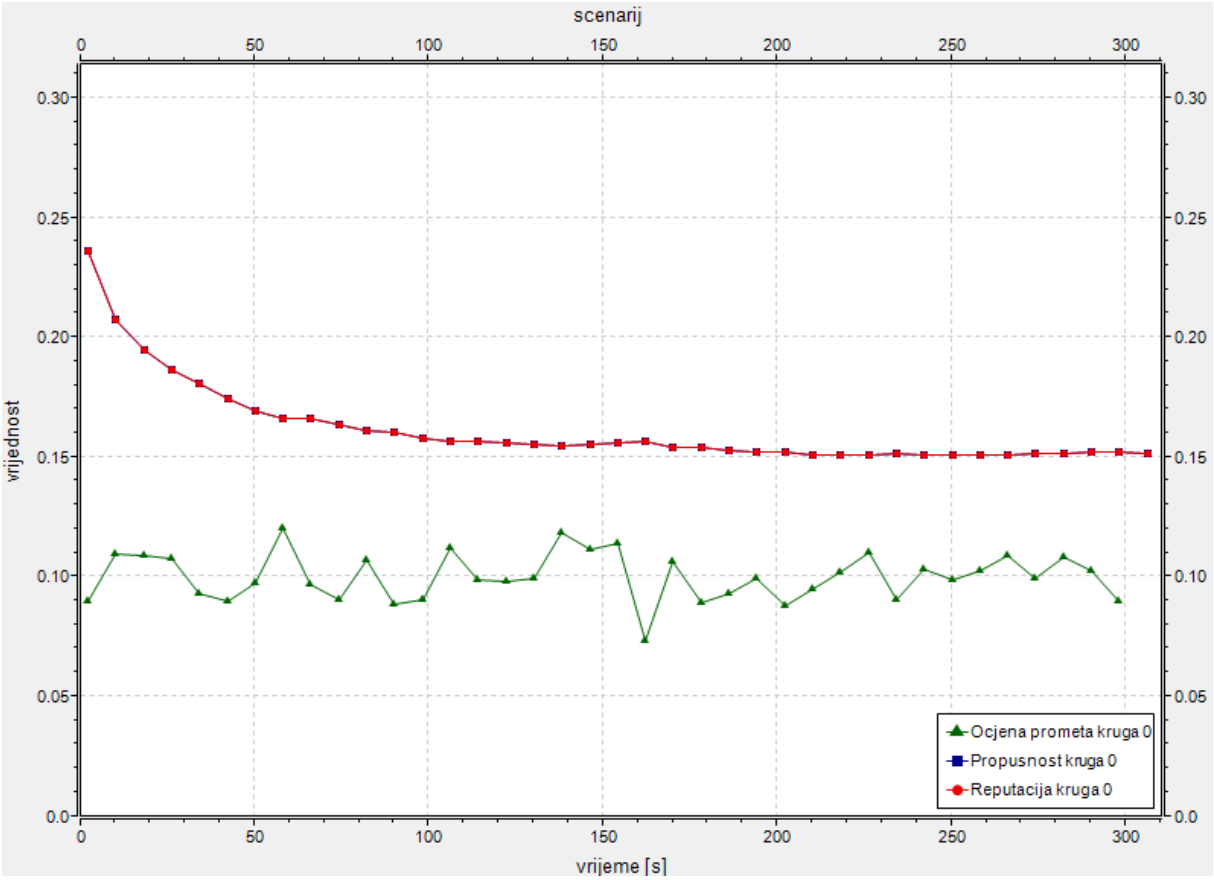
Slika 6.10 prikazuje simulaciju istog primjera uz promijenjen faktor pamćenja (lambda=0.3). Vidljivo je da uz manji faktor pamćenja, reputacija više prati trenutne promjene u ponašanju klijenta pa Alice ima i veću prosječnu reputaciju.



Slika 6.10. Nagrađivanje dobrog ponašanja klijenta uz faktor pamćenja 0.3. Ulazni čvor ima više prethodnika

3. simulacija

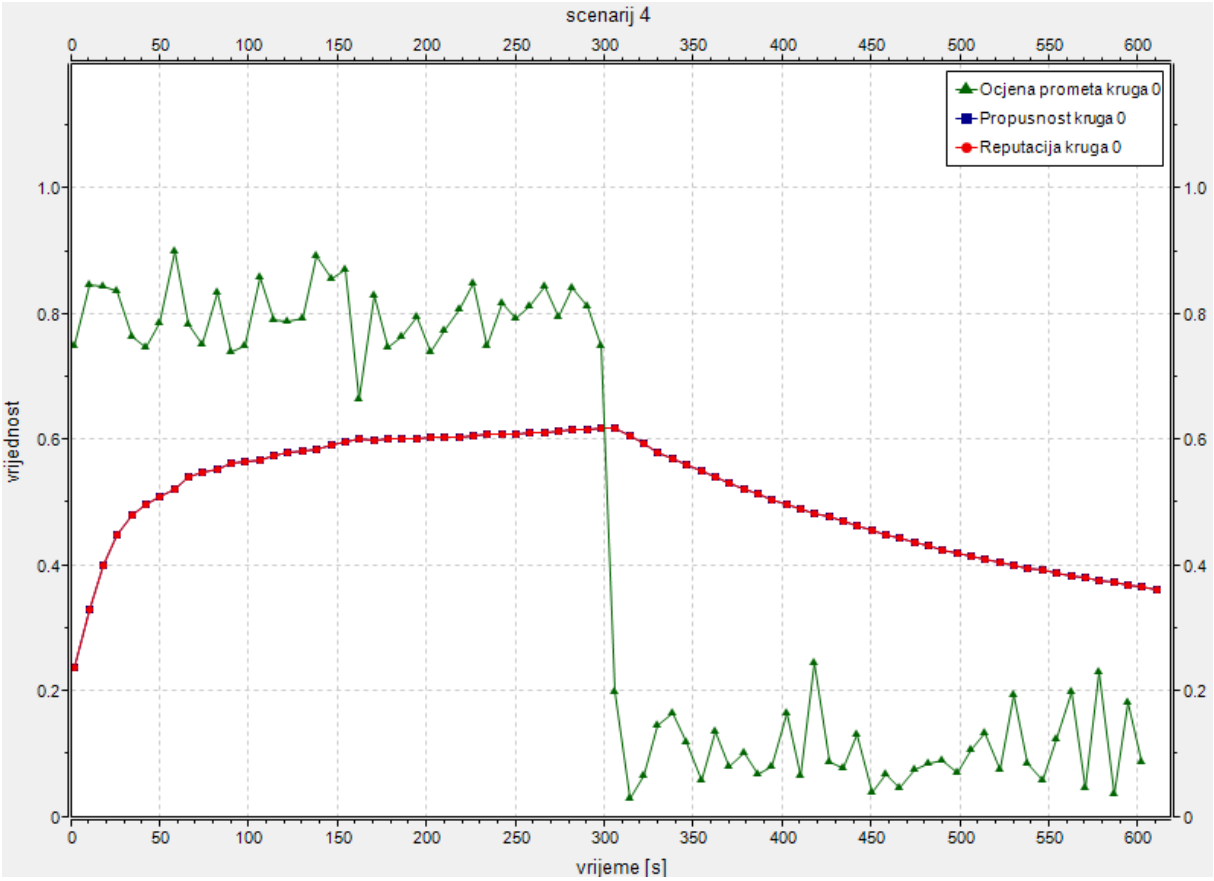
Slika 6.11 prikazuje opadanje reputacije klijenta uslijed lošeg ponašanja. Ovdje je zanimljivo usporediti vrijednost ažurirane reputacije s vrijednošću reputacije koju klijent ima uslijed zastarijevanja. Krug trajanja 5 minuta klijent završava s reputacijom 0.15, a zastarijevanje za to vrijeme je 0.986, odnosno vrijednost reputacije se smanjuje sa 0.2358 na 0.2325. Posve je očito da će klijent odbaciti smanjenu reputaciju i prihvatiti zastarijevanje.



