UNIVERZITET U NOVOM SADU
FAKULTET TEHNIČKIH NAUKA U NOVOM SADU

Miodrag Petković

PRILOG RAZVOJU METODE ZA DETEKCIJU NAPADA OMETANJEM USLUGE NA INTERNETU

DOKTORSKA DISERTACIJA

NOVI SAD
2018.

УНИВЕРЗИТЕТ У НОВОМ САДУ ●**ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА**
21000 НОВИ САД, Трг Доситеја Обрадовића 6

КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА

Редни број, **РБР**:	
Идентификациони број, **ИБР**:	
Тип документације, **ТД**:	Монографска документација
Тип записа, **ТЗ**:	Текстуални штампани материјал
Врста рада, **ВР**:	Докторска дисертација
Аутор, **АУ**:	Миодраг Петковић
Ментор, **МН**:	Проф. Др Илија Башичевић
Наслов рада, **НР**:	Прилог развоју методе за детекцију напада ометањем услуге на Интернету
Језик публикације, **ЈП**:	Српски
Језик извода, **ЈИ**:	Српски/Енглески
Земља публиковања, **ЗП**:	Република Србија
Уже географско подручје, **УГП**:	АП Војводина, Нови Сад
Година, **ГО**:	2018
Издавач, **ИЗ**:	ауторски репринт
Место и адреса, **МА**:	Факултет техничких наука, 21000 Нови Сад, Трг Доситеја
Физички опис рада, **ФО**: (поглавља/страна/ цитата/табела/слика/графика/прилога)	11/110/84/7/55/0/0
Научна област, **НО**:	Електротехничко и рачунарско инжењерство
Научна дисциплина, **НД**:	Рачунарска техника и рачунарске комуникације
Предметна одредница/Кључне речи, **ПО**:	Ентропија,напад ометањем услуге, фази логика,неуралне мреже, безбедност
УДК	
Чува се, **ЧУ**:	Библиотека Факултета техничких наука у Новом Саду
Важна напомена, **ВН**:	
Извод, **ИЗ**:	У овој докторској дисертацији предложен је и анализиран метод који комбинује примену ентропије одабраних обележја мрежног саобраћаја и Такаги-Сугено-Канг (TSK) неуро-фази модела у детекцији DoS напада. Ентропија је примењена јер омогућава детекцију широког спектра статистичких аномалија узрокованих DoS нападима док TSK неуро-фази модел даје додатни квалитет у коначном одређивању тачака почетка и краја напада повећавајући однос исправно и погрешно детектованих напада.
Датум прихватања теме, **ДП**:	27.1.2016.
Датум одбране, **ДО**:	

Чланови комисије,	Председник:	Др Мирослав Поповић, редовни професор	
	Члан:	Др Никола Теслић, редовни професор	
	Члан:	Др Мило Томашевић, редовни професор	Потпис ментора
	Члан:	Др Драган Кукољ, редовни професор	
	Члан, ментор:	Др Илија Башичевић, ванредни професор	

UNIVERSITY OF NOVI SAD ●**FACULTY OF TECHNICAL SCIENCES**
21000 NOVI SAD, Trg Dositeja Obradovića 6

KEY WORDS DOCUMENTATION

Accession number, **ANO**:		
Identification number, **INO**:		
Document type, **DT**:		Ph.D. thesis
Type of record, **TR**:		Monographic publication
Contents code, **CC**:		Textual printed document
Author, **AU**:		Miodrag Petković
Mentor, **MN**:		Prof. Dr Ilija Bašičević
Title, **TI**:		A contribution to the method for detection of denial of service attacks in Internet
Language of text, **LT**:		Serbian
Language of abstract, **LA**:		Serbian/English
Country of publication, **CP**:		Republic of Serbia
Locality of publication, **LP**:		AP Vojvodina, Novi Sad
Publication year, **PY**:		2018
Publisher, **PB**:		Author's reprint
Publication place, **PP**:		Faculty of Technical Sciences, 21000 Novi Sad, Trg Dositeja Obradovića 6
Physical description, **PD**: (chapters/pages/ref./tables/pictures/graphs/appendixes)		11/110/84/7/55/0/0
Scientific field, **SF**:		Electrical and Computer Engeneering
Scientific discipline, **SD**:		Computer Engineering and Communications
Subject/Key words, **S/KW**:		Entropy, denial-of -service, fuzzy logic, neural networks, security,
UC		
Holding data, **HD**:		Library of the Faculty of Technical Sciences, University of Novi Sad
Note, **N**:		
Abstract, **AB**:		In this thesis a new method for DoS attack detection is proposed. This method combines the use of entropy of some characteristic parameters of network traffic and Takagi-Sugeno-Kang (TSK) neuro-fuzzy model. Entropy has been used because it enables detection of wide spectar of network anomalies caused by DoS attacks, while TSK adds new value to final detection of the start and the end of an attack increasing ratio between true and false detections.
Accepted by the Scientific Board on, **ASB**:		27.1.2016.
Defended on, **DE**:		
Defended Board,	President:	Miroslav Popović, PhD, Full professor
	Member:	Nikola Teslić, PhD, Full professor
	Member:	Milo Tomašević, PhD, Full professor
	Member:	Dragan Kukolj, PhD, Full professor
	Member, Mentor:	Ilija Bašičević, PhD, Associate professor

Menthor's sign

Abstract

Denial-of-Service (DoS) attack is one of most frequent attacks on Internet today, and also an attack with the strongest impact onattacked target. The aim of the DoS attack is to prevent access of legitimate users to target system in order to get material gain or to damage reputation of the target system. Many methods for DoS attack detection, prevention and reaction have been developed so far, but DoS attcks technology is also developing. Thus, continual effort is needed in development of new methods of DoS detection.

The detection of denial of service (DoS) attacks based on internet traffic anomalies is a method which is general in nature and can detect unknown or zero-day attacks. One of the statistical characteristics used for this purpose is network traffic entropy. A sudden change in entropy may indicate a DoS attack. However, this approach often gives false positives, and this is the main obstacle to its wider deployment within network security equipment.

The goal of this thesis is to investigate the use of entropy of different parameters from TCP/IP headers with neuro-fuzzy model to achieve higher detection of the start and the end of DoS attacks and to decrease false detections at the same time.

In this thesis a new, two-step method for detection of DoS attacks is proposed. This method combines the approaches of network traffic entropy and the Takagi-Sugeno-Kang fuzzy system. In the first step, the detection process calculates the entropy distribution of some variables of network packets. In the second step, the Takagi-Sugeno-Kang fuzzy system (TSK-FS) method will be applied to these entropy values. The performance of the TSK-FS method will be compared with that of the typically used approach, in which cumulative sum (CUSUM) change point detection is applied directly to entropy time series. The results are expected to show that the TSK-FS DoS detector shows enhanced sensitivity and robustness in the detection process, achieving a high true-positive detection rate and a very low false-positive rate. As it is based on entropy, this combined method retains its generality and is capable of detecting various types of attack. An optimized variant of TSK-FS method, which can be implemented with fast hardware components will be proposed as a step to practical usage on network equipment.

Rezime

Napad ometanjem usluge (Denial of Service - *DoS*) je jedan od najzastupljenijih tipova napada na Internetu danas, i ujedno i tip napada sa velikim posledicama po napadnuti cilj. Cilj napada ometanjem usluge je onemogućavanje pristupa napadnutom sistemu od strane legitimnih korisnika, au svrhu pridobojanja materijalne koristi ili narušavanja ugleda ciljnog sistema. Do sada su razvijene su mnoge metode za detektovanje napada ometanjem usluge i odgovor na njih, ali s obzirom na da se napadi ometanjem usluge takodje razvijaju, potreban je stalan napor u usavršavanju tehnika za njihovu detekciju kao i odgovora na napade.

Detekcija napada ometanjem usluge zasnovana na anomalijama u saobraćaju na Internetu je metod koji je opšti po prirodi i može detektovati nepoznate napade kao i napade koji se prvi put dešavaju. Jedna od statističkih karakteristika mrežnog saobraćaja je i entropija. Iznenadna promena nivoa entropije može značiti početak napada ometanjemfusluge. Medjutim, taj pristup često daje lažne detekcije a upravo su lažne detekcije glavna prepreka široj primeni metoda zasnovanim na statističkim anomalijama u mrežnoj opremi.

Cilj istraživanja iz ove teze je da se primenom entropije odabranih parametara iz zaglavlja TCP paketa i Takagi-Sugeno-Kang neuro-fazi modela primenjenim na izmerenoj entropiji postigne veći stepen ispravnih detekcija početka i kraja napada kao i smanjen stepen pogrešne detekcije ili lažnih alarma.

U ovoj tezi predložen je novi metod za detekciju napada odbijanjem usluge koji se sastoji iz dve faze. U prvoj fazi, proces detekcije izračunava entropiju distribucije polja iz mrežnih paketa. U drugoj fazi Takagi-Sugeno-Kang fazi sistem (TSK-FS) je primenjen na izračunate vrednosti entropije. Performanse TSK-FS metoda biće uporedjene sa do sada korišćenim metodama u kojima je detekcija tačke promene (CUSUM) primenjena direktno na signalu entropije. Rezultati treba da pokažu da TSK-FS detektor napada ometanjem usluge povećava osetljivost i robusnost kao i da daje veoma nizak procenat lažnih detekcija. Kao metod zasnovan na entropiji, ovaj kombinovani postupak zadržava opštost i u mogućnosti je da detektuje različite tipove napada. Predložena je optimizovana varijanta TSK-FS metode u realnom vremenu koja može biti realizovana sa hardverskim komponentama kao korak ka praktičnoj primeni na mrežnoj opremi.

Sadržaj

Spisak tabela

Spisak slika

Spisak skraćenica

ACK	Acknowledge
APT	Advanced Persistent Threat
C&C	Command and Control
CAIDA	Center for Applied Internet Data Analysis
CUSUM	Cumulative Sum
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial of Service
DF	Don't Fragment
DNS	Domain Name Server
DoS	Denial of Servis
EWMA	Exponential weighted moving average
FNR	False Negative Rate
FPGA	Field-Programmable Gate Array
FPR	False Positive Rate
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IRS	Intrusion Response System
SDoS	Single Distributed Denial of Service
SLA	Service Level Aggreement
SYN	Synchronize, signal sinhronizacije kod uspostave veze
TCP	Transmission Control Protocol
TPR	True Positive Rate
TSK	Takagi-Sugeno-Kang
TSK-FS	Takagi-Sugeno-Kang Fuzzy System
TTL	Time to Live
UDP	User Datagram Protocol
WRLS	Weighted recursive least square

1. Uvod

Poslednjih dvadesetak godina svedoci smo burnog razvoja Interneta koji je postao deo svakodnevice većine ljudi na planeti i nezamenljiva komponenta u radu skoro svih organizacija i poslovnih subjekata. Svako narušavanje funkcionisanja mreže zato ima sve veće posledice na svakodnevne aktivnosti. Vesti o napadima putem globalne mreže pune medijske sadržaje ravnopravno sa vestima iz politike, sporta ili zabave. Informacije o masovnom objavljivanju tajnih državnih ili vojnih dokumenata, objavljivanje privatnih podataka putem društvenih mreža su teme koje se odavno ne smatraju da pripadaju domenu nauke ili visoke tehnologuje već su postale svakodnevne vesti. Kako se zavisnost savremenog načina života od medjusobne povezanosti bude povećavala, što je neminovan trend, tako će i negativni dogadjaji na globalnoj mreži povećavati svoj uticaj na naš svakodnevni život.

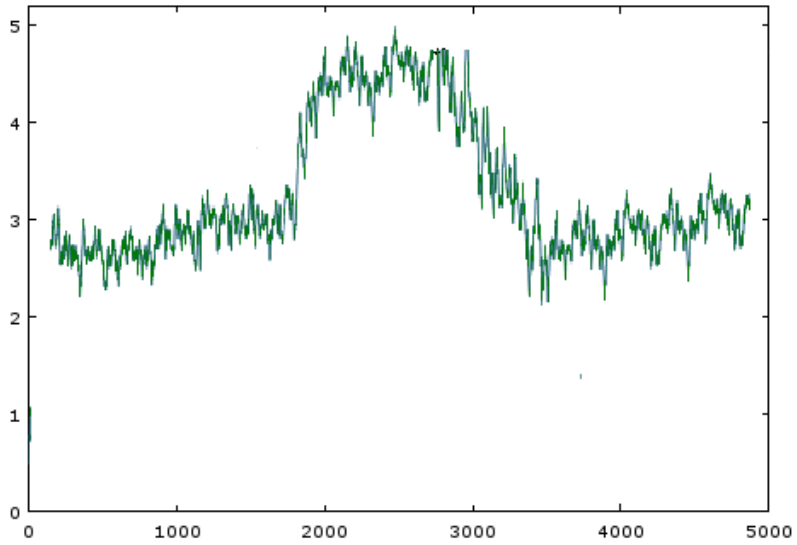
Teško je napraviti neku uopštenu podelu po tipovima napada, ali se može reći da otkrivanje informacija, neovlašćena izmena informacija, preuzimanje kontrole nad napadnutim resursima i sprečavanje pristupa napadnutom resursu su najčešće vrste napada koje pokrivaju veliku većinu dogadjaja na globalnoj mreži.Kad se posmatra sprečavanje pristupa resursima, masovni napadi ometanjem usluge (Distrubuted Denial of Service, DDoS) su po angažovanim resursima najviše zastupljeni napadi na internetu i tom temom se ovoistraživanje bavi.

Napadi ometanjem usluge od samog početka Internet ere predstavljaju jednu od najvećih pretnji na Internetu. Tokom vremena, usavršavanjem tehnologije, dolazi i do veće snage i učestanosti ovih napada. Svaka organizacija čije poslovanje je zavisno od Interneta podložna je napadima ometanjem usluge. Ovi napadi predstavljaju rastuću pretnju za normalno funkcionisanje kompanija, državnih službi javnih usluga i utiču na raspoloživost usluga kao i na reputaciju.

Cilj napada odbijanjem usluge je da se spreči pristup legitimnim korisnicima resursa koji je žrtva napada i tako nanese šteta kako u materijalnim tako i u nematerijalnom smislu. Razlozi napada, zavisno od napadnutog cilja, mogu biti politički, poslovni, finansijski ili jednostavno dokazivanje mogućnosti hakerskih grupa. Od četiri aspekta problematike napada odbijanjem usluga, sprečavanja, otkrivanja, odgovora na napad i ublažavanja napada, ovaj rad se bavi aspektom otkrivanja ili detekcije napada.

Uopšteno, postoje dva načina detekcije napada odbijanjem usluge, koji važe i za druge tipove mrežnih napada, a to su metodi bazirani na potpisu i metodi bazirani na statističkim anomalijama. Metodi bazirani na potpisu otkrivaju napad na osnovu unapred poznatih karakteristika koje odredjeni napad ima. Ovi metodi su prilagodjeni odredjenom tipu napada i najčešće ne mogu da detektuju neki drugi tip napada. Metodi baziranina statističim anomalijama otkrivaju napad poredjenjem neki statističkih osobina mrežnog

saobraćaja. Veličina koja se često koristi za otkrivanje anomalija mrežnog saobraćaja je entropija. Svaka nagla promena entropije neke od posmatranih veličina mrežnog saobraćaja može biti znak da je počeo napad (slika 1). Ovi metodi imaju karakteristiku opštosti i mogu da detektuju više topiva napada pa i potpuno nepoznat napad, takozvani napad nultog dana (zero-day attack). Nedostatak metoda zasnovanimna entropiji je pojava većeg broja lažnih alarma, tj. legitimnog dogadjaja koji izaziva promenu nivoa entropije na sličan način kao i napad ometanjem usluge. Problem lažnih alarma otežava praktičnu primenu metoda zasnovanih na statističkim anomalijama.



Slika 1: Svaka nagla promena nivoa entropije u vremenu znak je nekog dogadjaja koji narušava uobičajen saobraćaj na mreži. Taj dogadjaj može da bude i napad ometanjem usluge.

Cilj ove teze je da se da se ublaži ovaj problem i poboljša kvalitet detekcije metoda zasnovanih na entropiji primenom Takagi-Sugeno-Kang neuro-fazi metode.

Metod koji je o ovoj tezi promenjen izračunava entropiju u prvom koraku, a zatim na dobijen signal promene entropije u vremenu primenjuje Takagi-Sugeno-Kang (TSK) neuro-fazi metod. Primena neuralnih mreža i fazi logike ima ulogu poboljšanja detekcije u smislu povećanja ispravnih detekcijauz istovremeno smanjenje lažnih detekcija. Kao i svaki metod zasnovan na neuralnim mrežama, obavezan korak je proces obuke na signalu koji sadrži napade sa unapred unapred poznatim karakteristikama. Pošto je i dalje zasnovan na entropiji, metod zadržava opštost i sposoban je da detektuje širi spektar napada pa i one koji se potpuno novi i nepoznati.

U radu će se primeniti više tipova entropija i dve topologije simulirane mreže.

Izvršiće se poredjenja dobijenih rezultata sa konvencionalnim metodama koje koriste samo signal entropije.

Većina eksperimenata će biti izvršena na simuliranoj mreži gde su mogućnosti podešavanja postavki daleko veće nego na realnoj mreži. U drugoj fazi, metod će se primeniti na saobraćaj preuzet sa realne mreže.

Na kraju, biće predložen dizajn metode prilagodjen implementaciji na hardverskoj platformi.

Organizacija teze

Poglavlje 2 opisuje pojam napada ometanjem usluge i njegovo mesto delovanja u opštem modelu zaštitnih mehanizama. Daje se teorijska podela tipova napada po više kriterijuma. Opisuje se struktura napada, način formiranja infrastrukture napada, opisuje uticaj na poslovanje napadnutih subjekata i daju primeri poznatih napada koji su se dogodili poslednjih godina.Na kraju se prilažu redovni izveštajiiz relevantnih izvora koji kontinuirano prate ovu problematiku.

Poglavlje 3 izlaže teorijske osnove rada. Dat je pregled mera neuredjenosti informacija kao što su Shannon-ova, Tsallisova i T-entropija, kompleksnost i samosličnost koje se mogu iskoristiti kao osnova za detekciju anomalija u mrežnom saobraćaju.

Poglavlje 4 izlaže dalje teorijske osnove. Opisuje se fazi logika zbog lakšeg praćenja dalje uzlaganja, jednonovovska neuralna mreža i prelaz ka takagi-Sugeno-Kang modelu. Dat je i kraći matematički opis izvodjanja TSK modela koji se koristi u radu.

Poglavlje 5 opisuje detaljnije Takagi-Sugeno-Kang metodu, na koji način se formira model i poredi metodu sa srodnim metodama.

Poglavlja 6 prikazuje radove i rešenja koja su u relaciji sa tezom ili koja su potrebna za razumevanje izložene teze.

Poglavlje 7 opisuje postavke eksperimenata i razloge za odabir alata za izvodjenje eksperimenata, topologije mreže, vrste primenjene entropije i promenljivih čija se distribucija koristi za izračunavanje entropije.

Poglavlja 8 opisuje dizajn detektora napada, uključujući proces generisanja neuro-fazi modela kao i procese obuke i detekcije.

Poglavlja 9opisuje izvedene eksperimente sa simuliranim i realnim podacima. Eksperimenti su izvedeni na dve topologije simulirane mreže, tri tipa entropije, kombinovanjem entropija različitih veličina i na kraju su najbolje postavke primenjene na saobraćaj preuzet sa realne mreže.

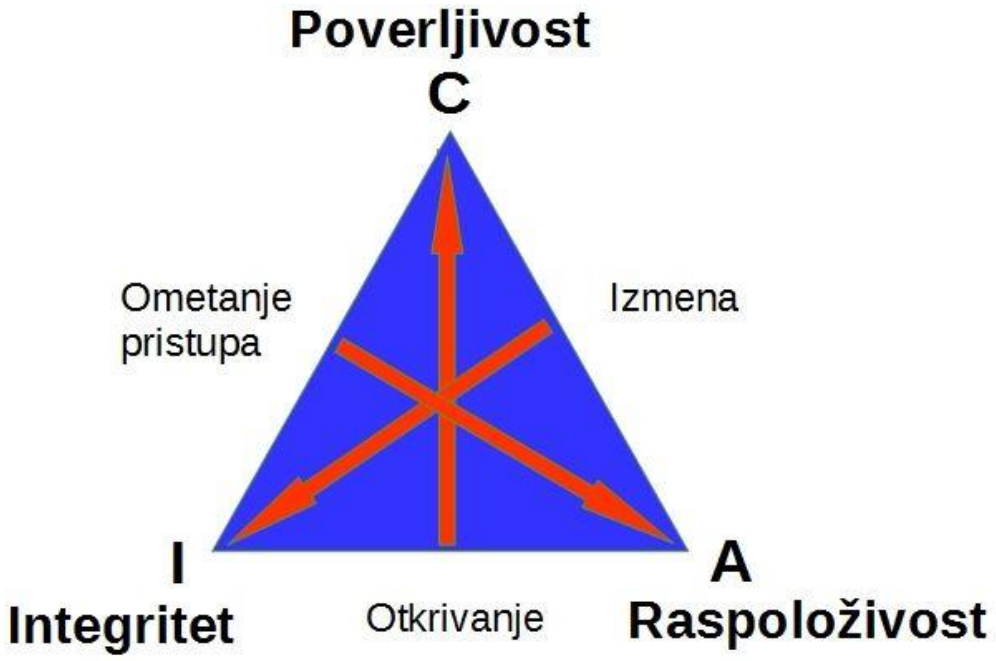
Poglavlje 10 daje predlog dizajna DDoS detektora koje se može praktično realizovati i kao softverska i kao hardverska komponenta. Predloženo rešenje treba da ima mogućnost brze protočne obrade mrežnih paketa uz minimalno zauzeće hardverskih ili softverskih resursa.

Poglavlje 11prezentuje zaključke koji se mogu izvući iz ove teze i predlaže moguće naredne korake i oblasti rada koji mogu biti zanimljive u daljem istraživanju.

2. Napad ometanjem usluge

Mesto napada ometanjem usluge u opštem modelu

Tri osnovne komponente zaštite računarskih sistema su poverljivost, integritet i raspoloživost. Opšteprihvaćen izraz za skup ove tri komponente je CIA trojstvo (**C**onfidentiality, **I**ntegrity, **A**vailability triad). (slika 2). Osim ove podele, neki autori dodaju i komponente kao što su privatnost, neporicanje, posed/kontrola, autentičnost, o čemu se i dalje vode rasprave, ali u ovom trenutku pojam CIA trojstvo je dominantan.



*Slika 2: Tri osnovne komponente bezbednosti su poverljivost, integritet i raspoloživost – poznate i kao CIA trojstvo (**C**onfidentiality, **I**ntegrity, **A**vailability) i odgovarajuće pretnje: otkrivanje, (neovlašćena) izmena iometanje pristupa.*

Poverljivost je komponenta koja obezbedjuje da informacija nije učinjena dostupnom ili otkrivena neautorizovanim licima, entitetima ili procesima. Podaci o bankovnim računima, brojevi kreditnih kartica, lični podaci, državni dokumenti, samo su neki primeri informacija čiji sadržaj ne bi smeo da dodje u posed neautorizovanih lica ili organizacija. Dobro je poznato kakve potrese u svetu izazove objavljivanje dokumenata od strane organizacije *Wikileaks*. Kao najočiglednija i najjasnija komponenta često se poistovećuje sa celokupnim pojmom zaštite. Metodi obezbedjivanja komponente tajnosti su šifrovanje podataka i komunikacija, kao i postavljena prava za pristup osetljivim informacijama.

Informacija ima vrednost samo ako je tačna. **Integritet**(celovitost, neokrnjenost) znači održavanje i osiguravanje tačnosti i celovitosti informacije tokom celog životnog ciklusa. To znači da informacija na svom putu od izvora ka odredištu ili u stanju mirovanja ne može biti izmenjena na nedozvoljen način, a da to ostane neprimećeno. Primena kriptografskih metoda kao *hash* vrednosti ili digitalni potpisi koriste se u očuvanju integriteta informacija. Primer informacija kod kojih je integritet ima dale veću težinu od tajnosti su javne informacije. Javne informacije objavljuju njihovi vlasnici bilo da su to kompanije, medijske kuće ili državne institucije. Samo vlasnici ovih informacija ili ovlašćeni entiteti mogu da kreiraju ili menjaju ove informacije. Neovlašćena izmena javnih informacija dovodi niza posledica kao što su pogrešno informisanje javnosti ili narušavanje ugleda vlasnika informacija. Posledice se često veoma dugo ispravljaju. Informacija o stanju bankovnog računa, s druge strane, ima značajnu komponentu poverljivosti, ali bi vlasnik istog računa bio daleko više pogodjen neovlašćenom izmenom stanja računa.

Raspoloživost (dostupnost) se može definisati kao mogućnost da se do informacije ili resursa dodje na pouzdan način u vremenski prihvatljivom intervalu [1]. To znači da informacija mora biti dostupna kada je potrebna. Pristup bankovnom računu radi izvršenja transakcije, pristup sajtu javnog informativnog servisa, pristup sajtu za elektronsku koji obavlja trgovinu, sve su to primeri usluga čijim onemogućavanjem bi bila naneta značajna šteta i za nosioca usluga i za korisnika. Pouzdanost, redundantnost i propusna moć komunikacionih linija za pristup informacijama redovno kreiranje rezervnih kopija (backup) najčešće su korišćeni metodi za obezbedjenje visoke raspoloživosti informacija.

Napad ometanjem usluge (Denial of Service, DoS) je akcija koja narušava baš komponentu **raspoloživosti**. Raspoloživost usluge je od izuzetnog značaja za sve sisteme koji svoje usluge nude većem broju klijenata putem mrežne infrastrukture, naročito Interneta. Napad ometanjem usluge se izvodi tako što se ciljanom sistemu pošalje veliki broj regularnih zahteva za obradu sa namerom da se iscrpe kapaciteti sistema i tako se onemogući pristup sistemu od strane redovnih korisnika. Resursi koje napadač nastoji da istroši su oni koji su ograničeni, nedovoljni ili neobnovljivi. Ti resursi mogu biti mrežni protok, memorija ili pojedine strukture podataka u memoriji, procesorska jedinica, protok ulazno-izlazne sprege, disk ili kombinacija navedenih resursa. S obzirom da se napad može izvesti slanjem regularnih zahteva a da ne postoji resurs koji je praktično neograničen, to znači da meta napada može biti i sistem koji nema ugradjene ranjivosti ili loše podešene parametre. Imajući ovo u vidu, jasno je kolika opasnost preti od napada odbijanjem usluge i da svaki subjekt na globalnoj mreži može osetiti posledice napada. U savremenom svetu zavisnost od globalne informacione povezanosti i korišćenja Interneta je sve veća.

Svaka logička ili fizička celina koja poseduje sopstvene interne resurse i spregu kojom se može pristupiti toj celini može biti podložna napadu odbijanjem usluge. U opštem slučaju proces obrade zahteva klijenta na resursima poslužioca odvije se na sledeći način:

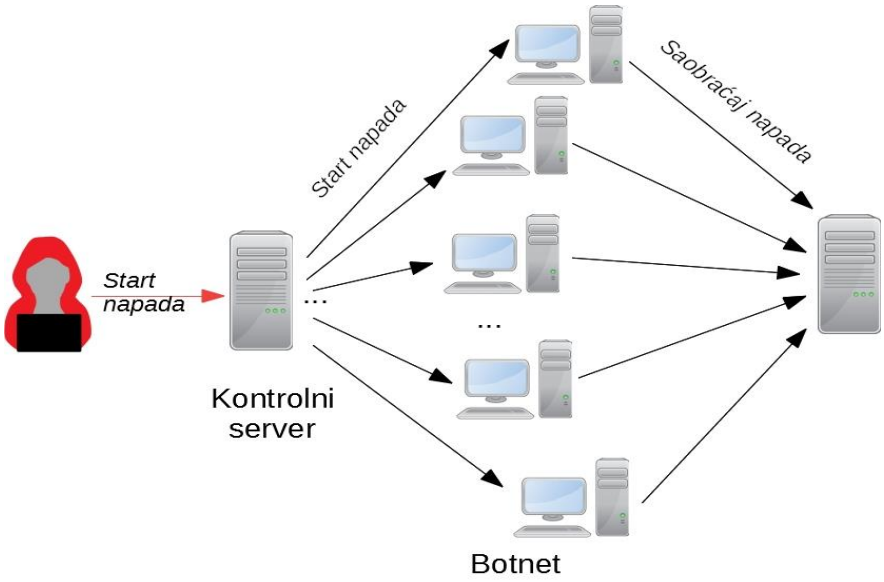
- Klijent šalje zahtev poslužiocu usluge preko definisane sprege.
- Poslužilac obradjuje zahtev i šalje odgovor klijentu.
- Da bi se zahtev opslužio, poslužilac mora da angažuje deo svojih resursa i za to koristi odredjeno vreme.
- Posle obrade zahteva resursi se oslobadjaju.
- Ako broj zahteva u jedinici vremena postane dovoljno veliki da se angažovani resursi brže zauzimaju nego što se oslobadjaju, konačno dolazi do efekta da više ni jedan zahtev ne može da se opsluži.

Ovakav pogled na problem napada ometanjem usluge pomaže da se šire sagleda problematika i da odmaknemo od podrazumevanog pogleda da su mete napada samo serveri. Poslužilac može biti uredjaj, aplikacija, bilo koja logička celina, čak i objekat u objektno orjentisanim jezicima. Koncept koji trenutno nadolazi u globalno povezanom svetu je Internet stvari (Internet of Things IoT). Raznorodni uredjaji dostupni preko Interneta koji su oko nas i koji utiču na kvalitet našeg života. Oni mogu biti u domovima, u automobilima, avionima, na ulicama, javnim prostorijama. Svaki od njih je realizovan tako da ima spregu preko koje komunicira sa spoljnim subjektima i poseduje sopstvene resurse pa samim tim mogu biti takodje mete napada ometanjem usluge. Posledice odbijanja usluge ovih uredjaja mogu dovesti do ozbiljnih posledica.Obrnuto, IoT uredjaji mogu poslužiti kao nosioci DoS napada. Ako se nalaze na mreži i imaju sopstvenu IP adresu, dostupan im je i globalni opseg IP adresa. Ukoliko postoji ranjivost kojom napadač zadobija pristup IoT uredjajima, moguće je instalisati zlonamerni kod i pretvoriti sve dostupne IoT uredjaje u agente DoS napada.

Infrastruktura distribuiranog napada odbijenjem usluge

Distribuirani napad odbijanjem usluge (DDoS) se najčešće izvršava koristeći tzv. Botnet (slika3). Botnet je skup računara distibuiranih često na veoma širokom geografskom području na kojima je instalisan zlonamerni kod. Zlonamerni kod se širi na isti način na koji se širi i bilo koji drugi zlonamerni kod poput virusa ili crva kao što je e-mejl ili poseta neproverenim web stranicama. Zlonamerni kod se instališe ako računar-žrtva nema instalisane dovoljno jake zaštitne mehanizme ili zaštitni mehanizmi nisu osveženi najnovijim verzijama. Razlika u odnosu na istalisanje virusa ili crva je što zlonamerni kod namenjen napadu odbijanjem usluge ne nanosi štetu računaru na kome je instalisan niti mu je to namena, već je cilj da ostane neprimećen. Računari na kojim je instalisan ovakav kod dejstvuju kao armija pod komandom napadača koji ostaje prikriven. Broj ovih računara može biti varirati od nekoliko desetina do nekoliko stotina hiljada.

Poznati Mariposa botnet je imao čak 3.5 miliona zaraženih računara pod svojom kontrolom. Korisnici ili vlasnici zaraženih računara obično nisu svesni da njihov računar sadrži zlonamerni kod kao ni vremena kada računar koji koriste upravo učestvuje u napadu na državni instituciju, medije ili kompletnu lokalnu internet infrastrukturu.



Slika 3: Tipičan botnet. Napadač je sakriven iza kontrolnog servera koji pokreće jednom komandom, tako da ga je teško otkriti. Kontrolni serveri startuju masovni napad ometanjem usluge na odabrani cilj.

Zadatak koda je da u uspavanoj fazi (odatle naziv zombi računar) čeka uputstvo od napadača kad i kako da izvrši napad. Napadač ne komunicira direktno sa bot-mašinama, već to čini posredno preko ‘gospodara’ ili Command & Control (C&C) servera. Za veće botnet mreže gospodari mogu biti organizovani u više nivoa, tako da svaki kontroliše optimalan broj agenata-botova. Ovakva infrastruktura napada otežava neutralisanje napada jer napadači deluju u pozadini i generišu vrlo malo saobraćaja, samo onoliko koliko je potrebno da se izda komanda. S druge strane, direktni napadači su u stvari i sami žrtve i gotovo je nemoguće neutralisati stotine hiljada napadač koji su distribuirani svuda po svetu. Komunikacija u botnetu se odvija preko jednostavnih IRC (internet relay chat) protokola.

Proces onesposobljavanja DDoS napada se odvija tako što se pronalaze i neutrališu C&C serveri, čime se onesposobljava i mreža bot-mašina kojom ovi serveri upravljaju. Noviji sofver za DDoS napade, međutim, omogućava i direktnu komunikaciju izmedju bot mašina tako da i posle onesposobljavanja C&C servera botnet može da funkcioniše.

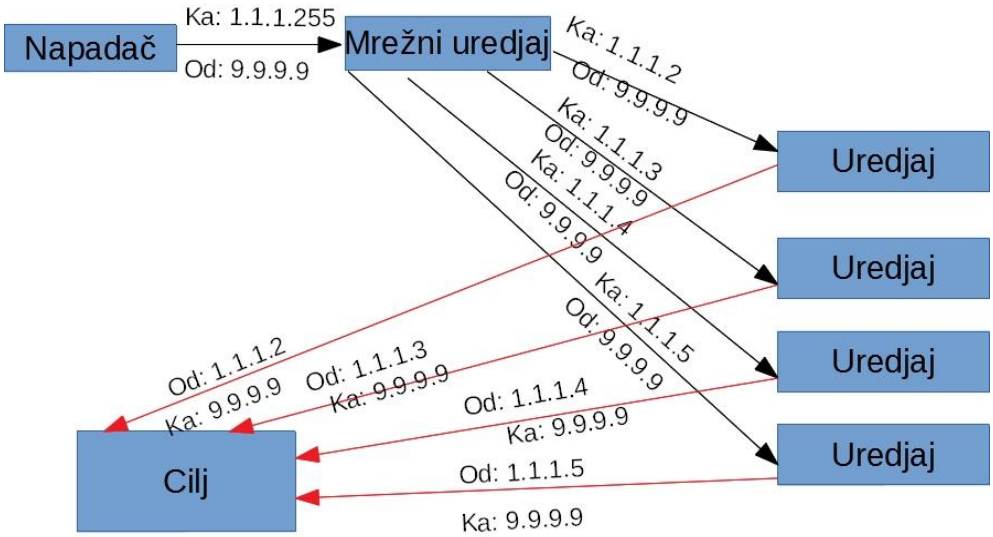
Proces izgradnje efikasne DDoS mreže odvija se postepenim otkrivanjem računara na kojim postoje bezbednosni propusti. Ti propusti se koriste da bi se zadobio pristup a zatim instalisao zlonamerni kod. Napadač najpre instališe kod kojim zadobija administratorska prava, “rootkit” kod. Pomoću ovog programa napadač instališe poseban process koji služi za daljinsku kontrolu računara. Ovaj process se nikada ne vidi u alatima

za prikaz aktivnih procesa. Zadatak mu je da prima komande od C&C servera. Kad je instalisan program za daljinsku kontrolu, napadač može da koristi kompromitovani računar kao posrednika u daljem instalisanju zlonamernog programa i na taj način automatizuje širenje bot-mreže. Na kompromitovanom računaru napadač će naći adrese drugih računara sa kojim kompromitovani računar već obavlja komunikaciju. Tako napadač dobija informacije o novim potencijalnim ranjivim računarima koje može direktno napasti ili indirektno preko već kompromitovanih računara i tako sakriti sopstveni identitet. Potencijal izgradjene bot-mreže zavisi od broja računara u njoj.

Izgradnja botneta može da se odvija i akcijama preko društvenih mreža kada se pozivaju zainteresovani učesnici da se pridruže akciji protiv nekog cilja. Ovako organizovani napadi obično imaju političku ili socijalnu pozadinu. Pošto svaki učesnik vrši napad sa svog računara, lako se izvrši identifikacija pojedinačnih napadača. I pored ovog, poslednjih godina ovo je popularan metod formiranja botneta.

Ozbiljnost problema DDoS napada se ogleda u tome da su dostupni praktično svima i jednostavni su za upotrebu. Napad se obično pokreće jednom komandom, a isto tako se I zaustavlja. Za samo izvođenje napada nije potrebno posebno tehničko znanje, s obzirom da postoje već organizovane infrastrukture DDoS napada koje se iznajmljuju na crnom tržištu. Na mnogobrojnim internet forumima mogu se naći ponude za ovaj tip usluga kao rent-a-DDoS. Cene se kreću od samo nekoliko dolara do nekoliko stotina dolara po satu napada, zavisno od jačine napada tj. broja angažovanih bot-mašina.

DDoS napadi mogu imati osobine refleksije/odbijanja i pojačanja (slika 4). Uslov da bi se refleksija dogodila je da adresa izvora bude lažirana. Ta lažirana adresa je po pravilu adresa žrtve. Kada odredišni subjekt primi poruku, on će odgovor poslati na adresu koja je predstavljena kao izvorna. Na taj način će se izvršiti „odbijanje“ poruke ka žrtvi. Pojačanje se dešava kad se sa jednog ili više izvora pošalje broadcast poruka. Svi primaoci poruke tada šalju odgovor na istu adresu i na taj način dolazi do efekta pojačanja. Najčešće se te dve tehnike izvode zajedno kao u slučaju napada Smurf i Fraggle.



Slika 4: DDoS napad sa refleksijom. Napadač sa lažnom adresom 9.9.9.9, adresom žrtve, šalje poruku širokog spektra (broadcast). Svi računari odgovaraju na poruku i na taj način zasipaju žrtvu iznenadnim jakim saobraćajem.

Mada postoje DoS napadi koji iskorišćavaju neku slabost ciljanog sistema, većina DoS se uspešno izvršava i kada o napadnuti sistem uopšte ne sadrži nikakvu slabost. To je važna osobenost ovog tipa napada koja ga izdvaja iz skupa poznatih tipova napada. Napadač jednostavno šalje veliku količinu validnih zahteva za uslugom koja prevazilazi kapacitete napadnutog sistema. Ovo je posledica ugradjene slabosti Interneta koji je inicijalno projektovan, i ostao takav, da svako može da ga koristi tj da se ne traže pristupna prava. Pristupa prava se koriste za pristup konkretnim resursima, ali ne i Internetu kao globalnoj mreži. Na taj način bilo koji uredjaj saIP adresom je vidljiv, direktno ili indirektno, bilo kom drugom uredjaju i to čini napad odbijanjem usluge lako izvodljivim.

