Republika Srbija

Kriminalističko-policijski univerzitet

Departman informatike i računarstva

Doktorska disertacija

Optimizacija trostruke modularne redundanse za određivanje praga u sistemima za detekciju napada

MENTOR:
prof. dr Petar Čisar

KANDIDAT:
Ivan Babić

Beograd, 2025.

Republic of Serbia

University of Criminal Investigation and Police Studies

Department of Information Technology

Doctoral Dissertation

Triple Modular Redundancy Optimization for Threshold Determination in Intrusion Detection Systems

MENTOR:
prof. dr Petar Čisar

STUDENT:
Ivan Babić

Belgrade, 2025

Naslov doktorske disertacije: Optimizacija trostruke modularne redundanse za određivanje praga u sistemima za detekciju napada.

Sažetak: Ova disertacija predstavlja razvoj hibridnog modela koji će se koristiti u sistemima za otkrivanje napada na mrežu - (IDS, eng. Intrusion Detection System) a koji se fokusira na primenu trostruke modularne redundanse (TMR, eng. Triple Modular Redundancy). U svrhu razvoja modela koristiće se TMR u kombinaciji sa tri poznata IDS algoritma, to su algoritam najbližih suseda (KNN, eng. k-nearest neighbours), algoritam kumulativnog zbira (CUSUM, eng. Cumulative Sum) i algoritam eksponencijalno ponderisanog pokretnog proseka (EWMA, eng. Exponentially Weighted Moving Average). Za dokazivanje efikasnosti i tačnosti modela odabrani su distribuirani napadi uskraćivanja usluge - (DDoS, eng. Distributed Denial of Service) jer su jedna od najzastupljenijih vrsta napada na mrežu a samim tim i razlog zašto se koriste u ovoj disertaciji. Naime, promenljivi prag odlučivanja, koji donosi odluku o postojanju napada na posmatranu i zaštićenu mrežu, određuje se korišćenjem kombinacije dobijenih vrednosti (broja paketa po sekundi) primenom gore navedena tri algoritma, tj. na prethodno zabeleženim podacima donošenjem odluke većinom glasova. Korišćenjem predložene metode moguće je dobiti vrednost praga odlučivanja koji je preciznije određen nego u slučaju primene bilo kog od tri navedena algoritma pojedinačno. Korišćenjem tehnike TMR-a dobija se dinamički prilagodljiv prag IDS sistema a samim tim se povećava njegova preciznost i efikasnost što posledično dovodi do smanjenja broja lažnih alarma i neotkrivenih napada. Za dokazivanje ispravnosti primenjenog pristupa koriste se javno dostupni skupovi podataka koji sadrže podatke o zabeleženim DDoS napadima na mrežu. Dobijeni rezultati sa predloženim rešenjem pokazali su bolje karakteristike nego svaki pojedinačno primenjen algoritam koji se koristi i to u proseku za 10,48% bolje od EWMA algoritma, 3,59% bolje od CUSUM algoritma i 0,71% bolje od KNN algoritma za korišćene skupove podataka. Razvijeni model detekcije sa predloženom metodom radi precizno i pravovremeno, što znači da su alarmi aktivirani pravilno i efikasno.

Ključne reči: sajber bezbednost, trostruka modularna redundansa, sistem za otkrivanje upada, algoritam k-najbližih suseda, algoritam kumulativnog zbira, eksponencijalno ponderisani pokretni prosek, uskraćivanje usluge, detekcija napada, prag detekcije.

Naučna oblast: Računarske nauke

Uža naučna oblast: Informacione tehnologije

The title of the doctoral dissertation: Triple Modular Redundancy Optimization for Threshold Determination in Intrusion Detection Systems.

Abstract: This dissertation presents the development of a hybrid model that is going to be used in Intrusion Detection Systems (IDS), where the focus is on the application of Triple Modular Redundancy (TMR). In the development of the model, TMR will be combined with three IDS algorithms: k-nearest neighbors (KNN), Cumulative Sum (CUSUM), and Exponentially Weighted Moving Average (EWMA). To demonstrate the efficiency and accuracy of this proposed model, Distributed Denial of Service (DDoS) attacks were chosen, they are one of the most common types of network attacks, which is why they are used in this dissertation. The threshold value indicating an attack on the network is determined by combining the values (packages per second) from the three algorithms, and a decision is made through majority voting based on past data. By using the proposed method, a threshold value is achieved that is more precisely defined than in the case of applying any of the three algorithms individually. The use of TMR provides a dynamically adjustable IDS threshold, which in turn increases its precision and efficiency, finally reducing the number of false alarms and undetected attacks. Publicly available datasets containing data on recorded DDoS network attacks are used to prove the accuracy. The results obtained with the proposed solution showed better performance than each individually applied algorithm, in average proposed solution is better than EWMA for 10,48%, CUSUM for 3,59% and for KNN 0,71% using selected datasets. The developed detection model with the proposed method operates accurately and promptly, meaning that alarms are triggered correctly and efficiently.

Keywords: cyber security, triple modular redundancy, intrusion detection system, k-nearest neighbors algorithm, cumulative sum algorithm, exponentially weighted moving average, denial of service, attack detection, threshold.

Scientific field: Computer Science

Narrow scientific field: Information technology

Sadržaj

1 Uvod **1**

2 Motivacija i pregled relevantnih istraživanja **4**
2.1 Motivacija 4
2.2 Pregled relevantnih istraživanja 9
2.2.1 Pojedinačni algoritmi 9
2.2.2 Trostruka modularna redudansa 23
2.2.3 Sistemi za detekciju upada 26

3 Metodologija i resursi za detektovanje napada **34**
3.1 Metodologija rada 34
3.1.1 KNN 34
3.1.2 EWMA 36
3.1.3 CUSUM 38
3.1.4 TMR 39
3.1.5 IDS 42
3.2 Analizirani skupovi podataka 44
3.2.1 CIC-IDS2017 44
3.2.2 CIC-DDoS2019 45
3.2.3 IoT 47

4 Rezultati - studija slučaja **49**
4.1 Arhitektura predloženog rešenja 49
4.2 Implementacija predloženog rešenja 51
4.2.1 Modelovanje saobraćaja 56
4.3 Konačni rezultati 58

5 Diskusija **80**
5.1 Uporedni rezultati 80
5.2 Unakrsna validacija rezultata 82
5.3 Primena TMR metode u IDS sistemu 84

6 Zaključak **86**

Literatura **88**

Stručna biografija **96**

Izjava o autorstvu **97**

Izjava o istovetnosti štampane i elektronske verzije doktorske disertacije **98**

Izjava o korišćenju **99**

Spisak slika

1 Prikaz klasifikacije k-najbližih suseda 6
2 Prikaz uticaja α parametra u EWMA algoritmu po danima 7
3 TMR algoritam u IDS sistemu 8
4 Primer EWMA grafikona sa graničnim vrednostima 37
5 Primer CUSUM grafikona sa graničnim vrednostima 39
6 TMR primena u IDS sistemu 41
7 TMR - prikaz sistema većinskog odlučivanja 50
8 Mrežni saobraćaj bez napada 56
9 Mrežni saobraćaj sa napadom tipa UDP flooding 57
10 Friday-WorkingHours - Mrežni saobraćaj sa napadom 59
11 Friday-WorkingHours - Obeležen napad 59
12 Friday-WorkingHours - Primenjen EWMA algoritam (za vrednost praga 150, i vrednost težinskog faktora α 0.20) 60
13 Friday-WorkingHours - Primenjen CUSUM algoritam (za vrednost praga 150, i vrednost odstupanja 25) 60
14 Friday-WorkingHours - Primenjen KNN algoritam 61
15 Friday-WorkingHours - Primenjen TMR algoritam 61
16 Friday-WorkingHours - ROC krive sa iskazanim AUC vrednostima . . 63
17 UDP - Mrežni saobraćaj sa napadom 64
18 UDP - Obeležen napad 64
19 UDP - Primenjen EWMA algoritam (za vrednost praga 100, i vrednost težinskog faktora α 0.30) 65
20 UDP - Primenjen CUSUM algoritam (za vrednost praga 136, i vrednost odstupanja 30) 65
21 UDP - Primenjen KNN algoritam 66
22 UDP - Primenjen TMR algoritam 66
23 UDP - ROC krive sa iskazanim AUC vrednostima 68
24 DrDoS_UDP - Mrežni saobraćaj sa napadom 69
25 DrDoS_UDP - Obeležen napad 69
26 DrDoS_UDP - Primenjen EWMA algoritam (za vrednost praga 100, i vrednost težinskog faktora α 0.25) 70
27 DrDoS_UDP - Primenjen CUSUM algoritam (za vrednost praga 100, i vrednost odstupanja 20) 70
28 DrDoS_UDP - Primenjen KNN algoritam 71
29 DrDoS_UDP - Primenjen TMR algoritam 71
30 DrDoS_UDP - ROC krive sa iskazanim AUC vrednostima 73

31 DoS synflooding - Mrežni saobraćaj sa napadom 74
32 DoS synflooding - Obeležen napad 74
33 DoS synflooding - Primenjen EWMA algoritam (za vrednost praga 100, i vrednost težinskog faktora α 0.14) 75
34 DoS synflooding - Primenjen CUSUM algoritam (za vrednost praga 100, i vrednost odstupanja 4) 75
35 DoS synflooding - Primenjen KNN algoritam 76
36 DoS synflooding - Primenjen TMR algoritam 76
37 DoS synflooding - ROC krive sa iskazanim AUC vrednostima 78
38 Primena TMR metoda u IDS 84

Spisak tabela

1 Prikaz matrice za klasifikaciju predviđanja 42
2 Tipovi napada u CIC-IDS2017 skupu podataka 46
3 Tipovi napada u CIC-DDoS2019 skupu podataka 47
4 Tipovi napada u IoT Network Intrusion skupu podataka 48
5 Friday-WorkingHours evaluacija rezultata 62
6 UDP evaluacija rezultata 67
7 DrDoS_UDP evaluacija rezultata 72
8 DoS synflooding evaluacija rezultata 77
9 Objedinjeni rezultati za 4 testirana napada 81
10 Unakrsna validacija - DrDoS UDP 83

Spisak skraćenica

ACK	Potvrdni odgovor (eng. Acknowledgment)
AC	Približno izračunavanje (eng. Approximate Computation)
AIDS	Sistem za otkrivanje upada na osnovu nepravilnosti (eng. Anomaly-based Intrusion Detection System)
ARP	Protokol za razrešavanje adresa (eng. Address Resolution Protocol)
ATMR	Približna trostruka modularna redundansa (eng. Approximate Triple Modular Redundancy)
AUC	Površina ispod krive (eng. Area Under Curve)
Botnet	Mreža zaraženih računara (eng. Bot Network)
CAIDA	Centar za primenjenu analizu internet podataka eng. Center for Applied Internet Data Analysis
CERT	Računarski tim za hitne slučajeve (eng. Computer Emergency Response Team)
CIC	Kanadski institut za sajber bezbednost (eng. Canadian Institute for Cybersecurity)
CNN	Konvoluciona neuronska mreža (eng. Convolutional Neural Network)
CUSUM	Kumulativni zbir (eng. Cumulative Sum)
CSV	Vrednosti razdvojene zarezima (eng. Comma-Separated Value)
DBSCAN	Prostorno klasterovanje aplikacija sa šumom zasnovana na gustini (eng. Density-Based Spatial Clustering of Applications with Noise)
DDoS	Distribuirani napad uskraćivanja usluge (eng. Distributed Denial-of-Service)
DL	Duboko učenje (eng. Deep Learning)
DNS	Sistem imena domena (eng. Domain Name System)
DoS	Napad uskraćivanja usluge (eng. Denial-of-Service)
DRDoS	Distribuirani reflektovani napad uskraćivanja usluge (eng. Distributed Reflective Denial-of-Service)
EWMA	Eksponencijalno ponderisani pokretni presek (eng. Exponentially Weighted Moving Average)
EM	Očekivanje maksimizacije (eng. Expectation-Maximization)
FMR	Odnos maskiranja grešaka (eng. Fault Masking Ratio)
FN	Lažni negativi (eng. False Negative)
FP	Lažni pozitivi (eng. False Positive)

FPR	Učestalost lažnih alarma (eng. False Positive Rate)
FTP	Protokol za prenos datoteka (eng. File Transfer Protocol)
HIDS	Host-bazirani sistem za otkrivanje upada (eng. Host Intrusion Detection System)
HLKNN	k-najbližih suseda visokog nivoa (eng. High-Level K-Nearest Neighbors)
HTTP	Protokol za prenos hiperteksta (eng. Hypertext Transfer Protocol)
ICMP	Internet kontrolni protokol za poruke (eng. Internet Control Message Protocol)
IDS	Sistem za otkrivanje upada (eng. Intrusion Detection System)
IP	Internet protokol (eng. Internet Protocol)
IoT	Internet stvari (eng. Internet of Things)
ISP	Internet servis dobavljač (eng. Internet Service Provider)
IT	Informacione tehnologije
KNN	k-najbližih suseda (eng. k-Nearest Neighbors)
LDAP	Protokol za lak pristup direktorijumu (eng. Lightweight Directory Access Protocol)
LOIT	Niskoorbitalni jonski top (eng. Low Orbit Ion Cannon)
MAC	Mekintoš (eng. Macintosh)
MITM	Napad presretanjem komunikacije (eng. Man-in-the-Middle)
ML	Mašinsko učenje (eng. Machine Learning)
MLP	Višeslojni perceptron (eng. Multi-Layer Perceptron)
MSSQL	Microsoft SQL Server
MUP	Ministarstvo unutrašnjih poslova
NetBIOS	Servis za osnovni unos i izlaz na mreži (eng. Network Basic Input/Output System)
NIDS	Mrežni sistem za otkrivanje upada (eng. Network Intrusion Detection System)
NMAP	Mapiranje mreže (eng. Network Mapper)
NMU	Autonomne jedinice za upravljanje mrežom (eng. Network Management Units)
NTP	Protokol za mrežno vreme (eng. Network Time Protocol)
NN	Neuronska mreža (eng. Neural Network)
PCAP	„Hvatanje“ paketa (eng. Packet Capture)

PortMap	Mapiranje portova (eng. Port Mapping)
R2L	Udaljeni korisnik kao lokalni (eng. Remote 2 Local)
RDP	Protokol za udaljenu radnu površinu (eng. Remote Desktop Protocol)
RegEx	Regularni izraz (eng. Regular Expression)
RGB	Crvena zelena plava (eng. Red Green Blue)
RNN	Rekurentna neuronska mreža (eng. Recurrent Neural Network)
ROC	Radne karakteristike prijemnika (eng. Receiver Operating Characteristics)
SIDS	Sistem za otkrivanje upada na osnovu potpisa (eng. Signature-Based Intrusion Detection System)
SNMP	Jednostavni protokol za upravljanje mrežom (eng. Simple Network Management Protocol)
SYN	Sinhronizacioni signal (eng. Synchronization)
SQL	Strukturni upitni jezik (eng. Structured Query Language)
SSH	Sigurna ljuštura (eng. Secure Shell)
SSDP	Jednostavni protokol za otkrivanje usluga (eng. Simple Service Discovery Protocol)
SVM	Metoda potpornih vektora (eng. Support Vector Machine)
TCP	Transmisioni kontrolni protokol (eng. Transmission Control Protocol)
Telnet	Telefonska mreža (eng. Telephone Network)
TFTP	Jednostavni protokol za prenos datoteka (eng. Trivial File Transfer Protocol)
TMR	Trostruka modularna redundansa (eng. Triple Modular Redundancy)
TN	Pravi negativi (eng. True Negative)
TP	Pravi pozitivi (eng. True Positive)
TPR	Stopa pravih pozitivnih rezultata (eng. True Positive Rate)
U2R	Korisnik kao root (eng. User 2 Root)
UDP	Protokol korisničkog datagrama (eng. User Datagram Protocol)
UDP-Lag	Kašnjenje UDP protokola (eng. UDP Lag)
WebDDoS	Web-distribuirani napad uskraćivanja usluge (eng. Web Distributed Denial-of-Service)
XSS	Napad kroz skriptovanje na strani klijenta (eng. Cross-Site Scripting)

1. Uvod

Bezbednost informacionih tehnologija (IT) je jedno od najvažnijih pitanja za vlade, korporacije, profesionalne korisnike i druge korisnike. Informacioni sistemi su od ključne važnosti za svakodnevno funkcionisanje, ali su izloženi čestim i sofisticiranim sajber napadima. Napadi mogu ozbiljno poremetiti vitalne usluge i infrastrukturu, čineći prevenciju i bezbednost prioritetom. Imajući u vidu da IT brzo i neprestano napreduju, ne može se zamisliti život bez informacionih tehnologija. Rizici po bezbednost nikada nisu bili veći nego danas, jer su tehnologija i internet dostupni za dve trećine svetske populacije. Velika većina te populacije poseduje barem neki informatički uređaj kao što je mobilni telefon, pametni sat, tablet ili računar. Uz to svaka veća institucija poseduje brojne uređaje povezane na internet (IoT, eng. Internet of Things), a većina tih uređaja je slabo zaštićena tokom povezanosti na javnu računarsku mrežu odnosno internet.