Slika 6.11. kažnjavanje lošeg ponašanja klijenta

4. simulacija

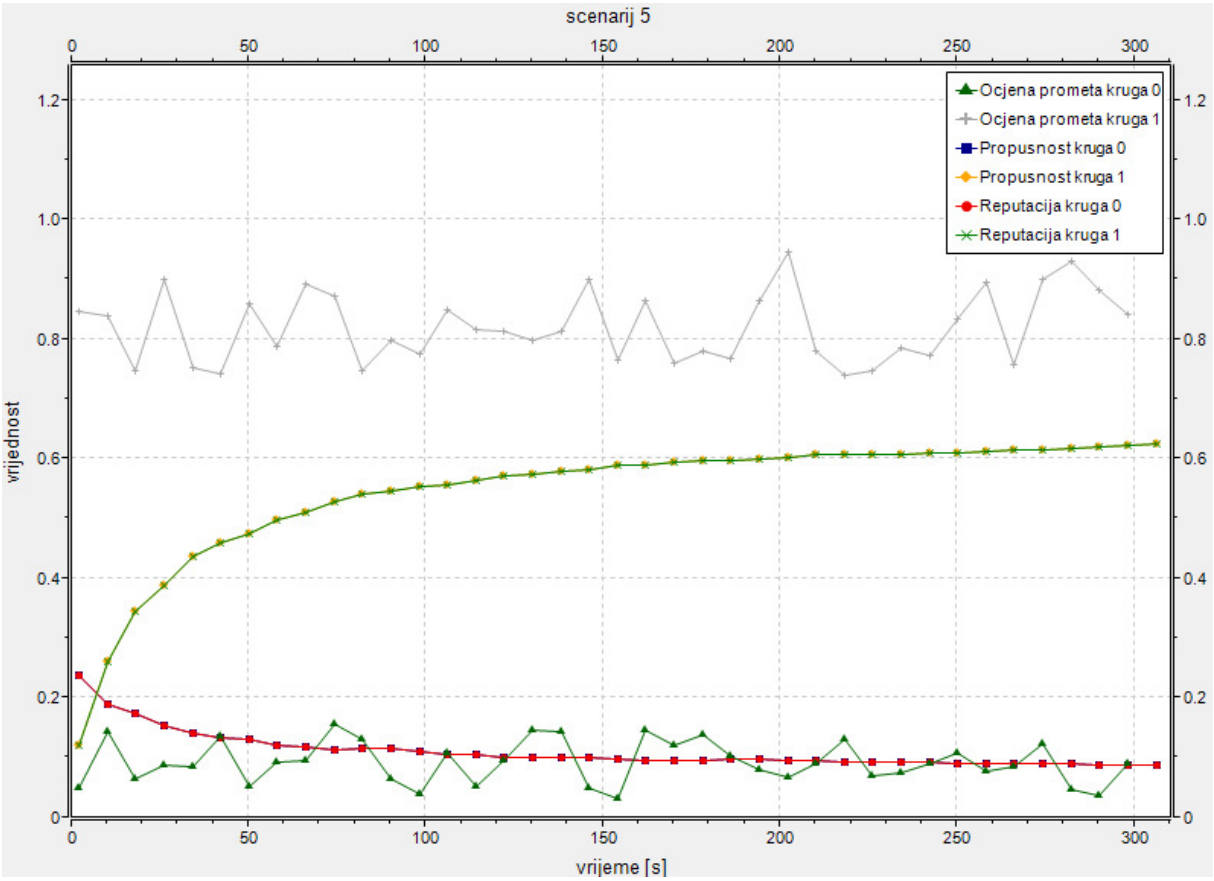
Slika 6.11 prikazuje klijenta koji gradi reputaciju prvih 5 minuta, a sljedećih 5 minuta koristi stečenu reputaciju za zlonamjerno ponašanje. Nakon nagle promjene ponašanja, reputacija krene iz monotonog rasta u monotoni pad.