Razne podele napada sa primerima

Bilo je dosta pokušaja da se klasifikuju DoS napadi. Klasifikacija napada ometanjem usluge se vremenom menjala kako se menjala tehnologija i kako su se menjali i sami napadi. Primer [2,3,79] .

Prema osnovnim tipovima napada

DoS napadi se mogu podeliti na

- Iscrpljivanje resursa, memorije, diska, komunikacionog protoka, kapaciteta ulazno-izlaznog prostora.
- Izmena ili uništenje postavki sistema.
- Fizičko onemogućavanje sistema.

U tezi se obradjuju napadi koji iscrpljuju resurse.

Prema tipu iskorišćene slabosti, mogu se podeliti na:

Napadi bazirani na konkretnoj slabosti. Ovaj tip napada iskorišćava uočenu slabost ciljanog sistema. Vrlo često se samo jednim pažljivo formiranim zahtevom može izazvati pad celog sistema. Da bi se pronašla slabost mora se dobro poznavati sistem koji se napada. Softver otvorenog koda je podložan ovom tipu napada jer je javno dostupan. Ako napadač pažljivom analizom koda pronadje slabost pre nego što to učini razvojni ili testni tim, on može lako osmisliti ciljani napad na oučenu slabost. Dešavalo se da otvoreni kod bude dugi niz godina u upotrebi pre nego što se uočila slabost koja je sve vreme bila prisutna. Kod zatvorenog koda ovakav napad je teže izvesti jer napadač mora pretpostaviti postojanje slabosti i onda pokušati da je iskoristi. Postoje brojni alati koji ispituju i/ili iskorišćavaju slabosti nepoznatog sistema.

Napadi poplavljivanja zahtevima. Kod ovog tipa napada ne mora nužno da postoji nikakva slabost. Napadač šalje veliki broj zahteva sa ciljem da se iscrpe resursi. Ovaj tip napada se razmatra u ovom radu.

Prema distribuiranosti napada se deli na **SDoS** (Single Denial of Service) i **DDoS** (Distributed Denial of service). Obično se akronim DoS koristi za uopšteni tip napada a DDoS za distribuirani. Ako se želi istaći da je napad izvršen sa jednog izvora, preporučuje se akronim SDoS. Iako izveden sa jednog izvora, i ovaj napad može da bude izuzetno opasan ako cilja odredjenu slabost sistema. Pošto obično nema dovoljne promene u saobraćaju mreže ne može se otkriti metodima statističkih anomalija tako da se u ovom radu obradjuje samo DDoS napad.

Prema metama napada, može se izvršiti podela po horizontalnom i vertikalnom principu.Prema horizontalnoj podeli, mete napada mogu da budu aplikacije, operativni sistemi, sama mrežna oprema, infrastruktura pa i uredjaji za detekciju i sprečavanja DoS napada. Prema vertikalnoj podeli DoS napadi se mogu izvesti na bilo kom nivou protokola.

Aplikacije su lake mete napada jer su pisane od strane većeg broja programera koji često ne obraćaju dovoljno pažnje na bezbednosne mehanizme. Pored toga brojnost aplikacija uveliko nadmašuje brojnost drugih meta kao što su operativni sistemi ili slojevi protokola pa je teže uspostaviti principe dizajna i izvršiti testiranje na propuste. Aplikacije se i mnogo češće menjaju tako da nove slabosti uvek mogu da se unesu. Ukoliko napadač poznaje neku ranjivost aplikacije ili modula koji neka aplikacija koristi, on može pažljivim odabirom parametara poziva ciljano izazvati izvršenje dela koda koji sadrži slabost. Primera ima bezbroj, samo da nepomenemo neke. U nekim XML parserima moguće je izazvati ogromno zauzeće memorije pomoću malog XML fajla koji se u memoriji širi preko granice postojećeg memorijskog prostora. Neke aplikacije za prikaz kompresovane slike takodje mogu da izazovu iskorišćavanje memorijskog

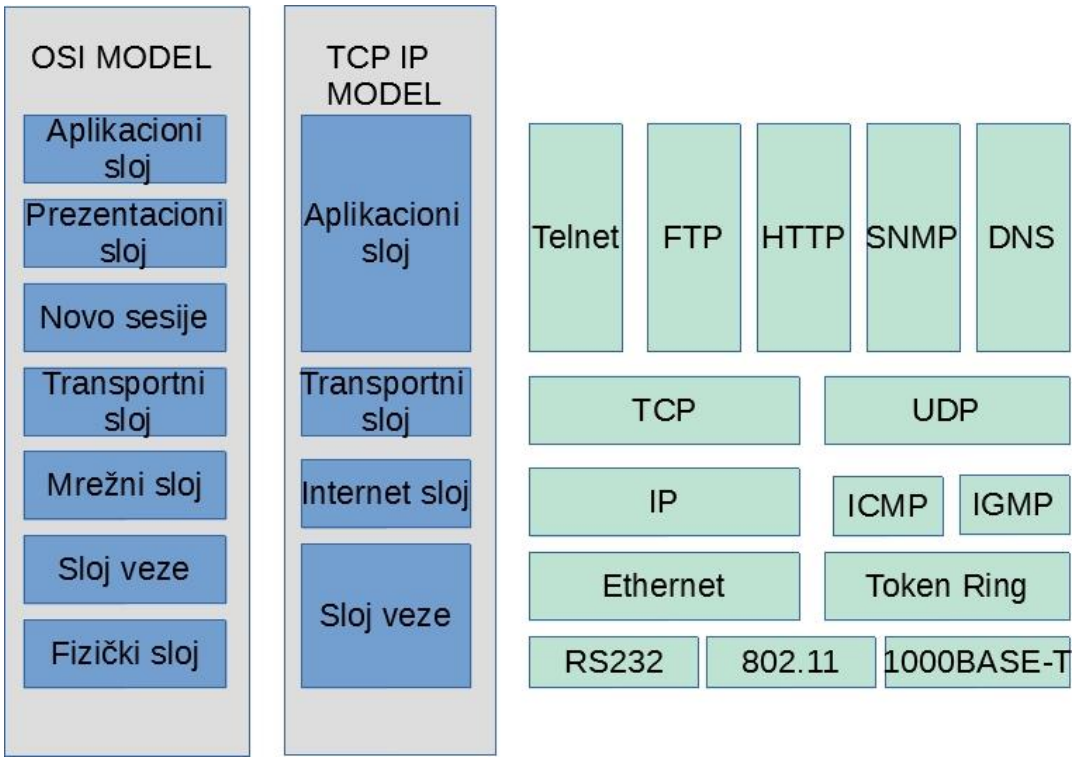
prostora zbog lošeg rukovanja nevalidnim podacima. Ukoliko bilo koji deo koda, funkcija ili klasa omogućava curenje memorije, učestalim pozivima može se takodje izazvati zauzeće memorije i prekid usluge.

Napad na **operativni sistem** je znatno opasniji jer može dovesti do pada celog sistema. U principu svaki napad koji iskorišćava slabosti programskog koda koji se izvršava u privilegovanom modu ujedno je i napad na operativni sistem, bez obzira da li inicijalno napadnuta aplikacija ili protokol.

Mrežna oprema kao i zaštitni zidovi i oprema namenjena detekciji i prevenciji napada takodje i sami mogu biti mete DoS napada. U slučaju rutera, ako je napad izveden sa adrese koja izgleda verodostojna kao adresa nekog drugog mrežnog uredjaja, izaziva se zauzeće svih tabela rutiranja. Kod uredjaja za detekciju i prevenciju napada, ako rade u modu sa praćenjem stanja, izaziva se takodje zauzeće tabela stanja. Pošto su ovi uredjaju podrazumevano podešeni da propuštaju saobraćaj, dalja detekcija napada postaje nemoguća.

Mnogi sistemi zavise od **infrastrukture** na koji se oslanjaju. Zato napadi na infrastrukturu imaju nesagledive posledice. Ispad iz rada DNS servera, dovodi do nemogućnosti korišćenja interneta. Ako je zona koju pokriva dati DNS veća tim su i posledice veće. Napad na cloud infrastrukturu dovodi do prekida funkcionisanja organizacija koje su se opredelile za ovakav vid poslovanja.

DoS napad je moguć na svakom od slojeva mrežnog modela. OSI model sadrži 7 nivoa (slika 5): Aplikacioni, prezentacioni, nivo sesije, transportni, mrežni, nivo veze i fizički nivo. Internet model s druge strane poznaje četiri nivoa: Aplikacioni, transportni, mrežni i nivo veze. U ovom modele se fizički nivo često posmatra kao spoljni nivo. Svaki mrežni nivo je po dizajnu nezavisna logička celina koja komunicira direktno sa nivoima iznad i ispod, kao i logički sa odgovarajućim nivoom na drugim čvorovima mreže. Kao nezavisna celina sadrži sopstvene resurse kao što je memorija ili memorijske strukture. Iz ovoga sledi da je DoS napad moguće izvršiti na svaki pojedinačni nivo mrežnog modela.



Slika 5: Napad je moguć na svakom od slojeva mrežnog modela.

Protokoli aplikativnog sloja su Telnet, FTP, HTTP, IMAP, SMTP/POP, SSH, IRC, XMPP , SNMP, DNS, BOOTP/DHCP, NTP, RTP, SIP, TLS/SSL. Većina ovih protokola funkcionišu po principu klijent/server. Ako zlonamerni klijent zatraži veliku količinu podataka, recimo u slučaju FTP ili HTTP protokola, i taj zahtev učestalo ponavlja, veoma lako dolazi do onemogućavanja usluge ostalim klijentima.

Neki poznati napadi

SYN preplavljivanje (SYN flood). Prilikom SYN ovog napada šalje se niz TCP / SYN paketa, često s lažnom adresom pošiljatelja. Čak i jedan napadač može poslati veliki broj zahteva sa iste adrese ali različitog porta. Svaki od tih zahteva tretira se kao zahtjev za vezu. Otvaranje TCP veze obavlja se u tri koraka. Ciljani računar odgovara na SYN poruku, rezerviše slog u internoj tabeli i čeka FIN paket da bi se završio proces otvaranja veze. Napadač nikada ne pošalje odgovor, što uzrokuje napola otvorene veze i konačno iscrpljivanje internih tabela.

Teardrop napad. IP protokol omogućava da se paket koji je preveliki podeli se na fragmente. U fragmente paketa upisuje se udaljenost od početka prvog paketa, što omogućuje ponovno sastavljanje paketa na drugoj strani. U ovom napadu napadač

postavlja neispravne podatke kao nevalidna udaljenost za jedan od fragmenata. Ako računar koji prima takav paket nema obradu tog slučaja rezultat će biti pad sistema. Ovaj napad je bio karakterističan za starije verzije TCP protokola.

Ping smrti (Ping of death) koristi ICMP protocol mrežnog nivoa. Izvodi se tako što se pošalje ping paket neuobičajeno velike dužine koji može da se beskonačno ponavlja. Ovo izaziva preplavljivanje bafera I pad sistema. Izvodi se veoma lako, pomoću jedne komande.

Smurf napad koristi ICMP protocol mrežnog nivoa. Izvodi se tako što se šalje ping na broadcast adresu, ali sa lažiranom adresom izvora, gde je kao izvor navedena adresa žrtve. Svi uredjaji koji prime ping komandu odgovaraju na istu i u stvari šalju masovni odgovor na adresu žrtve. Iako je ovaj napad

Fraggle napad je varijanta Štrumpf napada ali se umesto ICMP protokola koristi UDP protocol i port 7 za eho.

Posledice po poslovanje

Finansijski gubici su najvidljiviji oblik štete koje nanose DDoS napadi. Tačne finansijske gubitke je teško tačno izračunati jer u njih ne ulazi samo direktna šteta koja je proporcionalna vremenu nedostupnosti servisa nego i troškovi oporavka, odgovore na žalbe klijenata.

Osipanje korisnika. Najvažniji resurs kompanija čije poslovanje zavisi od Interneta su njihovi korisnici. Istraživanja su pokazala da prosečan korisnik odustaje od korišćenja web sajta ako mu je vreme odziva povećano za u proseku 400ms. Takodje će preći na web sajt konkurencije ako je prosečno vreme čekanja odziva veće od 250ms. Ako napad potraje korisnici počinju da se osipaju i veoma sporo se vraćaju.

Gubitak reputacije. Ako se slučajevi internet napada javno objave, to ima veoma loš uticaj na ugled kompanije koja je postala žrtva. Bez obzira koliko je kompanija uopšte odgovorna za taj dogadjaj, javnost često ne prašta i poljuljan ugled se teško vraća.

Sudsko gonjenje. Ako su korisnici usluga pretrpeli štetu zbog DDoS napada, oni mogu potražiti obeštećenje na sudu, posebno ako postoji SLA (Service Level Aggreement) izmedju isporučioca usluga (provider) i korisnika.

Motivi napada

Finansijska korist. Napadi koji imaju za cilj finansijsku korist spadaju u dve kategorije: na one kojima je cilj postizanje prednosti u odnosu na konkurenciju i na one koji napad koriste za iznudu. U prvom slučaju organizacija plaća DDoS napad na konkurentsku organizaciju i time postiže prednost na tržištu i tokom i izvesno vreme nakon napada. Finansijska korist na tržištu višestruko nadmašuje cenu naručenog DDoS

napada. U drugom slučaju napadač najpre sprovodi kratkotrajan napad, a zatim šalje poruku u kojoj se traži uplata određenog iznosa uz pretnju mnogo jačeg napada.

Politički motiv. U ovu grupu napada spadaju akcije grupa popularno nazvanih haktivisti. Akcijom DDoS napada ove grupe pokušavaju da stave na dnevni red neko političko ili socijalno pitanje. S obzirom da je cilj ovih napada zadobijanje medijske pažnje, mete ovakvih napada su ciljevi koji imaju politički ili javni značaj, kao mediji, velike društvene mreže državne institucije. Osim ovakvih grupa, nisu retki ni napadi na kompletne komunikacione infrastrukture celih država od strane organizacija pod kontrolom neke druge države. U ovakvim slučajevima teško je dokazati ko je stvarni naručilac napada.

Zabava i dokazivanje. Čak iako neka organizacija nema ni političku težinu ni bitan položaj na tržištu , to nije razlog da zaključi da ne može biti žrtva DoS napada. Pojedinci ili grupe mogu izvesti napad samo u svrhu dokazivanja , recimo na društvenim mrežama.

Vodjenje informacionog rata. APT (Advanced Persistent Threat) su organizacije koje imaju stalni motiv i napredne alate da izvedu selektivan i neprimetan napad. Cilj im je da funkcionišu duže vreme neotkrivene (za razliku od haktivista kojima je cilj da se za njihove akcije zna). Ovakve organizacije će imati u budućnosti sve veću ulogu u informacionim ratovima. Njihov proizvod je informaciono oružje i kao i svako drugo oružje ima za cilj da onesposobi ili čak uništi infrastrukturu neprijatelja. Postoje brojne tvrdnje da su neke APT povezane sa državnim obaveštajnim službama. Iranski nuklearni program je pretrpeo veliku štetu visokosofisticitanim napadom tako što su oštećene centrifuge za obogaćivanje nuklearnog goriva. U rukama terorista ovakvo oružje može imati još teže posledice.

Primeri napada

Primera napada odbijanjem usluge je bezbroj i to su napadi koji , uz kradju podataka, spadaju u one koji se najviše privlače pažnju javnosti. U daljem tekstu su opisani neki od njih koji su izazvali veliku medijsku pažnju a pokrivaju veliki deo spektra mogućih napada.

U vreme tenzija u regionu Kavkaza 2008 godine, web sajtovi državnih institucija Gruzije, banaka i medijskih kuća bilo su pogodjeni DDoS napadom sa nekoliko stotina hiljada računara. Sumnje su pale na kriminalnu organizaciju u Rusiji koja je funkcionisala kao APT, ali dalju vezu u liniji komandovanja nije bilo moguće dokazati.

Za vreme političkih demonstracija u Estoniji povodom uklanjanja spomenika i vojnih grobova iz sovjetske ere, dogodio se DDoS napad na celu internet infrastrukturu. Napad je trajao čak tri nedelje. Država je bila prinudjena da se kompletno isključi sa interneta [73].

2009 serveri velikih društvenih mreža Google, Facebook i Twitter su bili nekoliko sati pod udarom DdoS napada. S obzirom da su navedene kompanije medjusobna konkurencija, pretpostavka je bila da je motiv bio dokazivanje hakerskih grupa.

Za vreme utakmice Srbija Albanija oktobra 2014 i incidenta sa dronom, web sajtovi srpskih medijskih kuća su doživeli napad snage 40 gigabita u sekundi sa oko 1.5 miliona računara[81]. Cilj je bio da se stekne početna prednost u izveštavanju u prvim momentima od izbijanja incidenta i spreči izveštavanje srpskih medija.

Septembra 2015 počeo je veoma dug i kontinualan napad na sajtove povezane sa Olimijskim igrama u Riu 2016. Kampanja je koristila DDoS servis za izdavanje (Rent-a-bot) *LizardStresser*. Kako se vreme početka igara približavalo, napadi su pojačavani i u jednom trenutku su dostigli ukupnu jačinu od 540 Gbps. Zahvaljujući rešenjima firme Arbor Networks čiji su mehanizmi ugradjeni kod većine internet provajdera napad je uspešno odbijen.

1. Aprila 2016 grupa Anonimusi je izvela napad na web sajtove hotela predsedničkog kandidata Donalda Trampa u pokušaju da mu naruši reputaciju i spreči da se kandiduje za predsedničke izbore.

Masivni i selektivni DDoS napad je pokrenut novembra 2016. sa 24.000 računara lociranih u oko 30 zemalja ka nekoliko ruskih banaka sa lokacijama širom sveta. Pretpostavka je da je napad sproveden preko *Mirai* botneta ili nekog sa sličnim karakteristikama.

21. Oktobra 2016. izvršen je napad preko *Mirai* botneta koristeći oko 100.000 uredjaja na *Dyn*, veliki provajder DNS servisa [74]. DNS servis je ugradjen u osnovu Interneta. Pronalaženje IP adrese na osnovu naziva domena je od suštinske važnosti za funkcionisanje globalne mreže. Napad je onemogućio pristup globalnim platformama i servisima kao što su Twitter, Github, Spotify, Etsy na nekoliko sati, a posledice su osetili i PayPal, Amazon, CNN, Netflix, Airbnb i mnogi drugi. *Mirai* zlonamerni kod funkcioniše tako što pretražuje internet adrese tražeći IoT uredjaje poput IP kamera ili kućnih rutera. Pristupa im koristeći tabelu fabričkih korisničkih imena i lozinki koje nisu promenjene. Kada pristupi uredjaju *Mirai* instališe zlonamerni kod i na taj način širi mrežu botova. Problem je tim ozbiljniji što su često servisne lozinke ugradjene u firmver i ne mogu se menjati, tako da ranjivi uredjaji ostalu ranjivi tokom celog svog veka upotrebe. Po nekim istraživanjima (https://www.tripwire.com/state-of-security/latest-security-news/researchers-discover-500000-iot-devices-vulnerable-to-mirai-botnet/)
Mirai botnet poseduje oko 500.000 uredjaja pod kontrolom.

Strategije za odbranu

Iako je Internet u vreme njegovog nastanka inicijalno dizajniran da bude robustan za napada spolja, nije bilo predvidjena odbrana od sopstvenih korisnika koji su smatrani za dobronamerne. Kao globalna mreža kojoj svako može da pristupi Internet poseduje ugradjenu osobinu da su svi korisnici potencijalno vidljivi svima, tako da potencijalni napadač kao i cilj mogu biti locirani bilo gde u svetu.

Strategije za odbranu od DoS napada mogu se podeliti na četiri kategorije: sprečavanje, detekcija, odgovor i tolerancija [79,83].

Detekcija napada se deli na dve grupe: detekcija bazirana na osobinama napada (signature based) i detekcija zasnovana na anomalijama u saobraćaju (anomaly based). Komponente mrežne opreme za detekciju, IDS (Intrusion Detection System) su se najranije razvijene jer same ne pružaju nikakav odgovor na napad, već samo alarmiraju da je sumnjiva aktivnost u toku.

Kod detekcije zasnovane na *osobinama*, utvrdjuju se jedinstveni obrasci koje već poznati napadi ostavljaju i formira se baza obrazaca. Vrši se stalni nadzor saobraćaja na mreži u potrazi za poznatim obrascima. Metod je sličan detekciji prisustva virusa u računarskom sistemu. Baza obrazaca se mora stalno dopunjavati kako se novi obrasci pojavljuju. Metod je efikasan za detekciju poznatih tipova napada ali je neefikasan pri pojavi novih napada. Problem koji postoji kod ovih tipova detekcije je vremenski interval koji prodje od trenutka kada se nova pretnja pojavila do trenutka kada se baza obrazaca osveži novim obrascem. U toku tog vremenskog perioda nova pretnja neće biti detektovana. Ove metode se lako implementiraju i imaju nizak nivo pogresnih detekcija.[4]

Detekcija zasnovana na *statističkim anomalijama* saobraćaja najpre analizira normalan saobraćaj a zatim identifikuje odstupanja od takvog ponašanja. Za razliku od detekcije zasnovane na osobinama, ova detekcija može da otkrije i potpuno nove, nepoznate napade. Pošto se koristi prag detekcije, loša strana je što ove metode mogu pogrešno proglasiti normalno ponašanje kao zlonamerno (false positives) i zlonamerno ponašanje kao normalno (false negatives). Kvalitet metoda ovog tipa se odredjuje nivoom pogrešnih detekcija. Ova teza se bavi detekcijama zasnovanim na statističkim anomalijama.

Sprečavanje/prevencija se uglavnom svodi na detekciji lažiranih adresa i sprečavanju da takvi paketi dospeju do mreže koja se štiti [82]. Lažne adrese se detektuju na samom ulazu u mrežu. Ako je adresa dolaznog paketa adresa iz unutrašnje mreže, onda se paket odbacuje. Isto tako ako je izvorna adresa izlaznog paketa adresa koja ne pripada unutrašnjoj mreži, takodje se odbacuje jer je to indikacija da je DDoS napad pokušan iz same mreže. Jednostavan način za detekciju lažnih adresa je ako one pripadaju skupu rezervisanih adresa koje se ne mogu pojaviti na javnom domenu. (Kao adrese 192.168.x.x na primer). Sistemi za sprečavanje napada, IPS, (Intrusion

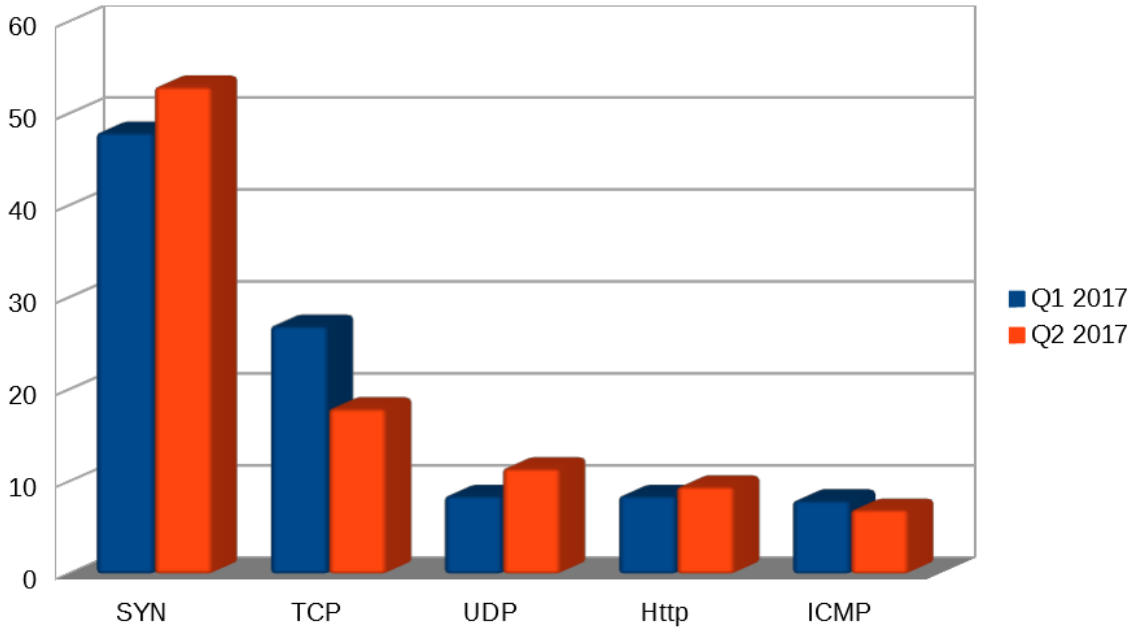
Prevenstion Systems) se poslednjih godina postale sastavni deo mrežne opreme i oslanjaju se na informacije koje šalje IDS komponenta.

Odgovor na napad se preduzima ako detekcija pruži informaciju da je napad u toku, sa informacijama o parametrima napada kao što su IP adresa napadača, vrsta napada, napadnuti resursi.Komponente koje preduzimaju odgovor na napad se nazivaju IRS (Intrusion Response System).Odgovor se pokreće automatski ili sa minimalnim učešćem administratora, tako da je vreme izmedju detektovanog napada i pružanja odgovora veoma kratko. IRS komponente, u zavisnosti od parametara napada, preduzimaju protivmere kojima pokušavaju da ublaže delovanje napada i zadrže sistem u radnom stanju . Sistemi za odgovor na napada ometanjem usluge su bili sporije razvijani u odnosu na sisteme za detekciju i sprečavanje jersu tehnološki najzahtevnije pošto je teško automatski odgovoriti na različite tipove napada koji se stalno usavršavaju.

Ideja **tolerancije** DoS napada je da se saobraćaj ne sprečava , čak i ako se utvrdi da je napad u toku, već da se što je moguće više ublaže posledice. Tolerancija na napad ne mora da se oslanja rezultate detekcije. Jedan od načina je povećanje broja servera sa balansiranim opterećenjem. Na ulazu u mrežu dobro konfigurisanom kontrolom zagušenja takodje je moguće smanjiti uticaj DoS napada. Postoji i ideja da se klijentu pre dozvole pristupa zadaje kriptografski zadatak na koji mora da da tačan odgovor. Na taj način se usporava DoS napad.

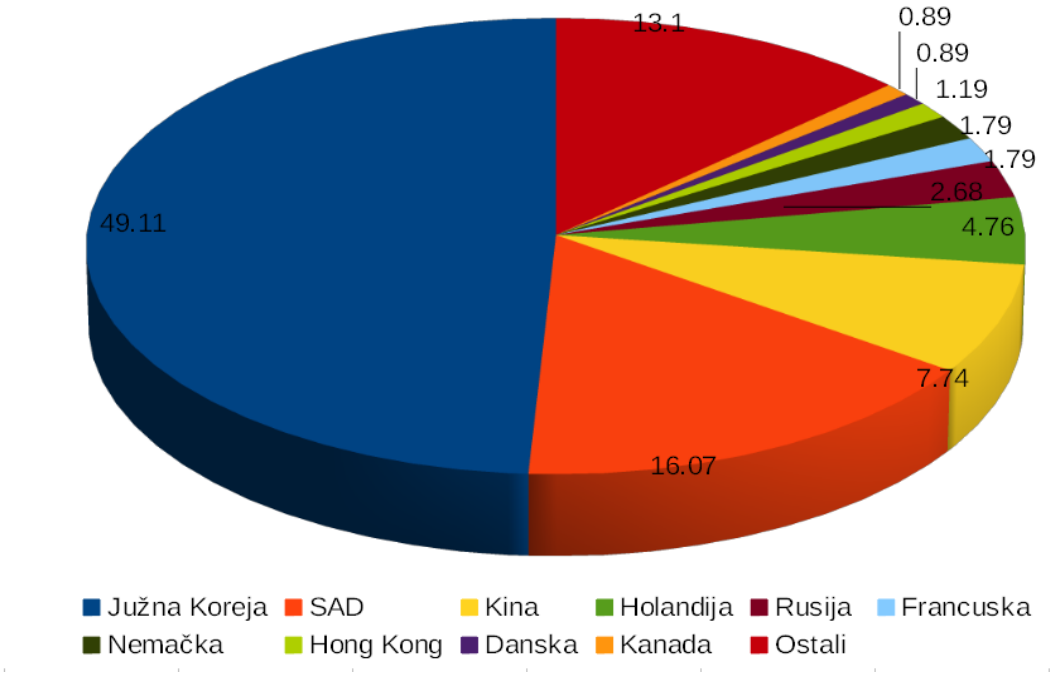
Pregled izveštaja o statistici DDOS napada u svetu

Kompanije i organizacije koje se bave bezbednošću informacija redovno objavljuju izveštaje po pitanju stanja i trendova DDoS napada u svetu. Prema izveštajima kompanije Kaspersky Lab [5]za drugi kvartal 2017, po tipu napada i dalje je dominantan je SYN flood napad, koji se uzima kao primer napada i u ovom radu, sa oko 53.26% ukupnog učešća u ukupnom broju registrovanih napada. Napad koji koristi TCP protokol primenjen je u 18.18% slučajeva, dalje slede UDP napad sa oko 11.91%, HTTP sa 9.38, i ICMP sa 7.27% (slika 6).



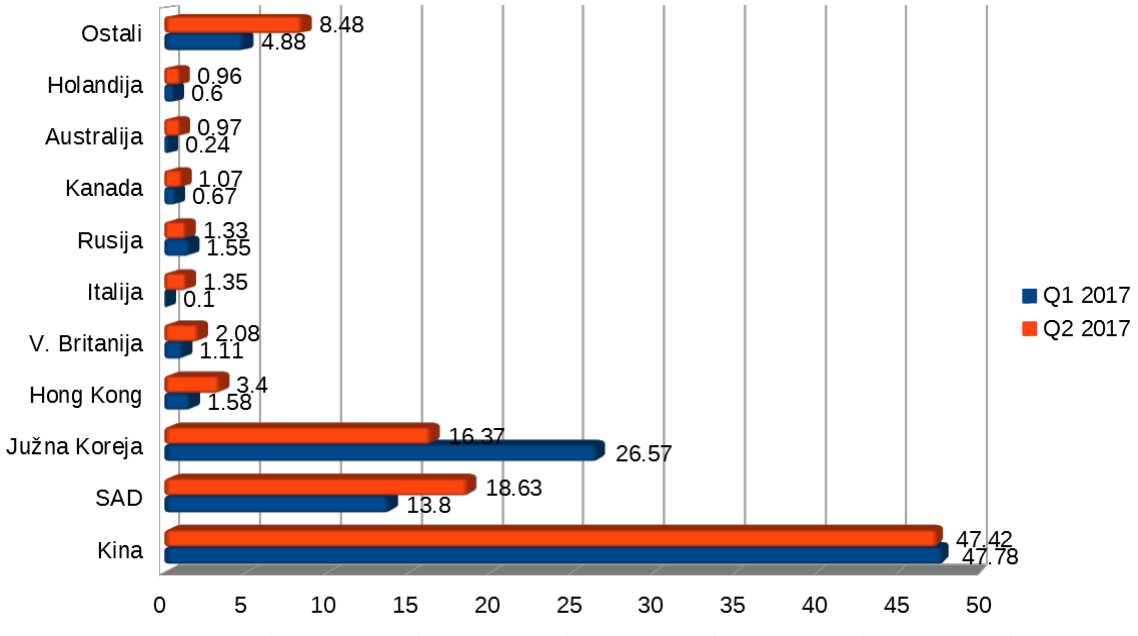
Slika 6: Raspodela napada po tipovima u izveštaju kompanije Kaspersky Lab za drugi kvartal 2017.

Po lokaciji C&C servera (slika 7) skoro polovina servera je locirano u Južnoj Koreji, oko 49% zatim slede SAD sa oko 16% i Kina sa 7.74%.



Slika 7: Raspodela napada po lokaciji kontrolnih servera u izveštaju kompanije Kaspersky Lab za prvi i drugi kvartal 2017.

Ove tri zemlje dominiraju i raspodelom ciljeva napada (slika 8), s tom što je u ovom slučaju najviše ciljeva u Kini sa oko 58%, zatim SAD i Južna Koreja sa po oko 14%.



Slika 8: Raspodela napada po lokaciji ciljeva napada u izveštaju kompanije Kaspersky Lab za prvi i drugi kvartal 2017.

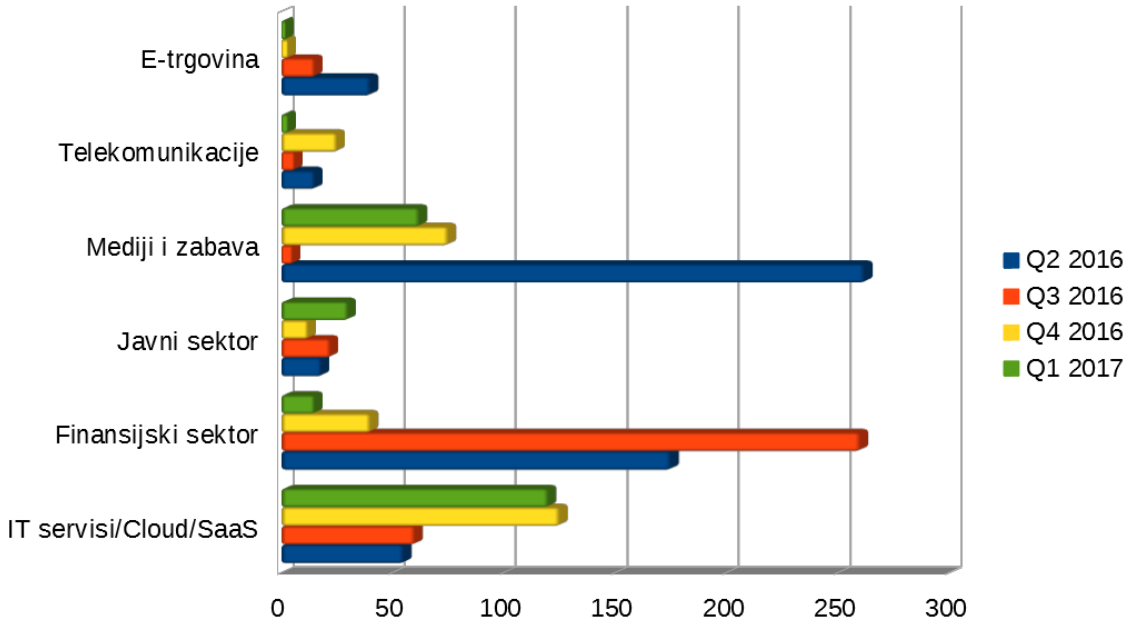
Po tipu OS koje koriste botnet mreže, oko 51.% otpada na Linux a oko 48% na Windows.

Najduži napad je trajao oko 277 časova, dok je velika većina napada, oko 85% trajala manje od 4 časa.

Prema izveštaju kompanije Verisign za prvi kvartal 2017 [6], najviše ciljeva napada, bilo je u sektoru IT usluga uključujući Cloud usluge, oko 58%, zatim slede finansijske institucije sa 28%. Detalji su prikazani u tabeli 1.Preko 36% napada su snage preko 5Gbps. Oko 43% napada koriste samo jedan tip napada dok su ostali kombinovani i sadrže i do 5 različitih tipova napada.

Najjači napad imao vršnu jačinu od 120Gbps i sastojao se od razdvojenih udara prosečne jačine 60Gbps i trajanja oko 15 časova. Ukupno trajanje cele aktivnosti bilo je 15 dana. Napad je bio kombinovanog tipa sa najviše korišćenim TCP SYN i TCP RST preplavljivanjima.

Na slici9 su prikazani vrhovi jačina napada po sektorima za četiri uzastopna kvartala od 2016 do 2017 godine.



Slika 9. Vrhovi jačine DDoS napada po industrijskim sektorima a pod nadzorom kompanije Verisign. Preuzeto sa https://www.verisign.com/assets/report-ddos-trends-Q12017.pdf

Tabela 1: Udeo DDoS napada po sektorima sa prosečnom jačinom napada za subjekte koji su koristili Verisign zaštitne mehanizme

Sektori	***Procenat napada po sektorima***	***Prosečna jačina napada***
Cloud servisi	58%	22.5 Gbps
Finansijske institucije	28%	1.7 Gbps
Mediji/zabava	6%	0.63 Gbps
E-trgovina i e-marketing	4%	32.6 Gbps
Telekomunikacije	2%	0.51 Gbps
Javni sektor	2%	31.9 Gbps

Alati za DDoS napade

Alati kojima je moguće izvesti napad odbijanjem usluge su lako dostupni na Internetu i njihova upotreba ne zahteva visoka tehnička znanja. Neki od njih su razvijeni upravo kao softver za testiranje napada odbijanjem usluge ili su napisani iz razloga da skrenu pažnju na opasnost ali su se ubrzo transformisali u oružje koje služi istoj svrsi protiv koje su sami nastali. U nastavku je dat kratak opis najaktuelnijih alata poslednjih godina. Detalji se mogu naći u [83].

LOIC (Low Orbit Ion Cannon). Generiše masivnu količinu TCP, UDP ili HTTP zahteva ka ciljnom serveru. Početna ideja autora ovog alata je bila da se koristi za izazivanje visokog mrežnog opterećenja servera u svrhu testiranja. Kao takav,LOIC ne sakriva svoju IP adresu pa ga mnogi volonteri koji učestvuju u politički motivisanim kampanjama koriste bez sakrivanja IP adrese, nesvesni da je njihova aktivnost vidljiva. To je 2011. godine dovelo do hapšenja grupe LOIC napadača.

HOIC (High Orbit Ion Cannon) je skrenuo pažnju na sebe uspešnim napadom na američko ministarstvo pravde kao odgovor na pokušaj zatvaranja sajta megaupload.com. To je u stvari skript nezavisan od platforme koji ima mogućnost instalisanja na klijentske računare tekst fajla sa dodatnim skriptom. Na taj način se menja karakteristika napada i veoma je teško prepoznati ovaj napad od strane zaštitnih mehanizama.

Hping je usavršena ping komanda sa dodatnim opcijama. Može da pokrene masivan TCP saobraćaj ka ciljnom računaru i to svaki put sa promenjenom IP adresom.

Slowloris je dizajniran za spori napad koji je teško detektovati. Upućuje se HTTP zahtev serveru i šalje HTTP zaglavlje u malim delovima . Server čeka na sledeći deo poruke koja dolazi sa velikim vremenskom zaostatkom. Rezervišu se resurse koji se sporo oslobadjaju. Kada se sve otvorene konekcije iscrpe, server više ne može da opslužuje zahteve.

R U Dead Yet - R.U.D.Y je takodje spori napad koji šalje HTTP POST zahtev u veoma malim delovima, jedan po jedan. Napadač može da otvori više istovremenih veza i tako iscrpe tabele otvorenih veza.

#Refref napad koristi postojeću ranjivost ciljnog sistema, za razliku od prethodno opisanih alata koji su efikasni i bez efektivne ranjivosti. Šalje se skriveni zahtev za izvršavanje SQL skripta koji sadrži beskonačnu petlju SQL upita, što na kraju obara SQL server. Dovoljan je jedan računar sa koga može da se izvrši obaranje servera. Poznat je primer ovog napada koji je trajao svega 17 sekundi a koji je izazvao zastoj ciljnog sajta od 42 minuta.