Što se tiče vladinih i nevladinih tela, kao i korporacija, IT bezbednost je donekle poboljšana, ali često nije adekvatna ili čak i ne postoji. Danas vlade imaju sopstvene računarske timove za hitne slučajeve (CERT, eng. Computer Emergency Response Team) koji se bave napadima i bezbednosnim incidentima, dok privatne korporacije imaju interne IT bezbednosne odseke ili angažuju eksterne stručnjake za organizovanje IT bezbednosne zaštite (eng. outsourcing). Čak i sa ovim merama za sprečavanje bezbednosnih incidenata, i dalje je moguće da se pretrpe napadi i bezbednosni prodori koji mogu prouzrokovati veliku štetu.

Predmet ove disertacije predstavlja pristup razvoju sistema za detekciju napada na mrežu (IDS, eng. Intrusion Detection System) koji se fokusira na primenu trostruke modularne redundanse (TMR, eng. Triple Modular Redundancy), a posledično i na rastući značaj bezbednosti u informacionim sistemima obzirom na široku upotrebu tehnologija i sve veći broj uređaja koji su povezani na javnu računarsku mrežu. Sistem za detekciju napada na mrežu, koji je jedan od rezultata disertacije, zasniva se na optimizaciji postojećih algoritama za detekciju napada. Na početku se uzimaju bilo koja tri već dobro poznata algoritma koja se koriste u pomenutim sistemima i to su algoritam najbližih suseda (KNN, eng. k-nearest neighbours), algoritam kumulativnog zbira (CUSUM, eng. Cumulative Sum) i algoritam eksponencijalno ponderisanog pokretnog proseka (EWMA, eng. Exponentially Weighted Moving Average) koji se zatim kombinuju u algoritam TMR radi dobijanja preciznijih rezultata.

Cilj ove disertacije je razvoj hibridnog modela zasnovanog na TMR za detekciju

napada na mrežu primenom postojećih algoritama korišćenih u takvim sistemima. Postojeći algoritmi se koriste sa algoritmom TMR kako bi se postigla veća tačnost rezultata, odnosno kako bi se preciznije odredio prag detekcije napada u realnom vremenu [1]. Cilj razvoja novog modela je povećanje preciznosti u odnosu na pojedinačno korišćene algoritme, čime se pokazuje da je TMR doprineo poboljšanju u primeni na sistemima za detekciju napada na mrežu.

Za validaciju rešenja razvijene metode, korišćeni su distribuirani napadi uskraćivanja usluge - (DDoS, eng. Distributed Denial of Service) kao najčešća vrsta napada koja ujedno predstavlja najveći problem ako unutar ciljanog sistema nije omogućena adekvatna zaštita. DDoS napad predstavlja veliki broj zahteva upućen sa različitih računara ili informatičkih uređaja koji pokušavaju da premaše kapacitet mreže koja je meta napada. Obično se distribuira putem prethodno inficiranog velikog broja računara ili drugih uređaja povezanih na internet, tzv. botnet mreže. Odabir adekvatnog načina za detekciju ovih napada [2, 3] predstavlja veliki izazov jer napadi dolaze u različitim oblicima, kao što su napadi poplavljivanja (eng. Flood attacks), napadi na protokol (eng. Protocol attacks) i napadi na aplikacionom sloju (eng. Application layer attacks) [4, 5]. U ovom radu fokus je na napade poplavljivanja, poput Hypertext Transfer Protocol (HTTP) flood i User Datagram Protocol (UDP) flood napada. DDoS napadi su najčešći i najopasniji, jer bi cela država, odnosno javna IT infrastruktura države, mogla biti blokirana sa dovoljno jakim DDoS napadom. Predloženo rešenje može da se koristi za bilo koji od napada poplavljivanja. Obično su takvi napadi masivni i mogu naneti značajnu štetu potencijalnim žrtvama, kao i imati finansijski uticaj na skoro svaki poznati sistem.

Opšta hipoteza ovog naučnog istraživanja sprovedenog u okviru predložene doktorske disertacije može biti formulisana na sledeći način: Integracijom poznatih algoritama za detekciju napada na mrežu u hibridni model koristeći TMR, kreira se robusniji IDS sistem koji svoju efikasnost dokazuje poređenjem rezultata na javno dostupnim skupovima podataka.

Metode koje se koriste u ovoj disertaciji su: deskriptivna metoda koja se odnosi na prikupljanje, opisivanje i harmonizaciju postojećih podataka, komparativna i analitička istraživačka metoda koja podrazumeva upoređivanje, vrednovanje i interpretaciju dobijenih rezultata, potom analizu podataka iz istraživanja drugih autora, kao i metode statističke obrade podataka. Predloženi razvoj kreiranja modela se zasniva na odabiru algoritama koji su relevantni i njihovo kombinovanje u model sa trostrukom modularnom redundansom u cilju dobijanja preciznijih

rezultata. Za postizanje postavljenog cilja, korišćene su kvalitativne i kvantitativne metode. Uz to su korišćena različita softverska rešenja od kojih se mogu izdvojiti programski jezik Python i statistički paket R sa odgovarajućim bibliotekama koje su opisane u odeljku 4.2.

Rezultat naučnog istraživanja koje je sprovedeno u okviru ove disertacije uključuje razvoj hibridnog modela za spregu algoritama kako bi se dobili najbolji rezultati. Osim toga, važan rezultat predstavlja i kreiranje sistema koji implementira postojeće algoritme u model sa TMR koji je zatim testiran i validiran na realnim skupovima podataka.

Ostatak disertacije je organizovan na sledeći način. Poglavlje 2 sadrži dva odeljka, pri čemu odeljak 2.1 sadrži motiv istraživanja, dok odeljak 2.2 sadrži pregled relevantnih istraživanja u svetu i kod nas iz oblasti koja je predmet ove disertacije. Poglavlje 3 počinje odeljkom 3.1, koje uvodi metodologiju rada gde su opisana tri odabrana algoritma: EWMA [6, 7], CUSUM [8, 9], i KNN algoritam, koji su korišćeni u kombinaciji sa TMR algoritmom koji je detaljnije opisan u ovom odeljku. Odeljak 3.2 sadrži analizirane skupove podataka koji su korišćeni za trening/obuku, testiranje i validaciju predloženog rešenja. Poglavlje 4 organizovano je u tri celine. Odeljak 4.1 koji sadrži arhitekturu predloženog rešenja, za kojim sledi odeljak 4.2 gde je predstavljena implementacija predloženog rešenja sa modelovanjem mrežnog saobraćaja. Konačno, na kraju poglavlja u odeljku 4.3 daje prikaz rezultata dobijenih korišćenjem ove metodologije. Diskusija dobijenih rezultata je predmet poglavlja 5 sa tri odeljka. Odeljak 5.1 sadrži uporedne rezultate dobijene na korišćenim skupovima podataka, odeljak 5.2 sadrži unakrsnu validaciju dobijenih rezultata dok odeljak 5.3 sadrži predlog praktične primene TMR metoda u IDS sistemima. Zaključna razmatranja sa posebnim osvrtom na dalje pravce istraživanja se daju na kraju disertacije u poglavlju 6.

2. Motivacija i pregled relevantnih istraživanja

Detekcija napada ima važnu ulogu u računarskim sistemima, jer od postupaka detekcije zavisi brzina i adekvatna reakcija sistema za zaštitu od napada. DDoS napadi se svakodnevno događaju, dok su na primer najosetljiviji i najvažniji računarski sistemi oni koji se koriste u zdravstvu, energetici, vodosnabdevanju... [10] Napad na neki od takvih sistema može imati nesagledive posledice koje nisu samo materijalne prirode.

U poslednjih nekoliko godina su zabeleženi neki od najvećih DDoS napada. U avgustu 2023. godine kompanija "Google", jedna od najvećih na svetu detektovala je DDoS napad koji je na svom maksimumu iznosio oko 398 miliona zahteva u sekundi [11]. Taj napad je pogodio nekoliko internet servis provajdera (ISP) odnosno kompanija koje se bave internet infrastrukturom.

U januaru 2023. godine, informatička infrastruktura Ministarstva unutrašnjih poslova (MUP) Republike Srbije, je bila 48 časova pod konstantnim DDoS napadima. Tokom tog perioda odbijeno je pet velikih napada i uspešno su zaštićeni podaci i baze MUP-a [12].

U avgustu 2023. godine kompanija "Cloudflare", jedna od vodećih kompanija u svetu za zaštitu od napada, detektovala je DDoS napad do tada najveći zabeležen [13]. Tom prilikom hiljade DDoS napada su upućeni prema kompanijama koje se bave pružanjem kockarskih usluga i igrama na sreću, 89 od tih napada su iznosili preko 100 miliona zahteva u sekundi, dok je najveći od njih iznosio 201 milion zahteva u sekundi. Prethodni najveći napad je bio detektovan februara 2023. godine i iznosio je 71 milion zahteva u sekundi.

2.1 Motivacija

Naučno istraživanje koje je predmet ove disertacije proisteklo je iz potrebe za povećanjem otpornosti informacionih sistema, koji su sve više izloženi sofisticiranim sajber napadima, dok je čovečanstvo istovremeno sve više zavisno od informacionih sistema koji zahtevaju sve veću pouzdanost odnosno dostupnost. Prevencija i detekcija napada na mreže postali su ključni aspekti zaštite vitalnih sistema. Rad [14] istražuje strategije detekcije napada, naglašavajući ključne izazove savremene tehnologije u prepoznavanju i prevenciji pretnji. Softver IDS i njegova efikasnost su tema ovog istraživanja jer je IDS jedna od osnovnih komponenti zaštite umreženih računarskih sistema od napada. Kako je istaknuto u radu [15], savremeni trendovi zahtevaju inovativne metode za optimizaciju

performansi. Optimizacijom metoda za detekciju napada kroz primenu trostruke modularne redundanse omogućava se preciznije, efikasnije i pravovremeno otkrivanje napada, kako bi se obezbedila veća sigurnost u takvim sistemima. Trostruka modularna redundansa se koristi za poboljšanje bezbednosti i pouzdanosti računarskih sistema još od nastanka računara [16], [17] i jedan je od razloga zašto je odabrana za ovo rešenje.

Postoje različiti pristupi otkrivanju mrežnih napada [18] koji se mogu podeliti u tri osnovne grupe: host-bazirani IDS (HIDS, eng. Host Intrusion Detection System), mrežno bazirani IDS (NIDS, eng. Network Intrusion Detection System) i hibridni sistemi. Na osnovu korišćenih metoda za detekciju, IDS se mogu podeliti na detekciju napada na osnovu potpisa (SIDS, eng. Signature-based Intrusion Detection System) i na osnovu nepravilnosti (AIDS, eng. Anomaly-based Intrusion Detection System). U radu [19] navodi se klasifikacija DDoS napada i mehanizama odbrane, omogućavajući dublje razumevanje problema i razvoj efikasnijih tehnika zaštite od napada.

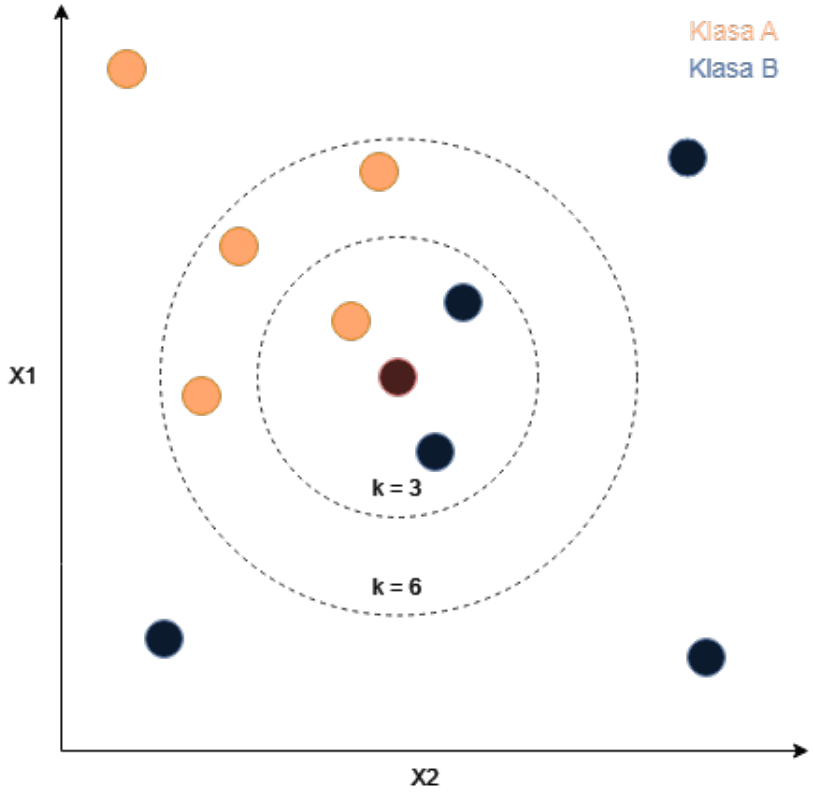
Fokus u ovom radu je na AIDS pristupu. Razvoj takvog sistema sastoji se od dve faze: prva je faza obučavanja (učenja) koja daje sliku o tome šta predstavlja regularan mrežni saobraćaj, druga faza je testiranje na skupovima podataka koji nisu do tada korišćeni. AIDS se može podeliti u nekoliko kategorija na osnovu metoda korišćenih za obučavanje: nadzirano učenje, nenadzirano učenje i probabilističko učenje, meko računarstvo, detekcija nepravilnosti bazirana na znanju i kombinovanom učenju.

AIDS pristup je odabran pošto ima brojne prednosti u odnosu na druge pristupe, a neki od njih su: mogućnost da otkrije nove napade (eng. Zero-day attacks) koji do tada nisu zabeleženi i mogućnost da otkrije napade iznutra.

Predloženo rešenje može se koristiti i za otkrivanje drugih vrsta napada, kao što su napadi *Probe*, *User to Root* (U2R). Jedan od tih napada je i napad prelivanja bafera (eng. Buffer Overflow) koji je tipa U2R i veoma je čest. Cilj tog napada je da pošalje više paketa nego što ciljani sistem može da obradi u jedinici vremena. Jedan od napada koji se često koristi je NMAP (eng. Network Mapper) napad, koji se koristi za skeniranje portova i IP adresa na ciljanom sistemu, odnosno na sistemu žrtve.

Korišćeni algoritmi su odabrani zbog svojih svojstava koja služe za detekciju napada. Prvi algoritam je KNN koji je jednostavan algoritam za klasifikaciju i regresiju [20]. Algoritam funkcioniše tako što, za dati ulazni podatak, traži k najbližih suseda u skupu podataka za obučavanje prema nekoj metričkoj

udaljenosti. U klasifikaciji, ulazni podatak se svrstava u klasu kojoj pripada većina njegovih najbližih suseda. U regresiji, predviđanje je prosek vrednosti njegovih suseda. Algoritam je neparametarski, što ga čini jednostavnim, ali može biti spor kada se radi o velikim skupovima podataka. Na slici 1 se može videti grafički prikaz klasifikacije u KNN algoritmu. Izbor vrednosti k je bitan što se može videti na prikazanoj slici, za k=3 novi podatak pripada klasi B, dok za k=6 isti podatak pripada klasi A. Udaljenost od najbližih suseda se najčešće meri Euklidskim rastojanjem, korišćenjem formule koja se nalazi u odeljku 3.1.1.