Slika 6.12. Prilagodljivo ponašanje pošiljatelja u istom krugu

5. simulacija

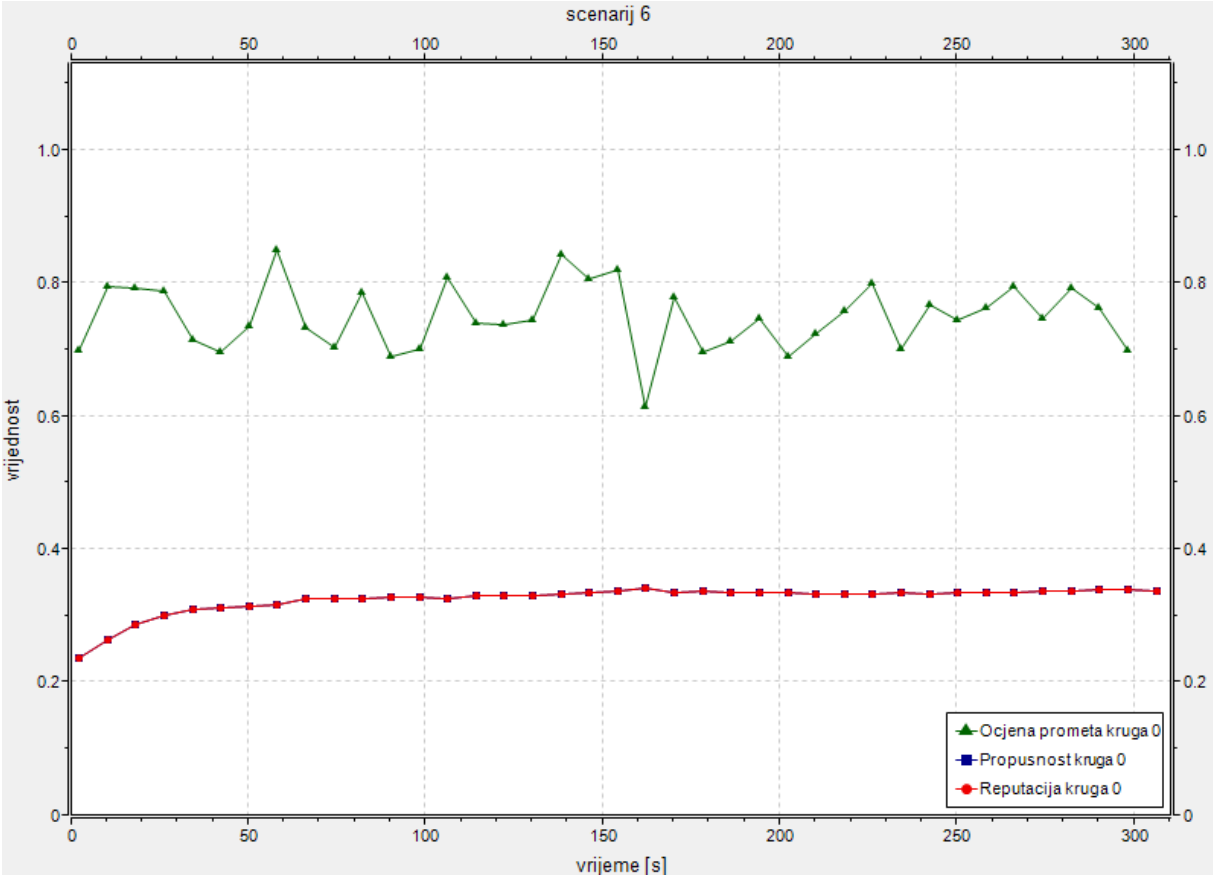
Slika 6.13 prikazuje klijenta koji provodi dva različita ponašanja u dva različita kruga. Predaje certificiranu reputaciju ulaznom čvoru prvog kruga i počinje zloupotrebljavati krug. Kada predoči istu reputaciju drugom krugu, u listi trenutno korištenih certifikata, imenički poslužitelj pronalazi sažetak certifikata i smanjuje vrijednost reputacije. Zato je početna vrijednost reputacije u drugom krugu manja. Drugi krug klijent koristi za građenje reputacije.



Slika 6.13. Prilagodljivo ponašanje pošiljatelja u dva kruga

6. simulacija

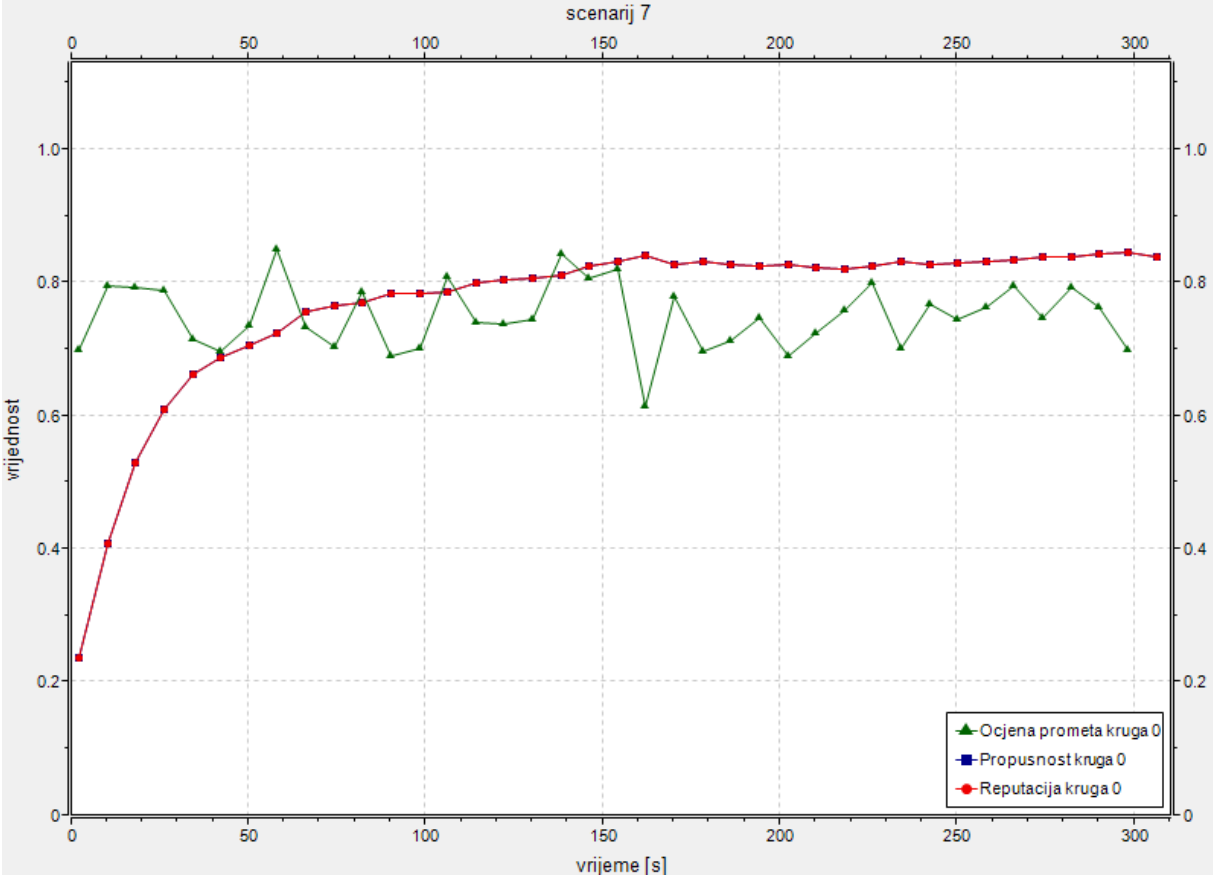
Slika 6.14 prikazuje nesrazmjer ponašanja klijenta i njegove reputacije. Ocjenu prometa namjerno umanjuje ulazni čvor.