Botnet - Iako nije samo softverski alat već infrastruktura za napad, botnet je najmoćniji vid napada odbijanjem usluge. Ne postoji jedinstven način formiranja botneta kao ni jedinstven način napada na odabrani cilj. Direktni napadači su korisnici računara koji nisu svesni da je na njihovim računarima instalisan zlonameran kod. Skoro je

nemoguće deaktivirati botnet jer se sastoji od čak miliona računara rasporedjenih po svetu.

Ostale anomalije mrežnog saobraćaja

DDoS napad nije jedini dogadja na mreži koji izaziva statističke anomalije saobraćaja. U [7] dat je pregled takvih dogadjaja od kojih su neki potpuno regularni dogadjaji amogu da imaju sličan odziv u promeni entropije da ih nije moguće razlikovati od DDoS napada. Razlikovanje ovih dogadjaja kako od DDoS napada tako i medjusobno još uvek je tema mnogih radova u ovoj oblasti [53], [55]. Najčešće se koristi kombinovanje metode zasnovane na anomalijama sa metodama zasnovanim na potpisima.

Alfa tok (Alpha Flows) je neuobičajeno velika količina podataka razmenjena izmedju dve tačke.

*Flash crowd*je neuobičajen porast saobraćaja ka jednom odredištu.

*Skeniranje adresa*je akcija ispitivanja mreže, najčešće nedozvoljena mada može biti i regularna, gde se ispituje vezaka velikom broju adresa a za relativno mali skup portova.

Slična akcija *je skeniranje portova*koja ispituje vezu ka velikom broju portova a za relativno mali skup IP adresa.

Pomeranje ulaznog saobraćaja (Ingress-Shift) preusmeravanje toka saobraćaja kao drugim delovima mreže usled poslovnih aktivnosti.

*Ispad mreže*je promena karakteristika saobraćaja usled kvara ili postupka održavanja.

Jak saobraćaj od jedne tačke ka mnogo tačaka, obično je to distribucija medijskih i drugih sadržaja.

Aktivnost zlonamernih programa - propagacija zlonamernog programskog koda ili aktivnost na ispitivanju ranjivosti sistema. Može se posmatrati kao varijanta skeniranja mreže ali je znatno složenijeg opsega.

3. Teoretske osnove detekcije anomalija saobracaja

Metodi zasnovani na anomalijama

Kod metoda zasnovanih na anomalijama u saobraćaju, osnovni problem je odredjivanje metrike koja bi pokazala kvantitativno odstupanje od uobičajenog saobraćaja. Za samu meru informacije postojinekoliko pristupa koji se koriste u metodama zasnovanim na anomalijama: upotreba entropije, upotreba složenosti, i upotreba samosličnosti.

Entropija

Entropija kao mera neuredjenosti sistema prvi put je uvedena u termodinamici od strane Clausius-a 1850. Shannon je 1948 [8] prilagodio entropiju teoriji informacija. U teoriju informacija entropija je uvedena kao mera nepredvidivosti ili neizvesnosti sistema. Entropija je najveća za potpuno slučajne podatke koji dolaze iz nekog izvora informacija, a najmanja kada izvor informacija daje potpuno predvidljive podatke. Iako na praktičnom nivou veza izmedju pojma entropije u termodinamici i u teoriji informacija nije očigledna, ista formula za entropiju se koristi meru informacije koju nosi promenljiva koja je izlaz iz diskretnog izvora informacija. Široko je korišćena Šenonova formula:

$$\mathrm{H}(Z) = -\sum_{i=1}^{n} p(z_i)\log(p(z_i)) \qquad (1)$$

Gde je z_i konkretna vrednost iz skupa Z a p(z_i) je verovatnoća da Z uzme vrednost z_i.

Vrednost entropije se normalizuje sa $\log_2 N$ gde je N broj mogućih različitih vrednosti unutar datog intervala. U teoriji informacija baza logaritma je 2.
Neke od važnih osobina entropije su:

Nenegativnost: $\forall p(x_i) \in [0,1] X_S \geq 0;$

Simetričnost: $H_S(p(x_1), p(x_2),...) = H_S(p(x_2), p(x_1),...)$;

Maksimalnost: $H_S(p(x_1),..., p(x_n)) \leq H_S(\frac{1}{n},..., \frac{1}{n}) = \log_a(n);$

Aditivnost: $H_S(X,Y) = H_S(X) + H_S(Y)$; (za nezavisne X i Y)

Ostale osobine mogu se naći u [9]

Shannon-ova entropija predstavlja kompromis izmedju doprinosa glavne mase (koncentracije dogadjaja koji se često pojavljuju) i doprinosa periferijatj. redjih dogadjaja. U ovom slučaju taj kompromis ne može da se menja. Da bi se omogućilo podešavanje ovog doprinosa, uvode se parametrizovane generalizacije Shannonove entropije, Tsallis entrolija [10] i Renyi entropija [11]. Obe entropije koriste parameter q koji se može menjati. Parametar q ako je se menja ka većim pozitivnim vrednostima ističe glavnu masu, a ako se menja ka negativnim vrednostima ističe periferiju tj. retke dogadjaje. Ova osobina može imati važnu ulogu u podešavanju osetljivosti detektora anomalija.Obe ove parametrizovane entropije izvode se iz Kolmogorov-Nagumo generalizacije pojma sredine:

$$< X >_{\Phi} = \Phi^{-1}(\sum_{i=1}^{n} p(x_i)\Phi(x_i)$$

Gde je Φ funkcija koja ispunjava postulat aditivnosti.

Renyi entropija se dobija upotrebom funkcije

$$\Phi(x_i) = 2^{(1-q)x_i}$$

Posle uvrštavanja ove funkcije u Kolmogorov-Nagumo generalizacijui niza transformacija, dobija se izraz za Renyi entropiju:

$$H_R(X) = \frac{1}{1-q}\log_a(\sum_{i=i}^{n} p(x_i)^q)$$

Kada se q približava 1, Renyi entropija se poklapa sa Shannon-ovom.

Tsallis entropija se dobija upotrebom funkcije

$$\Phi(x_i) = \frac{2^{(1-q)x_i} - 1}{1-q}$$

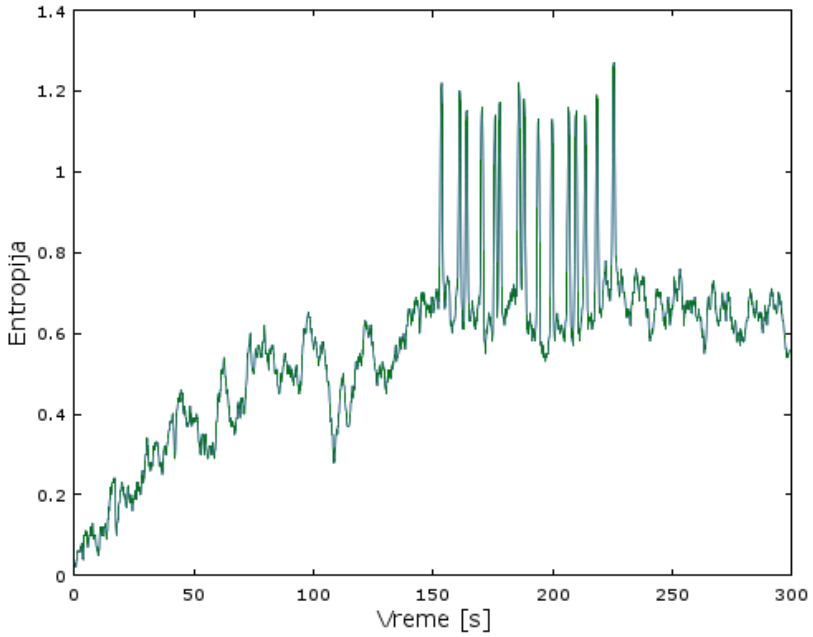
Posle uvrštavanja ove funkcje u Kolmogorov-Nagumo generalizaciju i niza transformacija, dobija se izraz za Tsallis entropiju:

$$H_T = (\frac{1}{1-q})(\sum_{i=1}^{n} p(x_i)^q - 1) \qquad (2)$$

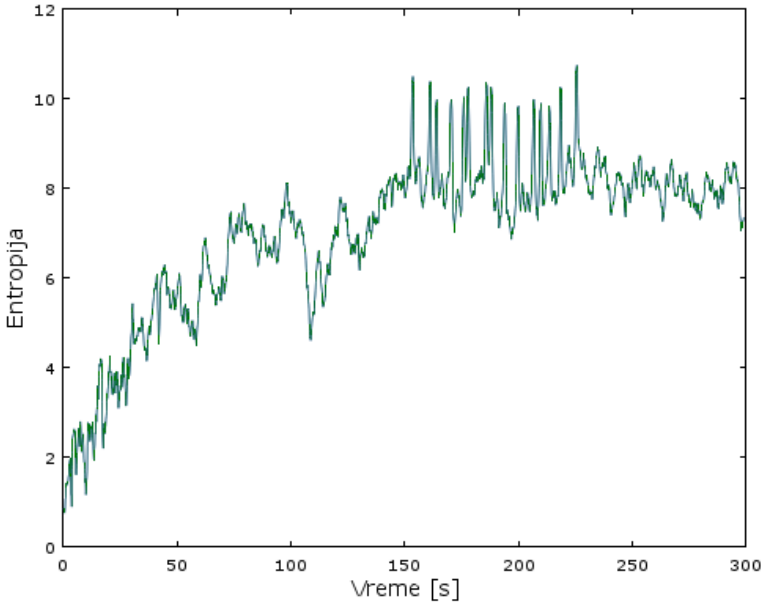
Za obe parametrizovane entropije važi:

- Za q > 1 ističe koncentraciju distribucije, za q < 1 ističe disperziju distribucije
- Za q $\rightarrow$ 1 konvergira ka Shannonovoj entropiji
- Tsallis entropija je osetljivija od Renyi entropije za vrednosti q < 0, dok je manje osetljiva za q > 0.

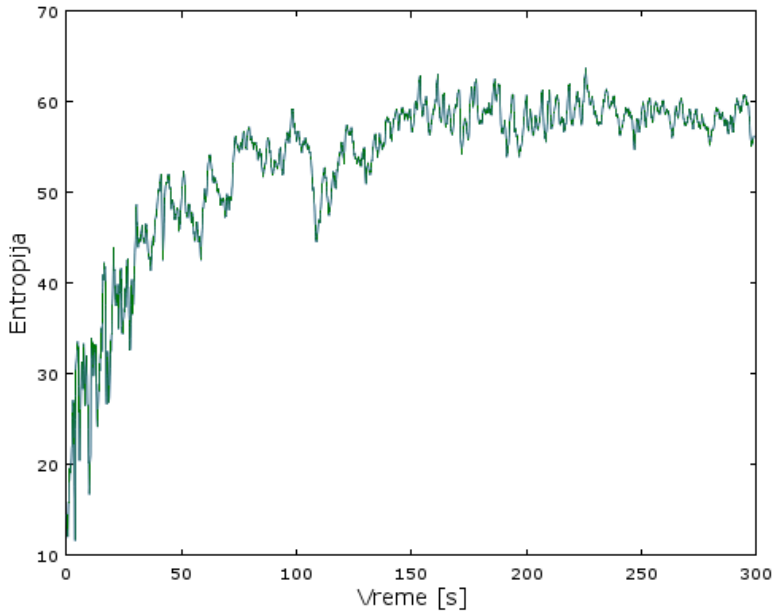
Osobina da se za q < 1 ističe disperzija distribucije je od velike važnosti za osetljivost detektora anomalija mrežnog saobraćaja. To se vidi na slikama 10-a do 10-c gde su prikazane entropije u istom eksperimentu za tri različite vrednosti parametra q.



Slika 10-a: Za parameter q=0.3 za Tsallisovu entropiju ističu se retki dogadjaji. Napadi izmedju 150 i 225 sekundi su izrazito izdvojeni u odnosu na normalan saobraćaj.



Slika 10-b: Za parameter q=0.7 za Tsallisovu entropiju retki dogadjaji su nešto slabije istaknuti ali i dalje jasno izdvojeni u odnosu na normalan saobraćaj.



Slika 10-c: Za parameter q=1.20 ističu se dogadjaji bliži srednjoj vrednosti, ekstremi se prigušuju. Napadi su sada jedva vidljivi.

U procesu detekcije DDoS napada, entropija se izračunava na uzorku uzastopnih paketa podataka za odabrana polja u zaglavlju paketa. Poredjenjem vrednosti entropije odabranih polja zaglavlja za jedna uzorak, sa entropijom odgovarajućih polja drugog uzorka detektuju se razlike u slučajnosti raspodele. Već je zapaženo da dok je mreža u uobičajenom stanju, vrednosti entropije za razna polja iz zaglavlja padaju u odredjen opseg vrednosti. Kada je mreža pod napadom, ovajopseg se značajno menjaju. U zavisnosti od konkretnog polja opseg može da se značajno smanji ili poveća. Na taj način je moguće detektovati napad.

Značaj metoda zasnovanih na anomaliji entropije je njihova opštost. Značajna promena u nivou entropije može biti znak da je mreža pod DoS napadom bez obzira na konkretan tip napada. Zato ove metode mogu da otkriju nove nepoznate vrste napada (zero-day attack). Većina metoda kreiranih za specifičan tip napada, iako efikasni za napad za koji su kreirani, ne mogu detektovati druge tipove napada.

Složenost

Kao mera složenosti-kompleksnostiinformacije unutar nekog niza simbola uzima se broj koraka koji je potreban da bi se posmatrani niz formirao. Za niz od potpuno slučajnih simbola potreban je broj koraka jednak dužini niza i njegova složenost je maksimalna. Sa druge strane složenost niza ’abab...ab’ je jednaka složenosti niza ’ab’. Centralnu ideju ideju u ovom pristupu zauzima kompleksnost Kolmogorova

[12,13,14]Ova mera složenosti informacije ne može da se numerički izračuna, kako je dokazano u [13] i [15]. Zato se koriste alternativne mere za kompleksnost koje mogu da se izračunaju kao **LZ** (Lempel-Ziv)[16,17,18] kompleksnost koja je usko povezana sa algoritmima za kompresiju. Kompleksnost je u ovom slučaju relacija izmedjumetrike komprimovane i originalne informacije. Ako se informacija ne može komprimovati onda je njena kompleksnost najveća. Postoji više varijanti algoritma za izračunavanje LZ kompleksnosti.

T-kompleksnost je takodje alternativna mera kompleksnosti stringa predlozena od Titchenera [19]. Kao i LZ familija kompleksnosti, i ona definise kompleksnost stringa kao broj elementarnih koraka potrebnih da se dati string konstruise. Postupak merenja kompleksnosti sastoji se u preslaganju stringa tako da se grupišu isti simboli. Ovaj postupak se naziva T-augmentacija. Detalji postupka konstruisanja datog stringa mogu se naci u [20][21]. T-kompleksnost se definise kao:

$$C_T = \Sigma \log(k_i + 1)$$

Gde su k_i težinski koeficijenti algoritma T-augmentacije.

Titchener je zapazio da je gornja granica T-kompleksnosti asimptotski ekvivalentna integralnom logaritmu [22]li(|x|) u intervalu $[1, \infty]$. Integralni logaritam se definiše kao

$$li(x) = \int_0^x \frac{dt}{\ln(t)}$$

Da bi se dobila mera informacija koja je kompatibilna sa Shannon-ovom entropijom, uvodi se T-informacija koja

$$I_T(x) = li^{-1}(C_T)$$

T-entropija je konacno izražena formulom:

$$H_T(x) = \frac{dI_T(x)}{d|x|} \tag{3}$$

Poseban slučaj je usrednjena T-entropija:

$$\overline{H}_T(x) = \frac{I_T(x)}{|x|} \tag{4}$$

T-entropija, budući da potiče od pojma kompleksnosti je osetljivija na na varijacije posmatrane veličine od Shannonove entropije. Tako je na primer entropija dva stringa: ’abababababab’ i ’abbbaabba’u slučaju Shannon ili Tsallis entropije identična, dok

T-entropija za ova dva stringa nije ista jer je potreban različit broj koraka da bi se dva stringa formirala [23]. I u slučaju mrežnog saobraćaja T-entropija je dobar kandidat za detekciju dogadjaja koje drugi metodi možda ne mogu da detektuju sa dovoljnom osetljivošću, pa je zbog toga T-entropija uključena u ovo istraživanje. Za računanje T-entropiju korišćen je program libflot [24].

Samosličnost

U matematici je samosličnost (self-similarity) osobina da je objekat u potpunosti ili delimično sličan sa svojim delom. Najpoznatiji oblik koji ima osobinu samosličnosti je Kohova kriva na slici 11. Morska obala je statistički samoslična svakom svom i najmanjem delu. Poznat je paradoks morske obale čija se tačna dužina ne može izmeriti, kao ni dužina Kohove krive, jer svaki njihov i najmanji deo zadržava karakteristike celine.

Dugo vremena u mrežnom saobraćaju se vreme pristizanja paketa modelovalo kao Poasonov process. Tek relativno nedavno pojavila su se istraživanja koja su pokazala da ovaj process pokazuje ponašanje koje se nije u prirodi Poasonovo[25]. Te studije su dokazale da mrežni saobraćaj pokazuje ponašanje koje se slično fraktalima i koje se naziva samosličnost. Mrežni saobraćaj (slika 12) varira u intenzitetu u toku dana ili radne nedelje. Na početku nekog posmatranog perioda aktivnost na mreži je manja a zatim postepeno raste sve dok ne dostigne maksimalne lokalne vrednosti za dati period. Medjutim, signal mnogih karakterističnih promenljivih u vremenu, bez obzira na intenzitet, je sličan za bilo koji vremenski interval. Jedan način da se definiše samosličnost je pomoću Hurstovog efekta. Za neki signal X u vremenu definiše se očekivanje:

$$E\left[\frac{R(n)}{S(n)}\right] = Cn^H$$

Gde su:

n broj odbiraka

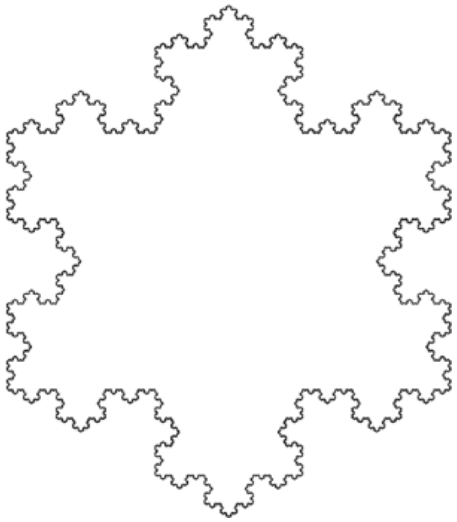
C konstanta

R(n) = max(0, W1, ...Wn) − min(0, W1, ...Wn), opseg vrednosti

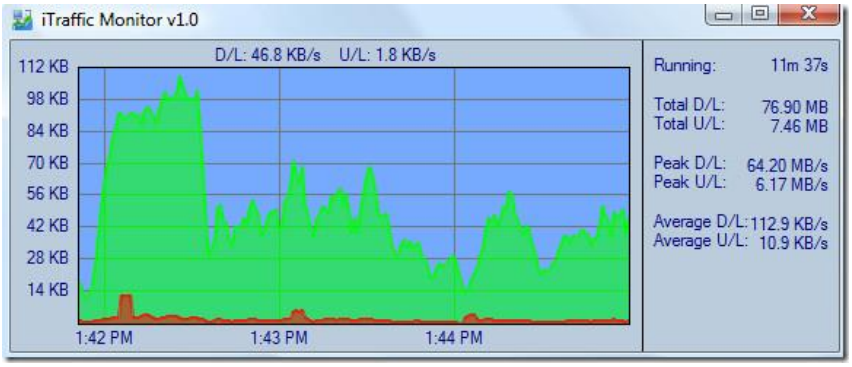
S(n) = $\sqrt{\frac{\sum_{i=1}^{n}(X_i - \overline{X})^2}{n-1}}$ standardna devijacija

$W_k = \sum_{i=1}^{n} X_i - k\overline{X}$, za k=1,2,…,n

Eksponent H je Hurstov eksponent ili parameter. Kada je 0.5 < H < 1 kriva pokazuje osobine samosličnosti. DDoS napad po svojoj prirodi narušava samosličnost mrežnog saobraćaja, tako da pri DDoS napadu dolazi do pada H parametra i ta se osobina koristi u detekciji.



Slika 11: Kohova kriva ima osobine samosličnosti.

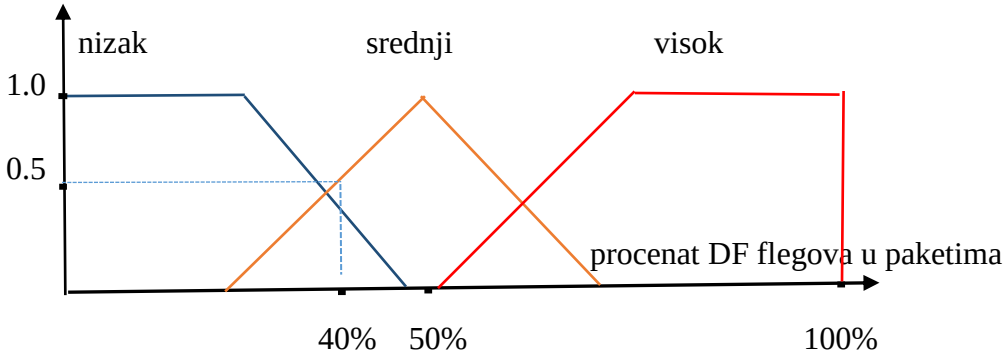


Slika 12: Mrežni saobraćaj pokazuje osobine samosličnosti svakog svog dela sa celinom. Narušavanje samosličnosti može da detektuje anomalije u saobraćaju.

4. Fazi logika

U situacijama kada se znanje o nekom sistemu nije moguće opisati u potpunosti precizno ili je taj opis podesnije dati u u kvalitativnom obliku. Često je bliže ljudskom poimanju iskazati veličine u obliku koji je blizak izrazima koje koristimo u svakodnevnoj komunikaciji nego kao precizne vrednosti. Čovek teško može da svojim čulima razlikuje temperaturu -3 od -4, ali će odrednica 'veoma hladno' mnogo jasnije saopštiti vrednost temperature. Logika da je nešto potpuno tačno ili potpuno netačno je nekada suviše kruta. U takvim slučajevima je mnogo je prirodnije dati podatak koliko je neka vrednost bliska vrednosti potrpuno tačno ili potpuno netačno. Logika koja se tada koristi naziva se fazi (rasplinuta) logika. Fazi logiku je uveo Lotfi Zadeh [26] 1965. U teoriju upravljanja fazi logikuje uveo Mamdani [27] 1976. Fazi logika ne poznaje tačne vrednosti. Vrednost neke veličine pripada nekom fazi skupu sa nekim stepenom pripadnosti koji varira u rasponu 0-1. Na slici 13Za x=40, pripadnost fazi skupu koji označava srednji nivo pojave dogadjaja je 0.5.

Funkcija koja ograničava površinu fazi skupa naziva se *funkcija pripadnosti*. Funkcija pripadnosti najčešće može biti trougaona, trapezoidna ili normalna raspodela. obično se bira funkcija koja omogućava jednostavnije numeričko izračunavanje izlazne vrednosti, tako da su trougao ili trapez veoma česte aproksimacije (slika 13). Na slici je dat primer primene fazi logike u detekciji dogadjaja na mreži posmatrajući pojavu DF (Don't fragment) flega u IP zaglavlju.



Slika 13: funkcije pripadnosti koje ograničavaju fazi skupove na primeru učestanosti DF flega u IP zaglavlju.

Faze u procesu

- Fazifikacija
- Primena pravila zaključivanja
- Agregacija pravila zaključivanja
- Defazifikacija

U procesu **fazifikacije** numeričkim vrednostima se dodeljuju stepeni pripadnosti svakom od fazi skupova. Fazi skupovi mogu imati lingvističke vrednosti ako postoji jasna struktura sistema koja se može opisati terminima govornog jezika. Na slici 13 vrednost učestanosti pojave DF flega se preslikava na nekoliko fazi skupova a stepeni pripadnosti su nizak, srednji i visok.

Fazi zaključivanje (Fuzzy inference system, FIS) je proces u kome se formiraju veze izmedju ulaznih fazi veličina i izlazne fazi veličine koja predstavlja zaključak.
Za ovaj proces se koristi lingvistička baza znanja o sistemu koja se primenjuje na fazi promenljive i dobijaju se izrazi u obliku:

IF (Premisa1) AND (Premisa2) THEN Zakljucak1
OR
IF (Premisa3) OR (Premisa4) THEN Zakljucak2

Primer sa slike može biti deo izraza za detekciju DDoS napada:

Ako je procenat DF flegova ***visok***
I
Ako je entropija ***visoka***
Onda je ***napad u toku***

Agregacija se koristi kada ima više pravila zaključivanja. U ovom koraku kombinuju se izlazi iz svakog pravila u jedinstven fuzzy skup korišćenjem operacije fuzzy agregacije. Najčešće korišćen operator agregacije je maksimum. Koriste se i zbir i probabilistički zbir.

Defazifikacija je proces koji iz fazi skupa izvodi kvantitativan tj tačan rezultat koji se koristi kao izlaz. Defazifikacija nije u opštem slučaju nužna, jer izlaz sistema može da bude i fazi skup.Slučaj kada je defazifikacija nužna su sistemi upravljanja jer su tada potrebne tačne izlazne vrednosti. Rezultat defazifikacije predstavlja numeričku vrednost koja najbolje reprezentuje fazi skup dobijen procesom zaključivanja.

Postoji mnogo metoda za odredjivanje tačke koja reprezentuje ceo fazi skup i tako se ponovo dobije numerička vrednost. Neke od najčešće korišćenih su:

- Metoda centra gravitacije (CoG, Center of Gravity)– traži se tačka koja predstavlja težište površine koja predstavlja fazi skup
- Metoda srednje vrednosti maksimuma (MoM) – srednja vrednost lokalnih maksimuma funkcije pripadnosti.
- Metoda polovljenja prostora – tačka koja polovi površinu površine ograničene funkcijom pripadnosti.

Proces defazifikacije može da bude veoma zahtevan, što je problem u sistemima upravljanja u realnom vremenu.Veliki broj metoda defazifikacije upravo je i posledica potrebe da se defazifikacija optimizuje.
http://www.dma.fi.upm.es/recursos/aplicaciones/logica_borrosa/web/fuzzy_inferencia/mamdani1_e

U praksi se najčešće koriste dva sistema zaključivanja: tip Mamdani i tip Sugeno (sa svojim podvarijantama). Kod sistema tipa Mamdani pretpostavlja da je izlazna veličina procesa zaključivanja takodje fazi skup. Ako postoji više pravila, obavezan je agregacioni proces rezultata svih pravila pre postupka defazifikacije, u kome se dobija funkcija pripadnosti.

Mamdani model ima sledeće prednosti:

- Mamdani model je intuitivan i kao takav mnogo podesniji za podatke koji se unose od strane čoveka.
- Mamdani model je široko prihvaćen.

S druge strane u nekim slučajevima Mamdani model ima odredjene slabosti:

- Mamdani model je praktično upotrebljiv samo ako postoji mali broj promenljivih.
- Broj pravila eksponencijalno raste sa brojem promenljivih uzroka.
- Što se više pravila konstruiše teže se određuje da li su ta pravila odgovarajuća za dati sistem.
- Pri velikom broju promenljivih uzroka teško je definisati jasnu (za čoveka) vezu izmedju uzroka i posledica.

Često u praksi imamo samo skup ulaznih podataka i izlaznih podataka i potrebno je na osnovu njih odrediti pravila. Sistem tipa Sugeno koji je predložen od strane Takagi, Sugeno i Kanga, [28][29][30] ima za cilj da se razvije sistematski pristup generisanju fazi pravila iz datog ulazno-izlaznog skupa podataka.
U poredjenju sa Mamdani modelom, prednosti TSK modela su:

- Podesan za sisteme kod kojih struktura nije unapred poznata
- TSK model je podesniji za izračunavanje.
- TSK model omogućava tehnike adaptacije tako da funkcije pripadnosti mogu da se prilagodjavaju po potrebi. Ovo je veoma važno pri modelovanju veoma dinamičnog saobraćaja kao što je Internet, gde se parametri okruženja veoma brzo menjaju.
- TSK model garantuje kontinuitet izlaznog prostora, što kod Mamdani modela ne mora biti slučaj.
- Broj pravila je manji nego u Mamdani modelu čak i za sisteme visokog stepena složenosti [31][32].

TSK model podržava sistematski pristup generisanju fazi pravila iz datog skupa ulazno izlaznih podataka gde struktura sistema nije unapred poznata. Detekcija statističkih anomalija u mrežnom saobraćaju gde se obradjuje velika količina ulazno-izlaznih podataka zahteva upravo taj tip modela. Kod opisa mrežnog saobraćaja u opštem slučaju teško je postaviti intuitivna pravila koja su bliža ljudskoj percepciji. To daje prednost TSK modelu u odnosu na najčešće korišćeni Mamdani fazi model.

Za Takagi-Sugeno-Kang (TSK) je karakteristična visoka preciznost u odredjivanju modela u kombinaciji sa brzim procesom obuke. Tipično fazi pravilo u TSK fazi modelu je u formi

akox je A
I
akoy je B

ondaz je f(x,y)

Gde su A i B fazi skupovi, dok je f(x,y) funkcija tačne (crisp) vrednosti. Obično je u polinomnoj formi mada može biti bilo koja funkcija. Kada je funkcija f konstanta radi se o TSK modelu nultog reda a za slučaj polinima prvog stepena model je prvog reda, koji se najčešće koristi

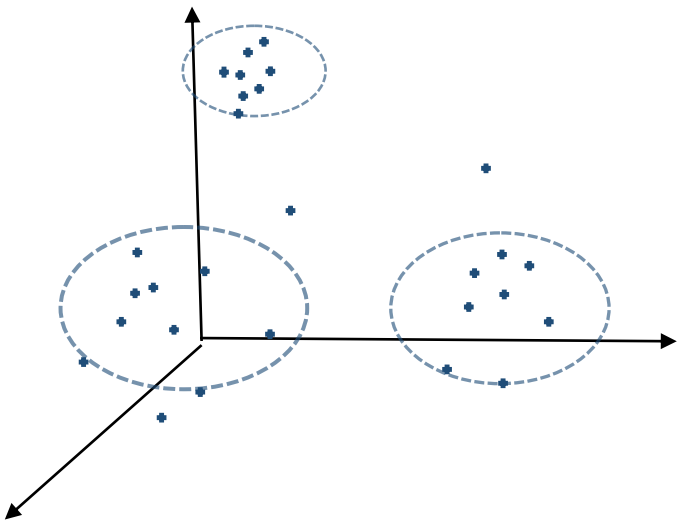
5. Takagi-Sugeno-Kang model

Kada imamo prikupljenu veliku količinu ulazno-izlaznih podataka nekog sistema, struktura nije očigledna i ekspertsko znanje tada ne može da formuliše fazi skupove i formira pravilakoja su razumljiva čoveku u obliku

„AKO je premisa1 I AKO je premisa2 ... ONDA je zakljucak1“.

Tada se nameće potreba da se proces identifikacije [78] strukture sistema automatizuje primenom metoda neuralnih mreža ili recimo data-mining-a. Slučaj koji se obradjuje u ovom radu upravo spada u tu klasu problema. Struktura sistema se odredjuje primenom neuralnih mreža, a zatim se primenjuje TSK model koji daje linearnu zavisnost izlaza od ulaza.

Karakteristika TSK modela je njegova visoka preciznost modeliranja i brz proces učenja. TSK model je već do sada uspešnoprimenjen na mnoge realne probleme. Neki od njih su aproksimacija statičkih nelinearnih funkcija, prognoza kretanja na berzama, prognoza potrošnje prirodnog gasa, procena brzine DC motora. Prednost TSK modela zasnovanog na fazi pravilima je što zahteva relativno mali broj pravila čak I za modeliranje relativno složeni sistema. Broj pravila je znatno manji nego kod primene Mamdani fazi modela [32].



Slika 14: Složen sistem se često može prikazati povezanih podsistema. Klasifikovanje tačaka u N-dimenzionalnom sistemu u klastere putem neuralnih mreža je prvi korak u definisanju TSK modela.

Ideja TSK modela je da se složen sistem može prikazati kao skup medjusobno povezanih podsistema. Podsistemi su u N-dimenzionalnom prostoru ulaznih vektora klasteri u kojima se tačke gomilaju (slika 14). Ovi podsistemi, ako se pouzdano klasifikuju, mogu biti opisani jednostavnijom funkcionalnom zavisnošću. Ako se medjuzavisnost tretira kao linearna, i ako jedno pravilo odgovara tačno jednom podsistemu, konačni model sa K pravila može se prikazati u sledećoj formi:

R_i : Ako x_1 pripada A_{i1}
i x_2 pripada A_{i2}
i. . .
i x_n pripada A_{in}

tada važi:

$$y_i = \mathbf{a_i x} + b_i, \quad i = 1, 2, \ldots, K \qquad (5)$$

Gde je R_ii-$_{to}$ pravilo, x_1, x_2, … x_n su ulazi , A_{i1}, A_{i2}, …, A_{in} su fazi skupovi dodeljeni svakoj ulaznoj promenljivoj, y_i je izlazna promenljiva za *i-to* pravilo. Vektor $\boldsymbol{a}_i$ i scalar $b_i$su parametri linearne zavisnosti. U našem slučaju ulazi su vrednosti entropije unutar posmatranog vremenskog prozora, a izlazi su vrednosti DDoS napada:

0 za odsustvo napada,
1 ili neki broj različit od 0, ako je sistem u datom trenutku pod napadom.

Izlaz TSK fazi modela za ulaz x_k je:

$$\hat{y}_k = \sum_{i=1}^{K} [\omega_i(x_k) y_i(x_k)], \qquad k = 1,2,\ldots,N \tag{6}$$

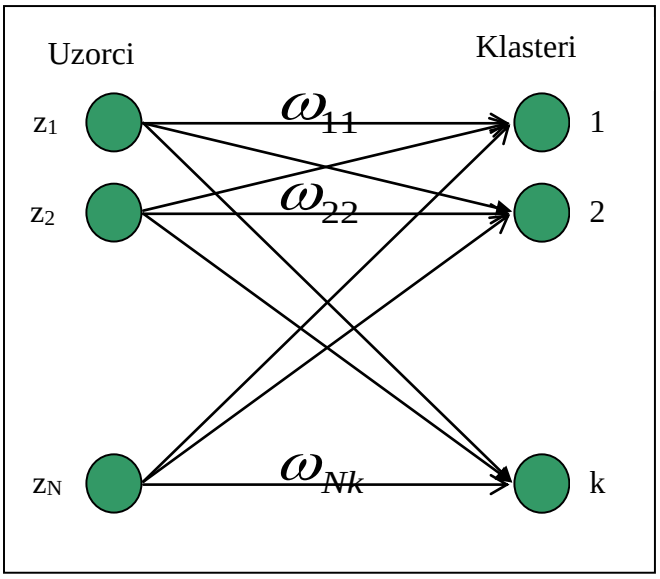
Gde je $\omega_i(x_k)$ normalizovan aktivacioni nivo za i_{to}pravilo k_{tog} ulaznog odbirka, i dato je kao ():

$$\omega_i(x_k) = \frac{\beta_i(x_k)}{\sum_{j=1}^{K} \beta_j(x_k)} \tag{7}$$

U prvom koraku, ulazno-izlazni prostor promenljivih izdeljen je na klastere. Algoritam za formiranje modela uzima podatke za učenje koji sadrže N ulazno-izlaznih uzoraka:

$$z_k = [x_k^T; y_k]^T \; k = 1,\ldots, N$$

gde je N ukupan broj svih odbiraka.



Slika 15: Struktura jednonivovske neuralne mreže

Svaki klaster predstavlja po jedan podsistem gde su ulazno-izlazni podaci grupisani. Podaci iz skupa za obučavanje koji su podeljeni po klasterima se dalje interpretiraju kao fazi pravila.

Jednonivovska neuralna mreža je grafički prikazana na slici 15. Svaki čvor u izlaznom nivou je u stvari centar odgovarajućeg klastera. Broj klastera je ulazni parameter algoritma. Dimenzija ulaznih podataka je N a dimenzija izlaza tj. broja klastera je na startu 1.Algoritam vrši iterativna podešavanja centara klastera koristeći metod najmanjeg kvadratnog rastojanja. Kada se koordinate centara klastera stabilizuju, u spoljnoj iteracionoj petlji se na slučajan način vrši približavanje centra klastera sa najmanje pridruženih ulaza ka klasteru koji ima najviše ulaznih uzoraka. Tako novi klaster dobija šansu da prikupi ulaze koji su mu najbliži i procedura se ponavlja dok svih K klastera ne budu optimalno postavljeni.Detaljan opis algoritma grupisanja je dat u [33,78].

Sledećoj faza je izračunavanje aktivacionih nivoa za pravila. Za svaki uzorak izračunava se euklidovo rastojanje d_{ik} od centra svakog od klastera. Kao rezultat, formira se fazi matrica particija U_{KxN}. Ova matrica sadrži vrednosti

$\mu_{ik} \in [0,1]$ za $1 \le i \le K$, $1 \le k \le N$,

koja predstavlja stepen pripadnosti k-tog odbirka i-tom klasteru.

Elementi matrice ***U*** se izračunavaju sledećim izrazom:

$$\mu_{ik}^{(l)} = \frac{1}{\sum_{j=1}^{K} \left(\frac{d_{ik}^2}{d_{jk}^2}\right)^{\frac{1}{(m-1)}}} \quad \text{za } d_{ik} > 0,$$

Ili:

$\mu_{ik}^{(l)} = 1$ za $d_{ik} = 0$

Vrednost aktivacionog nivoa i-tog pravila za svaki k-ti ulazni uzorak se dobija kao proizvod:

$$\beta ik = \beta i\,(\mathbf{x}k) = \prod_{j=1}^{n+1} \mu(z_{kj}) \quad k = 1, 2, 3, \ldots, N$$

Ovde se može upotrebiti prag ξ tako da ako je bilo koji od $\mu_{A_{ij}}(x_{kj}) < \xi$, $\mu_{A_{ij}}(x_{kj})$ se aproksimira nulom.

Normalizovani aktivacioni level ω_{ik} pravila $R_i$za k_{ti} uzorak se dobija korišćenjem Eq.(4), a dijagonalna matrica $\boldsymbol{W}i$ ($i = 1, \ldots, K$) dimenzije N x N se formira pomoću vrednosti aktivacionih nivoa.

Dalje se formira kompozitna matrica X' dimenzija Nx$K(n + 1)$:

$$X' = [(W_1 X_e), (W_2 X_e), \ldots, (W_k X_e)]$$

Gde matrica $\boldsymbol{X}e = [\boldsymbol{X}, 1]$ sadrži vrste [x_k^T ,**1**].