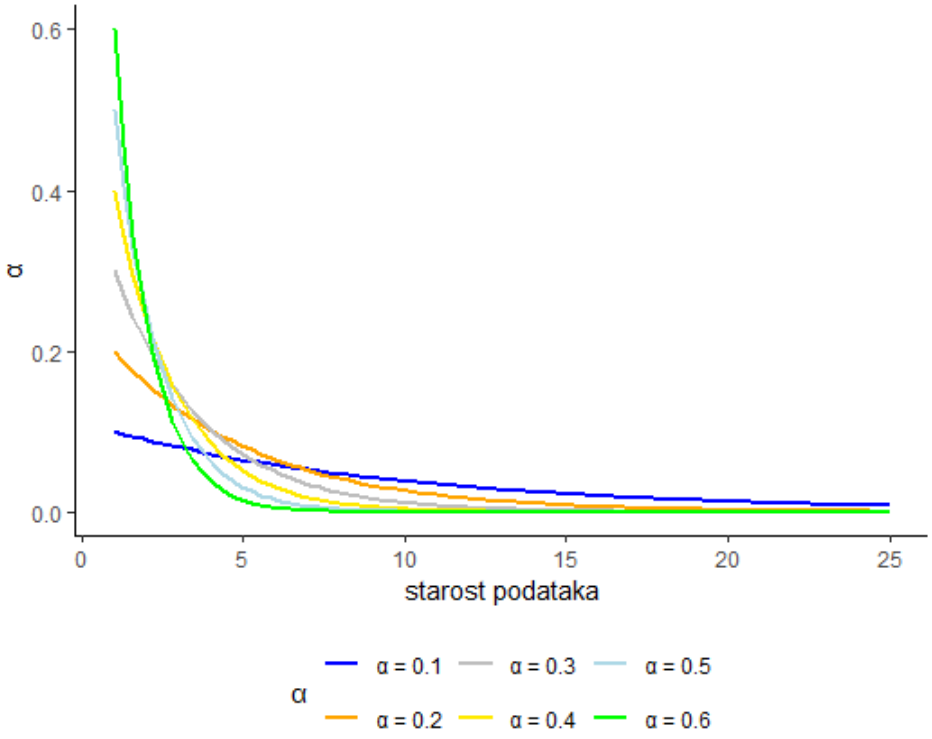


Slika 1: Prikaz klasifikacije k-najbližih suseda

Drugi algoritam koji se koristi je eksponencijalno ponderisani pokretni prosek (EWMA - eng. Exponentially Weighted Moving Average). On predstavlja kvantitativnu ili statističku meru koja se koristi za modelovanje ili opisivanje vremenskih serija. Pokretni prosek je osmišljen tako da starijim podacima daje manju težinu u poređenju sa skorijim podacima. Iz tog razloga, vrednost pondera se smanjuje eksponencijalno kako podaci postaju stariji, što je prikazano na slici 2. Jedini parametar koji korisnik algoritma mora da unese i koji je bitan za donošenje odluke je parametar α, ovaj parametar određuje koliko je trenutno posmatrani podatak bitan za izračunavanje. Što je vrednost parametra α veća, to su skoriji podaci relevantniji, pri čemu vrednost parametra α može uzeti vrednost između 0 i

1, tako da ako je vrednost parametra 1 onda se uzimaju u obzir samo najskoriji podaci. Uobičajeni opseg vrednosti parametra α za većinu primena je između 0,2 i 0,3. Jednačina po kojoj se EWMA izračunava se nalazi u odeljku 3.1.2.

EWMA algoritam često ima veliki broj lažnih pozitiva, ali uz manja podešavanja može davati dobre rezultate.

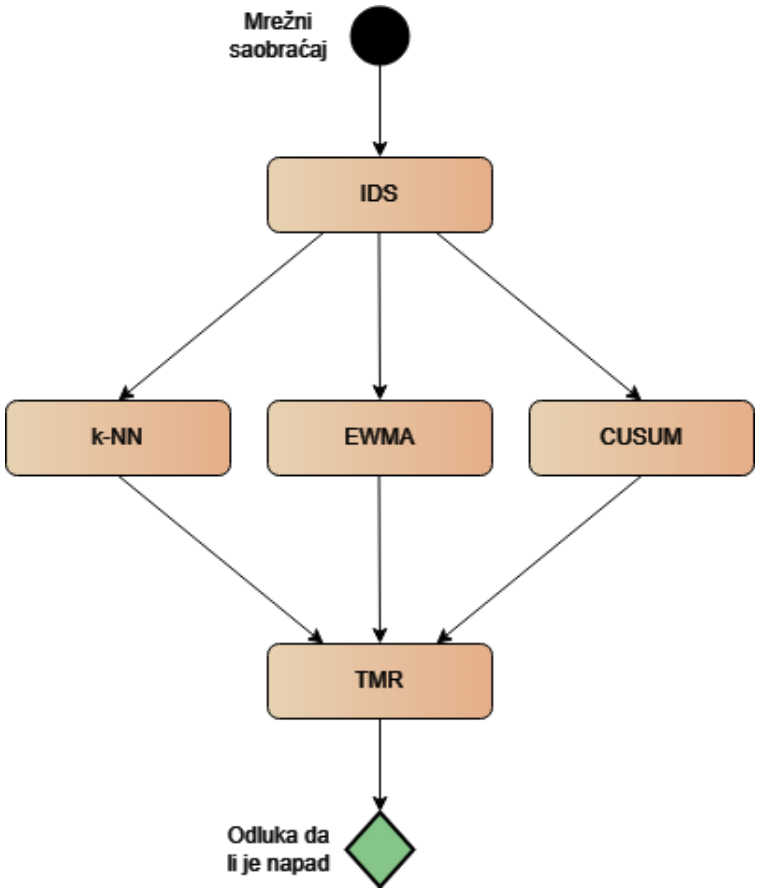


Slika 2: Prikaz uticaja α parametra u EWMA algoritmu po danima

Treći algoritam je CUSUM (eng. Cumulative Sum), algoritam koji detektuje promene. Ažurira se periodično i u realnom vremenu, to je jedna od njegovih prednosti jer se u mrežnom saobraćaju broj paketa menja konstantno tokom vremena. CUSUM je algoritam koji je optimizovan da meri bilo koje odstupanje od zadate vrednosti, može detektovati i najmanje promene. Sa CUSUM algoritmom izračunava se suma između dobijenih i očekivanih vrednosti. CUSUM se lako može prilagoditi konkretnom problemu i već postoje brojne varijacije ovog algoritma, a može se čak i podesiti da sam uči kako bi detektovao promene u različitim scenarijima.

CUSUM je zapravo srednja vrednost sume odstupanja od referentne vrednosti μ, koja predstavlja periodično ažuriranu vrednost u realnom vremenu [21, 22]. Formula za izračunavanje CUSUM vrednosti se nalazi u odeljku 3.1.3.

Tri pomenuta algoritma KNN, EWMA i CUSUM se u disertaciji kombinuju u algoritam trostruke modularne redundanse. Kada se radi o sistemima u kojima je potrebno minimizovati greške onda se najčešće koristi redundansa. Korišćenje redundanse zahteva više resursa nego prilikom normalnog funkcionisanja sistema u kojem se implementira, pri čemu je taj resurs najčešće taj resurs vreme ali može biti i količina ulaznih podataka. U radu [23] je pokazano da sa povećanjem kompleksnosti sistema posledično raste i vreme potrebno za detekciju.



Slika 3: TMR algoritam u IDS sistemu

Kod TMR algoritma za određivanje ispravnog rezultata koristi se većinsko odlučivanje. Za tri ulazna parametra koja se dobiju primenom tri navedena algoritma, dobićemo tri izlazna rezultata gde će nakon odlučivanja biti izabrana jedna zajednička izlazna vrednost. U ovom slučaju ta vrednost će određivati da li je došlo do napada ili nije [1].

Na slici 3 se vidi prikaz funkcionisanja TMR algoritma u jednom IDS sistemu. TMR donosi odluku da li je došlo do napada ili ne i time obezbeđuje preciznije rezultate.

2.2 Pregled relevantnih istraživanja

U nastavku rada prikazan je pregled istraživanja koja se bave odabranim algoritmima k-najbližih suseda, eksponencijalno ponderisanog pokretnog preseka i kumulativnog zbira, takođe je prikazan i pregled istraživanja koja se bave algoritmom trostruke modularne redundanse i IDS sistemima. U prvu grupu prikazanih istraživanja svrstani su radovi koji se bave algoritmom KNN [20], [24], [25], [26], [27], [28], a potom slede radovi posvećeni EWMA algoritmu [29], [30], [31], [32], [33], [34], [7]. Nakon navedenog slede radovi koji se bave CUSUM algoritmom [34], [9], [35], [36], [37], [38], [22], [39], nastavljaju se radovi koji se bave algoritmom TMR [40], [41], [42], [43], [44]. Poglavlje završavamo sa pregledom istraživanja čija je glavna tema bila IDS sistemi [45], [46], [47], [48], [49], [3], [50], [51], [5], [52], [53], [54], [18].

2.2.1 Pojedinačni algoritmi

Atawodi [20] predlaže unapređenje IDS sistema korišćenjem mašinskog učenja. Koriste se dva algoritma kako bi se poboljšala tačnost detekcije napada, pri čemu su to algoritmi k-najbližih suseda (KNN) i Slučajna šuma (eng. Random Forest). KNN algoritam se koristi za klasifikaciju ulaznih podataka na osnovu njihove podudarnosti sa skupovima podataka za obučavanje, dok algoritam Slučajne šume kreira više stabala odluke i kombinuje njihove rezultate kako bi odredio tip napada. Za istraživanje u ovom radu korišćen je NSL-KDD skup podataka, i on se sastoji od istorijskih podataka o različitim vrstama mrežnih napada kao i o normalnim mrežnim aktivnostima. Izazovi koji se susreću u ovom radu su preciznost detekcije, optimizacija izbora parametara (npr. vrednost k kod KNN algoritma) i tačnost klasifikacije između algoritama treniranih na različitim skupovima podataka. Kroz desetostruku unakrsnu validaciju, autor analizira performanse KNN i Slučajna šuma algoritama u detekciji napada. Algoritam Slučajna šuma se koristi zbog svoje mogućnosti klasifikacije putem strukture stabla, dok KNN omogućava prepoznavanje obrazaca ponašanja u podacima mrežnog saobraćaja. Korišćenjem ove metode, autor je uspeo da poveća tačnost i brzinu detekcije, optimizujući sistem za identifikaciju čak i sofisticiranih napada. Koristeći istorijske podatke o napadima, algoritmi su obučeni da prepoznaju i reaguju na potencijalne pretnje u realnom vremenu, poboljšavajući time efikasnost sistema za detekciju napada. U radu je prikazano da su oba algoritma postigla visoku tačnost, ali da algoritam Slučajne šume daje neznatno bolje rezultate koji idu i do 99,81% u nekim slučajevima. Poseban značaj pridaje se izboru svojstava zabeleženih napada, jer

one direktno utiču na efikasnost algoritama. Zaključak je da je kombinacija algoritama mašinskog učenja efikasnija u detekciji napada od pojedinačnih metoda i da se može koristiti za poboljšanje bezbednosti sigurnosnih sistemima u stvarnim mrežnim okruženjima, što je pokazano i u predloženom rešenju.

Kiyak sa svojim timom (2023) [24] pokazuje unapređenje algoritma k-najbližih suseda (KNN) koje poboljšava tačnost klasifikacije kroz dodatno smanjenje osetljivosti na šumove i odstupanja u podacima. Standardni KNN algoritam koristi k najbližih suseda za određivanje klase datog podatka, ali je često podložan greškama kada su podaci sa šumom ili izuzecima prisutni u skupu podataka. Algoritam k-najbližih suseda visokog nivoa HLKNN,predstavljen u ovom radu, fokusira se na ublažavanje ovih problema koristeći koncept „sused suseda“ u postupku klasifikacije, što značajno doprinosi većoj stabilnosti i tačnosti modela. U HLKNN algoritmu, osim standardnih najbližih suseda, uključeni su i susedi tih suseda kako bi se dodatno obezbedila stabilnost modela i kako bi se time sprečilo da šum utiče na ishod klasifikacije. Time se kreira širi opseg uticaja, koji omogućava algoritmu da bolje „razume“ okolinu svakog podatka. Koristeći ovaj način, HLKNN se pokazao otpornijim na promene i šumove u podacima, što omogućava njegovu primenu na zahtevnim klasifikacionim problemima. Efikasnost HLKNN algoritma potvrđena je kroz eksperimente na 32 različita skupa podataka, gde je tom prilikom HLKNN algoritam uspešno nadmašio tradicionalni KNN u tačnosti klasifikacije. Prosečna tačnost koju je HLKNN postigao iznosila je 81,01%, dok je klasični KNN ostvario prosečnu tačnost od 79,76%. Osim poboljšane preciznosti, HLKNN takođe uspešno rešava određene probleme sa klasifikacijom višeklasnih podataka koji su karakteristični za klasičan KNN algoritam. Zahvaljujući ovoj izmeni, HLKNN može imati primenu u različitim situacijama gde je klasifikacija od velike važnosti, poput medicinske dijagnostike, upravljanja podacima u IoT uređajima i kod analize bioloških uzoraka. Algoritam je pokazao značajna unapređenja posebno u oblastima gde je potreban balans između složenosti modela i preciznosti klasifikacije, što ga čini efikasnim alatom u savremenoj primeni mašinskog učenja. Ovaj članak [24] pokazuje da je KNN algoritam dobar izbor za predloženo rešenje.

Zhang i dr. (2016) [25] se bave unapređenjem klasičnog KNN algoritma za efikasnost rada sa velikim količinama podataka. Tradicionalni KNN algoritam je jednostavan i efikasan za male i srednje skupove podataka, ali postaje vremenski i računski zahtevan kada se koristi za obrade velikih skupova podataka zbog linearne pretrage kroz sve tačke u skupu podataka. Ovaj problem je posebno izražen kada

se povećava broj dimenzija ili kada se radi o skupovima sa milionima uzoraka, kao što je često slučaj u analizi podataka u industrijskom i naučnom kontekstu. Autori predlažu optimizovaniju verziju KNN algoritma koja koristi distribuirane obrade i paralelizaciju kako bi se smanjila složenost i vreme obrade podataka. Jedan od ključnih pristupa u ovom radu je korišćenje podele podataka, kako bi se podaci rasporedili na više mašina i time omogućila paralelna obrada. Ova podela podataka smanjuje opterećenje na jednoj mašini i omogućava algoritmu da efikasno obrađuje podatke u realnom vremenu. Osim distribuiranog pristupa, autori uvode tehnike za smanjenje dimenzionalnosti i poboljšanje performansi KNN algoritma, uključujući metodu koja koristi samo relevantne dimenzije za određene podatke. Time se smanjuje broj dimenzija koje algoritam obrađuje, što doprinosi smanjenju ukupnog broja izračunavanja i ubrzava pretragu k-najbližih suseda. Ovo dodatno poboljšava tačnost i preciznost klasifikacije jer algoritam koristi najvažnije karakteristike podataka. Eksperimenti u radu pokazuju da predloženi optimizovani KNN algoritam ostvaruje značajna ubrzanja u poređenju sa klasičnim KNN pristupom kada se primenjuje na velike skupove podataka. Na skupu podataka sa velikim brojem primeraka, optimizovani algoritam pokazuje bolje performanse i brže vreme izvršavanja zahvaljujući paralelizaciji i strategijama smanjenja dimenzionalnosti. Takođe, evaluacija algoritma prikazuje visok nivo tačnosti klasifikacije u poređenju sa drugim tehnikama klasifikacije, čime se dokazuje efikasnost i robusnost predloženog pristupa. U zaključku, autori naglašavaju da optimizovana verzija KNN algoritma ima široku primenu u analizama velikih skupova podataka, uključujući zadatke kao što su prepoznavanje obrazaca, medicinska dijagnostika i analiza ponašanja korisnika.