Slika 6.14. Zlonamjerni ulazni čvor

7. simulacija

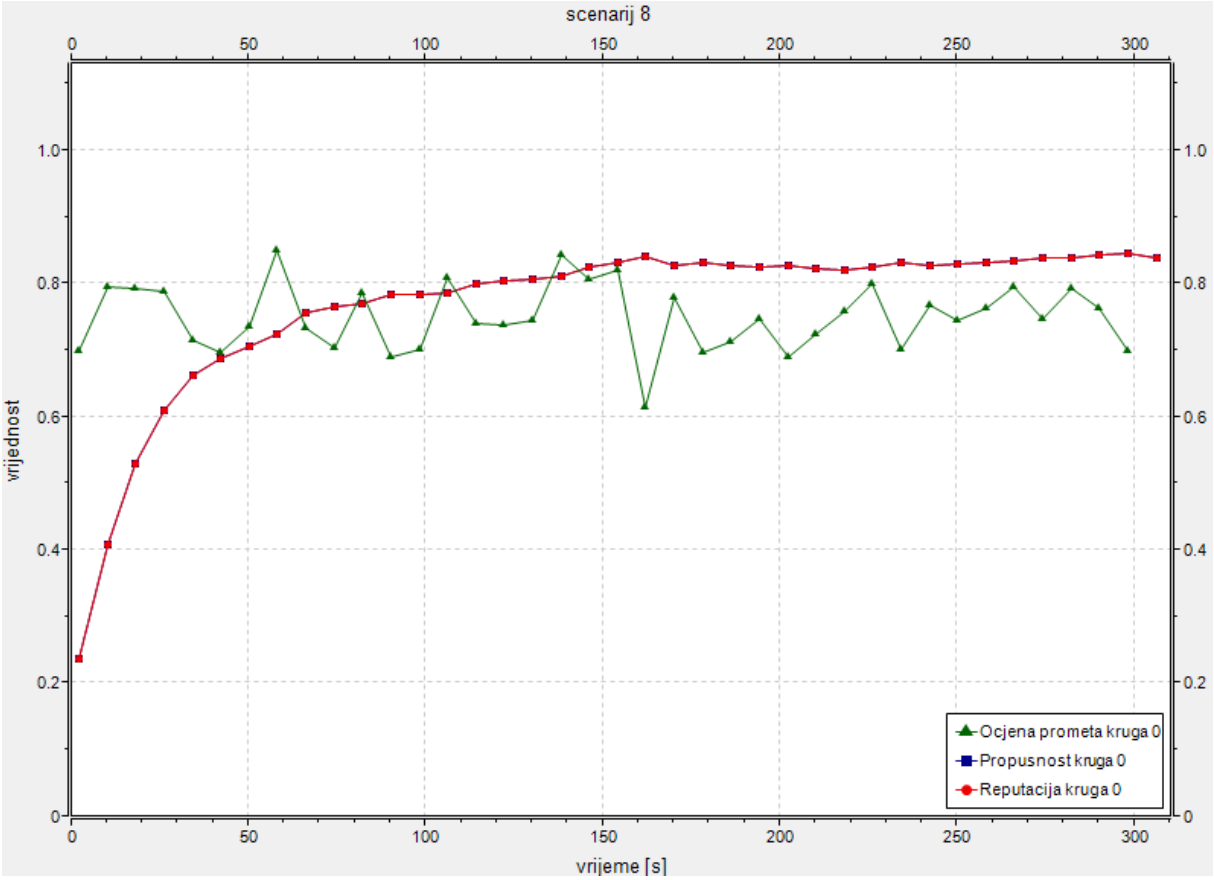
Slika 6.15 prikazuje nerealno visoki rast reputacije klijenta s obzirom na njegovo ponašanje zbog suradnje s ulaznim čvorom. U ovoj simulaciji ocjena prometa se uvećava za 50% iako ništa ne sprječava ulazni čvor u davanju maksimalne vrijednosti reputacije.



Slika 6.15. Suradnja ulaznog čvora i klijenta

8. simulacija

   Slika 6.16, slično kao i u prethodnom scenariju, prikazuje nerealno visoki rast reputacije klijenta s obzirom na njegovo ponašanje. U ovoj simulaciji klijent surađuje s izlaznim čvorom koji isto uvećava ocjene za 50%. Izlazni čvor je ipak manje efikasan u umjetnom građenju reputacije od ulaznog čvora zbog ponderiranja ocjena reputacijama izlaznog i srednjeg čvora.



Slika 6.16. Suradnja klijenta i izlaznog čvora

6.3. Osvrt na rezultate simulacija

Rezultati simulacija služe kao potvrda koncepta. Simulirana je mreža s minimalnim brojem korisnika i usmjernika, a dužina trajanja simulacije je reda veličine trajanja jednog kruga. Nije implementiran algoritam izabiranja čvorova kruga, već su za svakog klijenta unaprijed definirani čvorovi kruga i njihovi položaji u krugu. Reputacije usmjernika su također fiksirane i nije simulirano građenje reputacija usmjernika od nule.

Simulacije bi se mogle poboljšati uvođenjem većeg broja korisnika i usmjernika, te implementiranjem algoritma za biranje čvorova kako bi se dinamika mreže mogla promatrati u duljem vremenskom razdoblju. To bi omogućilo i simuliranje pametnijih strategija korisnika i usmjernika u ostvarivanju svojih legitimnih ili zlonamjernih ciljeva. Mreža bi se mogla simulirati iz početnih uvjeta i bilo bi zanimljivo doznati koja sve ravnotežna stanja

može zauzeti upotrebom reputacijskog sustava. Rezultati takvih simulacija bi se mogli iskoristiti za daljnje poboljšanje parametara, ali i protokola reputacijskog sustava.

Proširenjem simuliranog protokola na stvarni opseg bi se moglo izračunati mrežno opterećenje koje uvodi reputacijski sustav. Kako bi se izračunalo opterećenje imeničkih poslužitelja, trebalo bi simulirati i opterećenje računalnih resursa koje proizlazi iz operacija kriptografije javnog ključa i mrežni promet koji proizlazi iz sudjelovanja imeničkih poslužitelja u fazama izgradnje i zatvaranja krugova. Rezultati tih simulacija bi se mogli upotrijebiti za uvođenje određenog broja predposlužitelja ili specijaliziranih reputacijskih poslužitelja.

Za još kvalitetniju simulaciju mogu se iskoristiti uzorci stvarnog prometa mreže Tor –Tor metrics.