Na kraju parametri $\boldsymbol{a_i}^T$i$\boldsymbol{b_i}$jednačine (1)koji se nalaze u odgovarajućim delovima fazi pravila , se grupišu u vector:

$\theta' = [\theta_1^T, \theta_2^T, \ldots, \theta_K^T]^T$ dimenzija $K(n + 1)$

Gde je $\theta_i^T = [a_i^T; b_i]$ for $i = 1, \ldots, K$.

Jednačine (6) i (7) sad mogu da se predstave kao model u formi:

$$\hat{Y} = X'\theta' + \varepsilon \qquad (8)$$

Gde je ε is the greška aproksimacije.
Nepoznati parametar Θ' može se odrediti kao

$$\theta' = [(X')^T X']^{-1} (X')^T Y \qquad (9)$$

Detaljniji opis dat je u [34].

U ovom trenutku formiran je TSK model na osnovu ulaznih podataka za obuku kao i poznatog izlaza. Opisani postupak formiranja modela se izvršava jednom, u toku obuke a dobijeni model se primenjuje u izračunavanje izlaza za svakisvaki ulazni vektor. Model se može i adaptirati samo na osnovu ulaznog vektora i poznatog izlaza a da se ne ponavlja obuka. Ovo se izvodu koristeći WRLS (weighted recursive least square) algoritma za izračunavanje novog θ'(k+1) na osnovu θ'(k) i novog ulaznog vektora bez upotrebe zahtevne operacije invertovanja. Rekurzivni izraz WRLS algoritma je predstavljen kao:

$$\Phi(k+1) = \frac{1}{\lambda}\left[\Phi(k) - \frac{\Phi(k)x'(k+1)x'^T(k+1)\Phi(k)}{\lambda + x'^T(k+1)\Phi(k)x'(k+1)}\right]$$

$$\theta'(k+1) = \theta'(k) + \Phi(k+1)x'(k+1)\left[y(k+1) - x'^T(k+1)\theta(k)\right]$$

Gde je lambda faktor zaboravljanja koji daje veću težinu novijim ulaznim vektorima u odnosu na starije, Φ je matrica adaptacionog pojačanja, a $x^{'}$ je kompozitna matrica koja se sastoji od ulaznih vektora.

Snaga opisanog metoda, i razlog zašto je korišćen u ovom radu, je u tome da se model može adaptirati na osnovu ulaznog vektora i poznatog izlaza a da se ne mora ponavljati proces obuke. To je veoma važno kada se parametri detekcije DDoS napada menjaju usled dinamične promene okruženja.

6. Opis postojećih rešenja

Iako su u tekstu na na više mesta navode poredjenja rezultata i metoda sa drugim radovima, u ovom poglavlju su pobrojana i ukratko opisana rešenja koja se dotiču problematike izložene u tezi.

U eksperimentima opisanim u [7] autori su primenili Tsallis neekstenzivnu entropiju na dva mrežna saobraćaja preuzeta sa velikih univerzitetskih ili istraživačkih mreža. Prvi skup podataka sa mrežnim saobraćajem - dataset je preuzet sa „Abilene“ mrežehttp://abilene.internet2.edu/. [35] Ovaj dataset je sadrži podatke o saobraćaju u obliku IP tokova razmenjenih izmedju 11 pristupnih tačkaka tj. ukupno 121 izvor-odredište parova, tokom 7 meseci. Drugi skup je preuzet sa Geant panevropske mreže, generisan u okviru projekta Totem [36].U oba skupa podataka se ubacuju DDoS dogadjaji na kontrolisan način, da bi se dobili različiti intenziteti napada. Pokazano je da upotreba Tsallis entropije daje primetno bolje rezultate nego kad se primeni Shannon entropija. Tsallis entropija je izračunata koristeći optimalnu vrednost parametra q, koja se kreće oko vrednosti 0.9. Za razliku od metodologije primenjene u ovoj tezi, u ovom radu se samo utvrdjuje da li u nekom intervalu postoji ili ne postoji anomalija, a ne njen početak i kraj u vremenu.Interval je veoma dug (5-15 minuta) u odnosu na istraživanje u radu. Takodje, nema praga detekcije kojim se utvrdjuje promena stanja detektora.

U eksperimentu opisanim u [37], porede se rezultati dva detektora DDoS napada. Jedan je zasnovan na Shannonovoj entropiji a drugi [38] je podešen tako da efikasno prepozna DDoS napad tipa SYN poplava. Za detekciju početka odnosno kraja napada korišćen je CUSUM metod primenjen direktno na vremenskom signalu entropije. Performanse dva detektora poredjene su po osnovu procenta ispravnih i lažnih detekcija tj. grešaka tipa I (TPR, FPR) kao i kašnjenja promene stanja detektora. Eksperimenti pokazuju da metod zasnovan na Shannon entropiji beleži nešto slabije karakteristike od metoda specifično prilagodjenog datom tipu napada, ali takodje i ne zaostaju mnogo. To znači da će detektor zasnovan na entropiji dati zadovoljavajuće rezultate i za neki drugi tip napada za koji bi inače trebalo dizajnirati potpuno nov detektor.

U eksperimentu opisanim u [39], porede se rezultati dva detektora DDoS napada. Jedan je zasnovan na Shannonovoj entropiji a drugi na Tsallis entropiji. Kao generator saobraćaja korišćen je model u mrežnom simulatoru ns-2. Za detekciju početka odnosno kraja napada korišćen je CUSUM metod primenjen direktno na vremenskom signalu entropije. Performanse dva detektora poredjene su po osnovu procenta ispravnih i lažnih detekcija (TPR, FPR) kao i kašnjenja promene stanja detektora. Kao i u prethodnom eksperimentu, detektor koji koristi Tsallis entropiju pokazuje nešto bolje karakteristike.Postavke u ovom radu su korišćene i u tezi, koristi se simulator saobraćaja i CUSUM detekcija promene stanje. Eksperimenta iz ovog rada su delimično ponovljeni

u tezi radi poredjenja izlaza detekcije sa primenom TSK-FS metode i bez njene primene primene.

Problem performanse izračunavanja entropije u realnom vremenu je rešavan u [40]. Autori predlažu agregaciju IP paketa izmedju dve tačke u takozvani „tok“ (flow) tako da se kalkulacije izvode na nivou toka a ne na nivou paketa.

U radu [41,42] korišćena je fazi logika za detekciju DDoS napada. Posmatrana veličina je prosečno vreme izmedju uzastopnih paketa. Da bi se sakupilo dovoljno uzoraka za statističku obradu, paketi se grupišu u grupe od po 500, 1000, pa do 150000 paketa. Za svaku od ovih veličina grupa se izvodi nezavisan skup merenja da bi se isključio uticaj veličine grupe uzoraka na tačnost merenja. Računa se raspodela medjuvremena pristizanja paketa unutar posmatranih grupa paketa. Za vreme DDoS napada srednje vreme izmedju paketa se smanjuje. Da bi se izbegla upotreba fiksnog numeričkog praga za odstupanje srednjeg vremena izmedju paketa od srednjeg vremena normalnog saobraćaja, formira se fazi estimator koji odredjuje da li je unutar grupe uzoraka došlo do napada. Za mrežni saobraćaj korišćen je javni test saobraćaj DARPA LLS_DDOS_1.0-inside.dump. Poredjenjem sa datim (poznatim) trenucima napada unutar test saobraćaja postignuta je tačnost od 80% u odredjivanju perioda trajanja DDoS napada. Iako se koristi jedna veličina za detekciju napada, metod karakteriše opštost tako da dozvoljava primenu bilo koje druge veličine.

U [43,44,45] korišćena je T-entropija u detekciji DDoS napada.S obzirom da je T-entropija izvedena iz pojma kompleksnosti, parametri mrežnog saobraćaja se preslikavaju u simbole. Korišćeni su parametri koji mogu imati relativno mali broj diskretnih vrednosti i lako se preslikavaju u skup ASCII simbola. Za razliku od eksperimenata u ovoj tezi, preslikavanja izvorišnih i odredišnih IP adresa ovde nisu razmatrana, niti su IP adrese korišćene kao parametri u detekciji napada. Mrežni saobraćaj za eksperimentime je preuzet sa univerzitetske mreže u Oklendu (Novi Zeland) korišćenjem posebno dizajniranih mrežnih kartica koje u pasivnom režimu čitaju parametre paketa i beleže ih u datoteke u formatu prilagodjenom potrebama eksperimenata. Na ovaj način se dobije skup sa realnim saobraćajem, ali bez DDoS napada koji nije moguće izvesti na realnoj mreži bez uticaja na normalno odvijanje aktivnosti. Napadi su zato naknadno dodati u test saobraćaj. Nisu dati kriterijumi za detekciju početka kritičnog dogadjaja niti procenat tačnih i progrešnih već se eksperimenti zaustavljaju na grafičkom prikazu signala u vremenu.

U [46] prezentovano je rešenje za detekciju DDoS napada pomoću Wavelet transformacije koja spada uoblast samosličnosti. Normalan saobraćaj se tretira kao šum, dok se odstupanja tretiraju kao anomalije koje treba detektovati redukcijom šuma. Redukcija šuma ovde igra ulogu kao i TSK-FS metod jer rezultuje u smanjenju lažnih alarma.

Takodje baziran na samosličnosti je i rad [47]. Koristi se S-Transformacija i Renyi divergencija u utvrdjivanju odstupanja od samosličnosti. Autori navode da se

dobijaju nešto bolji rezultati u odnosu na primenu Wavelet transformacije. Koristi se DARPA test saobraćaj.

U [48] primenjena je tehnika Deep Learning u otkrivanju DDoS napada. Skup polja iz zaglavlja paketa korišćenih za klasifikaciju paketa su slična kao i u ovom radu. Oko 95% paketa sa malicioznim saobraćajem i oko 99% paketa sa normalnim saobraćajem su ispravno klasifikovani.

Poslednjih godina zbog lakše dostupnosti brzih hardverskih komponenti, softverski algoritmi se jednostavnije realizuju na hardverskim platformama. Eksperimenti u mnogim radovima se sada vrše direktno na FPGA komponentama. U [49] predloženo je rešenje FPGA arhitekture za detektovanje anomalija na mrežama velikih brzina. Rešenje se može konfigurisati u toku tako da je primenljivo na više tipova anomalija.

Efikasna detekcija DDoS napada u realnom vremenu je još uvek tema koja nije dovoljno obradjena. U [50]opisano je FPGA rešenje za brzu detekciju. Korišćeni su isti skupovi saobraćaja kao i u ovoj tezi. Metod održava u realnom vremenu profil normalnog saobraćaja i u skladu sa njim vrši klasifikaciju novopristiglhih paketa.

U [51] izlaže se rešenje za sprečavanje DDoS napada tipa SYN poplave, napada koji se uzima za primer u ovoj tezi, koristeći brze hardverske algoritme u FPGA arhitekturi. Algoritam reaguje na pojavu polu-otvorenih konekcija i sprečava dalji pristup mreži sa date adrese.

U [52], izložen je pregled problematike DDoS napada u infrastrukturi oblaka.

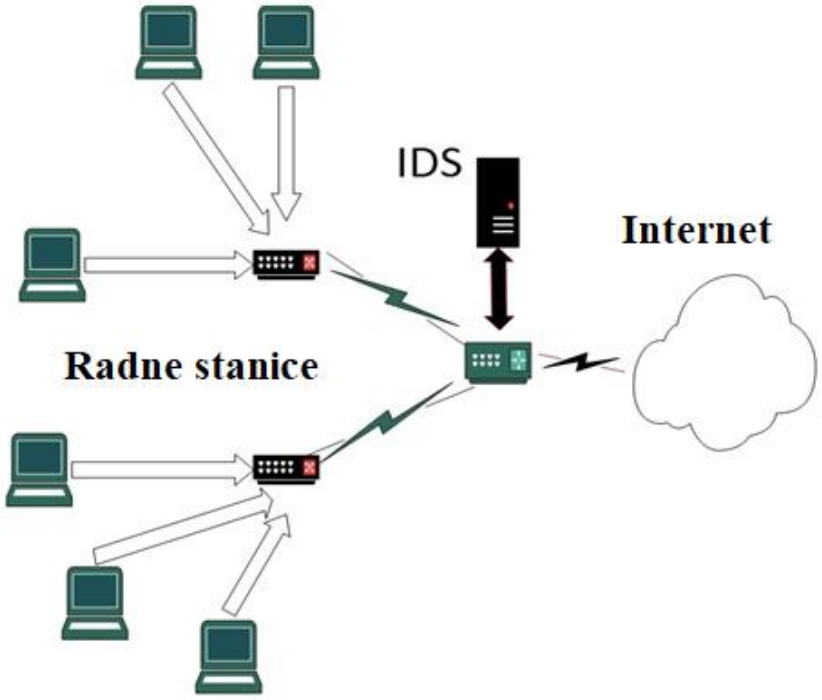
U [53] razmatra se problematika razlikovanja DDoS napada od Flash Event koji imaju vrlo slične karakteristike. Kada dodje do nagle promene entropije, dogadjaji se razlikuju po prisustvu IP adresa koje do sada nisu učestvovale u saobraćaju.Da bi se ovo postiglo IP adrese se pamte odredjeni interval vremena dok ne postanu zastarele.

7. Odabir infrastrukture za istraživanje

Topologija simulirane mreže

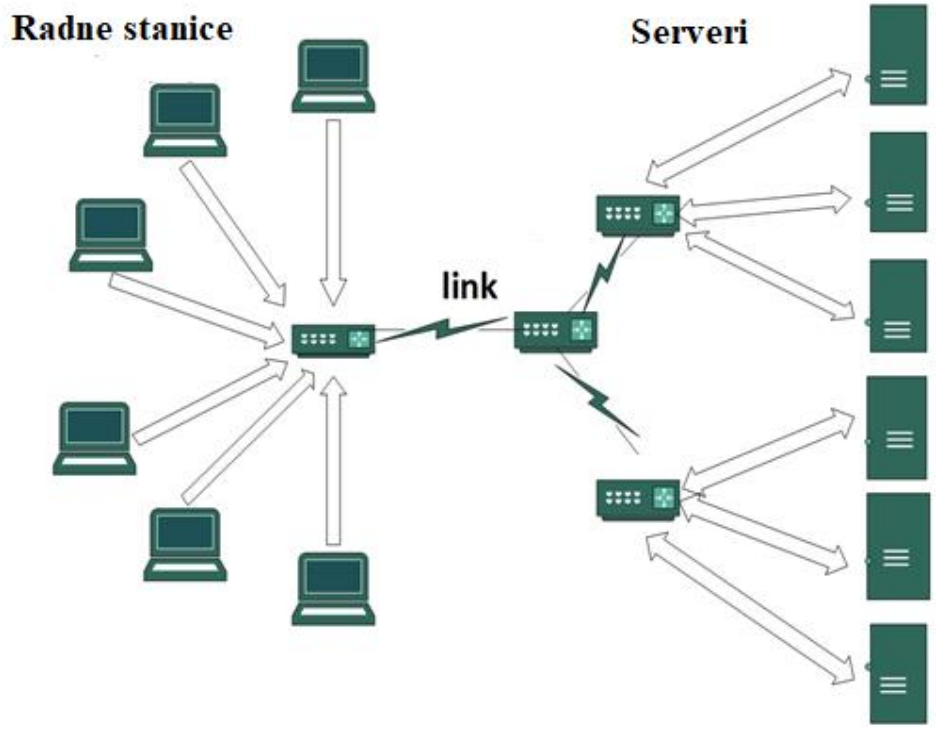
Odabir tačke na kojoj se meri saobraćaj u cilju detekcije DDoS napada je od izuzetne važnosti. U ovoj tezi su razmatrane dve najčešće korišćene topologije u istraživanjima:

Topologija ivične mreže (edge network) tj. mreža pre izlaza ka pružaocu usluga. Ova topologije je zanimljiva sa praktične tačke gledišta jer se napad detektuje u blizini izvora napada, gde je još moguće sprovesti kontramere. U blizini izvora napada detekcija je pouzdanija, raspon IP adresa je mnogo manji pa se ne zahtevaju veliki memorijski resursi za praćenje saobraćaja, lakše se primenjuju mere reakcije na napad jer su izvori napada u blizini. Tačka napada se nalazi negde u javnom domenu, iza tačke detekcije. Najbolji primer su recimo univerzitetske mreže koje imaju veliki broj korisnika i lokalnih mreža na relativno malom prostoru. Ovakve mreže su , upravo zbog svog koncepta otvorenosti, kao i prisustva mlade i dinamične populacije, laka meta za potencijalne napadače koji imaju širok spektar mogućnosti da instališu botnet agente.Tipična topologija ivične mreže je prikazana na slici 16.



Slika 16: Topologija ivične mreže.Napadi potiču sa radnih stanica u lokalnoj mreži, dok je cilj na javnoj mreži. Tačka detekcije je na ivici lokalne mreže.

Topologija velike razmere (large scale) se često primenjuje u istraživanjima ovog tipa. Naročito je korišćena nebalansirana topologija zvona (unbalanced dumbbel topology) prikazana na slici 17. Ova topologija više odgovara globalnoj internet mreži kao i realnom napadu. Izvori napada su na neuporedivo većem opsegu adresa i geografski široko distribuirani. Zato mrežni saobraćaj sadrži daleko više šuma u merenim signalima, entropija u našem slučaju, i očekivano ima više lažnih detekcija. U praktičnom smislu detektovan napad veoma teško može da se brani akcijama na samoj napadnutoj mreži zbog svoje globalne prirode.



Slika 17:Topologija velike razmere. Napadi kreću sa korisničkih radnih stanica na javnoj mreži, ciljevi napada su lokalni serveri.

Tačka u kojoj se detektuje napad je usko grlo simuliranog mrežnog saobraćaja. Sav saobraćaj sa izvora prolazi kroz uredjaj koji poseduje IDS mogućnosti i prolazi ka mreži koja je cilj napada. Ovako konfigurisana tačka detekcije i postojanje dve mreže, izvorne i odredišne su aproksimacija globalne mreže.

Realna mreža

U realnom vremenu saobraćaj može da se skine korišćenjem ultra brzih mrežnih kartica dizajniranih za tu svrhu. Jedan od proizvoda koji spadaju u tu klasu je DAG

kartica firme Endace [56]. Kartica je dizajnirana da vrši snimanje saobraćaja brzinom 622Mbps sa vremenskim pečatom, rezolucijom od 1 mikrosekund i sa GPS koordinatom. Kartica koristi većinu poznatih formata za prikaz mrežnog saobraćaja.

Mogu se upotrebiti i mrežni procesori kakvi se koriste u mrežnoj opremi kao Intel IXP 1200[57][58]. Time bi se dobila maksimalna praktično moguća brzina obrade,

Ovaj pristup zahteva razvoj na posebnoj platformi za dati mrežni procesor, što bi usporilo fazu istraživanja.Korišćenje namenskih mrežnih procesora je opravdano u fazi ispitivanja performansi i izradi prototipa konačnog proizvoda.

Softverski monitori

Programski paketi koji vrše nadgledanje saobraćaja na mreži takodje mogu biti iskorišćeni za skidanje saobraćaja za kasniju analizu. Ograničenje im je mala propusna moć jer se izvršavaju na radnoj stanici umesto na specijalizovanom hardveru. Ipak, i samo deo realnog saobraćaja je od velikog značaja. Jedan od takvih paketa je IDS program Snort[59]ili alat za analizu protokola WireShark [60].

Skupovi podataka sa DoS napadima

Za istraživački rad postoje javno raspoloživi test saobraćaji(dataset) koji predstavljaju sačuvan mrežni saobraćaj. Ovi skupovitest saobraćaja su preuzeti sa velikih mreža, tipično univerzitetskih, izvršena je anonimizacija adresa i prebačeni u neki od poznatih formata. Vrlo često su izvršena i dodatna filtriranja i prilagodjavanja konkretnim potrebama, tako da iako postoji veliki broj javno dostupnih skupova podataka, mora se pažljivo odabrati odgovarajući jer vrlo mali broj može da se upotrebi u konkretnom istraživanju.

Za potrebu ovog istraživanja, kriterijumi za evaluaciju test saobraćaja su bili sledeći:

- Sadrži DDoS napad. Većina skupova test saobraćaja su predvidjeni za uopštenu analizu saobraćaja.
- Sadrži saobraćaj na nivou pojedinačnih paketa a ne agregiranih skupova paketa izmedju dve tačke.
- Paketi sadrže vremenski pečat u rezoluciji od bar desetine sekunde.
- Sadrži nefiltriran saobraćaj tj i normalan saobraćaj i saobraćaj sa anomalijama.
- Sadrži meta-podatke o napadu. Ovi meta-podaci mogu biti u obliku tačnih vremena početka i kraja svakog pojedinačnog napada ili skupa adresa/portova koji učestvuju u napadu ili su ciljevi napada. Bez preciznih podataka o vremenima napada nije moguće izvršiti testiranje metoda detekcije.

U radu [7] se koristisaobraćaj sa realne mrežeinicijalno ne sadrži DDoS napad, nego se napadi naknadno programski ubacuju. Na ovaj način se delimično postiže realističnost eksperimenta jer se za bazu koriste stvarni podaci. Podaci o napadu se dalje mogu konfigurisati po potrebi što ovaj koncept čini zanimljivim za okvire istraživačkog rada. Varijacija ove ideje je korišćena u ovom radu i opisana je u eksperimentu sa realnim mrežnim saobraćajem.

Jedan od najstarijih i najčešće korišćenih skupova mrežnih podataka je KDD99 skup[61]. Ovaj skup je formiran za potrebe javnog nadmetanja u detekciji DDoS napada. Sadrži pet tipova mrežnih tokova, od kojih četiri sadrže po jedan DDoS napad. Ovaj skup je odavno posao zastareo mada je još može naći u nekim istraživanjima ali se više ne preporučuje. Sem toga, koristi tok (flow) umesto paketa koji se koristi u ovoj tezi. Tok je agregirani slog koji sadrži zbirne podatke o vezi dve tačke na mreži od njenog nastajanja do raskidanja, dok je za potrebe ovog rada korišćeno praćenje na nivou pojedinačnih paketa.

U ovom radu je delimično korišćen *CAIDA*saobraćaj[62] a prikupljeni mrežni saobraćaj je na novu paketa. Na sajtu istraživačkog centra (Center for Applied Internet Data Analysis)koji je vlasnik ovog test saobraćaja mogu se naći i linkovi ka radovima koji su koristili ovaj skup što je od posebnog značaja za istraživanje. Ipak, ni ovaj skup ne ispunjava u potpunosti zahteve postavljene u ovoj tezi jer nije inicijalno formiran samo za istraživanje anomalija u mrežnom saobraćaju već za relativno široku upotrebu. Dalje, sadrži mali broj dugih i jasno odredjenih napada koji su kao takvi jednostavni za detekciju. Ipak, izvedeni su eksperimenti i na ovom test saobraćaju jer je lako dostupan i da bi se na najbrži način verifikovao metod na realnom saobraćaju.

Drugi test saobraćaj koji je korišćen je DARPA_2009_DDoS_attack-20091105[63]. Ovaj saobraćaj skoro u velikoj meri zadovoljava potrebe eksperimenata u radu. Od velikog broja test saobraćaja dostupnih na sajtu, nekoliko njih su eksplicitno naznačeni da sadrže DDoS saobraćaj i da im je to osnovna namena. Sadrže i vremenske oznake na nivou paketa i paketi su dati su poznatom *pcap* formatu što ih čini čitljivim mnogim standardnim alatima za prikaz i analizu saobraćaja. Jedina nedostatak je što saobraćaj prikupljen samo izmedju prvog i poslednjeg trenutka napada a ne i normalan saobraćaj pre i posle napada. U toku vremena dok napadi traju normalan saobraćaj je sačuvan. Ovaj nedostatak je prevazidjen tako što se paketi normalnog saobraćaja na slučajan način dodaju na početak i kraj saobraćaja ne menjajući statistiku saobraćaja.

Odabir Simulatora

Simulatori mrežnog saobraćaja su zahvalan alat jer omogućavaju laku konfiguraciju saobraćaja što je od velike važnosti za istraživački rad, naročito u početnoj fazi dokazivanja ispravnosti ideje. Mana simulatora je što je veoma teško napraviti realističnu simulaciju, tako da je uvek potrebna verifikacija rezultata nad podacima iz

realne mreže. Za potrebe ove teze je odabran simulator **ns-2**[64] koji je poznat po visokoj konfigurabilnosti i koristi se u mnogim istraživanjima. To je softver otvorenog koda pisan u C++ jeziku, dok se upravljanje simulacijom i opis topologije mreže izvršavaju kao Tcl skript,da bi se izbegle suvišna prevodjenja tokom izvršenja simulacija. Postoji široka i javno dostupna baza skriptova i tolopogija namenjenih za ovaj simulator. Pošto je izvorni kod dostupan, mogu se vršiti i izmene u izvornom kodu samog programa, što je za potrebe ove teze i korišćeno da bi se simuliralo ponašanje koje je karakteristični za neke DDoS napade.

S obzirom da ns-2 spada starije alate za simulaciju mreža koji se već dugi niz godina koristi, izvršena je kratka analiza i razmatrani su i noviji mrežni simulatori i njihove karakteristike, konkretno ns-3, JiST, SimPy i OMNet++, da bi se utvrdilo da li se neki od njih može efikasnije koristiti u ovom radu.

Ns-3 kao naslednik ns-2 simulatora, koristi isključivo C++ programski jezik bez upotrebe Tcl skript jezika. Da bi se sistem modeliran u ns-2 prebacio u ns-3 ne postoji automatizovani proces, nego se taj proces mora odraditi ručno.

OMNeT++ nije mrežni simulator po definiciji, već je okvir za simulaciju diskretnih dogadjaja. Medjutim koristi se najčešće kao mrežni simulator zahvaljujući dobroj kolekciji modela protokola. Simulacija mreže se opisuje u posebnom jeziku koji se na kraju ipak prevodi u C++.

JiST pomogućuje simulaciju mreže u standardnom Java jeziku. Nije više podržan od originalnog autora, tako da nije pouzdan izbor za dalja istraživanja.

SimPyje procesno orjentisani simulator diskretnih dogadjaja. Nema javno dostupnu biblioteku modela mreža kao ostali simulatori. Simulacija se piše kao skup Python procesa koji medjusobno komuniciraju i razmenjuju objekte.

Nisu vršena direktna testiranja mogućnosti navedenih mrežnih simulatora nego su korišćeni već objavljeni rezultati uporednih testova. U [65][66] dat je pregled performansi po više kriterijuma od kojih su za ovo istraživanje bitni brzina i memorijsko zauzeće:

- Po memorijskom zauzeću u odnosu na veličinu mreže, ns-2 ima približno iste karakteristike kao ostali simulatori sa izuzetkom JiST koji ima zahteva oko dva puta više memorije.
- Po brzini izvršavanja u odnosu na veličinu mreže SimPy ima najslabije karakteristike, dok je ns-2 oko dva puta sporiji u odnosu na ostale simulatore.

S obzirom da ns-3, kao naprednija varijanta ns-2 simulatora ne može direktno koristiti modele već razvijene u ns-2 kao i da ne postoji alat za prebacivanje modela sa jednog simulatora na drugi, a da postoji velika javno dostupna biblioteka razvijenih modela za ns-2, zaključuje se da ns-2 simulator, iako već dugo u upotrebi, može da

zadovolji potrebe ovog istraživanja i da se upotrebom novijih alata ne bi postigla dovoljno značajna poboljšanja.

O odabiru promenljivih

Polja iz mrežnog paketa na osnovu čije se distribucija računa entropija moraju biti pažljivo odabrane. Više je razloga za ovakav pristup. Veliki skup mogućih vrednosti otežavava izračunavanje entropije sa gledišta performansi. Zato je potrebno preslikavanje celog skupa mogućih vrednosti na minimalan skup. S druge strane, ako je skup vrednosti veoma mali, potrebno je povećati vremenski prozor u kome se uzimaju uzorci. Entropije nekih vrednosti polja se smanjuju u slučaju iznenadnog dogadjaja, dok kod nekih polja dolazi do skoka vrednosti entropije. Kombinovanje polja sa ovakvom korelacijom mogu da dovedu do medjusobnog potiranja signala entropije. U ovom radu su razmatrana sledeća polja iz zaglavlja mrežnih paketa:

Vremenski žig. Ako se kao ulaz koristi saobraćaj preuzet sa realne mreže u nekom od standardnih formata kao što je pcap, polje vremenskog žiga (time stamp) će verovatno postojati. Samo polje vremenskog žiga ne nosi informaciju koja se može iskoristiti, ali je zato vreme izmedju dva susedna paketa veličina koja se bitno menja u tokom dogadjaja na mreži. Da bi se iskoristila ova veličina u detekciji dogadjaja, nije prigodno upotrebiti samu vrednost jer je skup mogućih vrednosti veoma veliki. Zato je potrebno preslikavanje na prihvatljivi malo skup vrednosti ili na skup simbola. Jedna mogućnost data je u tabeli 2 gde se opsezi medjuintervala preslikavaju na ASCII simbole.

Tabela 2. Primer preslikavanja širokog opsega mogućih vrednosti na prihvatljiv skup simbola.

Opseg vrednosti u mikrosekundama	Simbol
< 10	A
10-50	B
50-500	C
500-5000	D
5000-100000	E
>100000	F

Takodje možemo primeniti i logaritamsku funkciju za smanjivanje domena vrednosti i zadržati celobrojni deo:

$$tlog = log_{10}(\mathrm{T_m})$$

Gde je $T_m$vreme izmedju pristizanja dva susedna paketa u mikrosekundama.

Odredišna ili izvorišna IP adresa Opseg IP adresa je veoma širok (32 bita za IP4 mreže) i dinamično se menja, tako da prvi izbor za odabir promenljivih za praćenje entropije. Pošto je TCP protokol konekcijski orijentisan, i ista adresa se pojavljuje i kao odredišna i kao izvorišna u toku jedne konekcije, očekuje se da entropija obe vrste adrese budu korelirane. U slučaju DDoS napada, adrese napadnutih ciljeva se pojavljuju znatno češće od drugih adresa i time se izaziva promena entropije. Promena entropije adresa se pojavljuje i u slučaju dogadjaja kao što je skeniranje opsega adresa. Na performanse procesa izračunavanja entropije adresa negativno bi uticalo ako se koristi ceo opseg adresa, pa se odseca odredjen broj bita. To može biti ili manje značajan deo adrese, ili deo adrese koji je zajednički za posmatranu mrežu.

Odredišni ili izvorišni port. Portovi su takodje parametar čija se vrednost dinamički menja s tim što je opseg vrednosti mnogo manji nego kod IP adresa. Iako je opseg 16-bitni, najčešće se koriste dobro poznati portovi kojih je relativno mali broj. Pojava broja porta preko 1024 takodje može da bude signal nekog dogadjaja. Kod upotrebe simulatora saobraćaja znatno je teže napraviti simulaciju kod koje je distribucija portova realistična, nego što je to slučaj sa IP adresama. Iz tog razloga u radu se ne koristi ovaj parametar iako jenjegova upotreba u realnoj mreži itekako oprevdana.

Dužina paketa (payload size) , što nije isto što i dužina toka, manje varira nego sto se može na prvi pogled zaključiti. Najčešća vrednosti su 40, 1040 i 1500. Mrežna oprema često ograničava ovu vrednost na 1500. Pošto se većina pojedinačnih vrednosti iz celog opsega vrednosti retko javljaju preporučuje se da se dužina paketa preslikava na nekoliko simbola: za male vrednosti ispod 40 , dve ili tri grupe srednjih vrednosti izmedju 40 i 1040, i velike vrednosti preko 1040.

Protokol (8 bita) preko 140 protokola je predvidjeno u ovom trenutku. Iako je TCP dominantan protokol, promena ovog polja je dovoljno česta da može da se koristi u detekciji dogadjaja, naročito ako neki od napada koriste neki drugi protokol (IGMP Ping of death , UDP strumpf)

TTL polje (Time-to-live). Pošto različiti operativni sistemi postavljaju različite vrednosti vremena života paketa, entropija ovog polja može da se menja pojavom anomalija u saobraćaju.

Flegovi. Od tri flega u IP zaglavlju DF (Don‘t fragment) se pojavljuje u oko 85% paketa, tako da se pomoću njega mogu detektovati neke anomalije. U ovom radu je korišćen u detekciji DDoS napada na realnom saobraćaju.

ACK fleg kod TCP zaglavlja može da znači indikaciju da se na mrežu dogadja nešto neuobičajeno. To može biti duže pregovaranje oko uspostave veze što se dogadja kod opterećene mreže ili može biti znak SYN napada. U simuliranom saobraćaju nije pouzdan indikator, ali je u postavci eksperimenata u ovom radu već izmenjen izvorni kod simulatora ns-2, tako da se podrži ponašanje čvora u slučaju SYN napada kao i u realnom

saobraćaju. FIN fleg je komplementaran SYN flegu jer označava kraj pregovora oko uspostave veze i njegova distribucija je bude slična kod SYN flega.

Radi povećanja preciznosti detekcije, mogu se kombinovati više promenljivih, što je u ovom radu pokazano u nekoliko eksperimenata. Pri kombinovanju promenljivih mora se voditi računa o medjusobnoj korelaciji. Entropija nekih promenljivih može da približno prati promene entropije neke druge promenljive. U tom slučaju jedna od odabranih promenljivih mora biti isključena iz modela. Ovaj problem je posebno obradjen u [67].

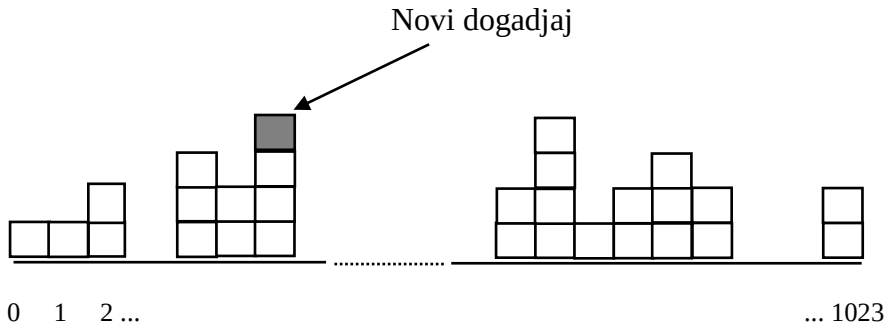
S obzirom da je tema teze primena fazi-neuralne mreže na signal entropije, nisu vršena dublja istraživanja po pitanju odabira polja zaglavlja paketa ili njihovih kombinacija nad kojim se računanje entropije jer to ne utiče na opštost. Ipak, optimalan odabir polja je jedan od mogućih pravaca daljih istraživanja. Za eksperimente u ovoj tezi odabrana su sledeća polja iz zaglavlja IP paketa:

- Odredišna i izvorišna IP adresa. Koriste se prvih 10 bita.
- Veličina paketapreslikana na manji broj simbola.
- Flegovi: DF za realnu mrežu, ACK za simuliranu mrežu.
- Medjuvreme izmedju paketapreslikano na manji broj simbola

8. Sinteza Detektora

Generator entropije

U rešenju detektora DoS napada, upotrebljen je u daljem tekstu opisani algoritam. Distribucija odabrane promenljive se formira i posmatra za male podintervale (tipično 0.1s). Uvodi se pomični prozor od M podintervala (tipično 10 što odgovara vremenskom intervalu od jedne sekunde). Koncept pomičnog prozora je bitan da bi se obuhvatili kratki dogadjaji koji bi mogli da ostanu neprimećeni ako se pripišu samo jednom podintervalu. Takodje, na taj način se umanjuje šum jer se implicitno vrši usrednjavanje. Ovaj koncept se koristi u mnogim istraživanjima ovog tipa [69].Za svaki podinterval formira se distribucija posmatrane promenljive da bi se izračunala entropija. Za svaku promenljivu od interesa alociran je niz (slika 18) čija dužina pokriva opseg vrednosti posmatrane veličine. Vrednosti promenljive se preslikavaju u indekse niza, tj. u skup prirodnih brojeva počevši od 0. U ovom istraživanju, posmatraju se distribucije broja bajta u paketu, medjuvremena pristizanja paketa, izvornih IP adresa, odredišnih IP adresa i pojedinih flegova. Za svaki pristigli paket se pripadajuća pozicija u nizu promenljivih povećava za jedan.



Slika 18: Registrovanje dogadjaja: za svaku promenljivu čija se distribucija posmatra, alociran je niz u dužini broja mogućih dogadjaja (na slici 1024). Pri pojavi novog dogadjaja, vrednost na odgovarajućem mestu se uvećava za jedan.

Na isteku podintervala se za ceo niz izračunava entropija po formuli (1) za Shannonovu entropiju ili po formuli (2) za Tsallis entropiju. Vrednosti entropije za M=10 (veličina pomičnog prozora) uzastopnih podintervala se koriste kao ulazni vektor u procesu obuke i detekcije (slika 19). U sledećem koraku pomični prozor se pomera za jedan podinterval tako da se procesiranje vrši za devet prethodnih i jedan novi podinterval.

Slika 19: Entropija se izračunava za svaki vremenski podinterval, a pamte se vrednosti entropije iz pomičnog prozora.

Broj mogućih vrednosti za koje se računa entropija mora biti optimizovan i zbog zauzeća memorijskih resursa i zbog brzine izračunavanja. Ukoliko je broj mogućih vrednosti prevelik (razmatramo hipotetički 2^{32} IP adresa), potreban je duži vremenski interval da bi se prikupilo dovoljno dogadjaja za reprezentativnu distribuciju. Po završetku datog vremenskog intervala izračunava se entropija. Računanje entropije po formuli (1) za veliki broj mogućih vrednosti može biti zahtevno ako se proces obavlja u realnom vremenu. Dakle, vremenski interval prikupljanja dogadjaja je dug, i na kraju tog vremenskog intervala mora se u kratkom vremenu, do pristizanja sledećeg paketa, izvršiti zahtevna kalkulacija nad velikim brojem simbola. Iz tih razloga mora se izvršiti preslikavanje celog opsega posmatrane veličine u prihvatljiv skup da bi se optimizovali i memorijski resursi i vreme obrade. Ovo nije toliko bitno za proces obuke koji se ne radi u realnom vremenu, ali za proces detekcije vreme izračunavanje postaje od primarnog značaja. Čak i za proces obuke, niz od 2^{32}pozicije bio bi nepotrebno veliki, tako da se optimizacija u svakom slučaju mora uzeti u obzir. U predloženoj sintezi detektora primenjene su sledeća preslikavanja iz razloga optimizacije skupa vrednosti:

Ako je se radi o IP adresama, uzima se odredjen broj značajnijih bita, recimo 10 , tako da sada imamoniz od 1024 moguća dogadjaja. Pojam značajnog bita nije nužno da bude po vodećim pozicijama u IP adresi, nego po pozicijama koje se više menjaju, što

zavisi od konfiguracije mreže. Za svaki pristigli paket odgovarajuća pozicija u nizu mogućih vrednosti se uvećava za jedan.