Nuti (2018) [26] u svom radu istražuje poboljšanje algoritma k-najbližih suseda kroz primenu Bajesovog pristupa za određivanje optimalnog broja suseda, parametra k, bez oslanjanja na statističke *Markov chain Monte Carlo* metode (MCMC). Tradicionalni KNN algoritmi se suočavaju s izazovom odabira parametra k, što značajno utiče na tačnost klasifikacije i regresije. U ovom radu se predlaže algoritam koji izračunava posteriornu distribuciju k specifičnu za svaki podatak, time redefinišući problem u detekciju promena u distribuciji podataka. Algoritam organizuje podatke prema udaljenosti od ciljne tačke i pretpostavlja da podaci bliži cilju potiču iz iste distribucije, dok udaljeniji podaci pripadaju različitim. Koristeći ovu pretpostavku, algoritam računa verovatnoću promena između različitih suseda i određuje optimalnu vrednost parametra k. Za razliku od tradicionalnih metoda koje koriste simulacije, ovaj algoritam nudi tačno i brzo rešenje. U radu se navodi da je predložena metoda testirana na klasifikacionim i regresionim skupovima

podataka, uključujući Ripley dataset i Nuclear Power Plant dataset. U poređenju s ručnim podešavanjem parametra k, algoritam je pokazao veću preciznost i efikasnost. Na Ripley datasetu, stopa greške je smanjena na 0.09 u poređenju s 0.13 za tradicionalni KNN, dok je vreme obrade smanjeno sa sati na milisekunde. Glavna prednost ovog pristupa je njegova lokalna analiza, gde se k određuje specifično za svaki podatak, za razliku od globalnih metoda. Nuti takođe ističe važnost odabira metrike udaljenosti, posebno u višedimenzionalnim problemima. Ovaj rad značajno doprinosi primeni Bajesovih metoda u KNN algoritmima, omogućavajući preciznije klasifikacije i regresije, kao i bolji uvid u verovatnoće donošenja odluka, čime se proširuje njihova primena u oblasti mašinskog učenja.

Patel i saradnici (2018) [27] se bave problemom klasifikacije neuravnoteženih podataka koristeći unapređeni algoritam fazi k-najbližih suseda (Fuzzy KNN), koji koristi adaptivni pristup za rešavanje problema dominacije većinskih klasa. Neuravnoteženi podaci predstavljaju značajan izazov u mašinskom učenju jer standardni klasifikatori često favorizuju većinske klase na račun tačnosti klasifikacije manjinskih klasa. Ovde autori uvode adaptivni pristup kojim prilagođavaju broj najbližih suseda k za svaku klasu u zavisnosti od njene veličine, omogućavajući tako bolju ravnotežu između klasa. Glavna inovacija je unapređenje fazi funkcije članstva korišćenjem različitih vrednosti k za različite klase. Većinske klase koriste veće k vrednosti, dok se za manjinske klase koriste manje vrednosti, čime se smanjuje mogućnost pogrešne klasifikacije manjinskih instanci. Algoritam koristi adaptivni pristup tokom faze obučavanja za izračunavanje članstva instanci u klasama, dok se u test fazi članstvo novih instanci određuje na osnovu udaljenosti do najbližih suseda i njihovog članstva u klasama. Na kraju, klasa sa najvećim članstvom se dodeljuje test instanci. Eksperimenti sprovedeni na deset skupova podataka sa različitim nivoima neuravnoteženosti pokazuju da predloženi algoritam daje bolje rezultate u poređenju sa postojećim metodama. Rezultati su analizirani pomoću standardnih mera, pri čemu predloženi algoritam konstantno nadmašuje konkurenciju u tačnosti i uravnoteženosti klasifikacije.

Parvin i saradnici (2008) [28] istražuju unapređenje klasičnog algoritma KNN kroz razvoj modifikovane verzije, nazvane MKNN. Glavna ideja ovog pristupa je da se za svaki uzorak u obuci izračuna dodatna vrednost, nazvana validnost, koja predstavlja koliko je uzorak relevantan za svoju klasu. Ova vrednost se koristi za ponderisanje prilikom klasifikacije novih podataka, što omogućava preciznije odluke u poređenju sa tradicionalnim KNN-om. Algoritam funkcioniše tako što prvo procenjuje validnost svakog uzorka iz skupa za obučavanje. Validnost se

računa na osnovu broja suseda koji pripadaju istoj klasi. Nakon toga, prilikom klasifikacije novog uzorka, koristi se ponderisana verzija KNN-a, gde su težine suseda određene njihovom udaljenošću i prethodno izračunatom validnošću. Ovaj pristup daje veću važnost uzorcima koji su stabilniji i bliži ispitivanom uzorku, dok smanjuje uticaj onih koji su manje pouzdani ili se nalaze dalje. Eksperimenti pokazuju da MKNN postiže bolje rezultate od KNN-a na različitim skupovima podataka, uključujući Wine, Isodata i Monk probleme. Ova poboljšanja se pripisuju dodatnim informacijama koje validnost pruža, omogućavajući robusniju klasifikaciju čak i u prisustvu šumova ili neinformativnih uzoraka. Uprkos dodatnom koraku procene validnosti, algoritam ostaje računski efikasan, jer se validnost izračunava samo jednom tokom faze obučavanja. Rezultati su pokazali da je MKNN značajno bolji izbor u scenarijima gde klasični KNN pokazuje slabosti, naročito kod višedimenzionalnih i šumovitih podataka.

Čisar i dr. (2010) [29] se bave primenom EWMA algoritma u detekciji upada u računare i mrežne sisteme. Cilj je da se identifikuju nepravilnosti koje bi mogle da ukažu na napade u računarskim sistemima, i to analizirajući promene u intenzitetu mrežnog saobraćaja. EWMA algoritam je metoda koja, uz pomoć ponderisanih proseka, omogućava praćenje i detekciju odstupanja u vremenskim serijama. Algoritam daje veći značaj novijim podacima, dok stariji podaci imaju manji uticaj. Parametar λ određuje koliko su relevantni stariji podaci; veća vrednost parametra λ daje prednost novijim podacima, dok manja vrednost λ pruža stabilnost prilikom detekcije, ali sporije reaguje na nagle promene. Autori su upotrebili EWMA kontrolne grafikone za praćenje promena saobraćaja u stvarnim mrežama, fokusirajući se na detekciju malih pomeranja u srednjim vrednostima koje mogu biti znak potencijalnih napada. Upotrebljena je autentična mrežna aktivnost, prikupljena alatima za praćenje, poput MRTG (eng. Multi Router Traffic Grapher) softvera [55]. Korišćeni su grafikoni za dnevni, nedeljni i mesečni saobraćaj, što je omogućilo utvrđivanje vrednosti koje ukazuju na pretnje od napada. Studija je analizirala i optimizaciju parametra λ kako bi se smanjili lažni alarmi, koji su izazov u primeni EWMA algoritma na mrežni saobraćaj. Lažni alarmi mogu ometati sigurnost sistema, pa je optimizacija ključna za tačniju detekciju napada. Rad razmatra i uticaj međuzavisnosti u vremenskim serijama posmatranog saobraćaja, što je bitno za preciznost algoritma u razlikovanju pravih napada od nasumičnih promena u saobraćaju, jer je potrebno posmatrati duži vremenski period, odnosno nedeljni ili mesečni saobraćaj, kako bi se dobili precizniji rezultati. Na osnovu dobijenih rezultata, autori su zaključili da statistika dobijena primenom EWMA algoritma može biti efikasna za detekciju upada kada

se parametri prilagode specifičnostima mrežnog saobraćaja, pri čemu posebnu pažnju treba posvetiti inicijalnim vrednostima i podešavanju λ.

U (Čisar i dr. 2019) [30] prikazane su i mogućnost primene statističkih metoda i fazi logike u otkrivanju nepravilnosti u mrežnim sistemima. Autori su se fokusirali na algoritam eksponencijalno ponderisanog pokretnog proseka (EWMA), koji pomaže u praćenju intenziteta događaja u mreži. EWMA statistika omogućava brzo detektovanje promena u mrežnom saobraćaju, čime se može utvrditi potencijalna pretnja. Ipak, standardni EWMA algoritam može biti poboljšan uključivanjem adaptivnog praga i fazi logike. Fati logika omogućava preciznije određivanje stepena rizika, što smanjuje broj lažnih alarma. Kombinacija EWMA algoritma sa fazi logikom može unapred upozoriti na mrežni napad, pružajući administratorima mogućnost da pravovremeno reaguju. U radu su razmotreni različiti tipovi funkcija pripadnosti i fazi pravila. Na primer, jedno od pravila može biti: „Ako su sva tri EWMA parametra visoka, generiši alarm“. Na ovaj način, fazi sistem omogućava klasifikaciju mrežnog stanja na tri klase: normalno, upozorenje ili alarm. Kroz simulaciju u alatu „Matlab Fazzy Logic Toolbox“, autori su testirali algoritam koristeći različite funkcije pripadnosti i procenjuju tačnost sistema. Simulacija potvrđuje da trostruko uzastopno prekoračenje kontrolne granice može izazvati alarm, dok uvođenje fazi pravila smanjuje verovatnoću grešaka u detekciji. Zaključak rada ističe da integracija fazi logike u EWMA algoritma omogućava detaljniju analizu mrežnih podataka i doprinosi boljoj bezbednosti sistema.

Čisar i saradnici (2010) [31] su pokazali da je primena eksponencijalno ponderisanog pokretnog proseka (EWMA) za otkrivanje upada u mrežne sisteme. Autori su analizirali efikasnost EWMA algoritma u detektovanju promena u intenzitetu mrežnog saobraćaja, koje mogu ukazivati na potencijalne pretnje. EWMA statistika je ključna u praćenju promena kroz vreme, pri čemu noviji podaci imaju veći značaj prilikom proračuna. Algoritam koristi parametar λ, koji određuje uticaj starijih podataka: manja vrednost λ daje veću važnost istorijskim podacima, dok veća vrednost λ stavlja akcenat na novije promene. Standardna vrednost parametra λ se obično postavlja između 0,2 i 0,3, a optimizacija ovog parametra može dodatno poboljšati performanse detekcije nepravilnosti. Rad uvodi adaptivni prag koji prilagođava granicu alarma u skladu sa srednjom vrednošću saobraćaja. Da bi se smanjio broj lažnih alarma, predloženo je da se alarm pokrene tek nakon što nekoliko uzastopnih vrednosti pređe vrednost praga. Takođe, autori uvode faktor vremena u algoritam kako bi okidanje alarma bilo relevantno samo ako je prekoračenje praga trajalo duže od određenog vremena, čime se dodatno

filtriraju slučajni skokovi u saobraćaju. Uz to, istražena je uloga autokorelacije u otkrivanju upada. Autokorelacija može pomoći u razlikovanju između pravih pretnji i normalnih varijacija u mreži, pri čemu nizak stepen autokorelacije omogućava algoritmu da efikasno detektuje i male promene u intenzitetu događaja. U zaključnim razmatranjima autori su istakli da EWMA algoritam, kada se primeni uz odgovarajuću optimizaciju parametara i adaptivni prag, pokazuje veliki potencijal za unapređenje detekcije upada u mrežnim sistemima. Njegova sposobnost da brzo i precizno reaguje na promene u mrežnom saobraćaju čini ga efikasnim alatom za rano otkrivanje pretnji i obezbeđivanje sigurnosti sistema.

Čisar i saradnici (2011) [32] istražuju primenu statističke metode eksponencijalno ponderisanog pokretnog proseka (EWMA) u otkrivanju nepravilnosti u saobraćaju računarskih mreža, i to posebno u kontekstu prepoznavanja mogućih napada. Cilj istraživanja je optimizacija EWMA parametara kako bi se smanjili lažni alarmi i povećala efikasnost detekcije u mrežnim okruženjima. Metoda EWMA se koristi za praćenje promena u intenzitetu saobraćaja, gde se novijim podacima daje veća težina u poređenju sa starijim podacima. Parametar λ (ponder) ima ključnu ulogu u kontroli osetljivosti metode na promene u intenzitetu saobraćaja. Veći λ daje veći značaj novijim podacima, dok manji λ povećava udeo starijih podataka. Izbor optimalne vrednosti λ je važan, jer standardne vrednosti (obično između 0,2 i 0,3) mogu dovesti do neprihvatljivog broja lažnih alarma kada se EWMA primeni na mrežni saobraćaj. Istraživanje koristi uzorke autentičnog mrežnog saobraćaja za analizu i određivanje optimalnih granica kontrole. EWMA vrednosti koje premašuju gornje granice kontrole interpretiraju se kao statističke nepravilnosti, što može ukazivati na potencijalni napad. Da bi se smanjio uticaj slučajnih varijacija na pojavu lažnih alarma, primenjuje se eksponencijalno izglađivanje, čime se povećava preciznost detekcije. Jedan od izazova istraživanja je i korelacija u podacima mrežnog saobraćaja. Autokorelacija može otežati tačnu procenu nepravilnosti jer su vrednosti u vremenskim serijama međusobno zavisne. Stoga, za razliku od nekorelisanih podataka, u autokorelisanim podacima resetovanje početnih vrednosti nakon detekcije nije potrebno, jer EWMA automatski prilagođava kontrolne granice. U radu je predložena metodologija za odabir optimalne vrednosti λ kroz iterativnu proceduru koja minimizira sumu kvadrata grešaka (SSE). Na osnovu eksperimenta sa različitim vrednostima parametra λ, ustanovljeno je da optimalna vrednost često odstupa od standardnih preporučenih vrednosti, što ukazuje na važnost prilagođavanja parametara specifičnim uslovima mrežnog saobraćaja. Zaključci rada naglašavaju potrebu za pažljivim izborom

EWMA parametara pre primene u mrežnom okruženju. Takođe, predložena je analiza dnevnih, nedeljnih i mesečnih obrazaca saobraćaja kako bi se osigurala statistička nezavisnost uzoraka, što je ključno za efikasnost algoritma u otkrivanju nepravilnosti. Ovaj rad doprinosi oblasti mrežne bezbednosti, nudeći optimizovane pristupe za primenu EWMA u detekciji nepravilnosti u saobraćaju, čime se povećava nivo sigurnosti računarskih mreža kroz smanjenje lažnih alarma i poboljšanje tačnosti detekcije.

Abbas sa svojim timom (2011) [33] se bavi unapređenjem performansi EWMA dijagrama, a koji su inače često korišćeni alati u statističkoj kontroli kvaliteta i prilikom otkrivanja promena u procesima. Cilj istraživanja je poboljšanje tačnosti i efikasnosti ovih dijagrama, kako bi se povećala njihova primenljivost u različitim industrijskim i naučnim kontekstima. Autori istražuju različite metode za prilagođavanje i optimizaciju parametara EWMA dijagrama, kao što su ponderi i pragovi za alarmiranje, kako bi se smanjila stopa lažnih alarma i povećala senzitivnost na stvarne promene u podacima. U radu su primenjeni različiti simulacioni modeli i statističke tehnike za testiranje performansi EWMA dijagrama, posebno u scenarijima gde su varijacije procesa minimalne i teško uočljive. Rezultati pokazuju da se performanse EWMA dijagrama mogu značajno unaprediti kroz optimizaciju parametara, što omogućava precizniju detekciju čak i malih odstupanja u podacima. Zaključak je da poboljšani EWMA dijagrami mogu značajno doprineti boljoj kontroli procesa i smanjenju rizika od neotkrivenih promena, što ih čini pogodnijim za primenu u kompleksnim industrijskim i sigurnosnim sistemima. Ove optimizovane metode mogu imati široku primenu, uključujući i sisteme za detekciju upada (IDS) u mrežnim i informacionim sistemima, gde su visoka tačnost i efikasnost presudne.