7. Zaključak

U dijelovima svijeta gdje ne postoji sloboda govora, a pogotovo gdje gotovo da ne postoji sloboda mišljenja, raste potreba za anonimnošću. Na Internetu je prikupljanje informacija o pojedincima sve češće i obilnije pa i osobe u razvijenim demokracijama žele sačuvati dijelove života privatnim, odnosno tajnim. Anonimnost i tajnost su stvarne potrebe modernog društva. Danas ne postoji općeprihvaćeni Internet standard koji garantira anonimnost, već postoje pojedine implementacije koje se još uvijek razvijaju. Jedan od popularnih sustava anonimnosti je i Tor. Anonimnost lako oslobađa od odgovornosti što mnogi zlonamjernici iskorištavaju, dovodeći funkcioniranje anonimnih sustava u pitanje. Jedan od načina kojim se pokušavaju smanjiti zloupotrebe u raspodijeljenim mrežnim sustavima su reputacijski sustavi. Međutim, reputacije su vezane za identitet pa je poseban izazov implementirati reputacije u anonimnom sustavu. Model koji se predlaže u ovom radu koristi certificiranu reputaciju koju klijent drži kod sebe i svojevoljno ju predaje ako želi koristiti sve dobrobiti anonimnog sustava. Jedini entitet kojem otkriva svoj privremeni identitet korišten u certificiranoj reputaciji je ulazni čvor, koji ionako direktno komunicira s klijentom. Ocjena ponašanja, odnosno prometa, klijenta se prenosi mrežom bez znanja o tome čiji promet se ocjenjuje.

Princip reputacijskog sustava u mreži Tor, temeljen na beta reputacijskom sustavu, je provjeren u simulacijskom okruženju OMNeT++ na jednostavnim primjerima. Rezultati simuliranja su potvrdili postavljene pretpostavke u ranije definiranim scenarijima. Nije pokazano funkcioniranje reputacijskog sustava u simulaciji sa stvarnim prometom. Funkcioniranje reputacijskog sustava se oslanja na efikasnost čvorova u detekciji lošeg ponašanja, a to je izvan opsega ovog rada. Ostaje upitna i mogućnost imeničkih poslužitelja u provođenju operacija kriptografije javnog ključa potrebnih u protokolu reputacijskog sustava. Idući korak je šira diskusija u stručnoj javnosti o mogućnosti proširenja protokola Tor i dublja analiza eventualnih napada koji ovaj sustav otvara.

U smjernicama budućeg razvoja Tora [91] uključena su razmišljanja o sustavima motiviranja (engl. incentives), što su zapravo reputacijski sustavi. Ovaj rad predstavlja jednu takvu mogućnost.

8. Literatura

[1] Alan Paller: Top Ten Cyber Security Menaces for 2008. URL: http://www.sans.org/press/top10menaces08.php (2008)

[2] Michael J. A. Berry, Gordon S. Linoff, *Data mining techniques for marketing, sales, and customer support*. John Wiley, 1997.

[3] Andreas Pfitzmann, Marit Hansen: Privacy and Data Security, TU Dresden. URL: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf (2011)

[4] Joris Claessens, Bart Preneel, Joos Vandewalle, "Solutions for Anonymous Communication on the Internet". *Proceedings of the International Carnahan Conference on Security Technology*, 1999.

[5] Heiko Tillwick, Martin Olivier, "Towards a framework for connection anonymity". *Proceedings of SAICSIT*, 2005.

[6] Michael G. Reed, Paul F. Syverson, David M. Goldschlag, "Anonymous Connections and Onion Routing". *Proceedings of International workshop on design issues in anonymity and unobservability*, 2001.

[7] S. Kent, R. Atkinson: Security Architecture for the Internet Protocol. URL: http://www.ietf.org/rfc/rfc2401.txt (1998)

[8] Alessandro Acquisti, Roger Dingledine, Paul Syverson, "On the Economics of Anonymity". *Financial Cryptography*, 2003.

[9] Jean-Francois Raymond, "Traffic analysis: protocols, attacks, design issues, and open problems". *International workshop on Designing privacy enhancing technologies: design issues in anonymity and unobservability* , 2000.

[10] David Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability". *Journal of Cryptology*, 1988.

[11] David Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms". *Communications of the ACM*, vol. 24, no. 2, 1981.

[12] Steven J. Murdoch, George Danezis, "Low-Cost Traffic Analysis of Tor". *IEEE Symposium on Security and Privacy*, 2005.

[13] Whitfield Diffie, Susan Landau, *Privacy On the Line: The Politics of Wiretapping*. MIT press, 1998.

[14] Paul Syverson, Gene Tsudik, Michael Reed, Carl Landwehr, "Towards an Analysis of Onion Routing Security". *International workshop on Designing privacy enhancing technologies: design issues in anonymity and unobservability* , 2001.

[15] Chi Bun Chan, Christina Nita-Rotaru: Anonymity Systems and Traffic Analysis. URL: http://homes.cerias.purdue.edu/~crisn/courses/cs603_Spring_2006/cs603_lect22.pdf

[16] C. Gülcü, G. Tsudik, "Mixing Email with Babel". *1996 Symposium on Network and Distributed System Security*, San Diego, 1996.

[17] L. Cottrell: Mixmaster and Remailer Attacks. URL: http://www.dia.unisa.it/professori/ads/corso-security/www/NEW/remailer-essay (2011, July)

[18] George Danezis, Roger Dingledine, Nick Mathewson: Mixminion: Design of a Type III Anonymous Remailer Protocol. URL: http://mixminion.net/minion-design.pdf

[19] Anonymizer. URL: http://anonymizer.com/

[20] Roger Dingledine, "Tor: an anonymous internet communication system".

[21] Roger Dingledine, Nick Mathewson, Paul Syverson, "Tor: The Second-Generation Onion Router". *SSYM'04 Proceedings of the 13th conference on USENIX Security Symposium*, 2004.

[22] Oliver Berthold, Hannes Federrath, Stefan Köpsell, "Web MIXes: A system for anonymous and unobservable Internet access". *Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*, 2000.

[23] Wei Dai: Post to Cypherpunks mailing list. URL: http://www.freehaven.net/anonbib/cache/pipenet10.html (1995)

[24] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner, "ISDN-mixes: Untraceable communication with very small bandwidth overhead". *GI/ITG Conference on Communication in Distributed Systems*, 1991.

[25] Michael J. Freedman, Robert Morris, "Tarzan: a peer-to-peer anonymizing network layer". *CCS '02 Proceedings of the 9th ACM conference on Computer and communications security*, 2002.

[26] Marc Rennhard, Bernhard Plattner, "Practical Anonymity for the Masses with MorphMix" in *Financial Cryptography*., 2004.

[27] Aviel D. Rubin, Michael K. Reiter, "Crowds: anonymity for Web transactions". *ACM Transactions on Information and System Security (TISSEC)*, 1998.