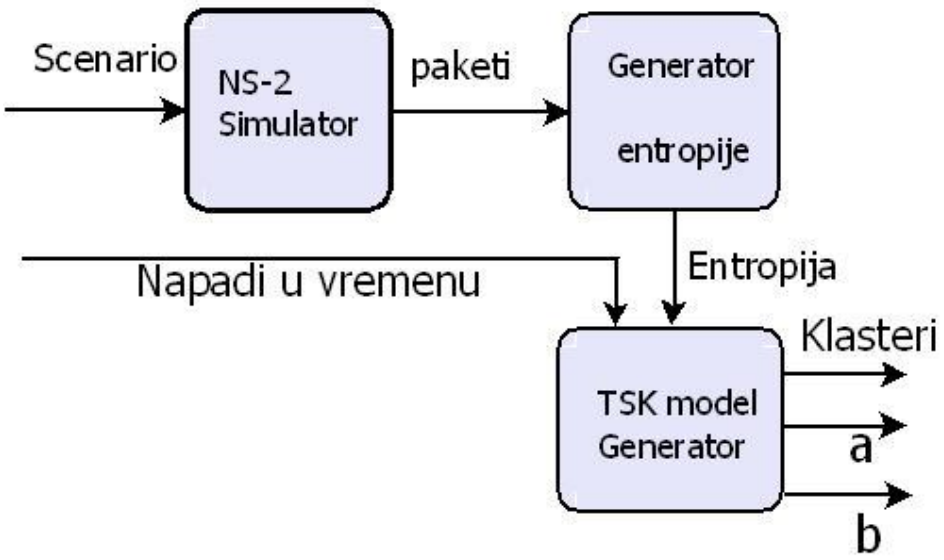
Kod distribucije portova se memorijski resursi se optimizuju uzimanjem u obzir manje značajnih bita jer su najčešće korišćeni standardni portovi sa niskim brojevima.

Za slučaj distribucije dužine paketa, optimizacija se vrši preslikavanjem vrednosti dužine paketa po opsezima u skup celih brojeva od 0 do 5 po opsezima , gde se na 0 preslikavaju kratki paketi, a na 5 najduži. Isto preslikavanja se vrši i za distribuciju medjuvremena pristizanja paketa.

Kod flegova iz IP zaglavlja nije potrebno preslikavanje jer postoje samo dve moguće vrednosti.

Generator modela

Za potrebe procesa obuke ulaznim uzorcimapridodaju se i poznate vrednosti napada za svaku tačku tj podinterval. Vrednost napada može imati dve vrednosti: 0.0 ako nema napada i X kada je napad u toku. Vrednost X se odredjuje tako da bude približno istog reda veličine kao i ulazni uzorci. Slika 20 prikazuje upotrebljene programske komponente. Ista postavka je upotrebljena i u [68]. Mreža se simulira korišćenjem standardnog ns-2 simulatora. Izlaz iz simulatora je datoteka *tracefile.txt*. U sledećem koraku entropija se izračunava za svaki podinterval kako je već opisano u prethodnom poglavlju.



Slika 20: Proces obuke. Simulator saobraćaja generiše pakete koji su ulaz u generator entropije. Na osnovu entropije u vremenu i poznatih vremena napada formira se model.

Izlaz iz generatora entropije a ujedno i ulaz u TSK-FS generator modela je niz vrednosti entropije za jednu od posmatranih promenljivih kome je pridružen i niz poznatih vrednosti napada za svaki podinterval. Za svaku promenljivuformira se poseban model.

Kao TSK-FS generator modela korišćen je postojeći program *TSK.exe* opisan u [70] uz minimalna prilagodjenja.U TSK-FNN generatoru modela najpre se formira ulazni vektor. Ovaj vektor (slika 21) sadrži N uzastopnih vrednosti entropije za N uzastopnih podintervala koji pripadaju jednom pomičnom prozoru, uz dodatak unapred poznate vrednosti napada za najnoviji (tekući) podinterval. N-1 prethodnih vrednosti entropije su potrebni da bi se uzeo u obzir trend vrednosti entropije i da bi se prigušio šum. Dimenzija ulaznog vektora je tako N+1.

E_0	E_1	E_2	E_3	E_4	E_5	E_6	E_7	E_8	E_9	Napad

Slika21: Format ulaznog vektora u procese obuke i detekcije: 10 poslednjih vrednosti entropije i vrednost napada za poslednji podinterval

Dalje seulazni vektor se obradjuje u TSK-FS procesu obuke koji je opisan u poglavlju (). Broj klastera fiksiran na K=5. U testovima sa variranjem broja klastera utvrdjeno je da povećanje broja klastera preko 5 ne doprinosi povećanju preciznosti modela, već utiče jedino na smanjenje performanse kalkulacija u realnom vremenu. Na izlazu generatora modela dobijamo model koji se sastoji iz sledećih komponenti:

Matrice $\boldsymbol{C_{NxK}}$ centara klastera dimenzija NxK gde je K=5 broj klastera a N=10 broj podintervala. Kolone matrice sadrže koordinate centara odgovarajućeg klastera u N-dimenzionom prostoru.

Matrice $\boldsymbol{A_{NxK}}$ čije se i-ta kolonakasnije u procesu detekcije skalarno množi sa ulaznim vektorom entropije $\boldsymbol{x_N}$ po formuli $\boldsymbol{y = a_i x + b_i}$, gde je *i* broj najbližeg centra klastera

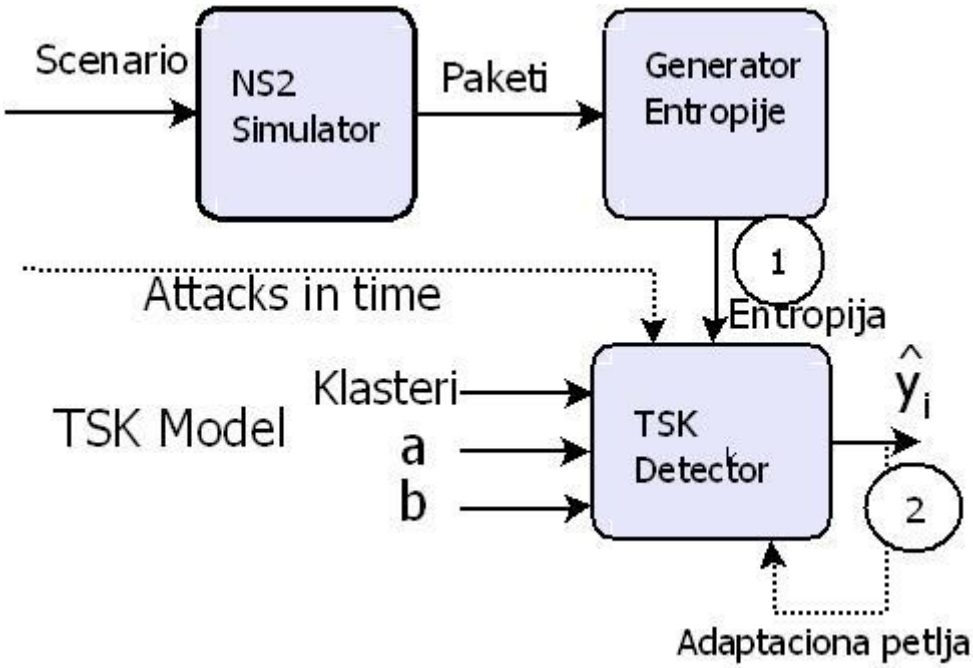
Vektora $\boldsymbol{b_K}$ dimenzijeKčijasei-takomponentakasnije u procesu detekcije dodaje skalarnom proizvoduuformuli $\mathbf{y = a_i x + b_i}$, gde je *i* brojnajbližeg centra klastera iz matrice $\boldsymbol{C_{NxK}}$.

Proces detekcije

Proces detekcije je prikazan na slici 22. Ulazni podaci su istog formata kao i podaci za obuku s tom razlikom da se vrednosti napada ne uzimaju u obzir, jer oni treba da se procene. Vrednosti napada, ako su poznati, mogu da i dalje figurišu u ulaznim podacima ali u tom slučaju njihova svrha bi bila testiranje tačnosti modela. Niz procenjenih vrednosti napada se izračunavaju korišćenjem formule (5). Prve dve

programske komponente su iste kao i u procesu obuke. Poslednja komponenta je TSK-FNN detektor.

Detektor obradjuje ulazne podatke na sledeći način: Za svaki ulazni uzorak$\boldsymbol{x_N}$, euklidovo rastojanje do svih centara klastera koji su sadržani u matrici $\boldsymbol{C_{NxK}}$se izračunava i odredjuje klaster na najkraćem rastojanju.Za tako odredjeni klaster se primenjuje odgovarajuće pravilo koristeći formulu ($\mathbf{y = a_i x + b_i}$) I na taj način se dobija procenjena vrednost napada u vremenu $\hat{y}_i$.

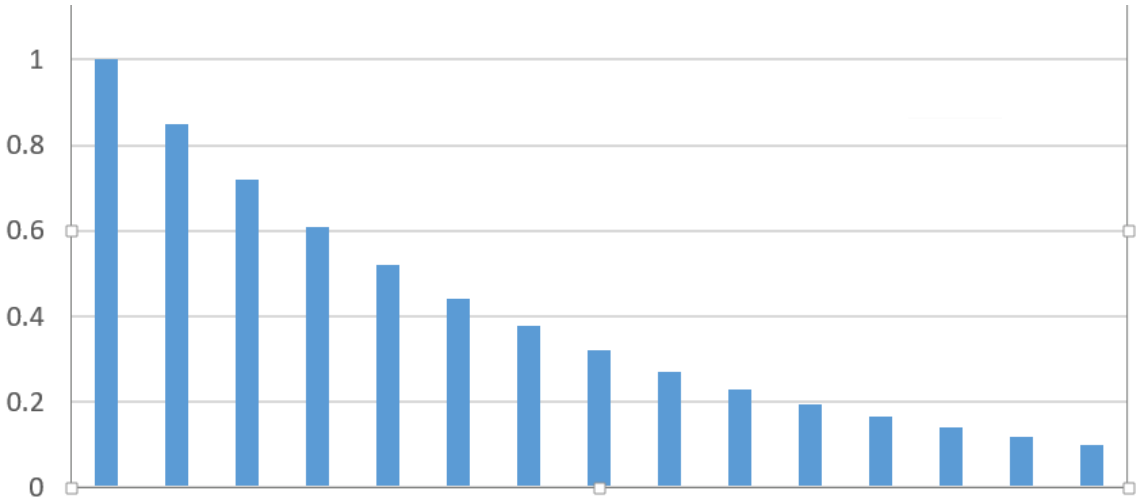


Slika 22: Proces detekcije. Za razliku od procesa obuke, model je ulaz- Izlaz je procenjena vrednost napada. Vremena napada sada se koriste samo za proveru tačnosti modela. Adaptaciona petlja ponavlja proces izračunavanja procenjene vrednosti dok ne dodje do lokalnog maksimuma. Tada su parametri detekcije na optimalnim vrendostima

U velikom broju radova koji se bave sličnom tematikom, proces detekcije anomalije mrežnog saobraćaja se često završava grafičkim prikazom signala entropije na kojem se vidi promena nivoa entropije u datom trenutku kao na slici 24. U ovom radu se imala u vidu praktična primenljivost metode na mrežnoj opremi, što isključuje pristrasno ljudsko opažanje. Pokazalo se da u nekim slučajevima, iako vizuelno može da se jasno potvrdi promena nivoa entropije, automatska detekcije usled prisustva šuma nije dovoljno pouzdana i generiše previše grešaka tipa I i II. Iz tog razloga pouzdana automatska detekcija promene nivoa entropije ima značajno mesto u prezentovanom metodu.

Automatska detekcija tačke promene promenljive $\hat{y}_i$ se dobija koristeći CUSUM [71]. CUSUM metoda kumulira odstupanja od procenjene srednje vrednosti niza uzoraka. Kada kumulirana razlika postane veća od zadatog praga, promena se smatra detektovanom. Bitno je napomenuti da prag kod CUSUM metode nema isto fizičko

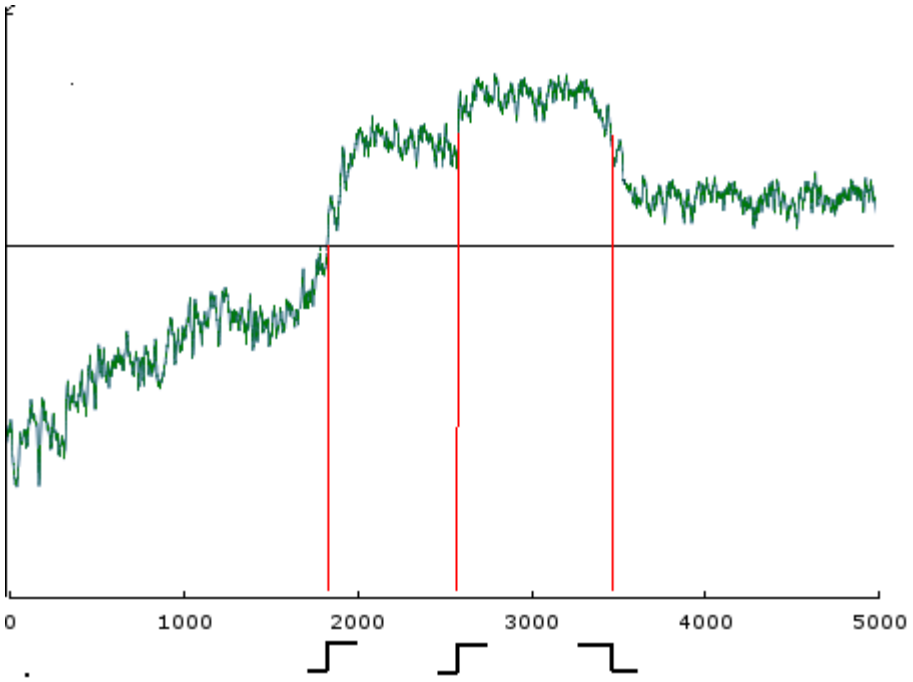
značenje kao vrednost praga samog signala. Srednja vrednost promenljive se procenjuje koristeći EWMA (exponential weighted moving average) metod. EWMA metod uzima u obzir dinamiku signala i srednju vrednost posmatra u odnosu na trenutno vreme, pri čemu novije vrednosti imaju veću težinu od vrednosti koje su udaljenije u vremenu. Postoji više načina kako se daje prednost novijom odbircima. Kod EWMA metoda značaj starijih odbiraka opada eksponencijalno kao na ilustrativnom primeru na slici 23.



Slika 23:EWMA metoda daje veći značaj novijim odbircima. Značaj starijih odbiraka opada eksponencijalno sa vremenom

Na taj način srednja vrednost signala nije fiksirana nego prati promene signala. Tačka promene signala se tako odredjuje u odnosu na dinamičku srednju vrednost. Razlika u detekciji promene signala bez i sa korišćenjuem EWMA metode vidi se na primerima prikazanim na slici 24. Ako se koristi fiksni prag, promena se detektuje kad signal predje odredjeni prag, tako da se u datom slučaju detektuje samo jedna promena. Na istoj slici prikazano je kako se pomoću EWMA metode detektuju se tri promene, dve u pozitivnom smeru i jedna u negativnom, kada signal promeni vrednost u odnosu na tekuću srednju vrednost, što je bliže realnoj situaciji u uslovima nestacionarnog saobraćaja.

Pretpostavlja se da su izlazi y_i nezavisne i ravnomerno rasporedjene vrednosti. Zato se postavljaju se dve hipoteze: raspodela pre i raspodela posle tačke promene. U parametrizovanoj varijanti metode, tačka promene se izračunava na osnovu log-likelyhood odnosa, dok se u neparametrizovanoj varijanti CUSUM metode tačka promene se računa koristeći korisničku funkciju. U ovom postupku se koristi neparametrizovana verzija.



Slika 24: CUSUM metoda detektuje tačke promene u odnosu na procenjenu srednju vrednost u bližoj okolini. Odstupanje od te vrednosti detektuje se kao promena. Na ovaj način se na datom signalu detektuju tri promene. Kad bi se koristio običan prag detektovala bi se samo jedna promena.

Za detekciju tačke promene se koristi sledeća formula:

$$\mu_n = \beta_1 y_n + (1-\beta_1)\mu_{n-1} \qquad (10)$$

$$d_n = \max\{0, d_{n-1} + y_n - (\mu_n + K)\}, \; d_0 = 0 \qquad (11)$$

$$\sigma_n^2 = \beta_2 \sigma_{n-1}^2 + (1-\beta_2)(y_n - \mu_n)^2, \; H = h\sigma_n \qquad (12)$$

Gde su značenja oznala koje figurišu u formulama sledeća:

H je prag odluke. Ako je $d_n > H$, promena je detektovana. Vrednosti za h, factor odluke variraju izmedji 1.0 i 8.0 u eksperimentima u ovom radu.

K je faktor devijacije i kreće se izmedju 0 i 0.1 u ovom radu.

μ_n je procenjena srednja vrednost izlaznog niza y_n.

d_n je brojač koji kumulira devijacije niza y_n u odnosu na $\mu_{n`}$ koje su veće od faktora K (minimum devijacije).

β_1 ***i*** β_2 su EWMA adaptivni faktori i njihove vrednosti su 0.75 i 0.90 ovom istraživanju.

σ_n je standardna devijacija izlaznog niza y_n.

Kod metoda detekcije napada opisanih u[37] [38] automatska detekcija se primenjuje na izlazu iz samog generatora entropije. U ovom radu je u process detekcije dodat još jedan korak obrade, TSK-FS detector. Svi rezultati eksperimenata opisanih u daljem teksu sadrže poređenja rezultata detekcije za oba slučaja – direktna detekcija na entropiji signala I detekcija posle TSKFS obrade.

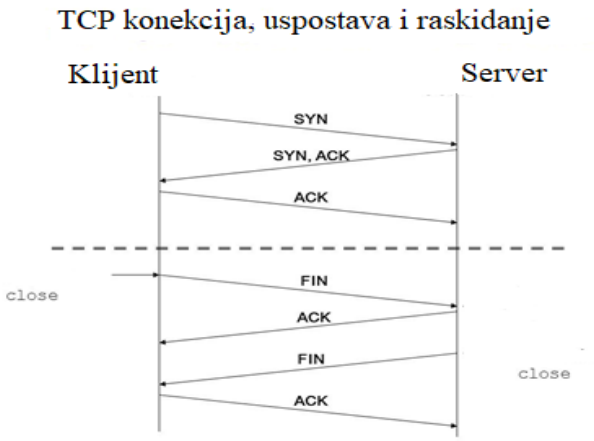
U idealnom slučaju izlaz iz TSK-FS detektora je X ili 0 tj. napad je u toku ili nije. Na prvi pogled ovde nije potrebna automatska detekcija tačke promene jer bi izlazi detektora trebali biti diskretne vrednosti pa bi bilo dovoljno postaviti fiksan prag odluke koji je manji od X. Medjutim, rezultati eksperimenata pokazuju da izlazni signal, koji je rezultat složenih matematičkih izračunavanja poputskalarnog množenja 10-dimenzionih vektora, nema diskretne vrednosti zbog uticaja šuma kao i preciznosti izračunavanja. Zbog toga se detekcija tačke promene pomoću CUSUM metoda primenjuje i na izlazu TSK-FNN detektora.

9. Rezultati

U ovom poglavlju opisani su eksperimenti koji su izvedeni najpre na simuliranom mrežnom saobraćaju, a zatim i na saobraćaju preuzetim sa realne mreže. Eksperimenti 1, 2, 4 i 5 su izvedeni u sličnoj postavcikao i u radu [68].

Izmena izvornog koda simulatora ns2

Ns-2 simulira uobičajeno ponašanje čvorova u mreži i u izvornoj implementaciji ne podržava ponašanje napadača potrebnu za eksperimente u ovom radu. Da bi se simuliralo ponašanje napadača koji koristi SYN poplavu mora se izmeniti ponašanje čvorova koji igraju ulogu napadača. Napadač-klijent šalje zahtev serveru za otvaranje veze sa SYN a server na nju odgovara takodje sa SYN (slika 25). Normalno ponašanje (three-way hanshaking) klijenta je da odgovori sa ACK, medjutim u slučaju SYN napada napadač ne reaguje i odbacuje paket. To izaziva da server po isteku timeout-a šalje novi SYN, držeći vezu poluotvorenu i tabele u internoj memoriji zauzete. Za tu svrhu izmenjen je originalni izvorni kod paketa ns-2 da bi se simuliralo ponašanje napadača kada ne šalje ACK.



Slika 25: Proces uspostave i raskidanja TCP veze. Ako klijent započne process a ne završi ga, veza ostaje poluotvorena. Ns-2 izvorni kod je promenjen da bi se simuliralo takvo ponašanje.

Eksperiment 1: Simulirana ivična mreža

U topologiji ivične mreže simulira se lokalna mreža sa 250 korisničkih stanica od kojih su od 20 do 80 pod kontrolom napadača i jedan server koji je cilj napada kako je prikazano na slici 16. Senzor za detekciju napada (IDS) je postavljen na izlaznom ruteru mreže (gateway) i vrši nadzor saobraćaja ka i od javne mreže. Serverkojijeciljnapadapodrazumevanosenalazinajavnojmreži, vannadgledanelokalnemreže. Istatopologijazaeksperimentjekorišćenaiuradu[37]. Napadi se detektuju posmatrajući izlazni saobraćaj. Ova topologija omogućava detekciju DDoS napada u blizini njegovog izvora, gde je moguće onemogućiti ili ublažiti ga lokalno.

Podaci za obuku su generisani pomoću 15 tačaka napada sa ukupnim vremenom napada od 75 sekundi. Vremena početaka i krajeva napada su poznata unapred. Broj pojedinačnih napada je 15. Svaka radna stanica pod kontrolom napadača izvodi SYN poplavu na svakih 5 sekundi. Trajanje svakog pojedinačnog napada je slučajna promenljiva sa normalnom raspodelom, srednjim vremenom od 1 sekunde i standardnom devijacijom od 200 ms. Osnovni saobraćaj se generiše od strane 170 do 230 agenata od kojih polovina generiše saobraćaj konstantne brzine (CBR u ns-2 terminologiji) sa objektima srednje veličine od 10kb a polovina HTTP saobraćaj srednje veličine od 30kb. Vremenski intervali izmedju transfera su eksponencijalno rasporedjeni sa srednjim vremenom od 30s.

Ovakva struktura napada, kao kratkih i u seriji je izabrana iz više razloga. Najpre, kod mnogih radova sa sličnom tematikom se detektuje jedan veliki i relativno dugotrajan napad. To ostavlja mogućnost da metoda detekcije nije dovoljno osetljiva ili robusna. Na način odabran u ovom radu se omogućuje da se tokom samo jednog eksperimenta detektuje (ili ne detektuje) veći broj dogadjaja i dodje do brojne vrednosti koja opisuje kvalitet detekcije tj. procenta tačnih i pogrešnih detekcija. Dalje, kratki napadi uvode potrebu za pojmom brzine detekcije i omogućavaju da se utvrdi da li napadi mogu da ostanu nedetektovani u slučaju brzih promena.

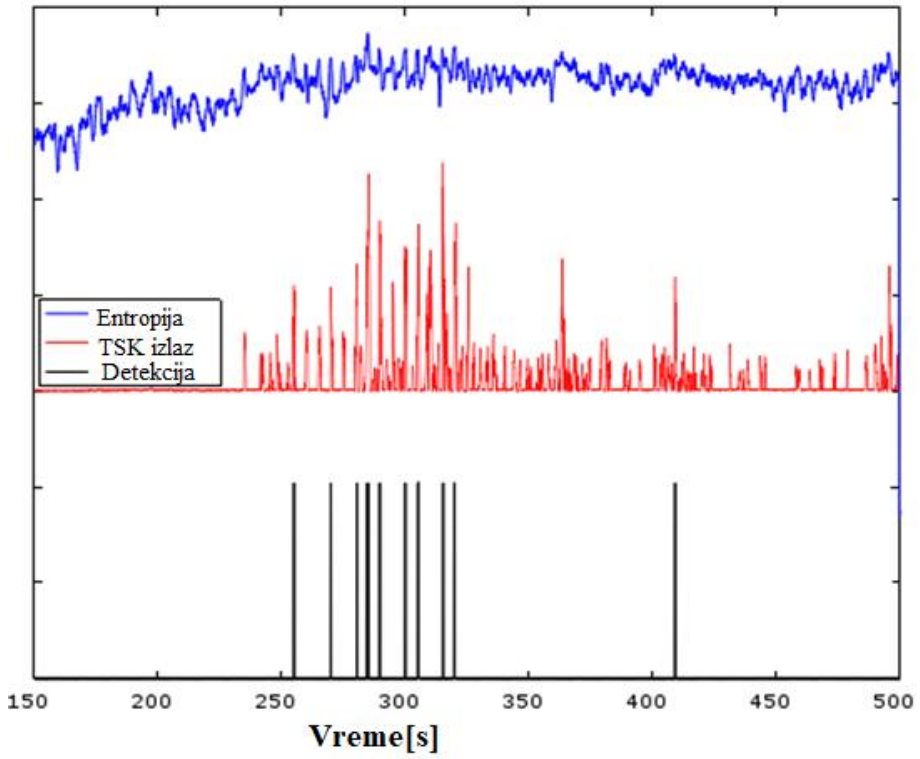
Eksperimenti su izvedeni pomoću ns-2 simulatora verzije 2.35 a simulirani napad je tipa SYN poplava (SYN flood) DDoS. Modul TCPAgent.cpp originalnog ns-2 izvornog koda je izmenjen tako da simulira reakciju čvora na SYN napad. Serija eksperimenata je izvedena sa brojem napada koji se kreće od 20 do 80 napadača. Za detekciju tačke promene je korišćen CUSUM metod (tačke 1 i 2 na slici 22). Tačka 1 je izlaz modula za izračunavanje entropije a tačka 2 je izlaz iz TSK-FS. Cilj eksperimenta je da se pokaže da primena TSF-FS metoda povećava tačnost detekcije i istovremeno smanjuje broj lažnih alarma (false positives).

Primer na slici26 prikazuje vrednosti Shannonove entropije izvorišnih adresa i odgovarajućih izlaza TSK-FS detektora za simulirani scenario sa 40 napadača na zajedničkom dijagramu. Gornji signal predstavlja entropiju,srednji - izlaz TSK-FS

detektora a donji signal je izlaz posle CUSUM detekcije tačke promene , kako je definisano jednačinama (10)(11) i (12). Napadi se dešavaju izmedju 250s i 325s.

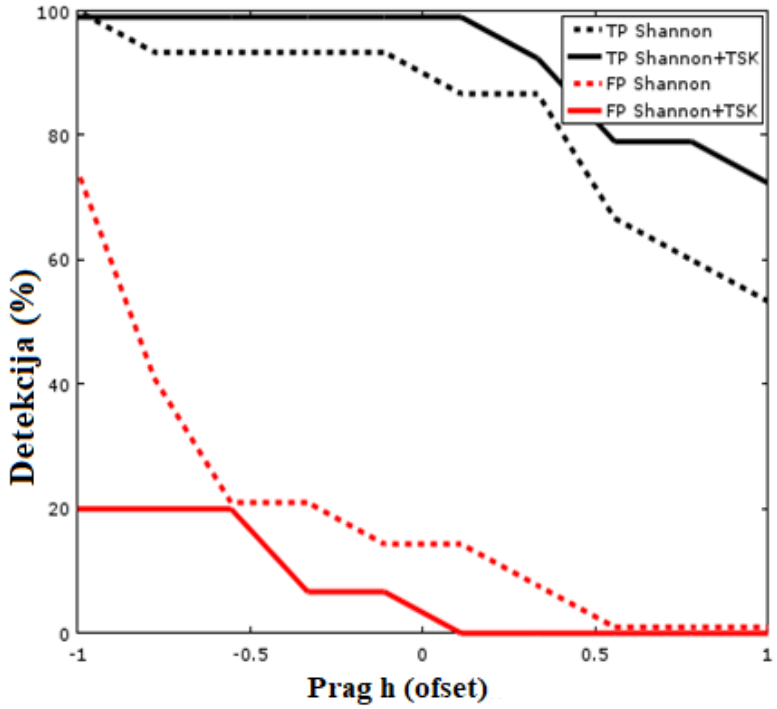
Slika26ilustruje ključni koncept ovog istraživanja.Gornji signal je nivo entropije. Na ilustrativnom primeru (odabran je slučaj sa slabijim napadima) nivo entropije tokom napada, izmedju 250 i 325 sekundi, je neznatno različit od nivoa entropije pri normalnom saobraćaju. Primena CUSUM ili bilo kog drugog metoda za detekciju tačke promene na ovakav signal dala bi ili mali broj ispravnih detekcija za visok prag detekcije ili veliki broj lažnih detekcija za nizak prag. Srednji signal na grafiku je izlaz posle primene TSK filtra. Saslikesevididaprimenajoš jednogstepenaobradeentropijeznatnopotiskuje šuminatajnačinseredukujebrojlažnihalarma.Ako se sada primeni detekcija tačke promene na ovakav signal, prag detekcije može više da varira tj. detekcija je robusnija. Na taj način dobijamo donji signal koji predstavlja izlaz TSK-FS detektora, sa devet ispravnih detekcija i jednom pogrešnom detekcijom.

Slika26takodje pokazujeidaprimenajoš jednogstepenaobradekao štojeTSK-FSmožeizazvatiipotiskivanjeregularnihalarma, štosena grafikuvidiunedostajućimvrhovima(šest nedetektovanih kratkih napada) upribližnouniformnomrasporedutačakapromene.



Slika 26: Stanja procesa TSK-FS detekcije prikazana na zajedničkom dijagramu: Entropija (gornji signal), TSF-FS izlaz, i konačna procena napada. Napadi su izmedju 250 i 325 sekundi od početka testa. Jačina napada je slaba, ali detekcija je još uvek efikasna.

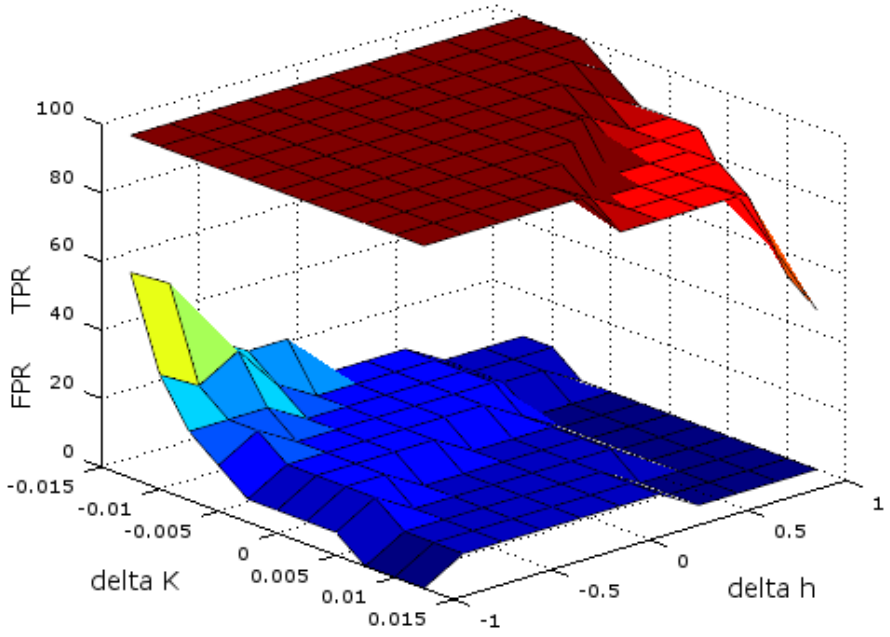
Slika 27prikazuje zavisnost detekcije od vrednosti praga h izjednačina (10)(11) i za konstantan faktor osetljivosti K. Dijagram je , zbog preglednosti, prikazan tako da je početak koordinatnog sistema postavljen na optimalne vrednosti h i K, gde razlika izmedju procenta tačnih detekcija TPR i pogrešnih, FPR (greške tipa I) dostiže maksimum. Kvalitet detekcije je odredjen time koliko je TPR blizu 100% i istovremeno koliko je FPR blizu 0%. Slika pokazuje da primena TSK-FS poboljšava kvalitet detekcije.



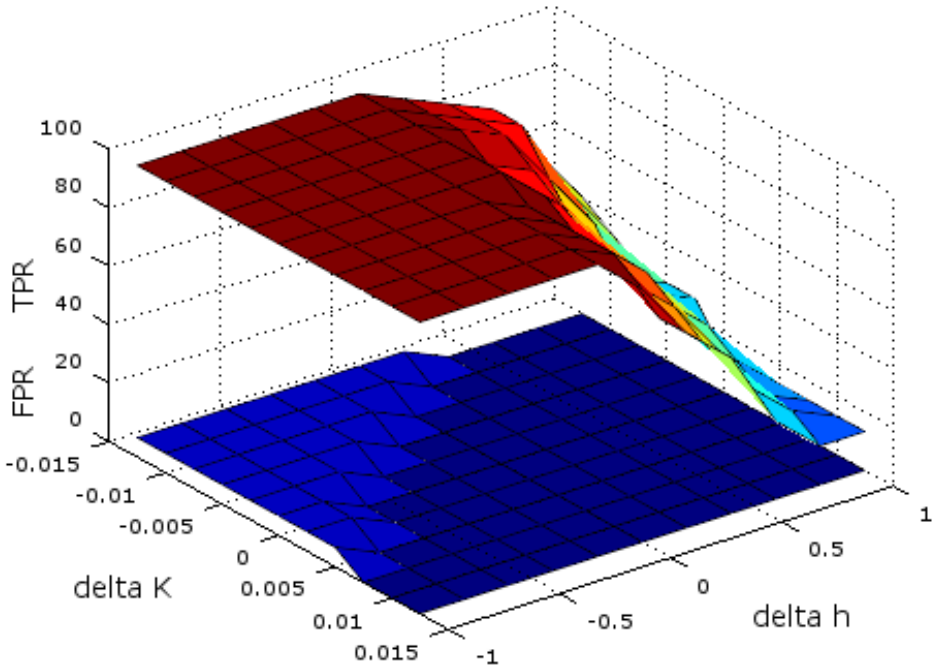
Slika 27: Detekcija u odnosu na visinu praga h za ivičnu topologiju i Shannon-ovu entropiju sa CUSUM detekcijom tačke promene i optimalnim vrenostima praga h i osetljivosti K.

U istraživanju je utvrdjeno da faktor osetljivosti K CUSUM metode detekcije tačke promene, ne bi trebalo da ima konstantnu vrednost. Oba parametra, h i K moraju se varirati da bi se dobila najbolja vrednost detekcije. Da bi se ova tvrdnja pokazala na jasniji način, prikazani su rezultati eksperimenata u trodimenzionalnom obliku. Slike28-a do 31-aprikazuju trodimenzionalnu zavisnost detekcije od parametara h i K za Shannon-ovu entropiju za broj napadača od maksimalnih 80 do minimalnih 20.Slike28-b do 31-bpokazuje istu zavisnost kada je TSK-FS primenjen na Shannon-ovu entropiju i kada broj napadača takodje varira od 80 do 20. Na dijagramima gornja površina označava vrednost TPR u zavisnosti of h i K a donja zavisnost FPR od istih parametara. Detekcija je pouzdanija kada su dve površine više razmaknute ili kad je TPR što bliža 100% a FRP bliža 0%, kao i u slučaju 2D dijagrama na slici 27. Početak koordinatnog sistema je postavljen zbog preglednosti tako da tačka (0,0) predstavlja tačku gde je razlika TPR i

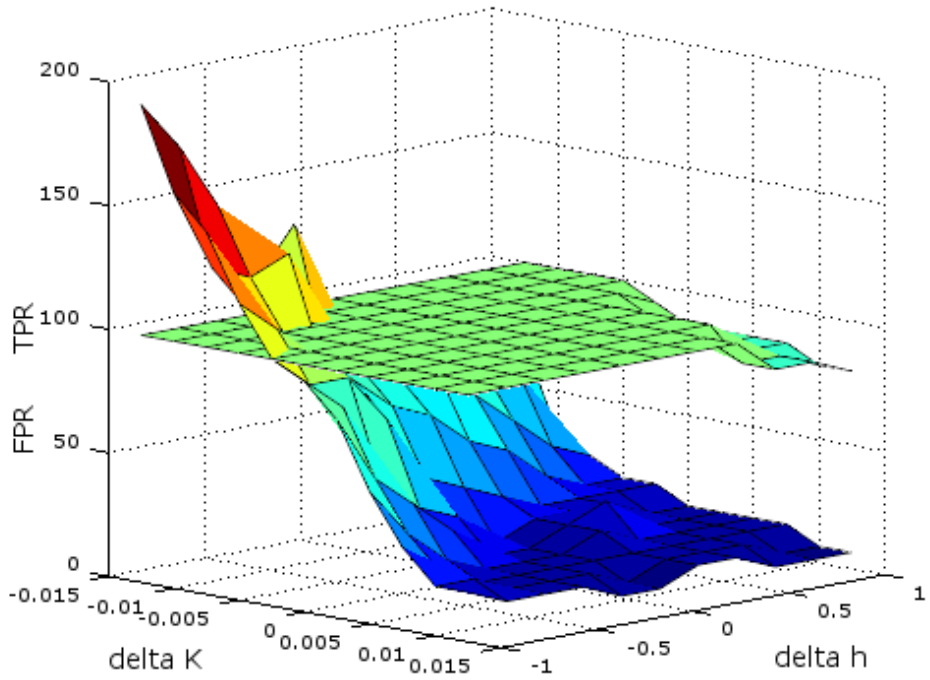
FPR na maksimumu. Dakle, ose h i K predstavljaju odstojanja od optimalnih vrednosti h i K.



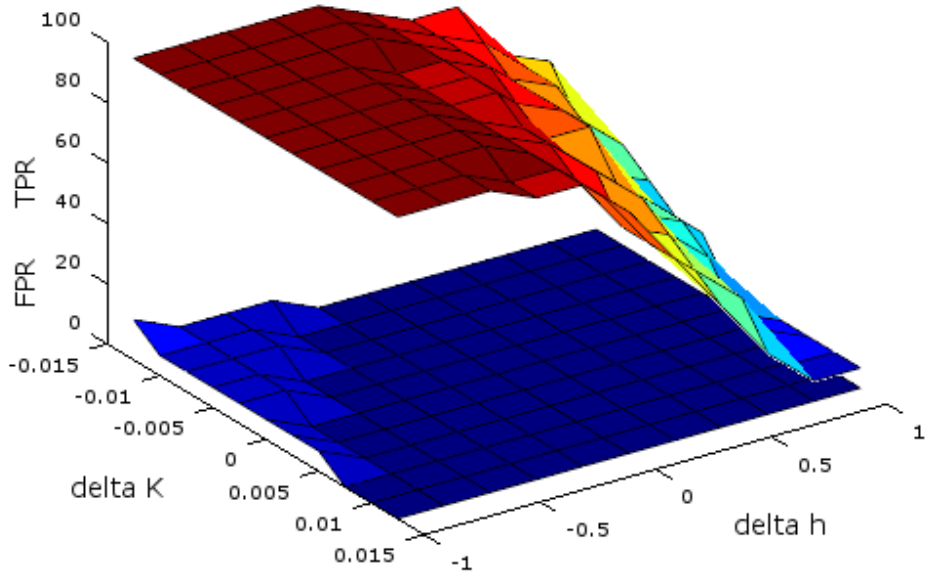
Slika 28-a: Trodimenzionalni prikaz zavisnosti procenta tačnih (TPR, gornja površina) i lažnih (FPR, donja površina) detekcija u zavisnosti od promene novoa praga h i promene osetljivosti K za 80 napadača. Topologija je ivična, Shannon-ova entropija, bez primene TSK-FS metoda. TPR je visoka za širok opseg parametara. FPR se povećava samo za veoma niske vrednosti parametara.