U (Sklavounos i dr. 2017) [34] prikazana je primena statističkih metoda za detekciju (R2L eng. remote to local) napada. R2L napad predstavlja slanje mrežnih paketa na udaljeni sistem bez lokalnog korisničkog naloga. Autori analiziraju promene u srednjoj vrednosti (TCP) izvornih bajtova koristeći dva algoritma: algoritam eksponencijalno ponderisanog pokretnog proseka (EWMA) i algoritam kumulativnog zbira (CUSUM). EWMA algoritam daje veću težinu novijim podacima, omogućavajući bržu reakciju na promene u srednjoj vrednosti. S druge strane, CUSUM akumulira odstupanja od referentne vrednosti, što olakšava detekciju malih, ali postojećih promena. U istraživanju su korišćeni podaci iz KDD'99 skupa podataka, standardnog skupa podataka za evaluaciju sistema za detekciju upada. Analizom su utvrđene optimalne vrednosti parametara

za obe metode, kako bi se postigla visoka tačnost detekcije uz minimalan broj lažnih alarma. Rezultati su pokazali da obe metode mogu efikasno detektovati R2L napade, ali sa različitim performansama u zavisnosti od karakteristika napada. Metoda EWMA je pokazala bržu detekciju naglih promena, dok je CUSUM metoda bila efikasnija u identifikaciji manjih, postepenih promena. Zaključak rada je da kombinacija algoritama EWMA i CUSUM može pružiti sveobuhvatan pristup za detekciju različitih tipova R2L napada, poboljšavajući ukupnu sigurnost mrežnih sistema.

Machaka sa saradnicima (2016) [7] istražuje upotrebu EWMA algoritma za otkrivanje DDoS napada u IoT infrastrukturi. Napominje se da DDoS napadi, posebno TCP SYN flooding, mogu izazvati ozbiljne poremećaje u mrežnim sistemima, i da je to posebno opasno za kritične infrastrukture koje su ranjive na ovu vrstu napada. TCP SYN flooding napad je zasnovan na eksploatisanju mehanizma trostrukog rukovanja (eng. three-way handshake) za uspostavljanje TCP konekcije. Šalje se veliki broj SYN zahteva za kreiranje konekcije, i dok ciljani sistem očekuje da dobije ACK kao potvrdu konekcije to se nikada ne dogodi i time se konzumiraju resursi ciljanog sistema. EWMA algoritam analizira promene u mrežnom saobraćaju kroz detekciju nepravilnosti i promene tačke detekcije. Eksperimenti su korišćeni za analizu uticaja različitih parametara algoritma, kao što su prag alarma (α, ponder (β), i broj uzastopnih prekoračenja praga detekcije (k). Rezultati pokazuju da algoritam ima visok nivo tačnosti pri otkrivanju napada visokog intenziteta, ali se pokazao manje efikasnim za napade niskog intenziteta. Veća vrednost α smanjuje lažne alarme, ali i može smanjiti stopu detekcije. Sa druge strane, veća vrednost β poboljšava tačnost detekcije, ali povećava vreme odziva. EWMA je testiran na stvarnim mrežnim podacima sa sintetički generisanim napadima. Algoritam je uspešno detektovao visokointenzivne napade, ali nije bio dovoljno osetljiv na napade sa postepenim povećanjem intenziteta. U zaključku se navodi da rad pokazuje potencijal EWMA algoritma za detekciju DDoS napada, ali ističe se potreba za unapređenjem njegove efikasnosti za različite tipove napada. Autori predlažu unapređenja koja bi bila zasnovana na poređenju sa drugimalgoritmima i razvoj metoda koje pružaju bolju prilagodljivost i preciznost.

U (Özçelik i dr. 2016) [9] pokazan je inovativni pristup za otkrivanje DDoS napada korišćenjem kombinacije CUSUM algoritma i entropije mrežnog saobraćaja. Klasične metode za detekciju DDoS napada često su nedovoljno efikasne ili zahtevaju unapred definisane obrasce napada, dok kombinacija CUSUM

algoritma i entropije mrežnog saobraćaja pruža prilagodljiviji pristup koji omogućava rano otkrivanje napada i smanjuje stopu lažnih alarma. Ovaj metod koristi CUSUM algoritam, koji prati nagle promene u mrežnom saobraćaju, u kombinaciji sa entropijom IP adresa iz zaglavlja mrežnih paketa. Entropija meri nivo neuređenosti u posmatranim podacima, a tokom DDoS napada entropija IP adresa se naglo menja zbog velikog broja različitih izvora (IP adresa) koji šalju zahteve. Predloženi metod koristi filtriranje talasa da ukloni dugoročne varijacije u vrednostima entropije, čime se poboljšava preciznost CUSUM algoritma u detekciji napada. Ova kombinacija omogućava algoritmu da bolje identifikuje nepravilnosti koje ukazuju na DDoS napade, istovremeno smanjujući mogućnost lažnih detekcija koje bi mogle nastati usled normalnih varijacija u mrežnom saobraćaju. Eksperimentalno testiranje sprovedeno je na mreži Univerziteta Clemson, gde je mrežni saobraćaj univerziteta korišćen kao osnovni (pozadinski) protok podataka, dok su klaster računari univerziteta korišćeni za generisanje simuliranih DDoS napada sa maksimalnim opterećenjem do 416 Mbps. Eksperimenti su obuhvatili merenje entropije u vremenskim serijama od po dve sekunde, čime je kreirana vremenska serija entropije IP adresa. Rezultati su pokazali da predloženi metod ima visoku stopu detekcije i nisku stopu lažnih alarma, značajno nadmašujući metode koje koriste samo entropiju bez dodatne obrade signala. Efikasnost metode analizirana je preko ROC krive, koja pokazuje da Cusum-Entropy metoda omogućava optimalnu tačku detekcije, gde je stopa pravih alarma visoka, a stopa lažnih alarma minimalna. U zaključku, rad naglašava važnost razvoja naprednih metoda za detekciju nepravilnosti u saobraćaju kritičnih mreža, poput državnih sistema i pametnih mreža, gde DDoS napadi mogu imati katastrofalne posledice.

Leu i saradnici (2005) [35] bave se primenom CUSUM algoritma za detekciju TCP-baziranih DDoS napada. DDoS napadi su veoma problematični jer ometaju rad mreža i usluga na internetu, a posebno su opasni za one koji zavise od stabilnog pristupa mrežnim resursima. U radu se predlaže sistem detekcije upada pod nazivom CUSUM IDS (CIDS), koji koristi CUSUM algoritam za identifikaciju napada, kao i za identifikaciju uloge svakog čvora u mreži tokom napada. CIDS je dizajniran tako da mrežu deli na autonomne jedinice za upravljanje mrežom (NMU), kao što su intranet preduzeća ili mreža univerziteta, unutar kojih prikuplja podatke o saobraćaju i otkriva nepravilnosti poređenjem sa regularnim saobraćajem. NMU je hardverska komponenta sistema koja je zadužena za sigurnost mreže i koja sprovodi testiranje segmenata sistema, praćenje mrežnih aktivnosti, automatsko ažuriranje, kao i obaveštenja o kvarovima i otkazima unutar sistema. CUSUM algoritam detektuje nagle promene u saobraćaju, što

omogućava CIDS-u da brzo identifikuje početak napada i odredi da li se čvor ponaša kao žrtva, napadač (zombi) ili reflektor u napadu. U radu je posebno obrađena analiza TCP SYN Flood napada, koji koristi ranjivost u trostrukom rukovanju TCP konekcije. U ovom napadu, zombi šalje veliki broj SYN paketa sa nasumično lažiranim IP adresama, čime zagušava resurse servera, dok reflektor u distribuiranom reflektovanom napadu uskraćivanja usluge (DRDoS) odgovara na SYN pakete koje prima od napadača slanjem SYN-ACK paketa prema žrtvi, što dodatno komplikuje detekciju jer ovi odgovori izgledaju kao legitimni mrežni saobraćaj. CIDS koristi CUSUM za praćenje nesrazmernosti između dolaznih i odlaznih SYN i SYN-ACK paketa na različitim čvorovima kako bi identifikovao napade. Eksperimenti sprovedeni u radu uključuju simulaciju DDoS i DRDoS napada u NMU okruženju, gde CIDS uspešno identifikuje žrtvu, zombija i reflektor koristeći definisane pragove za parametre CUSUM algoritma. Na osnovu analize prikupljenih podataka, sistem može prepoznati uloge čvorova tokom napada i poslati obaveštenje za sprovođenje daljih koraka, kao što su praćenje napadača ili filtriranje saobraćaja kako bi se smanjila šteta od napada. Zaključak rada je da CIDS predstavlja efikasan način za realno-vremensku detekciju i odgovor na TCP-bazirane DDoS napade. Korišćenje CUSUM algoritma omogućava da se detekcija vrši sa niskim troškovima obrade i visokom preciznošću, dok se saradnjom sa drugim NMU jedinicama može poboljšati otpornost mreže na DRDoS napade.

U (Ali i dr. 2021) [36] autori istražuju primenu prilagođenog CUSUM algoritma za otkrivanje nepravilnosti u industrijskim komunikacionim sistemima. Industrijski sistemi su sve češće meta sajber napada jer su sve više povezani na internet radi optimizacije procesa i razmene podataka. Takvi sistemi su ranjivi na napade poput DDoS-a i drugih vrsta ometanja u radu, što može dovesti do ozbiljnih gubitaka u proizvodnji i bezbednosnih rizika. Stoga su IDS sistemi neophodni kako bi se zaštitili ovi kritični infrastrukturni sistemi. Prilagođeni CUSUM algoritam u ovom radu služi za efikasnu detekciju nepravilnosti analizom mrežnog saobraćaja. U standardnim industrijskim komunikacionim protokolima, koji su često strogo definisani i predvidljivi, svaka značajnija promena u saobraćaju može ukazivati na potencijalni napad ili grešku u sistemu. CUSUM algoritam prati statističke promene u toku saobraćaja kako bi identifikovao odstupanja od uobičajenog saobraćaja. U radu su autori predložili prilagođavanje standardnog CUSUM algoritma kako bi bio osetljiviji na specifične industrijske saobraćajne obrasce i smanjio stopu lažnih alarma. To je ključno jer su industrijski sistemi veoma osetljivi na prekide, a visoka stopa lažnih detekcija može uzrokovati nepotrebne

prekide i povećati troškove rada. Prilagođeni CUSUM algoritam koristi unapred definisane pragove za detekciju nepravilnosti na osnovu istorijskih podataka o normalnom saobraćaju u industrijskim mrežama. Eksperimenti izvedeni u radu pokazali su da prilagođeni CUSUM algoritam može efikasno detektovati različite tipove nepravilnosti sa visokim stepenom preciznosti i niskom stopom lažnih alarma. Rad se posebno fokusira na industrijske protokole kao što su „Modbus“ i „Profinet“, koji se često koriste u industrijskim mrežama. Testovi su pokazali da se predloženi metod može primeniti u realnom vremenu i integrisati u postojeće industrijske kontrolne sisteme bez većih promena u njihovoj strukturi. U zaključku rada se naglašava da je prilagođeni CUSUM algoritam praktičan i efikasan alat za detekciju nepravilnosti u industrijskim komunikacionim mrežama. Implementacijom ovakvog sistema za detekciju nepravilnosti, industrijski sistemi mogu postati otporniji na sajber napade i sigurniji u pogledu neprekidnog funkcionisanja.

Chiu i ostali (2020) [37] ispituju primenu CUSUM algoritma za detekciju DoS i DDoS napada u okviru sigurnosnog sistema za 5G mreže. Razvoj 5G mreža donosi ogromne prednosti u brzini i kapacitetu prenosa podataka, ali takođe povećava ranjivost ovih mreža na različite vrste sajber napada, posebno DoS i DDoS napade, koji mogu ozbiljno poremetiti funkcionisanje mreže. CUSUM algoritam je korišćen u ovom radu jer omogućava efikasno otkrivanje nepravilnosti analizom statističkih promena u mrežnom saobraćaju. U suštini, CUSUM algoritam detektuje nagle promene u tokovima podataka koje mogu ukazivati na prisustvo napada. Algoritam prati kumulativne promene u saobraćaju, identifikujući kada one pređu unapred definisane pragove, što se koristi kao indikator za potencijalni napad. U radu se razvija autonomni sigurnosni sistem za 5G mreže, zasnovan na CUSUM algoritmu, koji može detektovati i odgovoriti na napade u realnom vremenu. Sistem je dizajniran tako da automatski prepozna promene u saobraćaju koje ukazuju na DoS ili DDoS napade i preduzima korake za ograničavanje njihovih efekata. Jedan od ciljeva ovog pristupa je minimizacija lažnih alarma, što se postiže finim podešavanjem parametara algoritma kako bi sistem prepoznao nepravilnosti, ali ignorisao normalne varijacije u saobraćaju. Eksperimentalni rezultati su pokazali da CUSUM algoritam u okviru autonomnog sigurnosnog sistema može precizno otkriti DoS i DDoS napade u 5G mrežama, čak i kada su napadi prilagođeni da izgledaju kao regularan saobraćaj. Testovi su sprovedeni u simuliranom 5G okruženju, gde je sistem bio u mogućnosti da razlikuje regularne od zlonamernih tokova podataka, obezbeđujući stabilnost mreže i kontinuitet usluga. Ovaj autonomni pristup smanjuje potrebu za ručnom intervencijom, što je posebno

korisno za 5G mreže koje podržavaju veliki broj povezanih uređaja istovremeno. U zaključi, autori ističu važnost primene CUSUM algoritma u realnom vremenu u sklopu sigurnosnih sistema za 5G mreže. Predloženi sistem doprinosi jačanju otpornosti 5G infrastrukture na napade uskraćivanja usluga, čime se osigurava stabilan rad mreže i pruža veći nivo zaštite za korisnike i njihove podatke.

Lu i saradnici (2009) [38] su istraživali kombinaciju CUSUM algoritma i algoritma očekivanja maksimizacije (EM) za detekciju nepravilnosti u mrežnom saobraćaju. EM algoritam u ovom istraživanju je služio za grupisanje vrednosti (tačaka) na osnovu njihovih karakteristika. Tradicionalni sistemi za detekciju upada (IDS) često se oslanjaju na već poznate obrasce napada, što ih čini neefikasnim protiv novih ili nepoznatih pretnji. Da bi se prevazišao ovaj nedostatak, autori predlažu hibridni pristup koji integriše SNORT[56], kao sistem zasnovan na potpisima, sa CUSUM algoritmom i EM algoritmom klasterovanja za detekciju nepravilnosti. CUSUM algoritam je statistička metoda koja detektuje promene u srednjoj vrednosti mrežnog saobraćaja, što ga čini pogodnim za identifikaciju naglih promena u mrežnom saobraćaju koje mogu ukazivati na napad. EM klasterovanje je tehnika koja grupiše podatke u klastere na osnovu verovatnoće, omogućavajući identifikaciju obrazaca u podacima bez prethodnog znanja o njihovoj strukturi. U predloženom hibridnom sistemu, SNORT prvo analizira saobraćaj koristeći potpise poznatih napada. Zatim, CUSUM algoritam prati statističke promene u saobraćaju kako bi identifikovao potencijalne nepravilnosti. Na kraju, EM klasterovanje grupiše sumnjive aktivnosti u klastere, čime pomaže u razlikovanju uobičajenog i zlonamernog saobraćaja. Za eksperimentalnu evaluaciju korišćen je DARPA'1999 skupa podataka nad kojim je pokazano da ovaj hibridni pristup uspešno detektuje veliki broj napada koje SNORT samostalno propušta, istovremeno smanjujući stopu lažnih alarma. Ovi rezultati ukazuju na to da kombinacija metoda zasnovanih na potpisima i detekciji nepravilnosti može značajno poboljšati performanse IDS sistema.