[28] Brian Neil Levine, Clay Shields, "Hordes: a multicast based protocol for anonymity". *Journal of Computer Security*, 2002.

[29] Sharad Goel, Mark Robson, Milo Polte, Emin Sirer, "Herbivore: A Scalable and Efficient Protocol for Anonymous Communication" Cornell University, Technical Report 2003.

[30] Rob Sherwood, Bobby Bhattacharjee, Aravind Srinivasan, "P5: A Protocol for Scalable Anonymous Communication". *IEEE Symposium on Security and Privacy*, 2002.

[31] Philippe Boucher, Adam Shostack, Ian Goldberg, "Freedom systems 2.0 architecture" Zero Knowledge Systems, Inc., White Paper 2000.

[32] Zach Brown, "Cebolla: Pragmatic IP Anonymity". *Ottawa Linux Symposium*, 2002.

[33] Marc Rennhard, Sandro Rafaeli, Laurent Mathy, Bernhard Plattner, David Hutchiso, "Analysis of an Anonymity Network for Web Browsing". *IEEE 7th Intl. Workshop on Enterprise Security*, 2002.

[34] Adam Back, Ulf Möller, Anton Stiglic, "Traffic Analysis Attacks and Trade-Offs in Anonymity Providing Systems". *IHW '01 Proceedings of the 4th International Workshop on Information Hiding*, 2001.

[35] Tor's extensions to the SOCKS protocol. URL: https://gitweb.torproject.org/torspec.git?a=blob_plain;hb=HEAD;f=socks-extensions.txt

[36] Roger Dingledine, Nick Mathewson: Tor Protocol Specification. URL: https://gitweb.torproject.org/torspec.git?a=blob_plain;hb=HEAD;f=tor-spec.txt (2010)

[37] Frank Dabek, M. Frans Kaashoek, David Karger, Robert Morris, Ion Stoica, "Wide-area cooperative storage with CFS". *18th ACM Symposium on Operating Systems Principles*, 2001.

[38] Matthew Wright, Micah Adler, Brian N. Levine, Clay Shields, "Defending Anonymous Communications Against Passive Logging Attacks". *SP '03 Proceedings of the 2003 IEEE Symposium on Security and Privacy*, 2003.

[39] p2pnet.net News: URL: http://www.p2pnet.net/story/11279

[40] Matthew K. Wright, Micah Adler, Brian Neil Levine, "The Predecessor Attack: An Analysis of a Threat to Anonymous Communications Systems". *ACM Transactions on Information and System Security*, 2004.

[41] Roger Dingledine, Nick Mathewson, Paul Syverson: Challenges in deploying low-latency anonymity. URL: http://www.onion-router.net/Publications/challenges.pdf (2005)

[42] Longy O. Anyanwu, Jared Keengwe, Gladys Arome, "Anonymity Leakage Reduction in Network Latency". *International Journal of Multimedia and Ubiquitous Engineering*, 2010.

[43] Brian N. Levine, Michael K. Reiter, Chenxi Wang, Matthew Wright, "Timing Attacks in Low-Latency Mix Systems". *Financial Cryptography*, 2004.

[44] Damon Mccoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, Douglas Sicker, "Shining Light in Dark Places: Understanding the Tor Network". *Privacy Enhancing Technologies Symposium*, 2008.

[45] Kim Zetter: Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise. URL: http://www.wired.com/politics/security/news/2007/09/embassy_hacks?currentPage=1 (2007)

[46] Mike Perry: TorFlow - Tor Network Analysis. URL: http://fscked.org/projects/torflow

[47] Torscanner. URL: http://code.google.com/p/torscanner/ (2010)

[48] Tor wiki. URL: https://trac.torproject.org/projects/tor/wiki/doc/badRelays (2011)

[49] Electronic Frontier Foundation: Legal FAQ for Tor Relay Operators. URL: https://www.torproject.org/eff/tor-legal-faq.html.en (2005)

[50] Stjepan Gros, Marko Salkic, Ivan Sipka, "Protecting TOR exit nodes from abuse". *MIPRO, 2010 Proceedings of the 33rd International Convention* , 2010.

[51] The Honeynet Project. URL: http://old.honeynet.org/index.html (2010)

[52] Patrick P. Tsang, Apu Kapadia, Sean W. Smith, Cory Cornelius, "Nymble: Blocking Misbehaving Users in Anonymizing Networks". *IEEE Transactions on Dependable and Secure Computing*, 2009.

[53] Kevin Bauer, Damon McCoy, Dirk Grunwald, Tadayoshi Kohno, Douglas Sicker, "Low-Resource Routing Attacks Against Tor". *WPES '07 Proceedings of the 2007 ACM workshop on Privacy in electronic society*, 2007.

[54] Tsuen-Wan "Johnny" Ngan, Roger Dingledine, Dan S. Wallach, "Building Incentives into Tor" Department of Computer Science, Rice University, 2008.

[55] Roger Dingledine, Paul Syverson, "Reliable MIX Cascade Networks through Reputation". *Financial Cryptography*, 2002.

[56] Tsuen-Wan "Johnny" Ngan, Dan S. Wallach, Peter Druschel, "Enforcing Fair Sharing of Peer-to-Peer Resources". *Peer-to-Peer Systems*, 2003.

[57] Atul Singh, Tsuen-Wan "Johnny" Ngan, Peter Druschel, Dan Wallach, "Eclipse Attacks on Overlay Networks: Threats and Defenses". *IEEE Infocom* , 2006.

[58] Robin Snader, Nikita Borisov, "A Tune-up for Tor: Improving Security and Performance in the Tor Network". *NDSS Symposium 2008*, 2008.

[59] Andrew Lewman: Tor Press and Media Information. URL: https://www.torproject.org/press/2009-03-12-performance-roadmap-press-release.html.en (2009, Mar.)

[60] Elli Androulaki, Mariana Raykova, Shreyas Srivatsan, Angelos Stavrou, Steven M. Bellovin, "PAR: Payment for Anonymous Routing". *PETS '08 Proceedings of the 8th international symposium on Privacy Enhancing Technologies* , 2008.

[61] Silvio Micali, Ronald L. Rivest, "Micropayments Revisited". *CT-RSA '02 Proceedings of the The Cryptographer's Track at the RSA Conference on Topics in Cryptology*, 2002.

[62] David Chaum, "Blind signatures for untraceable payments". *Advances in Cryptology - Crypto '82*, 1982.

[63] David Chaum, Amos Fiat, Moni Naor, "Untraceable Electronic Cash". *Proceedings on Advances in cryptology*, 1990.