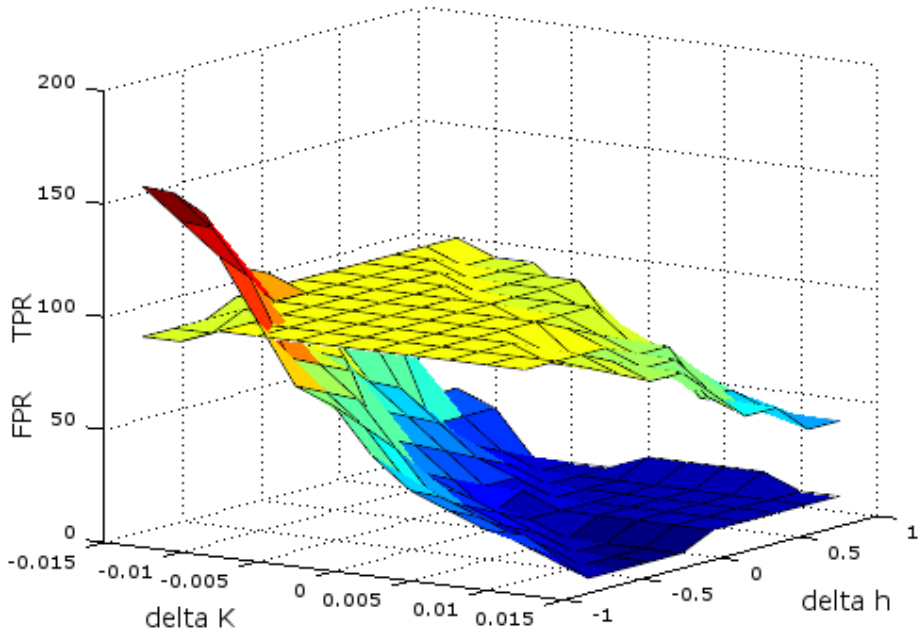
Slika 28-b: Ista postavka eksperimenta kao i za sliku 28-a ali sa primenom TSK-FS metoda. TPR je visoka za širok opseg parametara. FPR je niska za ceo opseg parametara h i K.



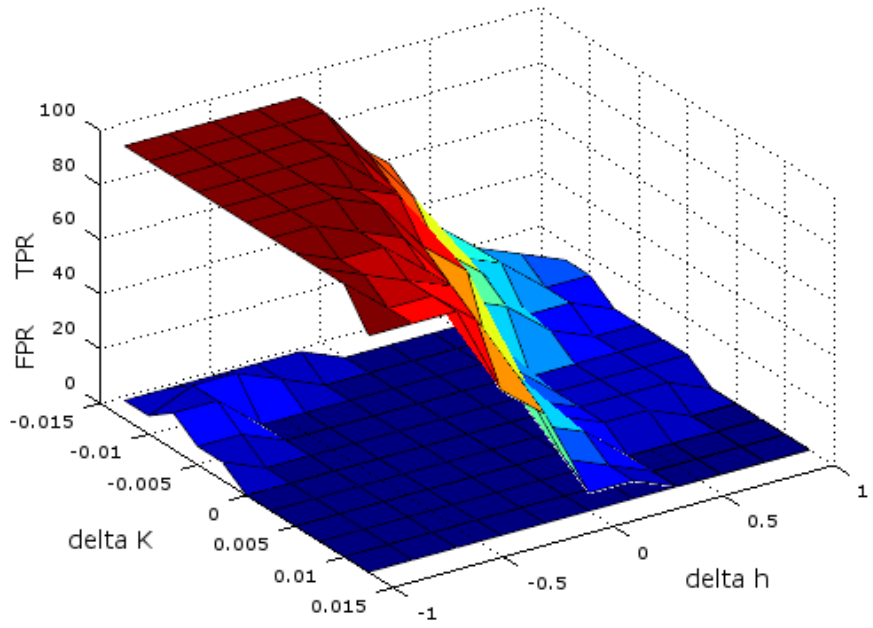
Slika 29-a: Eksperiment sa 60 napadača i bez primene TSK-FS metode. TPR je i dalje visoka ali se lažne detekcije naglo povećavaju sa smanjenjm vrednosti parametara detekcije.



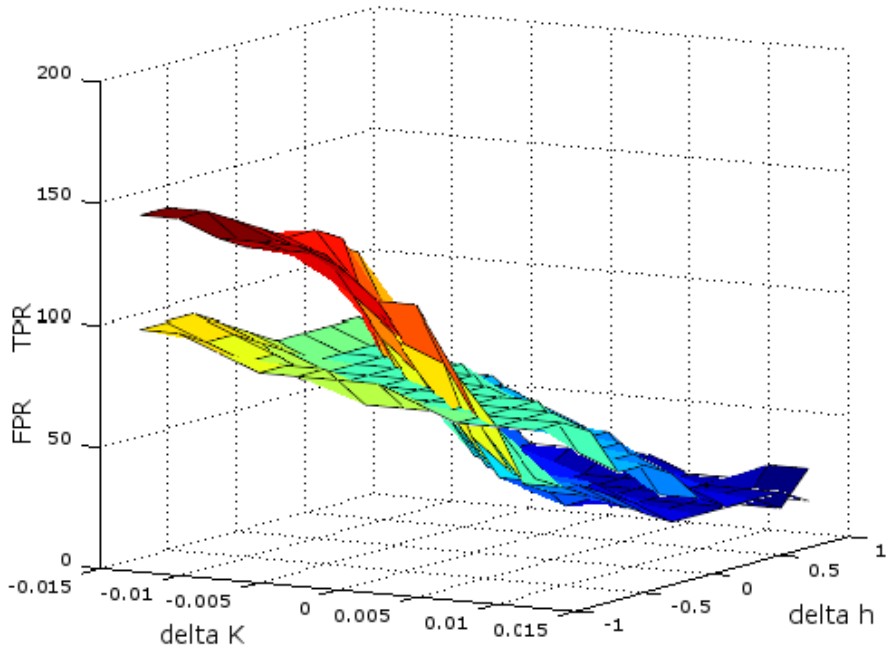
Slika 29-b: Eksperiment sa 60 napadača sa primenom TSK-FS metode. TPR je visoka dok su lažne detekcije i dalje niske.



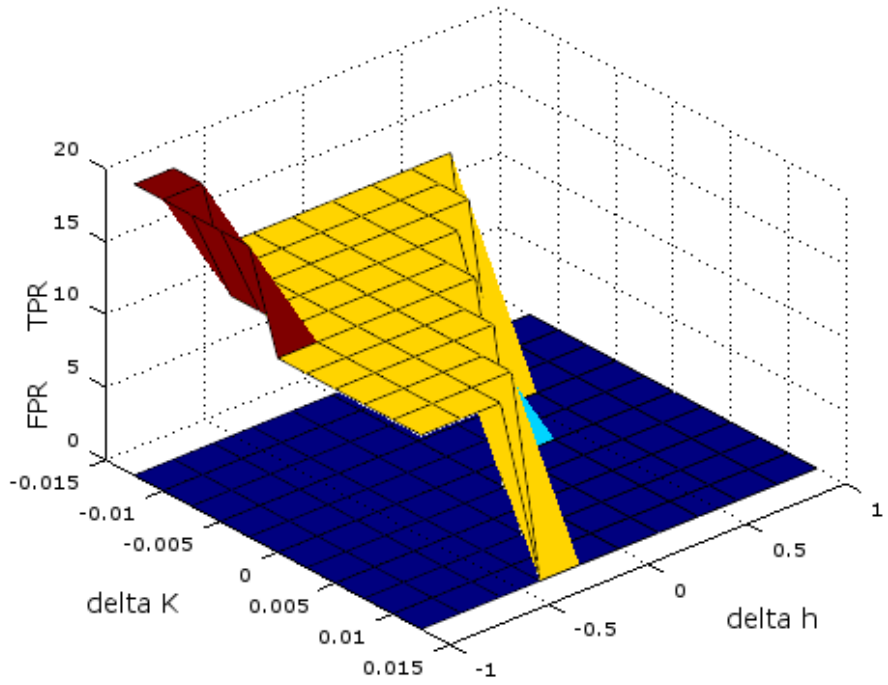
Slika 30-a: Dalje smanjenje jačine napada, 40 napadača i bez primene TSK-FS metode. TPR je i dalje visoka , FPR je sada visoka na širem opsegu parametara.



Slika 30-b: 40 napadača, površina TPR je i dalje blizu 100% ali na užem prostoru, za niže vrednosti parametara detekcija. FPR je niska, tako da je detekcija i dalje pouzdana.



Slika 31-a: Najslabiji napad, 20 napadača, površine TPR i FPR su sada već veoma bliske za ceo opseg parametara, detekcija praktično nije moguća.



Slika 31-b: Eksperiment sa minimalnim brojem napadača, 20, sa primenom TSK-FS metode. TPR je već niska ali su i lažne detekcije veoma potisnute, tako da je detekcija još uvek moguća, mada daleko od maksimuma.

Sa svih dijagrama se vidi da je detekcija pouzdanija, a razlika izmedju TPR i FPR ostaje značajna za širok opseg vrednosti parametara h i K za slučaj primene TSK-FS u poredjenju sa odgovarajućim slučajem (isti broj napadača) kada je detekcija izvršena samo na signalu entropije. Za slučaj detekcije tačke promene samo na signalu entropije vidljivo je da su na svim dijagramima površine TPR i FPR bliske, osim za izuzeno jak nivo napada.

Primetna je i razlika u detekciji ispravnih i pogrešnih prilikom slabljenja napada. Pri slabim napadima, signal entropije u toku napada se „utapa“ u signal normalnog saobraćaja. Da bi detekcija koja se vrši direktno na signalu mogla da detektuje slabe promene, prag detekcije mora da se smanjuje. Pri tome se detektuje i mnogo lažnih dogadjaja koje nastaju usled uobičajenih varijacija signala. Pri daljem snižavanju praga broj lažnih dogadjaja naglo raste, jer sada gotovo svaka varijacija signala izaziva i promenu stanja detektora.

Za razliku od direktne detekcije na signalu entropije, kada se primeni TSK-FS pri smanjenju jačine napada dolazi do smanjivanja i TPR i lažnih detekcija koje se sada ne povećavaju značajno pri smanjenju praga. TSK-FS metod uspeva da priguši lažne detekcije pri niskom nivou napada, ali cena se plaća smanjenom detekcijom pravih napada. Medjutim, i za ovako nizak nivo napada ipak dolazi do detektovanja nekih od njih. S obzirom da klasična detekcija na tom nivou napada više nije pouzdana, može se zaključiti da TSK-FS metod smanjuje donju granicu jačine napada pri kojoj je detekcija moguća uz istovremeno suzbijanje pogrešnih detekcija.

Ako se pod merom robusnosti detekcije smatra veličina regiona u kome parametri h i K mogu da variraju a da površine TPR i FPR još uvek budu dovoljno udaljene, takodje je vidljivo da na svim dijagramima primena TSK-FS metoda dozvoljava daleko veću slobodu promene parametara detekcije. Nizak nivo lažnih detekcija i robusnost detekcije u slučaju variranja parametara detekcije je veoma bitniza praktičnu primenu metode. Parametri h i K mogu da budu inicijalno fino podešeni, ali se uvek javlja mogućnost da u nepredvidivom i dinamičnom okruženju oni promene vrednost toliko da se detekcija pomeri u zonu nepouzdanosti. Takodje, u praksije čestobitniji štonižinivolažnihdetekcijaodnivoaispravnihdetekcijajergenerisanjelažnihalarmaznatnoom etauobičajeniprocessrada.Može se zaključiti da jeTSK-FSrobusnijimetoddetekcije koji dozvoljavavećuvarijacijuparametaradetekcije.

Za razliku prethodnih 3-dimenzionalnih prikaza samo za Shannon entropiju, u tabeli 3dat je numerički pregled rezultataistih eksperimenata. Ovde su dati i rezultati primene nekoliko tipova entropija. Za svaki od tipova entropija formiran je poseban TSK-FS model. Korišćena je entropijaizvorišne IP adrese za Shannon, Tsallis i T-entropiju. Vrednosti za tačne detekcije TPR i pogrešne detekcije FPR u tabeli su date samo za slučaj optimalnih vrednosti h i K za sve eksperimente, tj. za one tačke gde je razlika TPR i FPR maksimalna. Optimalne vrednosti h i K su dobijene preko opcione adaptacijske petlje (tačkasta linija na slici22). Kada se primeni adaptaciona petlja, test

detekcije se ponavlja dok se ne dostigne maksimalna razlika izmedju TPR i FPR. I odavde se može zaključiti da je detekcija napada robusnija kada je TSK-FS primenjen u odnosu na slučaj korišćenja samo signala entropije. Čak i za slučaj kada je jačina napada niska (poslednji red) a nivoi entropije sa i bez napada se ne razlikuju značajno , TSK-FS još uvek detektuje neke napade dok metode bazirane samo na entropiji ne detektuju više ni jedan napad. Vrednosti FNR, tj. greške tipa II, nisu posebno prikazane jer se dobijaju kao razlika izmedju TPR i 100% .

Tabela3: Poredjenje tačnosti detekcije za Shannon-ovu Tsallis (q=0.6) i T-entropiju bez primene i sa primenom TSK-FS metoda. Jačina napada varira izmedju 20 i 80 napadača.

Broj napadača	**TPR FPR**	**h K**	**TPR FPR**	**h K**
	Shannon		**Shannon+TSK-FS**	
80	94% 6%	6.8 0.02	100% 0%	4.0 0.03
60	87% 0%	3.4 0.07	100% 6%	4.6 0.01
40	20% 0%	6.6 .025	94% 6%	4.3 0.005
20	0% 0%	-	26% 0%	2.8 0.035
	Tsallis		**Tsallis+TSK-FS**	
80	100% 6%	5.8 0.03	100% 0%	4.2 0.03
60	87% 13%	5.6 0.03	100% 0%	4.6 0.01
40	61% 6%	5.0 0.005	87% 0%	3.8 0.005
20	26% 13%	8.8 0.03	54% 0%	3.3 0.03
	T-entropy		**T-entropy+TSK-FS**	
80	80% 40%	5.2 0.025	56% 6%	4.8 0.025
60	46% 26%	4.8 0.03	33% 0%	4.6 0.020

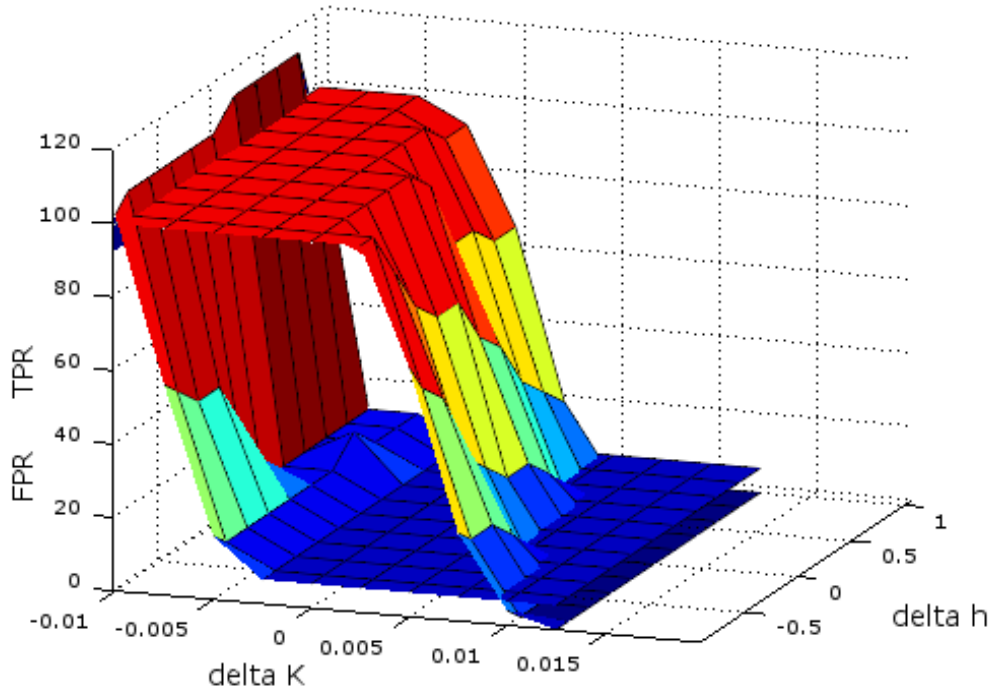
Gledano po tipovima entropija, Tsalis entropija daje nešto bolje rezultate posebno za napade niskog nivoa i kada se primeni u kombinaciji sa TSK-FS metodom. T-entropija daje slabiji procenat detekcije, naročito za nizak nivo napada. Za slučajeve sa 40 i 20 napadača detekcije nije bila moguća. Ovo se može objasniti osetljivošću T-entropije na promenu rasporeda simbola, i kao takva unosi daleko više šuma. Problem šuma je kod T-entropije je poznat razmatran je u [43]. Ipak, u kombinaciji sa TSK-FS i primena T-entropije i dalje daje smanjen FPR.

Slični eksperimenti sa primenom TSK-FS nisu do sada objavljivani, tako da neka direktna poredjenja nisu moguća. U radu [37] su izvedeni eksperimenti sa sličnom postavkom za Shannon entropiju, CUSUM detekciju tačke promene i ivičnu topologiju. Rezultati eksperimenta daju TPR približno 90% i FPR približno 18%. U ovojtezi se dobijaju čak bolji rezultati za sličnu postavku, ali to je zbog toga što se u tabeli 3 daju vrednosti za tačku gde su optimalne vrednosti parametra h i K gde je razlika TPR i FPR maksimalna, dok se u [37] koristi fiksno K.

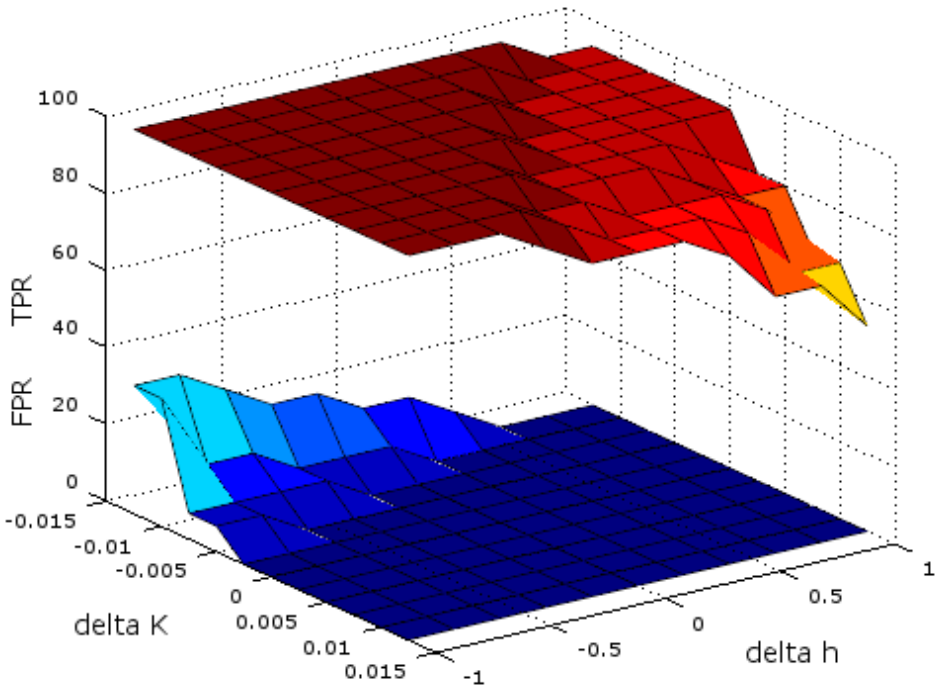
Eksperiment 2: Simulirana mreža velike razmere

U drugom skupu scenarijaprimenjena je topologija poznata kao nebalansirana ’dumbbell’ topologija. Mreža je sastavljena od 470 korisničkih radnih stanica u javnom domenu. Ova topologija simulira globalni napad sa interneta na server u lokalnoj mreži. Postoji 40 servera u lokalnojmreži od kojih je jedan žrtva napada. Postoji čvor u lokalnoj mreži koji je veza izmedju servera u lokalnom domenu i radnih stanica u javnom domenu u taj čvor sadrži i detektor napada (IDS). Napad se detektuje nadgledanjem saobraćaja ka lokalnoj mreži. Sve korisničke stanice su grupisane u jedan klaster , a osnovni saobraćaj su HTTP sesije generisane od strane korisničkih radnih stanica. Trajanje simulacije je 500 sekundi. Simulirani napad se kreće od niskog intenziteta, gde je samo 20 stanica pod kontrolom napadača, pa do 150 kontrolisanih stanica. Broj sesija je 200, a svaka sesija sadrži 250 stranica sa jednim objektom. Veličina objekta je Pareto II promenljiva srednje vrednosti 120 sa parametrom oblika (shape parametar) 1.2. Napadi se dešavaju u periodu od 250 do 325 sekundi, u vreme kad je opterećenje mreže dostiglo visok nivo. Podaci za obuku neuralne mreže su uzeti za scenario sa 60 napadača.

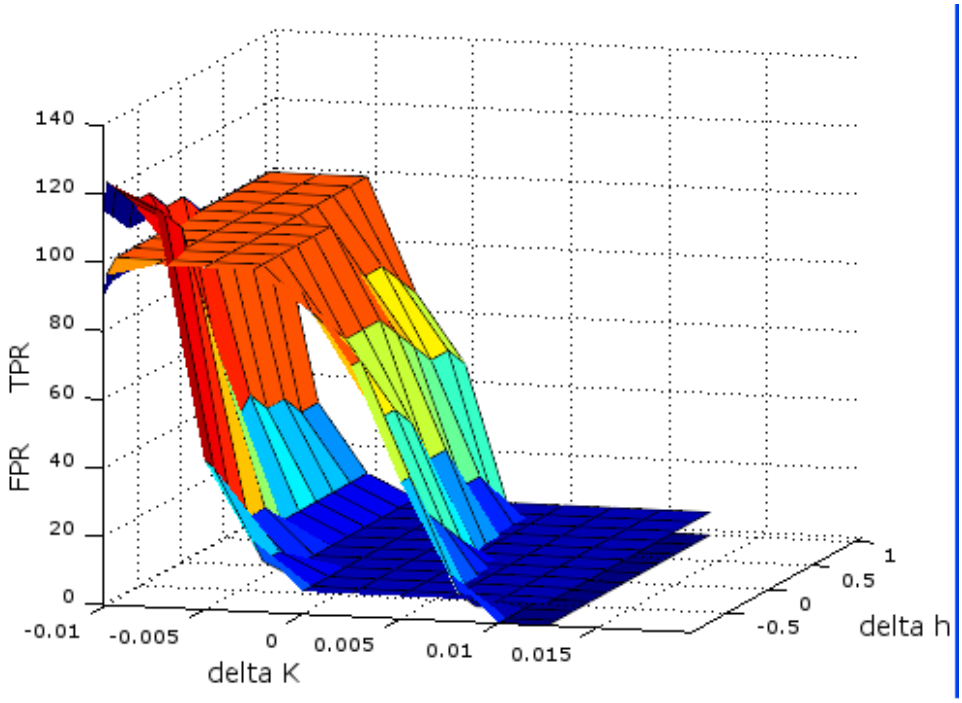
Slike 32-a do 35-a pokazuju trodimenzionalnu zavisnost detekcije od parametara h i K za Tsallis entropiju za broj napadača od maksimalnih 150 do minimalnih 20 je samo CUSUM detekcija promene primenjena na Tsallis entropiju. Slike 32-b do 35-b prikazuju istu trodimenzionalnu zavisnost kada je primenjen TSK-FS metod. Kao i na prethodnom skupu eksperimenata, na dijagramima gornja površina označava vrednost TPR u zavisnosti of h i K a donja zavisnost FPR od istih parametara.



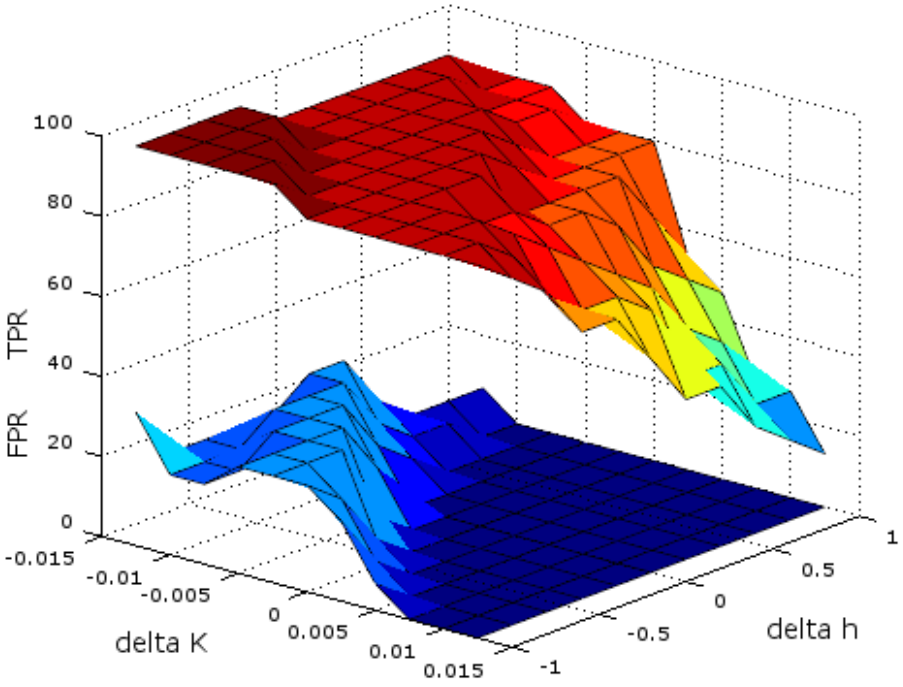
Slika 32-a: Trodimenzionalni prikaz zavisnosti procenta tačnih (TPR, gornja površina) i lažnih (FPR, donja površina) detekcija u zavisnosti od promene novoa praga h i promene osetljivosti K za 150 napadača. Topologija je velike razmere, entropija je Tsallis-ova, bez primene TSK-FS metoda. TPR je visoka za širok opseg parametara. FPR se povećava samo za veoma niske vrednosti parametara.



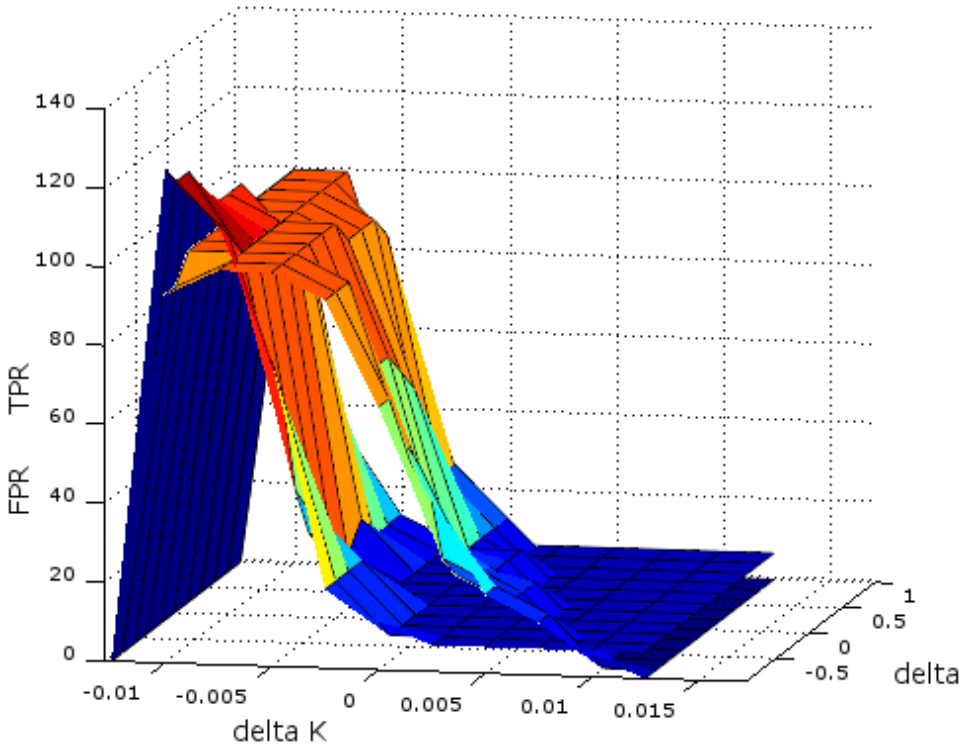
Slika 32-b: Ista postavka eksperimenta kao i za sliku 32-a ali sa primenom TSK-FS metoda. TPR je visoka za širok opseg parametara. FPR je niska za ceo opseg parametara h i K.



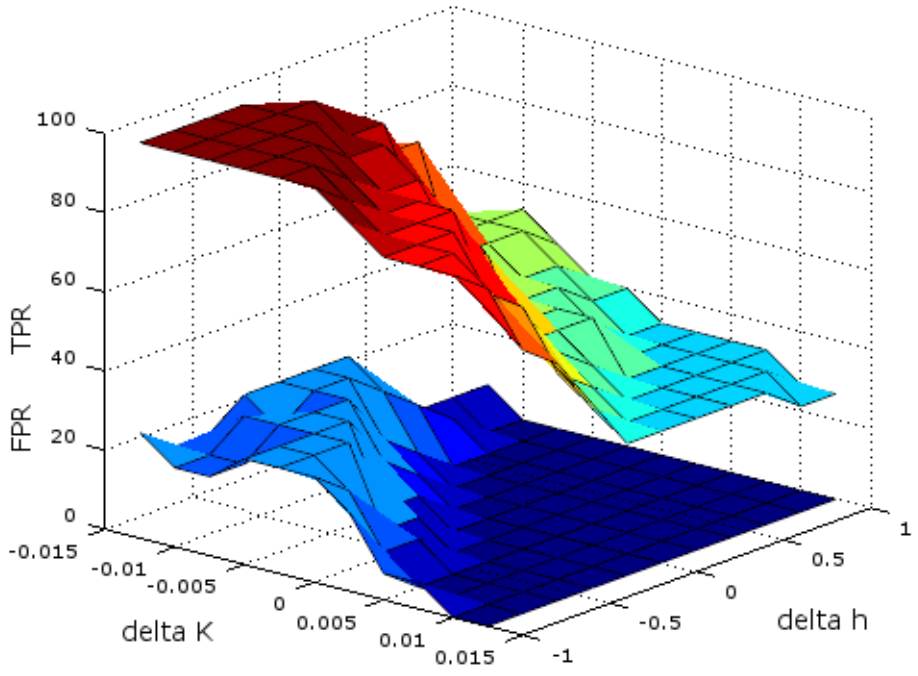
Slika 33-a: Eksperiment sa 110 napadača i bez primene TSK-FS metode. TPR je i dalje visoka ali se lažne detekcije naglo povećavaju sa smanjenjm vrednosti parametara detekcije.



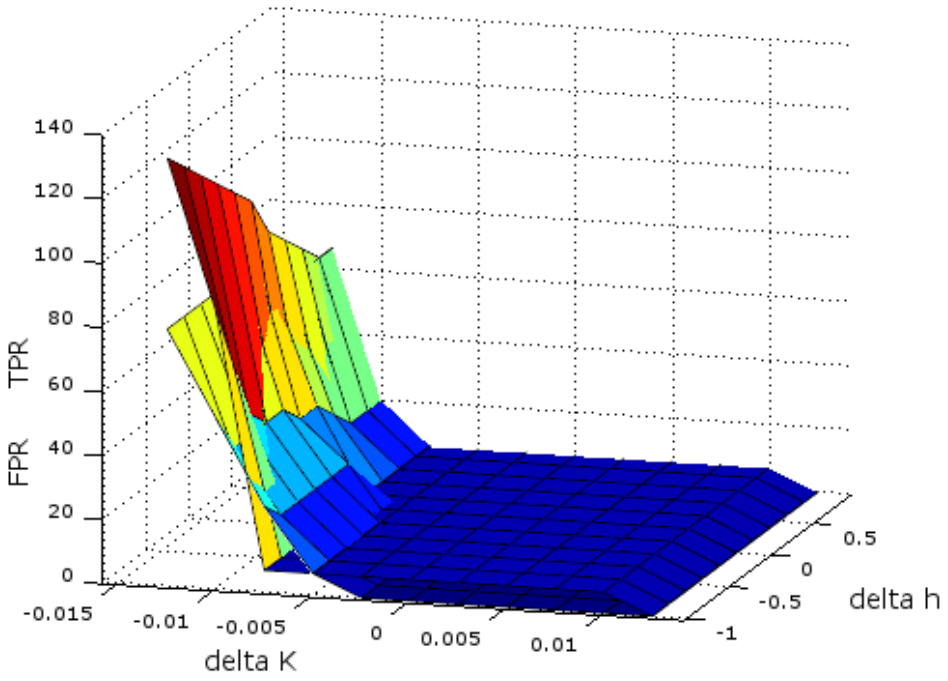
Slika 33-a: Eksperiment sa 110 napadača Tsallis entropija, sa primenom TSK-FS metode. TPR je i dalje visoka, lažne detekcije su nešto povećane sa smanjenjm vrednosti parametara detekcije.



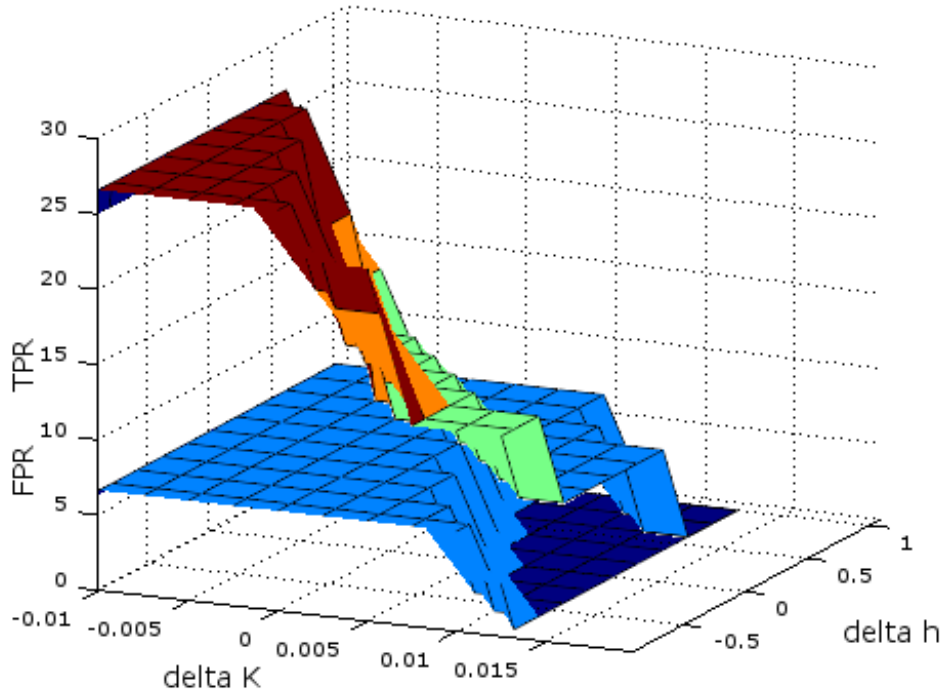
Slika 34-a: Eksperiment sa 70 napadača i bez primene TSK-FS metode, Tsallis entropija. TPR i FPR površine su već bliske, detekcija nepouzdana.



Slika 34-b: Eksperiment sa 70 napadača i sa primenom TSK-FS metode. TPR i FPR su za razliku od slike 34-a i dalje razmaknute, detekcija manje pouzdana ali i dalje moguća.



Slika 35-a: Veoma slab napad, 30 napadača, površine TPR i FPR su sada već veoma bliske za ceo opseg parametara, detekcija praktično nije moguća.



Slika 35-b: Eksperiment sa malim brojem napadača, 30, sa primenom TSK-FS metode. TPR je na oko 25% , ali je i FPR niska, tako da je detekcija još uvek moguća.

Na dijagramima se vidi da površine koje predstavljaju TPR i FPR su bliže jedna drugoj kada nije primenjen TSK-FS tj. detekcija je manje robusna. Odgovarajući dijagrami za istu postavku eksperimanta ali uz primenu TSK-FS pokazuju da je detekcija robusnija kada je TSK-FS metod primenjen a da su razlike izmedju površina TPR i FPR visoke za širok opseg CUSUM parametara h i K. Ovaj rezultat je važan za potencijalnu praktičnu primenu TSK-FS metoda u detekciji DDoS napada jer jednom odredjeni h i K parametri daju stabilan kvalitet detekcije kada se okruženje dinamično menja.

Tabela 4. prikazuje rezultate istih eksperimenata za distribuciju odredišnih adresa za large scale topologiju kada jačina napada varira od slabijeg ka jakom. I ovde su dati rezultati primene nekoliko tipova entropija. Za svaki od tipova entropija formiran je poseban TSK-FS model. Eksperimenti su radjeni zaodredišne IP adrese za Shannon, Tsallis i T-entropiju. Rezultati u tabeli 4. su prikazani samo za optimalne vrednosti *h* i *K* za datu jačinu napada. To su vrednosti pri kojima razlika TPR-FPR ima maksimum. I ovde se podrazumeva da je greška tipa II razlika izmedju 100% i TPR.