U (Machaka i dr. 2019) [22] autori istražuju primenu CUSUM algoritma za detekciju DDoS napada u sistemima Interneta stvari (IoT). Primarni fokus je na TCP SYN flood napadima, koji koriste ranjivosti TCP trofaznog uspostavljanja veze, šaljući veliki broj lažnih zahteva serveru kako bi iscrpeli mrežne resurse i onemogućili legitimne korisnike da pristupe. CUSUM algoritam koristi detekciju nepravilnosti kroz promenu statističkih karakteristika mrežnog saobraćaja. Eksperimenti su sprovedeni na podacima stvarnog mrežnog saobraćaja uz sintetički generisane napade kako bi se simulirali različiti intenziteti napada (niski i

visoki). Ključni parametri algoritma, kao što su faktor amplitude (α), težinski faktor (β) i prag (h), prilagođavani su da bi se optimizovala njegova efikasnost. Rezultati pokazuju da CUSUM algoritam ima visok stepen detekcije za napade visokog intenziteta, uz prihvatljiv nivo lažno pozitivnih alarma. Međutim, kod napada niskog intenziteta algoritam ima ograničene performanse, s obzirom na veći broj lažno pozitivnih alarma i sporiju detekciju. Ovaj rad doprinosi i razumevanju sigurnosnih izazova u IoT sistemima i nudi potencijalna rešenja za unapređenje detekcije DDoS napada.

Gualandi i dr. (2022) [39] istražuju kako optimizovani napadi na sajber-fizičke sisteme mogu da zaobiđu mehanizme detekcije napada, konkretno koristeći CUSUM algoritam. CUSUM je metoda koja detektuje nepravilnosti na osnovu praga, tj. akumuliranog odstupanja između očekivanog i stvarnog stanja sistema. Ovo istraživanje se fokusira na tzv. prikrivene (eng. stealth) napade koji su posebno projektovani da ostanu neprimećeni dok izazivaju maksimalno moguće odstupanje sistema od željenog stanja. Autori predlažu optimizacijski pristup kreiranju napada, uzimajući u obzir ograničenja sistema. U radu se upoređuju dva modela optimizacije kontrolnih signala: model sa prevencijom prekomernih vrednosti (Opt-P eng. Overflow-prevent) i model koji omogućava prekomerne vrednosti (Opt-A eng. Overflow-allow). Eksperimenti su pokazali da model Opt-A omogućava izvođenje znatno opasnijih napada u poređenju sa modelom Opt-P, jer Opt-A dopušta veće varijacije u sistemu bez izazivanja detekcije. Oba modela, međutim, pokazuju da duže trajanje napada može dovesti do većeg odstupanja, čak i kada napad ostane prikriven. Studija koristi masa-opruga-prigušivač (eng. mass/spring/damper) sistem kao primer, gde Opt-A model daje veće odstupanje za duže napade, u poređenju sa standardnim geometrijskim napadom. Masa-opruga-prigušivač sistem je pogodan za modelovanje objekata sa složenim materijalnim svojstvima, kao što je nelinearnost. Time se pokazuje da uz odgovarajuću optimizaciju, napadi mogu postići veći učinak nego ustaljeni pristupi. Preporuka autora je da se za sigurnosnu procenu sistema koristi Opt-A model koji otkriva najopasnije potencijalne napade. Takođe, kombinovanjem „stateless“ i „stateful“ sistema, odnosno sistema koji ne čuvaju i onih koji čuvaju stanje detekcije, može se dodatno smanjiti mogućnost uspešnog napada na sistem. Rad naglašava značaj uključivanja fizičkih ograničenja u modeliranje napada, kao i važnost optimizacije trajanja napada za efikasnu procenu rizika u sajber-fizičkim sistemima.

Nedeljković sa saradnicima (2019) [40] se bavi unapređenim sistemom za brzo

odgovaranje u okviru e-Uprave Republike Srbije. Sistem koristi algoritam trostruke modularne redundanse (TMR) kako bi poboljšao preciznost odgovora na upite građana putem tri različite mere sličnosti. TMR algoritam funkcioniše tako što tri modula istovremeno obrađuju isti upit koristeći različite mere sličnosti, a zatim se koristi većinsko odlučivanje kako bi se odabrao najtačniji rezultat. TMR se u ovom kontekstu koristi za određivanje najpouzdanije mere sličnosti, koja omogućava precizniju pretragu i klasifikaciju dokumenata u domenu kriminalistike. U radu se pored TMR algoritma obrađuju i različiti tipovi redundanse, koji su ključni za postizanje visoke pouzdanosti sistema. Postoje tri glavne vrste redundanse koje se koriste u ovakvim sistemima: hardverska, softverska i informaciona redundansa. Hardverska redundansa podrazumeva dodavanje dodatnih hardverskih komponenti kako bi se obezbedila stabilnost sistema u slučaju kvara. Softverska redundansa se koristi u obliku višestrukog programiranja (N-verzije), gde različiti softverski moduli istovremeno rešavaju isti zadatak. U slučaju neslaganja u rezultatima, većinskim odlučivanjem se bira najpouzdaniji odgovor. Ovaj pristup obezbeđuje visoku toleranciju na greške i zavisi od pouzdanosti samih algoritama. Informaciona redundansa uključuje višak informacija ili dodavanje vremenskih resursa za stabilizaciju rada sistema. Kod TMR algoritma, informaciona redundansa se ostvaruje tako što se svaki upit obrađuje kroz tri različite mere sličnosti (kosinusna, Jaccardova i euklidska), a zatim se većinskim odlučivanjem bira najbolji rezultat za dalju obradu. Ovi tipovi redundanse su primenjeni kako bi se povećala pouzdanost i preciznost sistema, jer omogućavaju toleranciju na greške i održavaju stabilnost sistema čak i u slučajevima pojedinačnih kvarova. Eksperimentalni rezultati potvrđuju da TMR pristup, sa primenom sve tri mere sličnosti, daje značajno bolje rezultate u odnosu na individualnu primenu mera. Postignuta preciznost je 49.67%, dok tačnost sistema iznosi 74.83%, što ukazuje na poboljšanje u odnosu na prethodne metode zasnovane na pojedinačnim merama sličnosti.

2.2.2 Trostruka modularna redudansa

U (Lyons i dr. 1962) [41] prikazana je primena algoritma trostruke modularne redundanse (TMR) kako bi se povećala pouzdanost računarskih sistema, posebno onih koji se koriste u zahtevnim okruženjima poput svemirskih i vojnih sistema gde je visoka pouzdanost ključna. Glavna ideja TMR-a je povećanje pouzdanosti sistema pomoću redundanse, tj. viška komponenti koje omogućavaju nastavak rada čak i ako jedan od modula otkaže. Na taj način, sistem postaje otporan na pojedinačne kvarove komponenti. Kroz matematičku analizu, rad objašnjava kako

se pouzdanost TMR sistema menja u zavisnosti od pouzdanosti pojedinačnih modula, kao i značaj savršenih glasačkih krugova. Autori navode da se pouzdanost sistema može dodatno poboljšati smanjenjem kompleksnosti i izborom pouzdanijih komponenti. U istraživanju je korišćena Monte Karlo simulacija na IBM 704 računaru kako bi se analizirali kvarovi TMR sistema pod različitim uslovima. Simulacije su korišćene za procenu realnog ponašanja TMR sistema, pokazujući kako različiti dizajni modula i glasačkih krugova mogu uticati na ukupan nivo pouzdanosti. Na osnovu simulacije, autori dolaze do zaključka da TMR može značajno poboljšati pouzdanost računarskih sistema, ali i da zahteva balans između dodatne opreme i povećane pouzdanosti, jer se može desiti da previše glasačkih krugova smanji pouzdanost. Konačno, rad zaključuje da je TMR veoma korisna tehnika, posebno prilikom primene u sistemima gde održavanje nije moguće tokom rada. Tehnika se može primeniti na digitalne sisteme u širem smislu, uključujući mehaničke i elektronske komponente, kao i na skladišne sisteme i ulazno-izlaznu opremu povezanu s digitalnim sistemima.

U (Arifeen i dr. 2020) [42] prikazana je približna trostruka modularna redundansa (ATMR) kao sredstvo za postizanje visoke pouzdanosti u digitalnim sistemima, uz smanjenje troškova koji nastaju zbog trostruke replikacije modula u klasičnoj trostrukoj modularnoj redundansi (TMR). Osnovni cilj ATMR-a je balansiranje između tačnosti proračuna i poboljšanja performansi. Klasična TMR metoda zahteva značajan prostor zbog replikacije, koja može povećati površinu čipa i potrošnju energije za 200%. ATMR se bavi smanjenjem tih troškova korišćenjem približnih verzija modula, gde dva od tri modula daju približno isti rezultat kao originalni modul za većinu ulaza, čime se postiže optimalna pouzdanost uz niži trošak. Približno izračunavanje (AC) omogućava tolerisanje određenog stepena grešaka u proračunima radi postizanja boljih performansi, kao što su niža potrošnja energije i manji prostor za skladištenje podataka. Korišćenjem AC metode, ATMR može smanjiti broj grešaka na kritičnim ulazima i postići ravnotežu između tačnosti i efikasnosti. Autori su detaljno opisali i uporedili različite ATMR metode, naglašavajući izazove kao što su velika složenost dizajna i osiguravanje otpornosti na greške. Među metodama su uključene one koje koriste generisanje približnih funkcija na osnovu proširenja ili redukcije primitivnih implikanata, algoritme za smanjenje tranzistorske topologije, i tehnike optimizacije kao što su multiobjektivna genetska optimizacija. Kroz primere u tabelama, prikazano je kako se različite metode koriste za optimizaciju ATMR dizajna. Zaključak rada ističe važnost specifičnih alata za generisanje približnih modula u ATMR-u, jer postoji potreba za alatima koji su posebno prilagođeni ATMR-u.

Rad takođe ukazuje na potrebu za boljim metodama za procenu tačnosti i efikasnosti u ATMR-u kako bi se ATMR dizajn učinio skalabilnijim i prilagodljivijim različitim hardverskim platformama.

U (Zhang i dr. 2008) [43] prikazan je dinamički model sistema tolerantnog na greške koji je baziran na trostrukoj modularnoj redundansi. Fokus istraživanja je na udaljenim računarima, gde su pouzdanost i dostupnost presudni za rad. Klasične metode poput višemodularne redundantnosti i povratnog oporavka često zahtevaju visoke troškove. Autori nude pristup koji optimizuje rad ovih sistema kroz softverska rešenja, smanjujući potrebu za dodatnim hardverskim komponentama a samim tim i troškove izgradnje sistema. Predloženi model koristi primarne i rezervne servere za izvršavanje klijentskih zahteva. Osnovna verzija se pokreće na primarnom serveru, dok rezervne ostaju neaktivne sve dok ne dođe do greške. Ako primarni server zakaže, rezervni preuzima njegovu ulogu, obezbeđujući kontinuitet sistema. Svaki server u sistemu može služiti kao primarni za jedan zadatak i rezervni za druge, čime se postiže balans u opterećenju sistema. Implementacija algoritma uključuje virtuelni mehanizam sinhronizacije za koordinaciju stanja između servera, omogućavajući konzistentnost pri promenama. Algoritam detekcije grešaka funkcioniše poređenjem stanja servera u redovnim vremenskim intervalima. Ukoliko se identifikuje greška, sistem prelazi u mod sa dva modula, što smanjuje pouzdanost i kapacitet, ali omogućava nastavak rada dok se server ne vrati u funkciju. Pouzdanost modela je analizirana matematički, uključujući srednje vreme između otkaza. Dobijeni rezultati ukazuju da predloženi pristup poboljšava efikasnost i smanjuje troškove, ali je potrebna dalja analiza kako bi se uključio faktor obnove sistema i tranzicija stanja u realnim scenarijima.

U (Balasubramanian i dr. 2016) [44] prikazano je unapređenje trostruke modularne redundanse (TMR) kroz projektovanje poboljšanog većinskog odlučivanja koji je otporan na greške. Pouzdanost ovakvih sistema zavisi od toga da li većinsko odlučivanje ostaje bez grešaka, što može biti problematično kod nanoelektronskih tehnologija gde se povećava učestalost kvarova zbog smanjenja dimenzija tranzistora. Autori su predložili novi tip odlučivanja koji ima veću otpornost na greške u odnosu na klasično odlučivanje, kako u situacijama kada greške nastaju u funkcionalnim modulima, tako i kada su prisutne unutrašnje greške prilikom samog odlučivanja. Analiza je sprovedena koristeći CMOS tehnologiju od 32/28nm, pri čemu je novo odlučivanje pokazalo manje kašnjenje, manju potrošnju energije i manju površinu u poređenju sa postojećim odlučivanjem. U radu su korišćene simulacije kako bi se prikazala otpornost

predloženog odlučivanja na različite vrste grešaka, uključujući privremene, povremene i trajne greške. Kroz ove simulacije izračunat je odnos maskiranja grešaka (FMR) za različite modele odlučivanja, što je mera koja pokazuje otpornost odlučivanja na greške. FMR je odnos ukupnog broja ispravnih izlaznih rezultata glasača u prisustvu unutrašnjih i/ili spoljašnjih grešaka, koje su maskirane, podeljen sa ukupnim brojem mogućih unutrašnjih i/ili spoljašnjih pojavljivanja grešaka. Predloženo odlučivanje je postiglo visoku vrednost FMR-a, što znači da je uspešno maskiralo većinu grešaka, i ima poboljšane performanse u odnosu na druga analizirana odlučivanja. Zaključak ovog rada je da je predloženi pristup odlučivanju značajno unapredio pouzdanost TMR sistema u nanoelektronskim okruženjima. Ova poboljšanja su od ključne važnosti za primene koje zahtevaju visoki nivo sigurnosti i pouzdanosti, kao što su svemirski i vojni sistemi, gde je višestruka otpornost na greške od esencijalnog značaja.

2.2.3 Sistemi za detekciju upada

Čisar i njegovi saradnici (2022) [45] se bave IDS sistemima koji koriste fazi logiku kao pristup za prepoznavanje neovlašćenih aktivnosti na mreži. IDS analizira mrežni saobraćaj u cilju očuvanja poverljivosti, integriteta i dostupnosti informacija koje mrežna barijera (eng. firewall) možda ne može da prepozna. Fazi logika je korisna jer može da uspostavi precizne nivoe pripadnosti različitim klasama i time smanji broj lažnih pozitiva i lažnih negativa u detekciji napada. Rad objašnjava kako IDS kombinuje više komponenti, kao što su senzori za prikupljanje podataka, detektor za analizu podataka i komponenta za reagovanje koja može biti pasivna (npr. obaveštavanje administratora) ili aktivna (npr. blokiranje IP adrese). Pored toga, objašnjeno je kako veštačka inteligencija, uključujući fazi logiku, može automatizovati proces korelacije podataka i poboljšati otkrivanje napada. Fazi logika omogućava klasifikaciju mrežnog saobraćaja kroz pravila zasnovana na fazi asocijacijama i koristi se za detekciju nepravilnosti i unapređenje tradicionalnih metoda poput eksponencijalno ponderisanog pokretnog proseka (EWMA) u cilju predviđanja nepravilnosti. Rad takođe prikazuje primenu fazi logike u kombinaciji sa popularnim alatima kao što je SNORT, koji je najpoznatiji sistem za detekciju i prevenciju upada na mrežu, čime se smanjuju lažni alarmi i povećava preciznost u prepoznavanju napada, kao što su skeniranje portova i slični incidenti.