[64] Jordi Sabater, Carles Sierra, "Review on Computational Trust and Reputation Models". *Artificial Intelligence Review*, 2005.

[65] P. Resnickand, R. Zeekhauserand, E. Friedman, K. Kuwabara, "Reputation systems". *Communications of the ACM*, 2000.

[66] L. Mui, M. Mohtashemi, A. Halberstadt, "A Computational Model of Trust and Reputation", 2002.

[67] Michael Kinateder, Kurt Rothermel, "Architecture and Algorithms for a Distributed Reputation System". *iTrust'03 Proceedings of the 1st international conference on Trust management*, 2003.

[68] B. Esfandiari, S. Chandrasekharan, "On how agents make friends: Mechanisms for trust acquisition". *Fourth Workshop on Deception, Fraud and Trust in Agent Societies*, 2001.

[69] Diego Gambetta, "Trust: Making and Breaking Co-operative Relations", pp. 213-237, 1990.

[70] Trung Dong Huynh, Nicholas R. Jennings, Nigel R. Shadbolt, "Certified reputation: how an agent can trust a stranger". *International Conference on Autonomous Agents*, 2006.

[71] Paul Resnick, Richard Zeckhauser, "Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system". *Advances in Applied Microeconomics*, 2002.

[72] Runfang Zhou, Kai Hwang, "PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing". *IEEE Transactions on Parallel and Distributed Systems*, 2007.

[73] Siddharth Maini, "A Survey Study on Reputation-Based Trust Management" 2008.

[74] Sepandar D. Kamvar, Mario T. Schlosser, Hector Garcia-Molina, "The EigenTrust Algorithm for Reputation Management in". *WWW '03 Proceedings of the 12th international conference on World Wide Web*, 2003.

[75] Clay Shirky: Clay Shirky's Writings About the Internet. URL: http://shirky.com/writings/powerlaw_weblog.html (2003)

[76] Aameek Singh, Ling Liu, "TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P Systems". *Peer-to-Peer Computing, 2003. (P2P 2003)*, 2003.

[77] V. Scarlata, Brian Neil Levine, Clay Shields, "Responder Anonymity and Anonymous Peer-to-Peer File Sharing". *Network Protocols Ninth International Conference on ICNP*, 2001.

[78] Minaxi Gupta, Paul Judge, Mostafa Ammar, "A reputation system for peer-to-peer networks". *NOSSDAV '03 Proceedings of the 13th international workshop on Network and operating systems support for digital audio and video*.

[79] Giorgos Zacharia, "Trust management through reputation mechanisms". *Applied*

Artificial Intelligence, vol. 14, pp. 881--907, 2000.

[80] Audun Jøsang, Roslan Ismail, "The Beta Reputation System". *15th Bled Electronic Commerce Conference*.

[81] Li Lu et al., "Pseudo Trust: Zero-Knowledge Based Authentication in Anonymous Peer-to-Peer Protocols". *Parallel and Distributed Processing Symposium, 2007. IPDPS 2007. IEEE International*, 2007.

[82] Chrysanthos Dellarocas, "The Design of Reliable Trust Management Systems for Electronic Trading Communities" Sloan School of Management, 2000.

[83] John R. Douceur, "The Sybil Attack". *IPTPS '01 Revised Papers from the First International Workshop on Peer-to-Peer Systems* , 2002.

[84] Brian Neil Levine, Clay Shields, N. Boris Margolin, "A Survey of Solutions to the Sybil Attack" University of Massachusetts Amherst, 2006.

[85] H Yu, "SybilGuard: A new defense against sybil attacks". *ACM SIGCOMM 2006 Conference*, 2006.

[86] Eric Friedman Alice Cheng, "Sybilproof Reputation Mechanisms". *P2PECON '05 Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems*, 2005.

[87] Roger Dingledine, Nick Mathewson, Paul Syverson, "Reputation in P2P Anonymity Systems". *In Workshop on Economics of Peer-to-Peer Systems*, 2003.

[88] Prashant Dewan, Partha Dasgupta, "P2P Reputation Management Using Distributed Identities and Decentralized Recommendation Chains". *IEEE Transactions on Knowledge and Data Engineering*, vol. 22, no. 7, 2010.

[89] URL: http://www.omnetpp.org/

[90] National Science Foundation: Tor Metrics Portal. URL: https://metrics.torproject.org/ (2011, June)

[91] Tor Incentives Design Brainstorms. URL: https://svn.torproject.org/svn/tor/branches/tor-0_1_1-patches/doc/incentives.txt

[92] Eibe Frank, Ian Witten, *Data Mining: Practical Machine Learning Tools and Techniques*, 3rd ed. San Francisco Morgan Kaufmann, 2011.

[93] Kevin Bauer et al., "On the Optimal Path Length for Tor", 2010. URL: petsymposium.org/2010/papers/hotpets10-Bauer.pdf