Tabela4: Poredjenje tačnosti detekcije za Shannon-ovu Tsallis (q=0.6) i T-entropiju bez primene i sa primenom TSK-FS metoda za topologiju velike razmere. Jačina napada varira izmedju 20 i 150 napadača.

broj napadača	**TPR FPR**	**h K**	**TPR FPR**	**h K**
	Shannon		**Shannon+TSK-FS**	
150	80% 13%	1.7 0.01	100% 6%	4.3 0.02
110	94% 6%	1.6 0.01	100% 0%	3.0 0.03
70	74% 20%	1.4 0.01	87% 6%	5.7 0.01
50	47% 13%	1.6 0.01	74% 0%	5.4 0.01
30	13% 13%	1.7 0.01	26% 0%	4.5 0.025
20	0% 20%	1.7 0.01	20% 6%	3.9 0.025
	Tsallis		**Tsallis+TSK-FS**	
150	100% 0%	4.8 0.025	100% 0%	6.0 0.035
110	100% 0%	4.8 0.015	100% 0%	6.0 0.035
70	100% 6%	3.8 0.015	100% 0%	5.8 0.035
50	94% 20%	3.8 0.012	86% 13%	5.6 0.035
30	13% 0%	3.8 0.015	47% 13%	4.6 0.03
20	0% 0%	4.8 0.012	23% 6%	6.0 0.025
	T-entropy		**T-entropy+TSK-FS**	
150	87% 20%	4.6 0.01	67% 0%	3.9 0.01
110	6% 6%	5.0 0.01	33% 0%	4.2 0.015
70	0% 20%	5.2 0.015	20% 6%	4.2 0.01

Ista zapažanja mogu se dati kao i za ivičnu topologiju. Kvalitet detekcije u eksperimentima sa primenjenom TSK-FS metodom je bolji nego kada se tačke napada detektuju samo na signalima entropije. Čak i za napade male snage, kada su varijacije entropije u odnosu na normalan saobraćaj suviše male i kada primena samo entropije više ne detektuje napade, uz primenu TSK-FS neki napadi se još mogu detektovati. Kao i u prethodnim eksperimentima, vidi se da se pri snižavanju praga broj lažnih dogadjaja naglo raste ako TSK-FS nije primenjen. (Slike 32-a do 35-a).

Ponovo, kao i u prethodnom skupu eksperimenata parametrizovana Tsallis entropija daje neznatno bolje rezultate u odnosu na Shannonovu entropiju, dok T-entropija daje upotrebljive rezultate samo za slučajeve kada su napadi jaki. U svim slučajevima, i za sve tipove entropija FPR ostaju niski.

U jednom od prvih radova gde je upotrebljena Tsallis entropija za detektovanje DDoS napada [72], postignuta je približno ista tačnost detekcije, sa parametrom q=0.9, dok je u ovom radu q postavljeno na vrednost 0.6.

Slični rezultati su prezentovani i u [39]tabela I. Rezultati u u ovom radu prikazani u tabeli 4 daju manji FPR nego u [39] tabela 1 za sličnu postavku eksperimenta. Razlog je to zato što je u [39] faktor osetljivosti CUSUM algoritma K fiksan, dok u ovom radu on varira, tako da je lokalni maksimum razlike TPR-FPR veći.U [69] autori izvode eksperimente za nekoliko tipova entropija. Iako je postavka eksperimenata drugačija, TPR i FPR imaju približne vrednosti kao i u eksperimentima u ovom radu bez primene TSK-FS.

Eksperiment 3: Kombinovanje promenljivih

Sa istom postavkom izvedeni su eksperimenti samodelom koji je formiran kombinacijom vrednosti entropija za pet ulaznih promenljivih: odredišna i izvorišna IP adresa, medjuvreme pristizanja paketa, dužina paketa i ACK fleg . Ulazni vektor se sastoji takodje iz 10 vrednosti entropija od kojih su pet trenutnih vrednosti a pet su uzeti 0.5 sekundi ranije (polovina podintervala) tako da se uzme u obzir trend promene za sve promenljive.

U tabeli 5vidimo rezultate za Shannon, Tsallis i T-entropiju. Primena tačke promene direktno na vrednost signala entropije ovde nije moguće primeniti jer imamo entropije za pet različitih promenljivih. Poredjenjem sa tabelom 4, ne može se utvrditi značajnija razlika u odnosu na eksperimente sa modelom formiranim na uzorku koji sadrži samo entropiju jedne promenjive. Pouzdanost detekcije je na istom nivou, broj TPR je visok a FPR nizak, a kako se ide ka slabijim napadima i dalje je metoda osetljiva i sa malim brojem lažnih detekcija. Za T-entropiju se dobijaju nešto bolji rezultati detekcije nego u eksperimentima sa jednom promenljivom. Razlog se može tražiti u tome da T-entropija ima manji šum ako se koriste promenljive sa manje simbola, kao što su flegovi i medjuvremena pristizanja, nego što je slučaj samo sa IP adresama. U [43],

gde se istražuje primena T-entropije, IP adrese se čak i ne koriste. Odatle se može zaključiti da bi T-entropija dala bolje rezultate na drugačijem skupu promenljivih koji ne sadrži IP adrese.

Prednost ovako formiranog modela, kombinovanjem entropija više veličina je u tome što napadi različitih karakteristika mogu imati i različit uticaj uticaj na promene entropija nekih veličina. Nekad taj uticaj može da bude i ravan nuli. Zato oslanjanje na entropiju samo jedne veličine nosi opasnost da neki napadi ostanu neotkriveni. Kombinovanjem entropija se ova mogućnost znatno umanjuje. Iako u ovom skupu eksperimenta, sa simuliranim saobraćajem nije postignuto vidljivo poboljšanje detekcije, u narednim eksperimentima sa realnom mrežom pokazaće se da kombinovanje entropija zaista dovodi do dobusnije detekcije.

Tabela5: Poredjenje procenta detekcije za Shannon-ovu Tsallis sa primenom TSK-FS metoda za topologiju velike razmere. Korišćeni signali entropije za 5 promenljivih iz IP zaglavlja.

Broj napadača	**TPR FPR**	**h K**
	Shannon+TSK-FS	
150	100% 6%	3.25 0.15
110	100% 13%	3.5 0.02
70	93% 6%	4.5 0.01
50	74% 6%	5.0 0.015
30	33% 13%	4.2 0.020
20	13% 0%	3.2 0.020
	Tsallis+TSK-FS	
150	100% 0%	4.4 0.025
110	100% 6%	5.6 0.030
70	100% 0%	5.2 0.035
50	94% 13%	4.6 0.030
30	53% 6%	4.9 0.030
20	26% 6%	5.5 0.020
	T-Entropija + TSK	
150	94% 13%	3.5 0.035
110	80% 13%	3.0 0.035
70	80% 26%	3.2 0.030
50	40% 20%	2.8 0.020
30	26% 26%	2.8 0.025

Eksperiment 4: Detekcija sa unakrsnim modelima

U dinamičnom okruženju karakteristike saobraćaja se često menjaju. To može biti usled promene topologije mreže, promene aktivnosti korisnika ili promene uslovljene primenom novijih tehnologija. Ukoliko bi ove promene izazivale toliku promenu u tačnosti modela da dodje do povećanja broja lažnih alarma ili zahtevale čestu obuku neuralne mreže da bi se postavili novi parametri detekcije, to bi sa praktičnog stanovišta bilo neprihvatljivo. Zato su sprovedeni su i eksperimenti sa unakrsnim topologijama tj. kada se model dobijen topologiju velike razmereprimeni na ivičnu topologiju. Rezultati su prikazani u tabeli 6, u prvom delu tabele. Ostatak tabele su rezultati iz eksperimenta 1sa ivičnom tolopogijom, radi lakšeg poredjenja. Vrednosti tačnosti detekcije su i ovde prikazane samo za optimalne vrednosti parametara h iK.

Iz tabele 6 se može zaključiti sledeće:

- Da je detekcija očekivano nešto lošija nego kada se primeni TSK-FS model sa odgovarajuće topologije, ali je vidljivo da je FPR i dalje niska.
- Kada se rezultati uporede sa eksperimentom 1 idetekcijom bez TSK-FS metode, dobijaju se nešto lošiji rezultati za jake napade, ali čak bolji za slabije napade.

Rezultati ovog eksperimenta pokazuju robusnost TSK-FS modela i da će se process detekcije sa jednom postavljenim parametrima odvijati i u promenjenim uslovima. Kvalitet detekcije bi se nešto smanjio, ali to daje vreme da se izvrši process obuke u novonastalim uslovima.

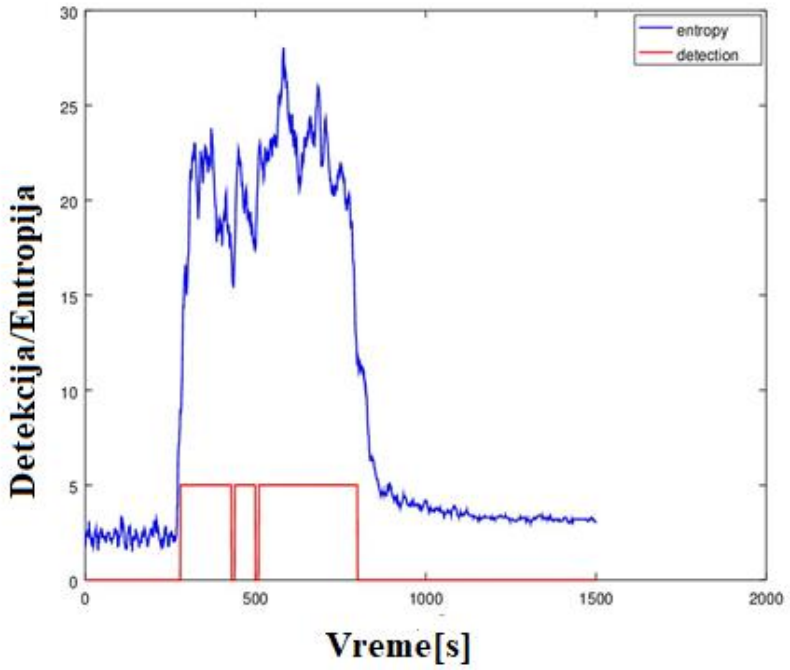
Tabela 6*Rezultati detekcije za unakrsne topologije. Modela dobijen za topologuju velike razmere primenjen je na ivičnu topologiju. Detekcija je još uvek dobra mada nešto lošija čak i u odnosu na eksperimente bez primene TSK-FS metoda.*

Broj napadača	**Shannon +TSK-FS sa modelom iz topologije velike razmere**				**Shannon**				**Shannon+TSK sa originalnim modelom**			
	TPR	**FPR**	**h**	**K**	**TPR**	**FPR**	**h**	**K**	**TPR**	**FPR**	**h**	**K**
80	87%	0%	5.8	0.05	94%	6%	6.8	0.02	100%	0%	4.0	0.03
60	73%	6%	9.5	0.055	87%	0%	3.4	0.07	100%	6%	4.6	0.01
40	54%	6%	6.5	0.15	20%	0%	6.6	.025	94%	6%	4.3	0.005
20	33%	13%	8.1	0.075	0%	0%	-		46%	0%	2.8	0.035

Eksperiment 5: Realan saobraćaj - CAIDA test saobraćaj

U ovom eksperimentu su upotrebljeni javno dostupni skupovi podataka. Model sa topologijom velike razmere je primenjen na CAIDA 20070804_141436 data set. Ovaj test saobraćaj je vrlo često korišćen u obradi anomalija mrežnog saobraćaja i prvi je koji

je bio dostupan za eksperiment. Saobraćaj ne sadrži metapodatke o napadima tako da vreme početka i kraja napada možemo samo pretpostaviti iz oblika signala entropije. Svrha ovog eksperimenta nije primarno bila da se postigne visok stepen detekcije na ovim podacima, nego da se primeni TSK-FS metod na realan saobraćaj kao korak ka praktičnoj implementaciji. Slika 36 prikazuje vrednosti entropije i odgovarajućih izlaza TSK-FS detektora za saobraćaj20070804_141436 za distribuciju odredišnih adresa. Nema lažnih alarma, a ceo period napada je detektovan kao tri bliska perioda napada.



Slika 36: *Dijagram nivoa entropije i signala detekcije za CAIDA saobraćaj. Ovaj skup nema podatke o vremenima napada, tako da je verifikacija uspešne detekcije samo vizuelna.*

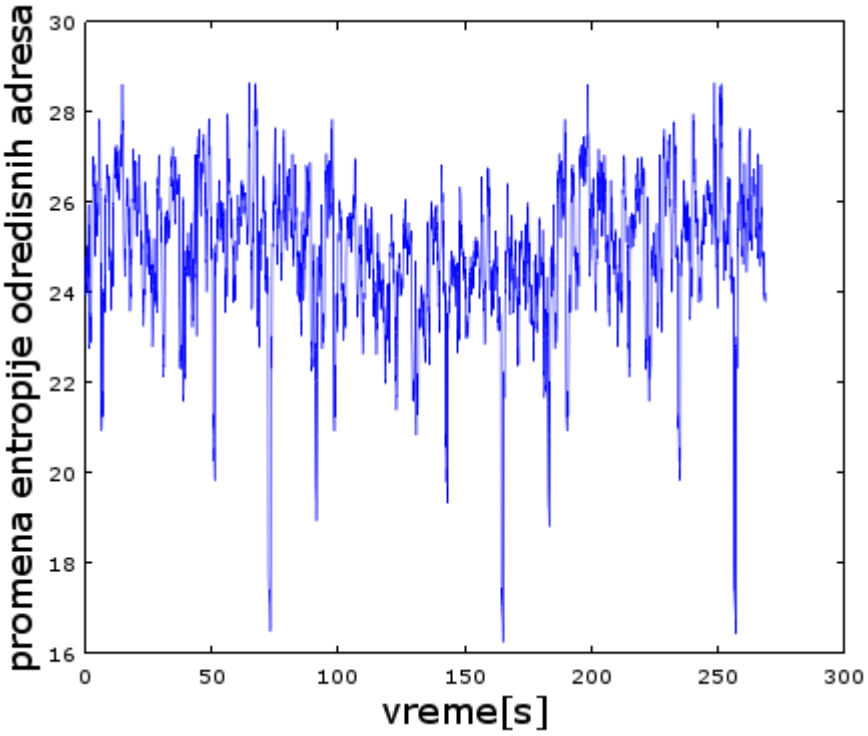
Eksperiment 6: Realan saobraćaj - DARPA test saobraćaj

U sledećem eksperimentu sa javno dostupnum saobraćajem, korišćen je test saobraćajDARPA_2009_DDoS_attack-20091105 [63]. Adresa žrtve je anonimizovana adresa 172.28.4.7 i nalazi se van lokalne mreže. Topologija je slična ivičnoj topologiji iz prvog skupa eksperimenata. Ovaj test saobraćajsadrži minimum potrebnih metapodataka, kao što su vremena pristizanja paketa u mikrosekundama i poznat cilj napada, da bi se mogao koristiti u eksperimentima primenjenim u ovom radu na simuliranom saobraćaju. Test podacisadrže samo saobraćaj u vremenu dok traju napadi. Saobraćaj pre i posle napada je izostavljen. Saobraćaj u vreme trajanja napada je kompletan tj sadrži i pakete napada i pakete uobičajenog saobraćaja koji nisu izostavljeni. U takvim okolnostima ne

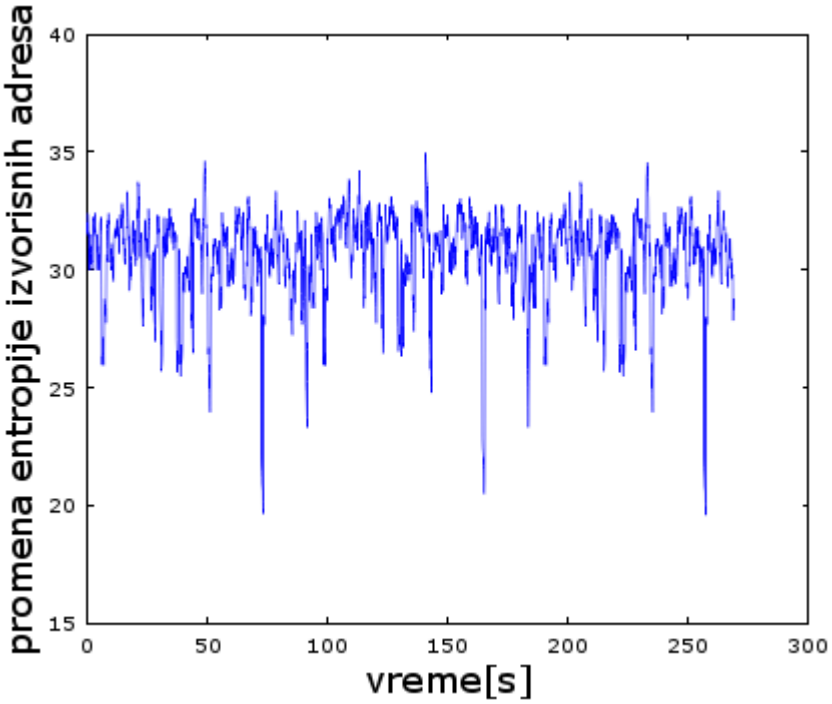
može se odrediti početak ni kraj napada jer bi signal entropije bio istog nivoa za ceo saobraćaj i ne bi postojale tačke promene. Da bi se izvršili isti eksperimenti kao i nad simuliranim saobraćajem bile su nužne modifikacije test saobraćaja:

i. Izvučeni su paketi koji ne pripadaju paketima napada i formiran je test saobraćajuobičajenog saobraćaja.
ii. Deo uobičajenog saobraćaja je pridodat na početak kao i na kraj saobraćaja sa napadima, tako da se dobije približno po jedna trećina uobičajenog saobraćaja na početku i na kraju novog test saobraćaja i u srednjem delu jedna trećina originalnog saobraćaja sa napadima.
iii. Manji fragmenti uobičajenog saobraćaja su ubačeni u saobraćaj sa napadima tako da se dobije slična postavka kao i u eksperimentima sa simuliranim saobraćajem, 15 kratkih napada od po 1 sekunde.Na ovaj način postavke prethodnih eksperimenata sa simuliranim saobraćajem i novih eksperimenata sa realnim saobraćajem su identične i možemo porediti njihove rezultate rezultate.

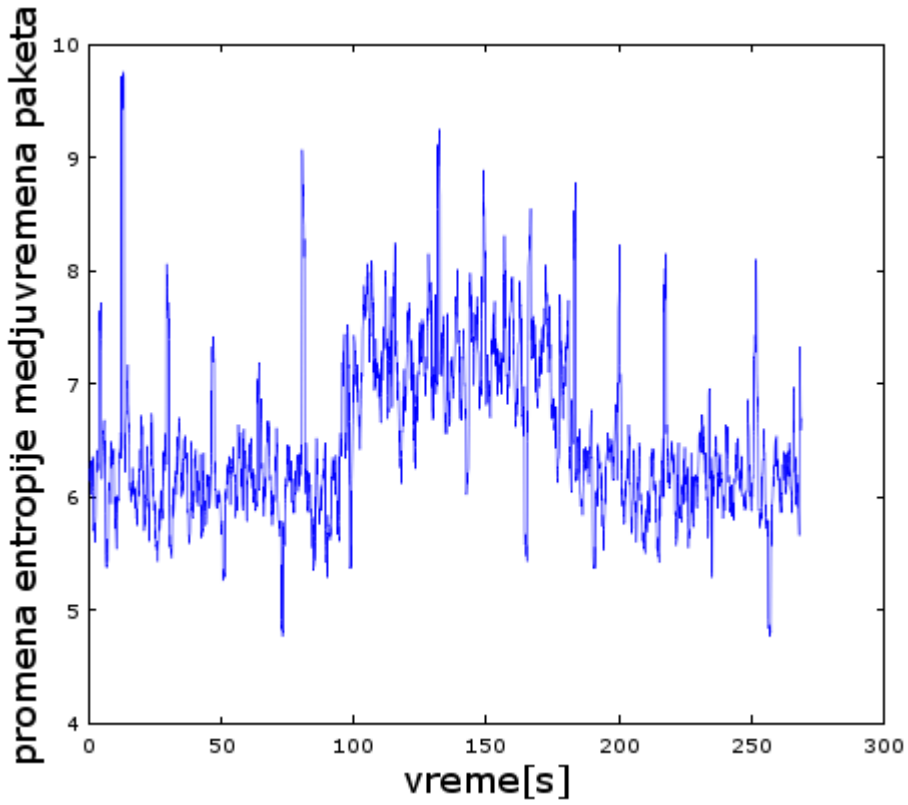
Signal Shannon-ove entropije za slučaj odredišnih adresa sada izgleda kao na slici 37.Vidi se da je entropija tokom napada (srednji deo grafikona) neznatno različita nego u slučaju uobičajenog saobraćaja. Samo oko 7% paketa učestvuje u napadu. Jačina napada približno odgovara najslabijoj jačini napada od 20 napadača iz eksperimanata sa simuliranim saobraćajem. Za razliku od simuliranog saobraćaja ovde ne možemo proizvoljno podešavati jačinu napada, tako da je moguć samo jedan eksperiment za jednu postavku.



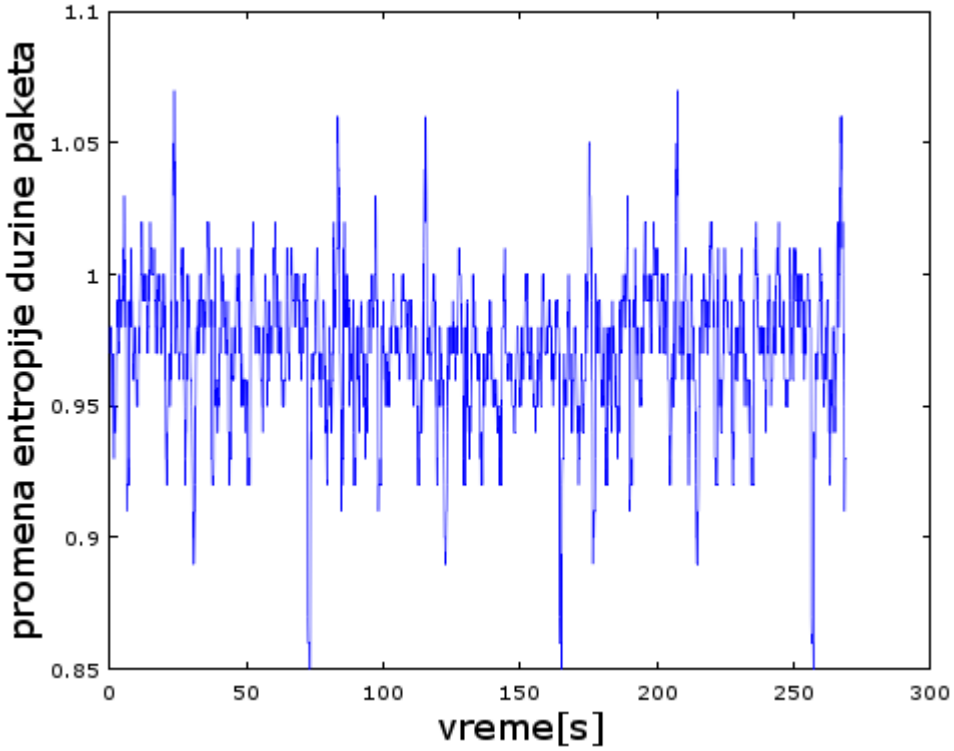
Slika 37: Signal entropije odredišnih IP adresa za DARPA saobraćaj. Napad se dogadja u srednjem delu dijagrama. Entropija se menja, ali je šum visok, pa bi detekcija na osnovu ovog signala bila nepouzdana.



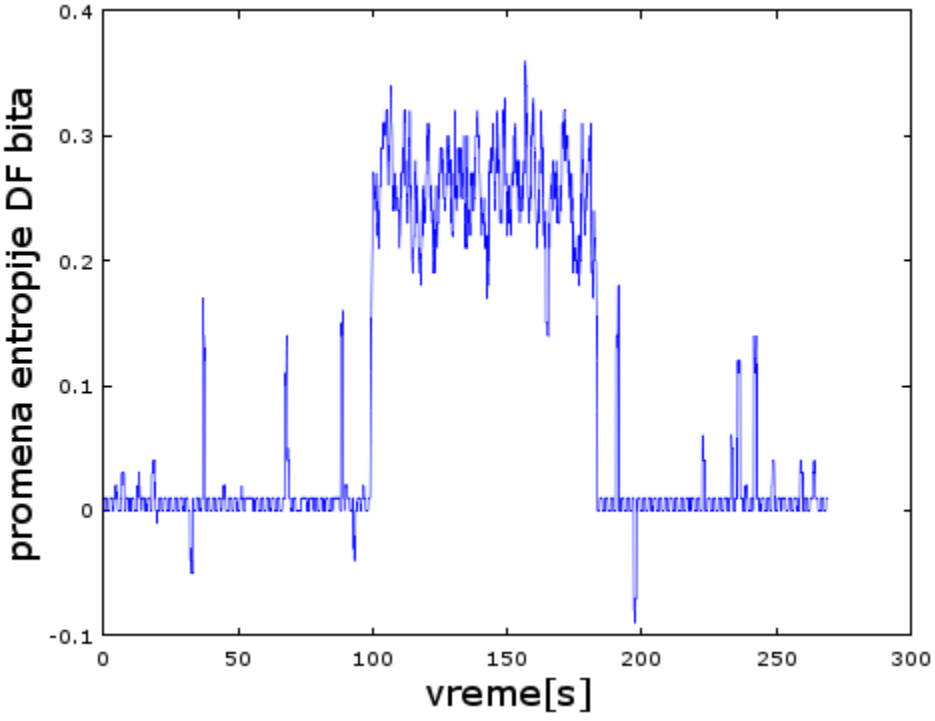
Slika 38: Signal entropije izvorišnih IP adresa za DARPA saobraćaj. Entropija se praktično ne menja, detekcija napada nije moguća.



Slika 39: Signal entropije medjuvremena pristizanja paketa za DARPA saobraćaj. Skok nivoa entropije je evidentan.



Slika 40: Signal entropije dužine paketa za DARPA saobraćaj. Vrlo blago smanjenje nivoa entropije. Uz veliki šum, detekcija veoma nepouzdana.



Slika 41: Signal entropije DF bita za DARPA saobraćaj. Skok entropije izrazit.

Na slikama37 do 41 su prikazani signali Shannon-ove entropije za izvorišne adrese, odredišne adrese, fleg DF, medjuvremena pristizanja paketa i dužine paketa bez modifikacije (iii) tj. još nisu ubačeni kratki segmenti od 1 sekunde nego srednji deo potiče od saobraćaja sa napadom, a početni i završni potiču od uobičajenog sadržaja. Uočljivo je da se entropije različitih veličina različito menjaju u slučaju napada, što zavisi od karakteristika samog napada. U metapodacima test saobraćaja, medjutim, nema podataka o vrsti napada. Entropije odredišnih i izvorišnih adresa kao i dužine paketa se neznatno menjaju. Istovremeno entropije medjuvremena pristizanja i DF flega pokazuju znatnija odstupanja od uobičajenog stanje. Ako bi se primenila entropija samo jedne veličine, ne bi se dobio zadovoljavajući model. Kod promenljivih koje daje slabu promenu entropije, šum je previše jak tako da bi formirani model bio neprecizan. Kod flega DF , entropija se izrazito menja tako bi model formiran na osnovu ovog signala na ulazu zahtevao takodje velike promene entropije, jer je proces obuke imao jak signal kao ulaz. Takav model ne bi detektovao slabije promene. Pored toga, model formiran na osnovu samo jedne veličine ne bi bio dovoljno robustan kada se entropija odabrane veličine ne bi dovoljno menjala u slučaju drugačijih karakteristika napada.Zato je proces obuke koristio kombinovan ulazni signal sledećih karakteristika:

- Sastavljen iz vrednosti entropija svih pet posmatranih promenljivih.
- Po pet vrednosti entropija je uzeto u datom vremenskom trenutku a drugih pet je uzeto pola sekunde (polovina podintervala) ranije.
- Nivoi signala entropija su u ulaznom uzorku skalirani tako da imaju približne srednje vrednosti, manje od 10.0, da bi podjednako doprinosili u formiranju modela.

Naovajnačinsuformiranadvarazličita test saobraćaja, jedankojisekoristisamozaprocesobuke, adrugisamozadetekciju.Kao i u eksperimentima sa simuliranim saobraćajem, ulaznim uzorcima pridodata je i vrednost napada, 0 ili 1. Vrednosti napada se koriste da bi se formirao model tokom obuke kao i da bi se proverila tačnost metode u tokom detekcije. U ovom eksperimentu nije moguće menjati jačinu napada pa je izveden po jedan eksperiment za Shannon, Tsallis i T-entropiju sa primenom TSK-FS metode. Rezultati su prikazani u tabeli 7.

Tabela 7: Završni eksperiment sa saobraćajem sa realne mreže. Korišćene entropije pet promenljivih iz IP zaglavlja. Rezultati su prikazani za optimalne vrednosti parametara h i K.

TPR FPR	**h K**
Shannon+TSK-FS	
94% 6%	2.35 0.25
Tsallis+TSK-FS	
100% 0%	4.0 0.035
T-Entropija + TSK-FS	
94% 13%	3.6 0.025

Model koji je formiran u procesu obuke za Tsallis entropiju sastoji se iz sledećih komponeni:

Matrica klastera CLA =

$$\begin{bmatrix} 5.037 & 4.970 & 4.852 & 4.858 & 4.937 \\ 6.197 & 6.170 & 6.478 & 6.072 & 6.965 \\ 6.082 & 6.035 & 6.014 & 19.90 & 6.198 \\ 4.869 & 4.847 & 4.822 & 4.783 & 4.874 \\ 0.1899 & 1.240 & 4.316 & 0.1445 & 6.079 \\ 5.033 & 4.941 & 5.019 & 4.939 & 4.877 \\ 6.192 & 6.548 & 6.193 & 6.204 & 6.874 \\ 6.093 & 6.079 & 6.084 & 23.07 & 6.149 \\ 4.868 & 4.865 & 4.857 & 3.654 & 4.844 \\ 0.1913 & 4.527 & 0.8551 & 0.1445 & 5.763 \end{bmatrix}$$

Matrica modela A =

$$\begin{bmatrix} 9.507e-5 & -2.486e-1 & -1.428 & 8.695e-2 & -1.976 \\ -4.123e-4 & -2.741e-2 & 8.026e-1 & -4.593e-2 & 2.162e-1 \\ -9.091e-4 & 1.746e-1 & 1.637e-1 & 3.239e-3 & 1.283 \\ 1.912e-3 & 1.177e-1 & -1.785e-1 & -2.930e-1 & 6.490e-1 \\ 2.801e-3 & 1.134e-2 & 4.081e-1 & -9.069e-2 & 2.337e-1 \\ 2.159e-2 & 6.359e-2 & -6.372e-1 & -2.150e-1 & -2.560e-1 \\ -1.322e-3 & 4.053e-2 & -2.271e-1 & 8.948e-2 & 6.894e-2 \\ -1.854e-2 & -1.359e-1 & 7.358e-1 & 1.604e-2 & -3.831e-1 \\ -2.926e-4 & -1.150e-1 & -5.345e-1 & -7.274e-3 & 9.583e-1 \\ -7.263e-4 & -5.414e-3 & 5.462e-2 & 9.570e-2 & 2.247e-2 \end{bmatrix}$$

Vektor B = [0.01171, 0.6086, 3.352, 1.345, -4.383]

Takagi-Sugeno-Kang fazi model za detekciju DDoS napada na test saobraćaju DARPA_2009_DDoS_attack-20091105sada izgleda ovako:

Pravilo 1:
Ako x pripada {5.037, 6.197, 6.082, 4.869, 0.1899, 5.033, 6.192, 6.093, 4.868, 0.1913}
Onda je $y=x_0$*9.507e-5 + x_1*-4.123e-4 + x_2*-9.091e-4 + x3*1.912e-3 + x_4*2.801e-3 +x_5*2.159e-2 + x_6*-1.322e-3+x_7*-1.854e-2 +x_8*2.926e-4+ x_9*-7.263e-4 + 0.01171

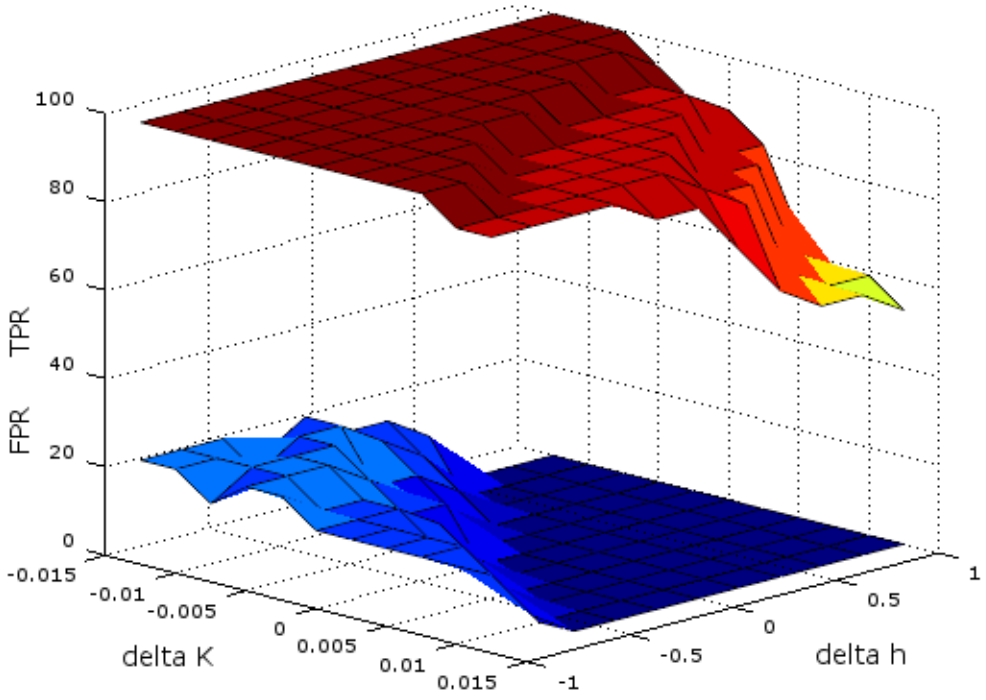
Pravilo 2:
Ako x pripada {4.970, 6.170, 6.035,4.847, 1.240, 4.941, 6.548, 6.079, 4.865, 4.527}
Onda je $y=x_0$*-2.486e-1+ x_1*-2.741e-2 + x_2*1.746e-1+ x_3*1.177e-1+ x_4*1.134e-2 +x_5*6.359e-2 + x_6*4.053e-2 +x_7*-1.359e-1 +x_8*-1.150e-1 + x_9*-5.414e-3+ 0.6086

Pravilo 3:
Ako x pripada {4.852, 6.478, 6.014, 4.822, 4.316, 5.019, 6.193, 6.084, 4.857, 0.8551}
Onda je $y=x_0$*-1.428+ x_1*8.026e-1+ x_2*1.637e-1+ x_3*-1.785e-1+x_4*4.081e-1+x_5*-6.372e-1+ x_6-2.271e-1 +x_7*7.358e-1+x_8*-5.345e-1+ x_9*5.462e-2 + 3.352

Pravilo 4:
Ako x pripada {4.858, 6.072, 19.90, 4.783, 0.1445, 4.939, 6.204, 23.07, 3.654, 0.1445}
Onda je $y=x_0$*8.695e-2+ x_1*-4.593e-2+ x_2*3.239e-3+ x_3*-2.930e-1+ x_4*-9.069e-2 +x_5*-2.150e-1+ x_6*8.948e-2+x_7*1.604e-2+x_8*-7.274e-3+ x_9*9.570e-2+1.345

Pravilo 5:
Ako x pripada {4.937, 6.965, 6.198, 4.874, 6.079, 4.877, 6.874, 6.149, 4.844, 5.763}

Onda je $y=x_0*-1.976+x_1*2.162e-1+ x_2*1.283 + x_3*6.490e-1+ x_4*2.337e-1+x_5*-2.560e-1+ x_6*6.894e-2+x_7*-3.831e-1+x_8*9.583e-1+ x_9*-2.247e-2 -4.383$



Slika 42: Zavisnost ispravnih i lažnih detekcija za saobraćajDARPA_2009_DDoS_attack-20091105od promene nivoa praga h i promene osetljivosti K uz primenu TSK-FS metoda. TPR je visoka za širok opseg parametara. FPR je povišena samo za veoma niske vrednosti parametara. TSK model je formiran za distribucije pet promenljivih. Saobraćaj je preuzet sa realne mreže.

Mada je ovaj eksperiment samo poslednji od niza eksperimenata, on je veoma značajan jer je izveden na modifikovanom realnom saobraćaju. Vidi se da je primenom TSK-FS metoda sa kombinovanim skupom promenljivih postignuta tačnost detekcije na realnom saobraćaju približna tačnosti na simuliranom saobraćaju. Procenat tačnih detekcija je visok a pogrešnih je i ovde nizak.

Može se zapaziti i da entropija distribucije flega DF (Don't Fragment) najviše doprinosi formiranju modela i tačnosti detekcije, ali to može da važi samo za napad u ovom konkretnom eksperimentu. U slučaju napada sa drugačijim karakteristikama DF fleg ne mora da se menja, pa bi njegov doprinos bio zanemariv. Ali zato bi se entropija distribucije neke druge promenljive značajnije menjala. U tome je prednost modela sa kombinovanjem promenljivih:napadač bi morao da osmisli napad koji ne menja entropije ni jedne od posmatranih promenljivih što mu značajno umanjuje, ako ne i potpuno

onemogućavamogućnosti u kreiranju napada koji je nevidljiv za TSK-FS detektor. U ovom primeru imamo kombinaciju pet promenjivih ali u opštem slučaju može se odabrati proizvoljan broj. Ograničenje je samo u performansama detektora.

10. Predlog idejnog rešenja za primenu TSK-FS metode na hardverskim komponentama

Od samog početka rada na ovoj tezi, vodilo se računa o mogućnosti praktične primene. Mesto gde bi se TSK-FS metoda implementirala je u prvom redu mrežna oprema, što zahteva optimizovanje svih izračunavanja. Dalje, metoda bi se mogla implementirati kao softverski umetak (plugin) u softverskim alatima za analizu saobraćaja kao sto je Wireshark ili detektorima napada kao što je Snort. Da bi se omogućila primena metode kao modula za rad u realnom vremenu nužna je optimizacija u smislu upotrebe brzine izvršavanja i upotrebe resursa. Sva izračunavanja vrednosti signala entropije kao i kasnije procesiranje u dosadašnjim eksperimentima nisu se odvijali u realnom vremenu. Samo generisanje modela, kao process koji je najzahtevniji po pitanju vremena i memorijskih resursa, i dalje se može izvršavati van realnog vremena. Procesi koji moraju i dalje da se obavljaju u realnom vremenu su izračunavanje entropije, primena TSK-FS modela i finalna CUSUM detekcija početka i kraja napada.U daljem tekstu će biti opisano idejno rešenje detektora DDoS napada koje funkcioniše u realnom vremenu i sa minimumom memorijskih resursa.