Čisar i dr. (2022) [46] proučavaju primenu neuronskih mreža (NN) i mašinskog učenja (ML) za optimizaciju pravila internet zaštitnog zida (eng. Firewall). Zaštitni zidovi su ključni za bezbednost mreža, kontrolišući protok saobraćaja na

osnovu pravila koja administratori definišu. Korišćenjem zaštitnog zida skupa podataka i Weka softvera, autori su razvili NN model za simulaciju pravila zaštitnog zida, testirajući parametre poput broja neurona, brzine učenja, momentuma i broja epoha. Optimizovani parametri omogućili su tačnost od 98,96%, što potvrđuje efikasnost modela u oponašanju rada zaštitnog zida. Autori takođe analiziraju algoritme za klasifikaciju podataka, uključujući Random Forest, J48 i višeslojni perceptron (MLP), pri čemu se Random Forest pokazao najpreciznijim za primenu na skupu podataka zaštitnog zida. Osim toga, autori su istražili mogućnosti klasterovanja podataka kroz algoritme k-srednjih vrednosti (eng. k-means), (EM) i (DBSCAN). Algoritam k-srednjih vrednosti je postigao bolju tačnost i brže rezultate u odnosu na ostale, što ga čini pogodnim za otkrivanje nepravilnosti. Rad pokazuje da neuronske mreže i algoritmi mašinskog učenja mogu značajno unaprediti sigurnost mreža kroz efikasnije filtriranje i klasifikaciju saobraćaja. Primena ovih tehnika omogućava zaštitnom zidu da preciznije identifikuje i blokira potencijalno opasne aktivnosti, što doprinosi sveobuhvatnijem sigurnosnom sistemu mreže.

Čisar i saradnici (2009) [47] istražuju model-algoritam zasnovan na statističkoj analizi za otkrivanje upada u računarske i mrežne sisteme kroz promene u intenzitetu mrežnog saobraćaja. Algoritam koristi podatke o saobraćaju korisnika iz softvera MRTG [55], analizirajući dnevne, nedeljne i mesečne trendove mrežnog saobraćaja kako bi identifikovao tipične karakteristike saobraćajnih obrazaca. Na osnovu tih karakteristika, algoritam formira model saobraćaja koji beleži obrasce kroz četiri perioda u toku dana: noćni saobraćaj, jutarnje povećanje, dnevni saobraćaj i večernje smanjenje. Korišćenjem statističkih alata poput srednje vrednosti i standardne devijacije, utvrđene su kontrolne granične vrednosti (limiti) koji obuhvataju očekivane vrednosti saobraćaja za svaki od ovih perioda. Svaka vrednost saobraćaja koja prelazi ove granice označena je kao nepravilnost, što može ukazivati na potencijalni napad. U cilju verifikacije, autori su primenili algoritam na podatke nekoliko korisnika i utvrdili da u raznim vremenskim periodima nema prekoračenja kontrolnih limita, što potvrđuje tačnost metode i minimizira mogućnost lažnih alarma. Takođe, istraživanje je pokazalo male razlike u vrednostima maksimalnog i prosečnog saobraćaja, čime se dodatno opravdava primena ovog statističkog modela. Jedna od ključnih prednosti ovog pristupa je mogućnost detekcije napada u realnom vremenu, što je ključno za brzo reagovanje na pretnje. Algoritam može da se prilagodi promenama u saobraćaju kroz periodične promene parametra, što ga čini fleksibilnim i sposobnim da se prilagođava vremenskim promenama saobraćajnih obrazaca. U zaključak ovog rada

se ukazuje da statistički modeli i kontrolne granične vrednosti mogu značajno doprineti efikasnosti sistema za otkrivanje upada, omogućavajući pravovremenu detekciju potencijalnih pretnji. Ovi pristupi ne samo da pomažu u identifikaciji stvarnih pretnji, već takođe smanjuju broj lažnih alarma, što je ključno za očuvanje resursa i pravilno funkcionisanje sistema.

U (Čisar i dr. 2010) [48] prikazana je primena statističke analize u detekciji upada u mrežne sisteme. Autori se fokusiraju na algoritam koji koristi karakteristike mrežnog saobraćaja korisnika za detekciju nepravilnosti koje mogu ukazivati na potencijalne napade. Osnovna ideja algoritma je da identifikuje obrazac saobraćaja kroz dnevne, nedeljne i mesečne periode kako bi stvorio referentni model. Pomoću ovog modela moguće je statistički odrediti granice normalnog saobraćaja i izdvojiti vrednosti koje odstupaju od ovih normi, što se dalje tretira kao nepravilnost. U analizi se koriste uzorci lokalnih maksimuma mrežnog saobraćaja, koji se obrađuju primenom deskriptivne statistike. Izračunavanjem srednje vrednosti i standardne devijacije uzoraka, autori su postavili gornje i donje kontrolne limite saobraćaja sa visokom preciznošću (interval pouzdanosti od 99%). Svi podaci koji premašuju te granice označeni su kao sumnjivi, što potencijalno ukazuje na prisustvo upada ili napada na mrežu. Rad takođe razmatra mogućnost prilagođavanja modela trenutnim uslovima saobraćaja, što omogućava njegovu adaptaciju i smanjenje lažnih alarma. Autori sugerišu da se prilikom detekcije koristi i vremenski faktor kako bi se pravovremeno uočile različite vrste napada, uključujući one koji su trenutno prepoznatljivi kao i napadi koji se dešavaju tokom dužih vremenskih perioda. Kroz ovu metodologiju, autori predlažu adaptivni algoritam koji može automatski ažurirati kontrolne limite na osnovu prosečnih vrednosti saobraćaja, omogućavajući fleksibilnu detekciju pretnji u realnom vremenu. Na ovaj način, unapređuje se bezbednost mreže jer se smanjuje mogućnost propusta u otkrivanju napada, dok se smanjuje broj lažnih uzbuna.

U (Ozkan Okay i dr. 2021) [49] prikazan je sveobuhvatan pregled dosadašnjih istraživanja na temu IDS sistema. U radu su sistematizovane tri glavne metodologije detekcije upada: detekcija zasnovana na potpisima (eng. signature-based), na nepravilnostima (eng. anomaly-based) i analiza protokola (eng. stateful protocol analysis). Svaka metodologija ima specifične prednosti i mane. Detekcija zasnovana na potpisima koristi predefinisane obrasce za identifikaciju poznatih napada, dok je manje efikasna za nepoznate napade. Metod zasnovan na nepravilnostima koristi odstupanja od uobičajenog ponašanja mreže

kako bi identifikovao pretnje, što ga čini korisnim za detekciju novih napada, ali je sklon generisanju lažnih alarma. Analiza protokola upoređuje događaje sa univerzalnim profilima protokola, ali je kompleksna i često zahtevna po resursima. Pored metodologija, rad prikazuje upotrebu različitih skupova podataka koji se koriste za testiranje i evaluaciju IDS sistema, kao što su KDD'99 i NSL-KDD, i daje pregled popularnih IDS alata i njihovih karakteristika, prednosti i nedostataka. Dalje, autori razmatraju aktuelne izazove u oblasti, kao što su promenljive prirode napada i nedostatak univerzalnih skupova podataka za treniranje modela. Posebno se ističe važnost integrisanja mašinskog učenja i razvoja hibridnih IDS sistema koji kombinuju različite tehnike kako bi se povećala preciznost i smanjio broj lažnih alarma. Autori naglašavaju da su IDS sistemi postali neophodni za bezbednost organizacija zbog sve veće zavisnosti od tehnologije i informatičkih sistema. Zaključak rada je da su potrebni dalji napori u istraživanju kako bi se prevazišle postojeće mane IDS sistema, kao i da je potrebno razvijati nove tehnike i alate za efikasnu detekciju sve sofisticiranijih pretnji.

Keunsoo i dr. (2008) [3] istražuju metode otkrivanja DDoS napada pomoću analize klastera, omogućavajući identifikaciju pripremnih faza napada. DDoS napadi predstavljaju ozbiljnu pretnju mrežnoj stabilnosti, pri čemu napadači koriste velike količine zaraženih uređaja za generiranje ogromnog broja paketa, iscrpljujući resurse ciljane mreže. U ovom radu je predložen pristup koji koristi analizu klastera za razlikovanje normalnog saobraćaja i svake faze napada posebno, od početne pripreme do samog napada. Kao parametri za detekciju, odabrane su entropija IP adresa i pripadajućih portova, entropija tipa paketa, učestalost specifičnih paketa (ICMP, UDP, TCP SYN) i broj paketa. Ove karakteristike omogućavaju identifikaciju nepravilnosti u saobraćaju karakterističnom za DDoS napade. Testiranje je izvedeno korišćenjem DARPA 2000 skupa podataka, a rezultati pokazuju da je metoda uspešno podelila podatke u faze: normalno stanje, pripremu (faze 1 i 2), napad i post-napad. Metoda je posebno efikasna u detekciji rane pripreme napada, omogućavajući ranu reakciju. U zaključku se navodi da predloženi pristup pruža jednostavno i efikasno rešenje za rano otkrivanje DDoS napada. U budućim radovima preporučuje se proširenje metode na različite vrste DDoS napada i obrada dodatnih skupova podataka radi unapređenja preciznosti i veće primene.

U (Zhou i dr. 2019) [50] autori se fokusiraju na detekciju nepravilnosti u mrežnom saobraćaju kao ključnom delu bezbednosti računarskih mreža. Autori predstavljaju model za detekciju nepravilnosti zasnovan na višestepenoj

autoregresiji koristeći informacije o entropiji. Mrežno ponašanje karakteriše distribucija entropije, gde značajne razlike ukazuju na normalno ili neuobičajeno ponašanje. Model koristi trećestepenu linearnu autoregresiju za predviđanje entropije u vremenskim serijama, a razlika između predviđenih i stvarnih vrednosti služi kao indikator nepravilnosti. Eksperimenti su izvedeni u simuliranom mrežnom okruženju sa ubačenim DDoS napadima, koristeći alate poput Wireshark-a za analizu mrežnih podataka. Rezultati pokazuju da predloženi model postiže stopu detekcije veću od 95%. Analiza entropije izvora napada i ciljanih IP adresa pokazuje da model precizno identifikuje trenutke u vremenu kada nepravilnosti nastaju, dok odnos entropije pruža dodatni sloj tačnosti u otkrivanju nepravilnosti. Model se adaptivno prilagođava mrežnim promenama, a koristi parametre poput raspona entropije i standardne devijacije za podešavanje praga detekcije. Autori na kraju zaključuju da predloženi model značajno unapređuje tačnost detekcije mrežnih nepravilnosti, dok eksperimenti potvrđuju njegovu efikasnost u otkrivanju DDoS napada. Ovaj rad doprinosi oblasti bezbednosti računarskih mreža pružajući robustan metod za realnu primenu u identifikaciji neuobičajenih obrazaca u mrežnom saobraćaju.

Rahmani sa svojim timom (2009) [51] analizira model za detekciju DDoS napada korišćenjem statističkog pristupa. Rad predlaže model zasnovan na analizi koherentnosti između broja primljenih paketa i broja IP konekcija. Ključna hipoteza je da legitimno povećanje broja paketa prati proporcionalno povećanje broja IP konekcija, dok kod DDoS napada dolazi do disbalansa između ova dva parametra. U istraživanju su korišćeni realni podaci baze Centra za primenjenu analizu internet podataka CAIDA, uključujući legitimne i maliciozne saobraćajne tokove. Metodologija uključuje analizu histograma, statističko modelovanje koristeći eksponencijalnu distribuciju, kao i primenu centralne granične teoreme za procenu verovatnoće. Detekcija nepravilnosti vrši se izračunavanjem statističkih odstupanja između referentnog i posmatranog saobraćaja. Rezultati pokazuju da predloženi model može pouzdano razlikovati legitimna i maliciozna povećanja saobraćaja, uz minimizaciju lažnih alarma. Prednost metode je jednostavnost implementacije, jer zahteva analizu samo izvornih IP adresa. Zaključuje se da model omogućava detekciju napada u realnom vremenu i smanjuje problem lažnih pozitiva, što je ključno za efikasnu zaštitu mreža. U zaključku ovog rada se ukazuje da je potrebno istražiti primenu na različitim tipovima saobraćaja i mreža, kao i identifikaciju IP adresa uključenih u napade.

U (Sanmorino i dr. 2013) [5] autori istražuju kako otkriti i sprečiti DDoS

napade koristeći obrasce protoka mrežnog saobraćaja. DDoS napadi koriste mnoštvo kompromitovanih uređaja za preplavljivanje ciljanog sistema ogromnom količinom saobraćaja, onemogućavajući legitimnim korisnicima pristup. U radu su definisane glavne vrste DDoS napada, uključujući SYN Flooding, ICMP Flooding i napade male brzine. Fokus istraživanja je na razvoju metode zasnovane na obrascima protoka koja omogućava razlikovanje legitimnog od malicioznog saobraćaja. Predloženo rešenje uključuje tri koraka: prikupljanje podataka iz tabele protoka, detekciju nepravilnih obrazaca i primenu višeslojnog firewall-a za blokiranje zlonamernih paketa. Korišćeni su simulacijski alati za testiranje u tri scenarija: normalna mreža, nezaštićena mreža i zaštićena mreža. Rezultati su pokazali da predložena metoda može blokirati 95% malicioznih paketa, dok omogućava prolaz legitimnog saobraćaja. U zaključku se navodi da se metoda detekcije zasnovana na obrascima protoka pokazuje efikasnom i ekonomičnom, bez potrebe za naprednom tehnologijom. Međutim, za dalja istraživanja potrebno je testiranje u realnim mrežnim okruženjima kako bi se unapredila otpornost na faktore poput gubitka signala i zagušenja mreže.

U (Kim i dr. 2020) [52] autori istražuju upotrebu modela zasnovanih na dubokom učenju (DL eng. deep learning) za detekciju DoS napada u IDS sistemima. Konvencionalne IDS metode, koje se oslanjaju na prepoznavanje poznatih potpisa ili neuobičajenih obrazaca ponašanja, teško detektuju nepoznate i sofisticirane napade. Model predložen u ovom radu koristi konvolucionu neuronsku mrežu (CNN eng. Convolutional Neural Network) za prepoznavanje karakteristika DoS napada na osnovu obučavanja nad skupovima podataka KDD CUP 1999 i CSE-CIC-IDS 2018. KDD CUP 1999 skup podataka je klasičan IDS skup koji uključuje četiri glavne kategorije napada, dok CSE-CIC-IDS 2018 predstavlja moderniji skup sa naprednijim vrstama DoS napada. CNN model je prilagođen tako da koristi transformaciju podataka u slike (u sivim tonovima i RGB formatu) kako bi se iskoristila moć mreža za obradu slika. Eksperimenti su sprovedeni kroz binarnu i višeklasnu klasifikaciju, a rezultati su upoređeni sa modelima zasnovanim na rekurentnim neuronskim mrežama (RNN eng. Recurrent Neural Network). Rezultati pokazuju da CNN nadmašuje RNN u tačnosti detekcije, posebno u višeklasnim zadacima, sa prosečnom tačnošću iznad 99% za KDD skup i 91,5% za CSE-CIC-IDS 2018. RGB slike su se pokazale boljim od sivih tonova, dok su optimalne performanse postignute sa tri konvoluciona sloja za manja jezgra (2x2, 3x3) i dva sloja za veća jezgra (4x4). Zaključeno je da je CNN model efikasan za razlikovanje sličnih DoS napada i da bi budući rad mogao proširiti ovu metodologiju na druge kategorije napada i IDS skupove podataka.

Wang (2004) [53] u svojoj disertaciji predstavlja hibridni sistem za detekciju upada. Ključni problem koje rad obrađuje je unapređenje preciznosti detekcije nepravilnosti i smanjenje broja lažnih alarma u sistemima za detekciju upada, uz omogućavanje otkrivanja poznatih i novih pretnji. Rad integriše različite pristupe, uključujući metode detekcije zasnovane na nepravilnostima, specifikacijama i prepoznatim napadima, kako bi se postigla efikasnija detekcija. U disertaciji su razvijeni novi kerneli koji koriste metodu potpornih vektora (SVM, eng. Support Vector Machine) za poboljšanje detekcije nepravilnosti. Ovi kerneli omogućavaju detekciju uz manje lažnih alarma i veću tačnost u poređenju sa tradicionalnim metodama. Poseban doprinos je uvođenje „jednoklasnog SVM“ pristupa za detekciju nepravilnosti, koji eliminiše potrebu za označenim podacima za obuku, što značajno olakšava implementaciju sistema. Druga važna inovacija je integracija metoda zasnovanih na specifikacijama sa detekcijom nepravilnosti. Specifikacije, koje definišu legitimno ponašanje sistema, pomažu u smanjenju lažnih alarma filtriranjem ponašanja koja su pravilna, ali retka. Sistem takođe omogućava automatsko generisanje softverskih agenata za detekciju upada, koji koriste formalne modele za kreiranje koda za detekciju poznatih ali i novih napada. Eksperimenti su pokazali da predloženi hibridni pristup postiže visoku stopu detekcije uz smanjenje lažnih alarma. Rad takođe identifikuje mogućnosti za dalja istraživanja, poput razvoja novih kernela i automatskog podešavanja parametara za SVM metode. Disertacija pruža osnovu za dizajn i implementaciju naprednih sistema za zaštitu računarskih mreža.