Dodatak A: konfiguracije simulacija

U simulacijama je korištena datoteka `omnetpp.ini` sljedećeg izgleda:

```
[General]

[Config tc1]
network=tor_rep.Tc1
Tc1.or[*].today = "10.1.2011 18:30:39"
Tc1.alice.reputation = xmldoc("clients.xml",
"//*[@name='alice']/reputation")
Tc1.alice.circuits = xmldoc("clients.xml", "//*[@name='alice']/circuits")
Tc1.or[*].reputation = 0.9
Tc1.**.timeEvalInterval = 8s
Tc1.or[*].lambda = 6h
Tc1.or[*].betaLambda = 0.9 #less is more forgetful

[Config tc2]
network=tor_rep.Tc2
Tc2.or[*].today = "10.1.2011 16:30:00"
Tc2.alice.reputation = xmldoc("clients.xml",
"//*[@name='alice']/reputation")
Tc2.alice.circuits = xmldoc("clients.xml", "//*[@name='alice']/circuits")
Tc2.bob.reputation = xmldoc("clients.xml", "//*[@name='bob']/reputation")
Tc2.bob.circuits = xmldoc("clients.xml", "//*[@name='bob']/circuits")
Tc2.or[*].reputation = 0.9
Tc2.**.timeEvalInterval = 8s
Tc2.or[*].lambda = 6h
Tc2.or[*].betaLambda = 0.3 #less is more forgetful

[Config tc3]
network=tor_rep.Tc3
Tc3.or[*].today = "10.1.2011 18:30:39"
Tc3.badAlice.reputation = xmldoc("clients.xml",
"//*[@name='badAlice']/reputation")
Tc3.badAlice.circuits = xmldoc("clients.xml",
"//*[@name='badAlice']/circuits")
Tc3.or[*].reputation = 0.9
Tc3.**.timeEvalInterval = 8s
Tc3.or[*].lambda = 6h
Tc3.or[*].betaLambda = 0.9 #less is more forgetful

[Config tc4]
network=tor_rep.Tc4
Tc4.or[*].today = "10.1.2011 18:30:39"
Tc4.smartAlice.reputation = xmldoc("clients.xml",
"//*[@name='smartAlice']/reputation")
Tc4.smartAlice.circuits = xmldoc("clients.xml",
"//*[@name='smartAlice']/circuits")
Tc4.or[*].reputation = 0.9
Tc4.**.timeEvalInterval = 8s
Tc4.or[*].lambda = 6h
Tc4.or[*].betaLambda = 1 #less is more forgetful

[Config tc5]
network=tor_rep.Tc5
Tc5.or[*].today = "10.1.2011 18:30:39"
Tc5.twoFaceAlice.reputation = xmldoc("clients.xml",
"//*[@name='twoFaceAlice']/reputation")
```

```
Tc5.twoFaceAlice.circuits = xmldoc("clients.xml",
"//*[@name='twoFaceAlice']/circuits")
Tc5.or[*].reputation = 0.9
Tc5.**.timeEvalInterval = 8s
Tc5.or[*].lambda = 6h
Tc5.or[*].betaLambda = 1 #less is more forgetful

[Config Tc6]
network=tor_rep.Tc6
Tc6.or[*].today = "10.1.2011 18:30:39"
Tc6.alice.reputation = xmldoc("clients.xml",
"//*[@name='alice']/reputation")
Tc6.alice.circuits = xmldoc("clients.xml", "//*[@name='alice']/circuits")
Tc6.or[*].reputation = 0.9
Tc6.**.timeEvalInterval = 8s
Tc6.or[*].lambda = 6h
Tc6.or[*].betaLambda = 0.9 #less is more forgetful
Tc6.or[0].cheating = 0.5

[Config Tc7]
network=tor_rep.Tc7
Tc7.or[*].today = "10.1.2011 18:30:39"
Tc7.alice.reputation = xmldoc("clients.xml",
"//*[@name='alice']/reputation")
Tc7.alice.circuits = xmldoc("clients.xml", "//*[@name='alice']/circuits")
Tc7.or[*].reputation = 0.9
Tc7.**.timeEvalInterval = 8s
Tc7.or[*].lambda = 6h
Tc7.or[*].betaLambda = 0.9 #less is more forgetful
Tc7.or[0].cheating = 1.5

[Config Tc8]
network=tor_rep.Tc8
Tc8.or[*].today = "10.1.2011 18:30:39"
Tc8.alice.reputation = xmldoc("clients.xml",
"//*[@name='alice']/reputation")
Tc8.alice.circuits = xmldoc("clients.xml", "//*[@name='alice']/circuits")
Tc8.or[*].reputation = 0.9
Tc8.**.timeEvalInterval = 8s
Tc8.or[*].lambda = 6h
Tc8.or[*].betaLambda = 0.9 #less is more forgetful
Tc8.or[2].cheating = 1.5
```

Korištena je i `clients.xml` datoteka sljedećeg izgleda:

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
      <client name="alice">
            <reputation>
                  <value>0.5</value>
                  <owner-id>alice</owner-id>
                  <signer-id>dir</signer-id>
                  <timestamp>10.1.2011 14:00:00</timestamp>
            </reputation>
            <circuits>
                  <circuit>
                              <node>or[0]</node>
```

```
                        <node>or[1]</node>
                        <node>or[2]</node>
                  <behavior>
                        <mean>0.75</mean>
                        <stddev>0.05</stddev>
                        <time-limit>5 min</time-limit>
                        <target-reputation>0.7</target-reputation>
                  </behavior>
            </circuit>
      </circuits>
</client>
<client name="bob">
      <reputation>
            <value>0.5</value>
            <owner-id>bob</owner-id>
            <signer-id>dir</signer-id>
            <timestamp>10.1.2011 14:00:00</timestamp>
      </reputation>
      <circuits>
            <circuit>
                        <node>or[0]</node>
                        <node>or[3]</node>
                        <node>or[4]</node>
                  <behavior>
                        <mean>0.65</mean>
                        <stddev>0.05</stddev>
                        <time-limit>5 min</time-limit>
                        <target-reputation>0.7</target-reputation>
                  </behavior>
            </circuit>
      </circuits>
</client>
<client name="badAlice">
      <reputation>
            <value>0.5</value>
            <owner-id>badAlice</owner-id>
            <signer-id>dir</signer-id>
            <timestamp>10.1.2011 14:00:00</timestamp>
      </reputation>
      <circuits>
            <circuit>
                        <node>or[0]</node>
                        <node>or[1]</node>
                        <node>or[2]</node>
                  <behavior>
                        <mean>0.1</mean>
                        <stddev>0.01</stddev>
                        <time-limit>5 min</time-limit>
                  </behavior>
            </circuit>
      </circuits>
</client>
<client name="smartAlice">
      <reputation>
            <value>0.5</value>
            <owner-id>smartAlice</owner-id>
            <signer-id>dir</signer-id>
            <timestamp>10.1.2011 14:00:00</timestamp>
      </reputation>
      <circuits>
```

```
                  <circuit>
                        <node>or[0]</node>
                        <node>or[1]</node>
                        <node>or[2]</node>
                  <behavior>
                        <mean>0.8</mean>
                        <stddev>0.05</stddev>
                        <time-limit>5 min</time-limit>
                        <target-reputation>0.7</target-reputation>
                  </behavior>
                  <behavior>
                        <mean>0.1</mean>
                        <stddev>0.05</stddev>
                        <time-limit>5 min</time-limit>
                  </behavior>
            </circuit>
      </circuits>
</client>
<client name="twoFaceAlice">
      <reputation>
            <value>0.5</value>
            <owner-id>twoFaceAlice</owner-id>
            <signer-id>dir</signer-id>
            <timestamp>10.1.2011 14:00:00</timestamp>
      </reputation>
      <circuits>
            <circuit>
                  <node>or[0]</node>
                  <node>or[1]</node>
                  <node>or[2]</node>
            <behavior>
                  <mean>0.1</mean>
                  <stddev>0.05</stddev>
                  <time-limit>5 min</time-limit>
            </behavior>
            </circuit>
            <circuit>
                  <node>or[3]</node>
                  <node>or[4]</node>
                  <node>or[5]</node>
            <behavior>
                  <mean>0.8</mean>
                  <stddev>0.05</stddev>
                  <time-limit>5 min</time-limit>
            </behavior>
            </circuit>
      </circuits>
</client>
</root>
```