Zahtevi za sintezu automata za detekciju DDoS napada u realnom vremenu

Da bi obrada mogla da se vrši u realnom vremenu, potrebni su ubrzanje i optimizacija algoritma. Hardverski resursi koji bi se koristili sadrže ograničene resurse za skladištenje ulaznih podataka medjurezultata i izlaza su ograničeni. U predloženom postupku pretpostavljeni su sledeći uslovi:

- Mrežni paketi se moraju direktno obradjivati u sirovom formatu u kome pristižu sa mreže bez konverzije u druge formate.
- Mrežni paketi se moraju početi obradjivati po pristizanju svakog pojedinačnog paketa, a obrada se mora završiti pre pristizanja narednog paketa.
- Vrednost entropije se mora ažurirati pri pristizanju svakog paketa.
- Obrada mora biti protočna, tj. ne smeju se vršiti obrade nad velikom količinom akumuliranih nizova podataka, nego sve obrade moraju narednu vrednost dobijati iz tekuće vrednosti.
- Izlazna vrednost TSK-FN detektora se izračunava za svaki podinterval.

Računanje entropije u realnom vremenu

Izračunavanje nivoa entropije se pokazalo kao vremenski najzahtevniji proces, pa se njemu posvetila posebna pažnja u dizajnu. Postoje dva osnovna problema kod izračunavanja entropije u dosadašnjim eksperimentima:

a) Ne može se izračunati vrednost verovatnoća

   p_i *= (broj dogadjaja tipa i)/(ukupan broj dogadjaja)*

   dok se ne završi zadati interval obrade, jer je ukupan broj dogadjaja sve do završetka intervala nepoznata veličina.

b) Po završetku intervala obrade (tipično 1/10 sekunde), mora se izvršiti izračunavanje svih verovatnoća, njihovih logaritama i sabrati svi rezultati da bi se dobila vrednost entropije u datom trenutku.

Ako se obrada vrši nad paketima prikupljenim u datotekama, izračunavanje entropije je trivijalan zadatak. Medjutim, pri brzom pristizanju paketa u realnom vremenu jasno je da koncept obrade mora da se menja. U predloženom rešenju koristi se protočna obrada sa kružnim baferima pomoću kojih se u malom broju koraka dobija nova vrednost entropije iz tekuće vrednosti. Da bi se rešio navedeni problem pod a), ne posmatra se ukupan broj dogadjaja u datom vremenskom intervalu, već se posmatra promenljivi vremenski interval u kome će se dogoditi unapred odredjeni broj dogadjaja. Taj broj dogadjaja može biti izabran tako da bude stepen broja dva zbog računanja logaritma kao i zbogoperacije delenja koje se onda svodi na pomeranje broja u desno. Na taj način, ako je ukupan broj dogadjaja 2^{10}, verovatnoća p_i se računa kao:

p_i*=(broj dogadjaja) / 1024*
ili
p_i *=(broj dogadjaja) >> 10* (u fiksnom zarezu)

Vremenski interval sada nije tačno odredjen, ali to ne predstavlja problem jer će se tačna vrednost entropije menjati na izlazu posle svakog paketa. Naredna komponenta koja čita i obradjuje vrednosti entropije može uzimati odbirke sa periodom odabiranja koja je jednaka proizvoljnoj vrednosti, tako da se naredni procesi obrade ovom izmenom ne menjaju. Strukture podataka koje se koriste u ovoj implementaciji računanja entropije su sledeće:

Bafer dogadjaja je niz koji ima onoliko elemenata koliko ima mogućih dogadjaja (preslikanih na indekse niza) koji se posmatraju. Ako je to IP adresa čijih se 12 značajnijih bita posmatraju, niz dogadjaja će imati 2^{12}=4096 elemenata. Ako se posmatra fleg u zaglavlju paketa, broj elemenata će biti samo 2. Pri pojavi bilo kog dogadjaja, element na odgovarajućoj poziciji u nizu se uvećava za jedan.

Kružni bafer sa vrednostima trenutnih entropija. Pri pojavi n-tog dogadjaja na istoj poziciji vrednost entropije za dati dogadjaj je

$$e=n/1024*\log_2(n/1024)$$

Prethodna vrednost za dati dogadja je bila:

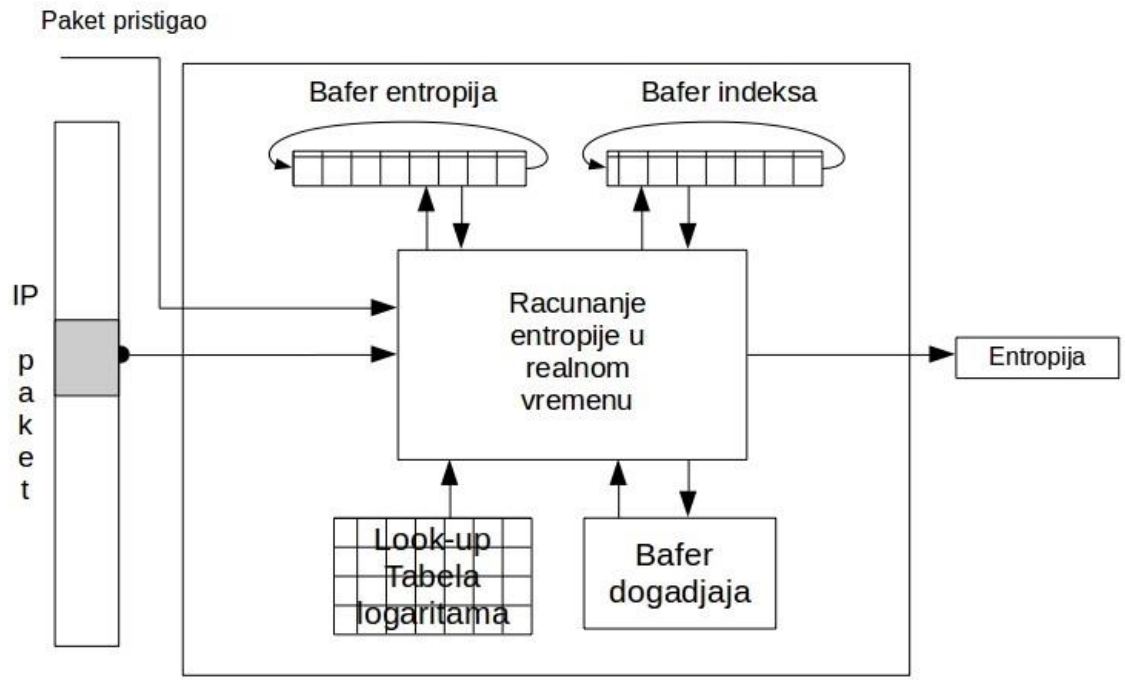
$$e=(n-1)/1024*\log_2((n-1)/1024)$$

Pošto se pamti samo jedna vrednost ukupne entropije, trenutna vrednost ukupne entropije treba da se menja za razliku ove dve vrednosti. Ovim se rešava problem b) tako što se ne vrše složena izračunavanja na kraju svakog vremenskog intervala, nego se stalno dodaje promena vrednosti entropije:

$$delta\_e(n) = n*(10-\log_2(n)) – (n-1)*(10-\log_2(n-1))$$

Da bi se izbeglo računanje logaritama može se koristiti look-up tabela sa maksimalno 1024 vrednosti funkcije *delta_e*.

Kružni bafer sa vrednostima indeksa dogadjaja. Kada pristigne poslednji paket odnosno poslednji dogadjaj od ukupnog broja dogadjaja (2^{10} u ovom primeru), ne stratuje se ponovo računanje entropije, nego se poništava najstariji dogadjaj tj, brojač dogadjaja se umanjuje za jedan na poziciji najstarijeg dogadjaja koji sad više nije važeći. Zato mora da se vodi lista dogadjaja u obliku kružnog bafera koji sadrži indekse dogadjaja. Ovim se dodatno optimizuje izračunavanje vrednosti ukupne entropije.



Slika 43. Blok šema izračunavanja entropije u realnom vremenu.

```
#define RING_SIZE 2048
double entropy_ring[RING_SIZE];
int16event_index_ring [RING_SIZE];
int16  event_buffer[1024];
double log_lookup_table[RING_SIZE];
int count = 0;
double v = 0.0;
int pos = 0;
double entropija = 0.0;
double e_point;
while(1) {
Wait_for_new_packet();
dst_addr = read_from_packet();
dst_addr = dst_addr << 22;
event_buffer[dst_addr]++;
v = event_buffer[dst_addr];
e_delta = log_lookup_table[v];
entropy_ring[count] = e_point;
event_index_ring[count] = dst_addr;
count = (count + 1) % RING_SIZE;
e_dif = entropy_ring[count];
pos = event_index_ring[count];
```

```
if(event_ring [pos]) dst_ports_ring[pos]--;
entropija += e_delta-e_dif;
}
```

Programski kod 1: Protočno izračunavanje Shannon-ove entropije za odredišne IP adrese

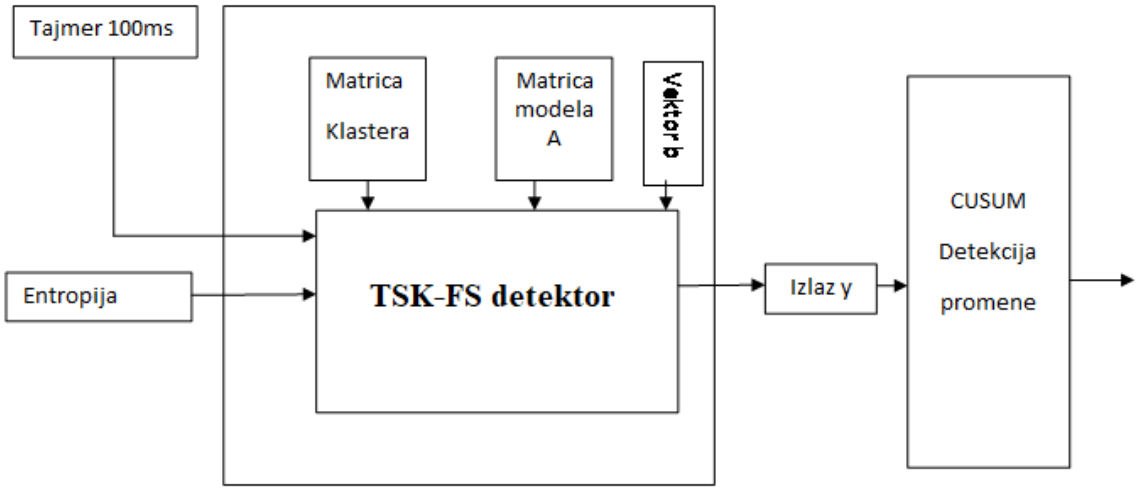
Iz datog algoritma se odmah može naslutiti da vrednost entropije postaje tačna tek posle pristizanja 1024-og paketa i od tog trenutka će se održavati tačna vrednost na nivou svakog novog paketa. Taj početni period „gradjenja“ vrednosti entropije je veoma kratak: U simuliranom sistemu koji se koristi u ovom radu za jednu sekundu pristigne oko 12000 paketa, tako da će tačna vrednost entropije biti dostugnuta veoma brzo.

Izračunavanje izlazne vrednosti prema TSK modelu

Komponenta koja vrši izračunavanje izlazne vrednosti y iz TSK-FS detektora sastoji se iz dva koraka. U prvom se odredjuje odstojanje ulaznog vektora (10 poslednjih vrednosti entropije) sa centrima klastera i odredjuje najbliži. U drugom koraku se vrši skalarno množenje ulaznog vektora sa koordinatama najbližeg klastera i na taj način dobija izlaz iz TSK-FS detektora. Ni jedan od ovih koraka nije zahtevan za izračunavanje, tako da nije bila potrebna promena dizajna.

Strukture podataka koje se koriste u ovoj komponenti su dobijene u procesu generisanja modela koji se ne vrši u realnom vremenu:

- Matrica centara klastera, dimenzija 10x5 za primer iz ovog rada.
- Matrica a modela, dimenzija 10x5 za primer iz ovog rada.
- Vektor b modela sa 10 elemenata.



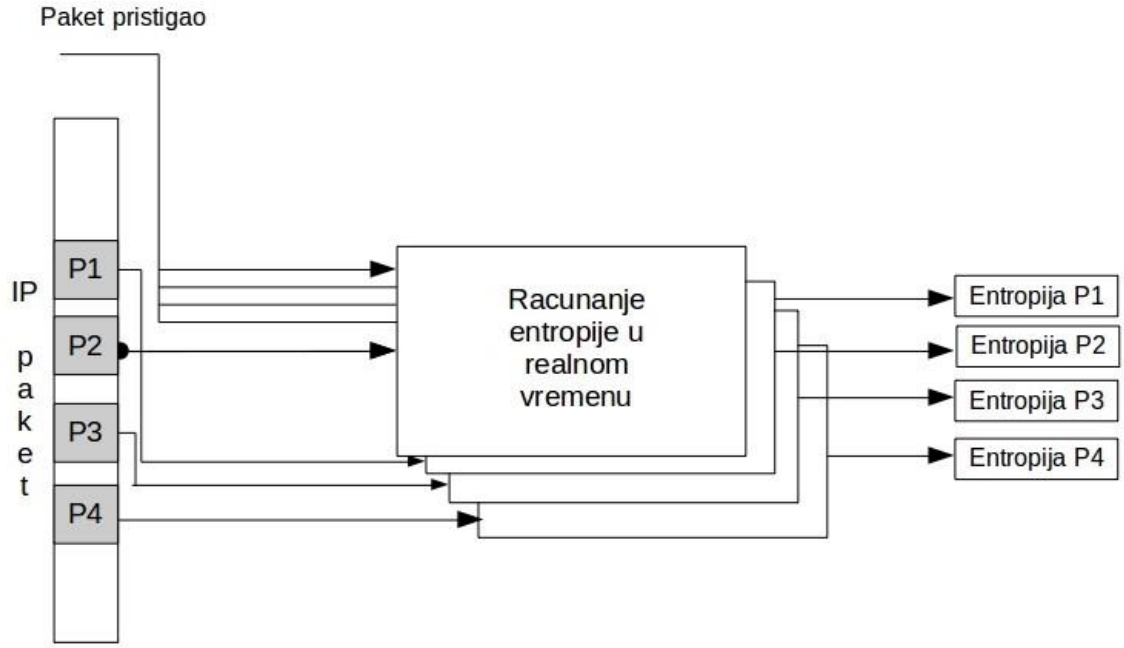
Slika 44: Blok šema TSK-FS detekcije za realizaciju na hardverskim komponentama.

```
#define NUM_OF_CLUSTERS 5
#define SLIDING_WINDOW_WIDTH 10
/* promenljive za racunanje izlaza po TSK pravilima */
double a[SLIDING_WINDOW_WIDTH][ NUM_OF_CLUSTERS];
double cla[SLIDING_WINDOW_WIDTH][ NUM_OF_CLUSTERS];
double b[NUM_OF_CLUSTERS];
double uzorak[10];
double sum;
int ring_pos = 0;
int klaster;

/* Promenljive za CUSUM algoritam */
double H,h;
double beta1 = 0.79, beta2 = 0.95;
double mi_n, mi_n_1;
double dn,  dn_1 = 0.0;
double sigman, sigman_1;

/* Izlaz iz TSK i ulaz u CUSUM detekciju promene */
double y;

/* Izlaz CUSUM detekcije promene */
double napad;

while(1) {
```

```
wait_100ms();
uzorak[ring_pos] = entropija;
/* trazenje najblizeg centra klastera */
for(klaster = -1, j = 0; j < NUM_OF_CLUSTERS; j++) {
        for(sum = 0.0,i = 0; i < SLIDING_WINDOW_WIDTH + 1; i++) {
          distance = cla[curr_pos][j]-uzorak[(i+ring_pos)%10];
          if(distance < 0) distance  = -distance;
        sum+= distance;
        }
        if(sum < min) {
                min = sum;
                klaster = j;
        }
}
 ring_pos++;
/* racunanje pravila po formuli y = Ax + b */
for(i = 0,y = 0.0; i < SLIDING_WINDOW_WIDTH; i++){
        y += uzorak[(ring_pos+i)%10]*a[i][klaster];
}
y += b[klaster];
/* CUSUM algoritam */
mi_n = beta1*y + (1.0 - beta1)*mi_n_1;
if( dn_1 + y -(mi_n +K) > 0)
        dn = dn_1 + y -(mi_n +K);
else
        dn = 0;
sigman = (1.0 - beta2)*(y-mi_n)*(y-mi_n) + beta2)*(sigman_1);
H = h*sqrt(sigman);
dn_1 = dn;
mi_n_1 = mi_n;
sigman_1 = sigman;
/* izlaz */
if(dn > H) napad = 1.0;
else napad= 0.00;
}
```

Programski kod 2: Izračunavanje procene napada koristeći TSK model i CUSUM detekciju tačke promene.

Komponenta koja vrši finalnu detekciju napada je implementacija CUSUM algoritma koji je već opisan i nije zahtevna ni po memorijskim resursima ni po vremenu izvršavanja. Na izlazu daje 0 ako je procena da napad nije u toku ili 1 ako je procena da je napad u toku.



Slika 45. Paralelno izračunavanje entropijeu realnom vremenu za više promenjivih iz zaglavlja IP paketa. Brzina obrade ostaje ista, broj komponenti se umnožava.

Performanse predloženog rešenja

Predloženo rešenje nije zahtevno ni po zauzeću memorije ni po vremenu izvršavanja. Radna memorija potrebna za računanje entropije po predloženom algoritmi za kružni bafer veličine 2048 i za 1024 moguća dogadjaja je manja od 22 kB. Za računanje izlazne vrednosti po TSK-FS postupku, tj. za smeštaj modela i radnih promeljivih potrebno je manje od 1KB radne memorije. FPGA rešenje sa ovakvim zauzećem memorije je izvodljivo i sa relativno slabijim komponentama.

Što se tiče vremenskih performansi, u radu nije izvršeno egzaktno merenje jer bi realizacija postupka sa FPGA komponentama izlazila iz definisanog okvira teze. Kritično je jedino računanje entropije koje mora da se obavi za svaki pristigli paket u realnom vremenu. Ostali stepeni obrade, računanje izlaza po TSK modelu i detekcija promene se izvode jednom u 100ms pa ne predstavljaju usko grlo. Medjutim, mogu se iskoristiti rezultati iz drugih radova, pa tako ako se uzmu u obzir rezultati prezentovani u radu [49], ovakav algoritam je oko 18 puta brži u FPGA realizaciji nego u odgovarajućoj softverskoj realizaciji i može da obradi pristigle pakete na mreži brzine do 3.32Gbps.

Za slučaj obrade više polja iz zaglavlja paketa, tj. za slučaj kombinovanog modela, potrebno je realizovati više ovakvih blokova (slika 45) koji bi paralelno računali entropije više odabranih veličina. U tom slučaju memorijsko zauzeće se linearno povećava sa brojem odabranih polja iz paketa, dok brzina obrade ostaje ista.

11. Zaključak

U radu je izvršena evaluacija kombinovane metode za detekciju distribuiranog napada odbijanjem usluge (DDoS) baziranoj na nekoliko vrsta entropije i Takagi-Sugeno-Kang neuralnoj mreži. CUSUM (Cumulative Sum) metod je korišćen za detekciju tačke promene u svim eksperimentima. Distribucije polja iz zaglavlja TCP paketa koje su posmatrane su izvorišna IP adresa, odredišna IP adresa, dužina paketa, DF fleg i medjuvreme pristizanja paketa. Izlazna datoteka iz ns-2 simulatora mrežnog saobraćaja su korišćene kao podaci za obuku i kao test podaci. Eksperimenti su izvedeni za dve topologije, tri vrste entropije i dva javno dostupna test saobraćaja sa realnim mrežnim saobraćajem. Topologije su lokalna mreža sa sa ciljem napada van mreže i detektorom na izlaznoj ivici i topologijavelike razmere sa HTTP osnovnim saobraćajem i ciljem napada u lokalnoj mreži.

Eksperimenti potvrdjuju da predloženi TSK-FS metod u značajnoj meri poboljšava kvalitet detekcijenapada ometanjem usluge tako da se mogu izvesti sledeći zaključci:

- Primenom TSK-FS metoda na bilo koji od tri tipa entropije, šum u signalu entropije je značajno suzbijen omogućujući precizniju detekciju tačke promene.
- U svim eksperimentima lažnedetekcije su značajno potisnute, čak i u slučaju napada niskog intenziteta kod koga je odstupanje vremenskog signala entropije malo u odnosu na normalan saobraćaj.
- TSK-FS metod, u odnosu na poznate metode koje koriste samo entropiju povećavarobusnost detekcije i dozvoljavavećuvarijacijuparametaradetekcije.
- TSK-FS metod, u odnosu na poznate metode koje koriste samo entropijusmanjuje donju granicu jačine napada pri kojoj je detekcija moguća uz istovremeno suzbijanje lažnih detekcija.
- Ispravne detekcije imaju visoku vrednost a lažnedetekcije ostaju na niskim vrednostima za širi opseg konfiguracionih parametara detekcije. Ovaj rezultat je važan za potencijalnu praktičnu primenu predložene metode u mrežnim uredjajima za detekciju upada (IDS).
- Što se tiče primene različitih tipova entropije, eksperimenti pokazuju da nešto bolje rezultate ima primena Tsallis entropije u odnosu na Shannonovu entropiju, a da T-entropija daje nešto slabije rezultate u odnosu na druge dve entropije osim u slučajevima kombinovanja više vrednosti entropije.
- Metod je bio uspešan i kada je TSK-FS model generisan za jednu topologiju primenjen na test podatke za različitu topologiju, što pokazuje otpornost prema promeni okruženja.
- Konačno, metod je dao dobre rezultate i kada se primenina saobraćaj preuzetsa realnih mreža.Model koji je formiran kombinovanjem entropija dobijenih od više promenljivih se pokazao kao optimalan za realan saobraćaj.

Na kraju rada, kao na osnovu rezultata eksperimenata,predložen je dizajn detektora napada ometanjem usluge koji koristi protočno izračunavanje entropije i koji je prilagodjen za rad u realnom vremenu, optimalan u pogledu iskorišćavanje vremenskih i memorijskih resursa i primenljiv na hardversku implementaciju.

Kao metod koji koristi entropiju, predloženi metod zadržava opštost u primeni i može da detektuje dogadjaje nezavisno od njihovog tipa kao i potpuno nove dogadjaje. Sa druge strane primena fazi-neuralne mreže povećava osetljivost i robusnost metode. Predloženi metod se može koristiti u mrežnoj opremi kao dopuna postojećim metodama koje su zasnovane na osobinama, a koji nisu predvidjeni za detektovanje nepoznatih dogadjaja.

Postoji nekoliko pravaca daljeg istraživanja:

- Fino podešavanje metode za smanjivanje lažnih alarma pri regularnom povećanju saobraćaja (flush crowd).Model formiran kombinovanjem promenljivih ovde bi mogao da bude primenljiv.
- Odredjivanje optimalnog sastavaulaznih uzoraka. U radu su korišćeni ulazni uzorci sastavljeni samo od vrednosti entropije, jedne ili više promenljivih.S obzirom da je pokazano da se vrednosti napada mogu dobiti u realnom vremenu i za brze mreže, zanimljiv pravac bi bio kombinovanje rezultata TSK-FS detekcije sa vrednostima nekih parametara mrežnog saobraćaja ili polja iz zaglavlja paketa.
- Ispitivanje mogućnosti da se na osnovu preuzetog realnog saobraćaja formira simulacioni model koji bi davao simulirani saobraćaj koji je statistički približan originalnom saobraćaju. Na taj način bi se zadržala realističnost saobraćaja uz dodatnu mogućnost podešavanja parametara simulacije što je prednost upotrebe simulatora.
- Ispitivanje mogućnosti primena koncepta Deep Learning, tehnologije koja doživljava naglu ekspanziju u mnogim oblastima, za detektovanje napada odbijanjem usluge.
- Hardverska realizacija detektora napada u realnom vremenu koji bi se mogao ugraditi u postojeću komercijalnu mrežnu opremu.

Reference

1. Abliz, Mehmud: Internet Denial of Service Attacks and Defense Mechanisms, University of Pittsburgh Technical Report, No. TR-11-178, (2011)
2. Mirkovic, J., Reiher, P.: taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communications Review; vol. 34, issue 2, pp. 39–53, 2004. doi: 10.1145/997150.997156 (2004)
3. Abbass ASOSHEH, Naghmeh Ramezani: A Comprehensive Taxonomy of DDoS Attacks and Defense Mechanism Applying in a Smart Classification, WSEAS Transactions on Computers, Volume 7 Issue 4, April 2008. ISSN: 1109-2750.
4. T. Ditcheva and Lisa Fowler, "Signature-based Intrusion Detection" class notes for COMP290-040, University of North Carolina at Chapel Hill, Feb. 2005.
5. Kaspersky Lab: Kaspersky DDoS Intelligence Report Q2 2017.https://securelist.com/ddos-attacks-in-q2-2017/79241/ (2017)
6. Verisign Distibuted Denial of Service Trends Report, Volume 4, Issue 1 1st quarter 2017, https://www.verisign.com/assets/report-ddos-trends-Q12017.pdf
7. Lakhina, A., Crovella, M., Diot, C.: Mining anomalies using traffic feature distributions. Proceedings of the 2005 Conference on Applications, Technologies, Architectures, and Protocols For Computer Communications SIGCOMM 05, Philadelphia, vol 31, issue 4, pp. 217–228, 2005. doi:10.1145/1080091.1080118 (2005)
8. Shannon, C.E.: A Mathematical Theory of Communication. The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948.
9. ImreCsiszár: Axiomatic Characterizations of Information Measures, Rényi Institute of Mathematics, Hungarian Academy of Sciences , DOI:10.3390/e10030261 (2008)
10. Tsallis, C.: Possible generalization of Boltzmann-Gibbs statistics". *Journal of Statistical Physics*. **52**: 479–487. doi:10.1007/BF01016429 (1988).
11. Rényi, A.: On measures of information and entropy. Proceedings of the fourth Berkeley Symposium on Mathematics, Statistics and Probability 1960. pp. 547–561. (1961)
12. Kolmogorov A. N. Kolmogorov: A new metric invariant of transitive dynamical systems and automorphisms in Lebesgue space, Dokl. Acad. Nauk. SSSR 119 (1958)
13. Kolmogorov A. N. Kolmogorov: Three approaches to the quantitative definition of information, Probl. Inform. Transmis., 1, 1965, pp. 4–7

14. https://en.wikipedia.org/wiki/Kolmogorov_complexity, (last visited on February 4th, 2018).
15. G. J. Chaitin: On the lengths of programs for computing finite binary sequences, J. Ass. Comput. Mach., 13, pp. 547–569, 1966.
16. A. Lempel and J. Ziv: On the complexity of finite sequences, IEEE Trans. Inform. Theory 22 (1976) 75-81.
17. J. Ziv and A. Lempel: Universal Algorithm for Sequential Data Compression, IEEE Trans. Inform. Theory, Vol 23, No. 3, May 1977, pp. 337-343.
18. J. Ziv2 and A. Lempel: Compression of Individual Sequences via Variable-Rate Coding, IEEE Trans. Inform. Theory, Vol 24, No. 5, September 1978, pp. 530-536.
19. Titchener, M.R.: A Deterministic Theory of Complexity, Information, and Entropy. In Proceedings of IEEE Information Technology Workshop, February 1980
20. Ulrich M. Speidel and Jia Yang: A T-decomposition algorithm with O(n log n) time and space complexity. ISIT 2005. Proceedings. DOI: 10.1109/ISIT.2005.1523285. (2005)
21. Rebenich, N.: Fast Low Memory T-Transform: string complexity in linear time and space with applications to Android app store security. PhD thesis, University of Victoria, British Columbia, Canada.(2012)
22. Eric W. Weisstein: Logarithmic integral. http://mathworld.wolfram.com/LogarithmicIntegral.html (last visited on February 04th, 2018).
23. Kulkarni A., Bush, S.: Detecting Distributed Denial-of-Service Attacks Using Kolmogorov Complexity Metrics. Journal of Network and Systems Management, vol. 14, issue1, pp. 69-80, 2006.doi: 10.1007/s10922-005-9016-3 (2006)
24. libflothttps://github.com/ardeego/libflott
25. Will E. Leland, Murad S. Taqqu, Walter Willinger, and Daniel V. Wilson. On the self-similar nature of Ethernet traffic (extended version). IEEE/ACM Trans. Netw, 2:1–15, 1994.
26. Zadeh, L. A. "Fuzzy sets". *Information and Control*. **8** (3): 338 – 353. doi:10.1016/S0019-9958(65)90241-X. (1965).
27. Mamdani, E.H.: Advances in the linguistic synthesis of fuzzy controllers, International Journal of Man-Machine Studies,Volume 8, Issue 6, November 1976, Pages 669-678 , doi: 10.1016/S0020-7373(76)80028-4 (1976)
28. Sugeno, M., *Industrial applications of fuzzy control*, Elsevier Science Pub. Co., 1985.

29. T. Takagi and M. Sugeno, "Fuzzy identification of systems and its applications to modeling and control," IEEE Trans. Syst., Man, Cybern., vol. 15, pp. 116-132, Jan . 1985.
30. M. Sugeno, G.T. Kang: Structure identification of fuzzy model, Fuzzy Sets and Systems, Volume 28, Issue 1, October 1988, Pages 15-33, doi: 10.1016/0165-0114(88)90113-3 (1988)
31. Comparison Abdelwahab Hamam, Nicolas D. Georganas: A comparison of Mamdani and Sugeno fuzzy inference systems for evaluating the quality of experience of Hapto-Audio-Visual applications, Haptic Audio visual Environments and Games, IEEE International Workshop on DOI: 10.1109/HAVE.2008.4685304 (2008)
32. Ke Zeng, Nai-Yao Zhang, Wen-Li Xu.: A Comparative Study on Sufficient Conditions for Takagi–Sugeno Fuzzy Systems as Universal Approximators. IEEE Transactions on Fuzzy Systems, vol. 8, issue 6, pp. 773-780, 2000. doi: 10.1109/91.890337 (2000)
33. Kukolj, D., Atlagic, B., Petrov, M.: Unlabeled data clustering using a re-organizing neural network Cybern Syst Int J, vol. 37, issue 7, pp. 779–790, 2006. doi:10.1080/01969720600887152 (2006)
34. Kukolj, D.: Design of adaptive Takagi-Sugeno-Kang fuzzy model. Applied Soft Computing, vol. 2, issue 2, pp. 89-103, 2002. doi:10.1016/S1568-4946(02)00032-7 (2002)
35. Abilene Network, http://abilene.internet2.edu/.
36. The TOTEM project, https://totem.info.ucl.ac.be/.
37. Basicevic, I., Ocovaj, S., Popovic, M.: Evaluation of entropy-based detection of outbound denial-of-service attacks in edge networks. Security and Communication Networks; vol. 8, issue 5, pp. 837-844, 2015, doi: 10.1002/sec.1040 (2015)
38. Siris, V.A., Papagalou, F.: Application of anomaly detection algorithms for detecting SYN flooding attacks. Computer Communications, vol. 29, issue 9, pp. 1433–1442, 2006. doi: 10.1016/j.comcom.2005.09.008 (2006)
39. Basicevic, I., Ocovaj, S., Popovic, M.: Use of Tsallis entropy in detection of SYN flood DoS attacks, Security and Communication Networks, vol. 8, issue 18, pp. 3634-3640 ,2015. doi: 10.1002/sec.1286 (2015)
40. Ciza, Thomas, Jisa David: DDoS Attack Detection Using Fast Entropy Approach on Flow- Based Network Traffic, Procedia Computer Science, Elsevier, Volume 50, Pages 30-36, https://doi.org/10.1016/j.procs.2015.04.007 (2015)
41. Shiaeles, S.N., Katos, V., Karakos, A.S., Papadopoulos, B.K.: Real time DDoS detection using fuzzy estimators. Computers & Security, vol. 31 issue 6, pp. 782-790, 2012. doi:10.1016/j.cose.2012.06.002 (2012)

42. Shiaeles,S.N,: Real time detection and response of distributed denial of service attacks for web services, PhD Thesis, University of Trace, Xanthi, (2013)
43. Eimann, Raimund E.A: Network event detection with entropy measures, PhD thesis, University of Auckland, New Zealand (2008)
44. R. Eimann, U. Speidel, N. Brownlee: A T-Entropy Analysis of the Slammer Worm Outbreak, Proceedings of the 8th Asia-Pacific Network Operations and Management Symposium (APNOMS), Okinawa, Japan, September 27-30, 2005, pp. 434–445 (2005)
45. Speidel, U., Eimann, R., Brownlee, N.: Detecting network events via T-entropy. 6th International Conference on Information, Communications & Signal Processing ICICS, Singapore, pp. 1–5, 2007. doi: 10.1109/ICICS.2007.4449642 (2007)
46. Vancea, F.: Intrusion detection in NEAR system by Anti-denoising Traffic Data Series using Discrete Wavelet Transform, Advances in Electrical and Computer Engineering, vol 14, issue 4, pp.43-48, 2014, doi:10.4316/AECE.2014.04007 (2014)
47. Pukkawana, Sirikarn: Unsupervised Anomaly Detection in Massive Traffic using S-Transform and Renyu Divergence, Doctoral Disserataion, Nara Institute of Science and Technology, Japan, (2015)
48. Quamar Niyaz, Weiqing Sun, Ahmad Y Javaid: A Deep Learning Based DDoS Detection System in Software-De_ned Networking (SDN). The University of Toledo, USA
49. Sailesh Pati Ramanathan Narayanan Gokhan Memik Alok Choudhary Joseph Zambreno, Design and Implementation of an FPGA Architecture for High-Speed Feature Extraction.
50. N. Hoque, H. Kashyap, D.K. Bhattacharyya, Real-time DDoS attack detection using FPGA
51. Shaila R. Ghanti, G.M. Naik: FPGA System for Preventing TCP SYN Flood Attack, International Journal of VLSI Design, pp. 39-43, (2012)
52. Adrien Bonguet, Martine Bellaiche, A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing.
53. Sajal Bhatia: Detecting Distributed Denial-of-Service Attacks and Flash Events,PhD thesis, Institute for Future Environments Science and Engineering Faculty
54. Queensland University of Technology (2013)
55. N. Jeyanthi, N. Ch. Sriman Narayana Iyengar: An Entropy Based Approach to Detect and Distinguish DDoS Attacks from Flash Crowds in VoIP Networks, International Journal of Network Security, Vol.14, No.5, PP.257-269, Sept. 2012
56. The DAG Project. http://dag.cs.waikato.ac.nz/

57. Feinstein, L., Schnackenberg, D., Balupari, R., Kindred, D.: Statistical Approaches to DDoS Attack Detection and Response. Proceedings of the DARPA Information Survivability Conference and Exposition, vol. 1, pp. 303-314, 2003.doi: 10.1109/DISCEX.2003.1194894 (2003)
58. INTELhttps://www.tu-ilmenau.de/fileadmin/public/iks/files/lehre/wi/WI-IXP.pdf
59. Snort:https://www.snort.org/
60. Wireshark:https://www.wireshark.org/
61. KDD:http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
62. Hick, P., Aben, E., Claffy, K., Polterock, J.: The CAIDA "DDoS Attack 2007" Dataset, http://www.caida.org/data/passive/ddos-20070804_dataset.xml (2007)
63. The ANT Lab: Analysis of Network Traffic, https://ant.isi.edu/datasets
64. ns2 https://www.isi.edu/nsnam/ns/
65. Weingartner, E., vom Lehn, H., Wehrle K.: A Performance Comparison of Recent Network Simulators. ICC '09. IEEE International Conference on Communications, 2009. doi: 10.1109/ICC.2009.5198657 (2009)
66. Khana A. R., Bilalb S.M. , Othmana, M.: A Performance Comparison of Network Simulators for Wireless Networks, Cornel University Library, arXiv:1307.4129 (2013)
67. Nychis, G., Sekar, V., Andersen, D.G., Kim, H., Zhang, H.: An empirical evaluation of entropy-based traffic anomaly detection. Proceedings of the 8th ACM SIGCOMM Conference on Internet Measurement, Vouliagmeni, Greece, pp. 151–156, 2008, doi:10.1145/1452520.1452539 (2008)
68. Petkovic, M., Basicevic, I., Kukolj, D., Popovic, M.: Evaluation of Takagi-Sugeno-Kang fuzzy method in entropy-based detection of DDoS attacks. Computer Science and Information Systems, Vol. 15, No. 1. (2018)
69. Berezinski, P., Jasiul, B., Szpyrka, M.: An Entropy Based Network Anomaly Detection Method. Entropy 2015, vol. 17, issue 4, pp. 2367-2408, 2015. doi:10.3390/e17042367 (2015)
70. Gordana Cmiljanović, Realizacija programske podrške samoorganizujućeg TAKAGI-SUGENO FUZZY modela, Diplomski rad, Fakultet Tehničkih Nauka, Novi Sad, (2001)
71. Page, E. S. "Continuous Inspection Scheme". Biometrika. **41** (1/2): 100–115, (1954).
72. Ziviani, A., Gomes, A.T.A., Monsores, M.L., Rodrigues, P.S.S.: Network anomaly detection using nonextensive entropy. IEEE Communications Letters, vol. 11, issue 12, pp. 1034–1036, 2007. doi: 10.1109/LCOMM.2007.070761 (2007)
73. https://asert.arbornetworks.com/estonian-ddos-attacks-a-summary-to-date/
74. https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

75. Handley, M., Rescorla, E.: DoS considerations. RFC 4732, RFC Editor, (2006)
76. Vordos, Ioannis: Mitigating Distributed Denial of Service Attacks with Multi-Protocol Label Switching, PhD Thesis, Naval Postgraduate School Monterey, CA, (2009)
77. Bašičević, I., Kukolj, D., Popović, M.: On the application of fuzzy-based flow control approach to High Altitude Platform communications., Applied Intelligence, Springer; vol. 34, issue 2, pp. 199-210, 2011. doi:10.1007/s10489-009-0190-y (2011)
78. Kukolj D, Levi E (2004) Identification of complex systems basedon neural and Takagi-Sugeno fuzzy model. IEEE Trans Syst Man Cybern 34(1):272–282 doi:10.1109/TSMCB. 2003.811119
79. Dhruba Kumar Bhattacharyya, Jugal Kumar Kalita: DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance. CRC Press Taylor & Francis Group, ISBN 978-1-4987-2965-9 (2016)
80. Mohamed Idhammad, Karim Afdel,Mustapha Belouch: DoS Detection Method based on Artificial Neural Networks,International Journal of Advanced Computer Science and Applications, Vol. 8, No. 4 (2017)
81. Zoran Živković, Društvo za informacionu bezbednost Srbije, http://dis.org.rs/wp/wp-content/uploads/2015/05/03_Zivkovic.pdf
82. Shimrit Tzur-David: Network Intrusion Prevention Systems:Signature-Based and Anomaly Detection, PhD thesis, The Hebrew University of Jerusalem, (2011)
83. DDoS Survival Handbook, Radware, www.radware.com, (2013)
84. Wagner, A., Plattner, B.: Entropy based worm and anomaly detection in fast IP networks. 14th IEEE International Workshops on Enabling Technologies: Infrastructure For Collaborative Enterprise, Linkoping, pp. 172–177, 2005.doi: 10.1109/WETICE.2005.35 (2005)