U (Faizal i dr. 2009) [54] predlaže se tehnika za detekciju brzih napada u mrežnim sistemima pomoću sistema za otkrivanje upada. Fokus istraživanja je na „brzim napadima“, koji generišu veliki broj konekcija u kratkom vremenskom periodu, ugrožavajući mrežnu bezbednost. Autori definišu statičku vrednost praga detekcije za razlikovanje normalnog od malicioznog mrežnog saobraćaja, koristeći posmatranja realnog saobraćaja i eksperimentalne simulacije, a verifikaciju rezultata sprovode statističkom kontrolom procesa. Metodologija uključuje analizu mrežnog saobraćaja sa mreža vladinih agencija i simulacija (npr. DARPA99), kao i eksperimente u kontrolisanom okruženju. Normalno ponašanje operativnih sistema, kao što su Windows XP i Linux, analizirano je kako bi se utvrdio prag detekcije za brze napade. Shewhart kontrolni dijagrami korišćeni su za verifikaciju, gde svaki događaj koji prelazi prag od 3 konekcije po sekundi označava potencijalni napad. Rezultati pokazuju da metoda efikasno identifikuje nepravilnosti, poput malicioznih DNS zahteva i aktivnosti crva. Predloženi prag može se koristiti za realnu mrežnu zaštitu. Dalje istraživanje uključuje detekciju napada putem UDP i

ICMP protokola, kao i razvoj dinamičkih tehnika za prilagodljivo određivanje praga.

Khraisat i dr. (2019) [18] prikazuje pregled IDS sistema, ključnih tehnika za detekciju, skupova podataka i izazova sa kojima se suočavaju IDS sistemi. Rad obuhvata dve glavne metode detekcije: detekciju zasnovanu na potpisima (SIDS) i detekciju zasnovanu na nepravilnostima (AIDS). SIDS funkcioniše tako što prepoznaje poznate pretnje kroz obrasce (potpise) napada, dok AIDS identifikuje odstupanja od normalnog ponašanja u mreži, što ga čini korisnim za otkrivanje novih napada, ali sklonim lažnim alarmima. Rad takođe razmatra razne skupove podataka koji se koriste za evaluaciju IDS sistema, kao što su KDD Cup 99, NSL-KDD, ADFA i CICIDS2017. Ovi skupovi podataka omogućavaju istraživačima da razvijaju i testiraju IDS sisteme u kontrolisanim okruženjima, ali neki od njih, poput KDD Cup 99, su zastareli i ne obuhvataju novije tipove napada. Dalje, rad analizira tehnike kojima se napadači služe kako bi zaobišli IDS, uključujući fragmentaciju paketa, maskiranje (eng. obfuscation), enkripciju i preopterećenje sistema. Maskiranje na primer menja kod samog napada da bi on bio teže prepoznatljiv, dok enkripcija može sakriti zlonamerne aktivnosti od sistema za detekciju. Dalji razvoj IDS sistema uključuje potrebu za smanjenjem lažnih alarma, prilagođavanje novijim oblicima pretnji, kao i razvoj skupova podataka koji verno predstavljaju realne pretnje. Autori ističu da u razvoju IDS sistema treba da se usmere ka kombinaciji tehnika, poput hibridnih sistema koji koriste i detekciju potpisima i nepravilnostima, kao i ka primeni mašinskog učenja kako bi se poboljšala preciznost i otpornost IDS sistema.

Radovi koji se bave pojedinačnim algoritmima su bili inspiracija za njihov odabir. U pregledu radova koji se odnose na algoritme KNN, EWMA i CUSUM može se zaključiti da su odabrani algoritmi dokazano efikasni, da imaju široku primenu, ali i da mogu da se dodatno unaprede uz određene modifikacije. TMR metod uvodi unapređenje svojom otpornošću na greške i time doprinosi pouzdanosti IDS sistema. Važnost detekcije napada je iskazana u radovima koji se bave IDS sistemima i jedna je od glavnih motivacija za pisanje ove disertacije.

3. Metodologija i resursi za detektovanje napada

U prvom odeljku je data metodologija rada u okviru koje su predstavljeni pojedinačni algoritmi: KNN, EWMA i CUSUM, koji su kasnije integrisani u finalni sistem koristeći TMR. Drugi deo je posvećen analiziranim skupovima podataka koji su svi javno dostupni i odnose se na zabeleženi mrežni saobraćaj koji sadrži napade, što omogućava poredivost rezultata i ponovljivost eksperimenta.

3.1 Metodologija rada

Sigurnosni softver je u današnje vreme važan deo svake organizacije. Suočavanje sa bezbednosnim incidentima nikada nije bilo teže nego što je to danas. DDoS napadi su jedna od najvećih pretnji IT bezbednosti svake organizacije, tako da se veliki napori ulažu u rešavanje tog problema na efikasan način.

Napadi su uobičajena pojava u računarskom svetu, i može proći neko vreme dok se novi tipovi napada ne otkriju softverom za detekciju. DDoS napadi, ransomware i druge pretnje po bezbednost računarskih sistema postali su deo svakodnevnog života. U ovoj disertaciji analiziraju se nepravilnosti u mrežnom saobraćaju gde bi svaka nepravilnost trebala da bude detektovana i pravilno obrađena. Analiza mrežnog saobraćaja je ključna za zaštitu računarskih sistema. U ovom radu predstavljena je metoda koja koristi TMR za detekciju nepravilnosti u mreži i to koristeći pokretne granične vrednosti, a kako je navedeno u [1].

Detekcija nepravilnosti može da se vrši na različite načine [2]. Glavni cilj je otkrivanje napada što je ranije moguće, odnosno smanjenje vremena odziva i obaveštavanje korisnika da je napad u toku, ali i smanjenje broja lažnih pozitiva na minimum, tj. poboljšanje tačnosti. Tri algoritma koja su odabrana i koji su najprikladniji za ove ciljeve su: algoritam K-najbližih suseda, eksponencijalno ponderisani pokretni prosek i algoritam kumulativnog zbira. U narednim odeljcima će biti opisan svaki od ovih algoritama pojedinačno, uključujući i njihove varijante. Za svaki ćemo dati opis metode, prednosti i nedostatke, kao i smernice za unapređenje.

3.1.1 KNN

K-najbližih suseda (KNN) je jednostavan i efikasan algoritam za klasifikaciju koji se često koristi u različitim oblastima [20]. Kao nenadzirana klasifikaciona metoda, KNN se razlikuje po tome što ne zahteva parametarske pretpostavke o distribuciji podataka, što ga čini fleksibilnim i pogodnim za primenu na različitim tipovima

podataka [57]. Zbog svoje jednostavnosti, KNN je često primenjivan u zadacima kao što su na primer klasifikacija teksta i prepoznavanje obrazaca.

Sam algoritam funkcioniše tako što za svaki novi podatak koji treba klasifikovati pronalazi k najbližih tačaka u skupu za obučavanje koristeći meru udaljenosti, najčešće euklidsku udaljenost. Klasa se dodeljuje na osnovu većinskog odlučivanja među ovim najbližim susedima, s tim da se može uvesti i ponderisanje na osnovu udaljenosti kako bi bliži susedi imali veći uticaj na konačnu klasifikaciju. Euklidska udaljenost se računa na sledeći način:

$$d\left(x, y\right) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \tag{1}$$

- x_i - i-to posmatranje;
- y_i - i-to posmatranje;

Jedan od glavnih izazova prilikom primene KNN algoritma je njegova zavisnost od vrednosti parametra k koja mora biti pažljivo izabrana kako bi algoritam imao optimalnu tačnost. Ako je vrednost parametra k previše mala, model može biti osetljiv na šum u podacima, dok previsoka vrednost parametra može dovesti do prevelike generalizacije, to se najbolje može videti na slici 1. Optimalna vrednost parametra k se često određuje eksperimentalno, kroz iterativno ispitivanje različitih vrednosti.

Primena KNN algoritma takođe može biti korisna i u IDS sistemima. Analizom obrazaca u istorijskim podacima KNN može da identifikuje nove događaje kao sumnjive ili benigne na osnovu sličnosti sa prethodno klasifikovanim podacima. Ovaj pristup može pomoći u prepoznavanju zlonamernih aktivnosti i pretnji, odnosno napada.

Glavna prednost KNN algoritma leži u njegovoj jednostavnosti i efikasnosti pri radu sa različitim vrstama podataka. Takođe je jednostavan za implementaciju i dobro funkcioniše u situacijama gde je potrebno klasifikovati podatke u realnom vremenu ili gde se često dodaju novi podaci, što je slučaj u predloženoj metodi. Međutim, njegova najveća mana je u tome što je „lenji“ algoritam, što znači da ne vrši nikakve proračune tokom faze obučavanja već sve obavlja u trenutku klasifikacije. To može biti problematično kod velikih skupova podataka jer zahteva puno vremena i procesorskih i memorijskih resursa za računanje udaljenosti između svih podataka.

Da bi se prevazišli ovi nedostaci, obično se predlaže kreiranje modela sa reprezentativnim tačkama, čime se smanjuje potreba za čuvanjem svih podataka i povećava efikasnost klasifikacije. Na ovaj način, KNN može biti optimizovan za brže i efikasnije odlučivanje, posebno u slučajevima sa velikim brojem podataka [28].

3.1.2 EWMA

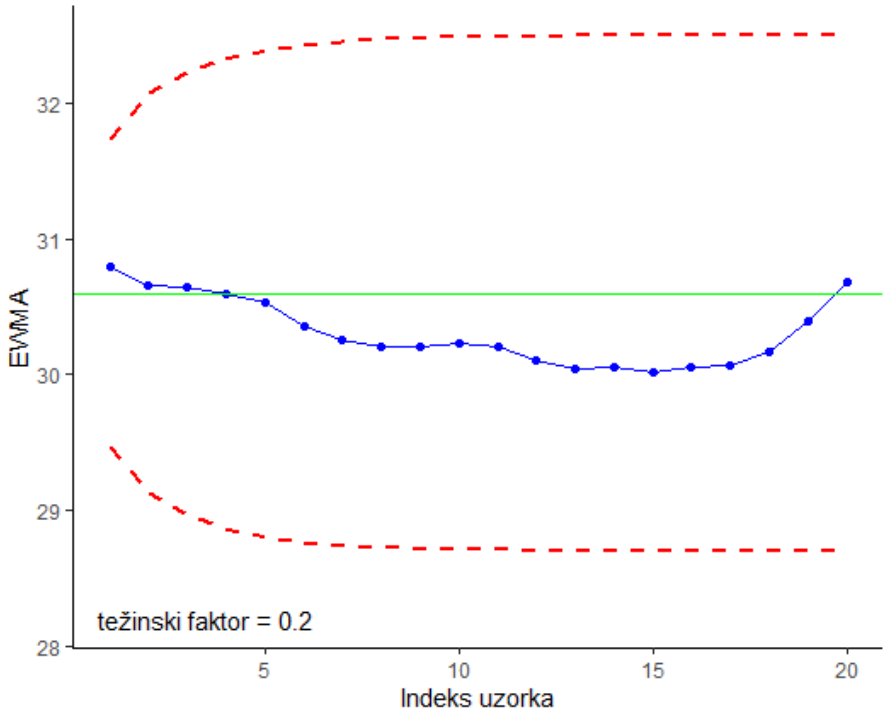
Eksponencijalno ponderisani pokretni prosek (EWMA) je algoritam koji se koristi za analizu i predviđanje vremenskih serija. U suštini, EWMA algoritam omogućava efikasno računanje srednjih vrednosti koje su eksponencijalno ponderisane prema novijim podacima čime im se daje veća važnost u odnosu na starije vrednosti [29]. Ovo ga čini veoma pogodnim za primene gde su poslednje promene u trendovima važnije od istorijskih podataka.

Osnovna formula za računanje EWMA vrednosti glasi:

$$S_t = \alpha X_t + (1 - \alpha) S_{t-1} \tag{2}$$

- S_t - predstavlja eksponencijalno ponderisani pokretni prosek u trenutku t,
- X_t - vrednost posmatrane promenjive u trenutku t,
- α - (alfa) konstanta koja kontroliše koliko brzo se EWMA prilagođava novim vrednostima (često je $0 < \alpha < 1$).

Kada je vrednost α veća, EWMA algoritam daje veću važnost novijim podacima, što rezultira bržim reagovanjem na promene. Kada je vrednost α manja, tada su istorijski podaci važniji, te algoritam reaguje sporije. Na slici 4 se može videti kako se donja i gornja granica obeležene crvenom bojom stabilizuju vremenom, za grafikon su uzete proizvoljne vrednosti kako bi se ilustrovao način rada EWMA algoritma, indeks uzorka predstavlja vremenski interval u sekundama.



Slika 4: Primer EWMA grafikona sa graničnim vrednostima

EWMA funkcioniše tako što algoritam eksponencijalno smanjuje težinu podataka kako se udaljava u prošlost. Svaka sledeća vrednost se dobija kao linearna kombinacija prethodno izračunate EWMA vrednosti i trenutne vrednosti. To jest, ako dođe do velike promene u podacima, EWMA algoritam će to registrovati, ali će brže reagovati na nove podatke, a istovremeno, ako nema značajnih promena u podacima, vrednosti će se menjati postepeno i stabilnije.

EWMA algoritam ima široku primenu i često se koristi u oblastima kao što su finansijska analiza, kontrola kvaliteta u industriji, telekomunikacije i mreže i slično. U finansijskoj analizi koristi se uglavnom za analizu cena akcija, odnosno analizu kretanja cena akcija u određenom vremenskom periodu, analizirajući koliko je cena akcija sklona menjanju i kratkom periodu, gde je važno brzo reagovati na promene tržišta. Prilikom kontrole kvaliteta u industriji se koristi za otkrivanje malih odstupanja u procesu proizvodnje. U telekomunikacijama i mrežnim sistemima se koristi za detekciju promena u mrežnom saobraćaju i predviđanje nepravilnosti, upravo za to je i korišćen u predloženom rešenju.

Neke od prednosti EWMA algoritma su to što je efikasan i jednostavan za implementaciju [30], uz to brzo reaguje na promene kada je to potrebno i pogodan je za praćenje podataka u realnom vremenu jer je izračunavanje EWMA vrednosti

relativno jednostavno [29], [33], [34].

Mane EWMA algoritma su to što je osetljiv na izbor vrednosti parametra α, jer pogrešan izbor vrednosti može dovesti do prevelike osetljivosti ili ignorisanja novih podataka [32]. Takođe EWMA algoritam nije prikladan za podatke sa takozvanim sezonskim varijacijama jer nema načina da ih prepozna [31].

3.1.3 CUSUM

CUSUM je algoritam koji detektuje promene. Ažurira se u realnom vremenu i periodično, što je pogodno za ovo rešenje jer mrežni saobraćaj obično ima veliki broj paketa koji se konstantno menjaju tokom vremena. CUSUM je algoritam koji se koristi za kontrolu kvaliteta, optimizovan je za merenje bilo kakvog odstupanja od određene vrednosti i koristi se za detekciju malih promena proseka. Sa CUSUM-om, izračunava se zbir razlika između stvarnih i očekivanih vrednosti, što predstavlja CUSUM vrednost. CUSUM se lako može prilagoditi i već postoji niz varijacija ovog algoritma, čak se može prilagoditi da bude samoučeći kako bi detektovao promene pri različitim nivoima opterećenja mreže.

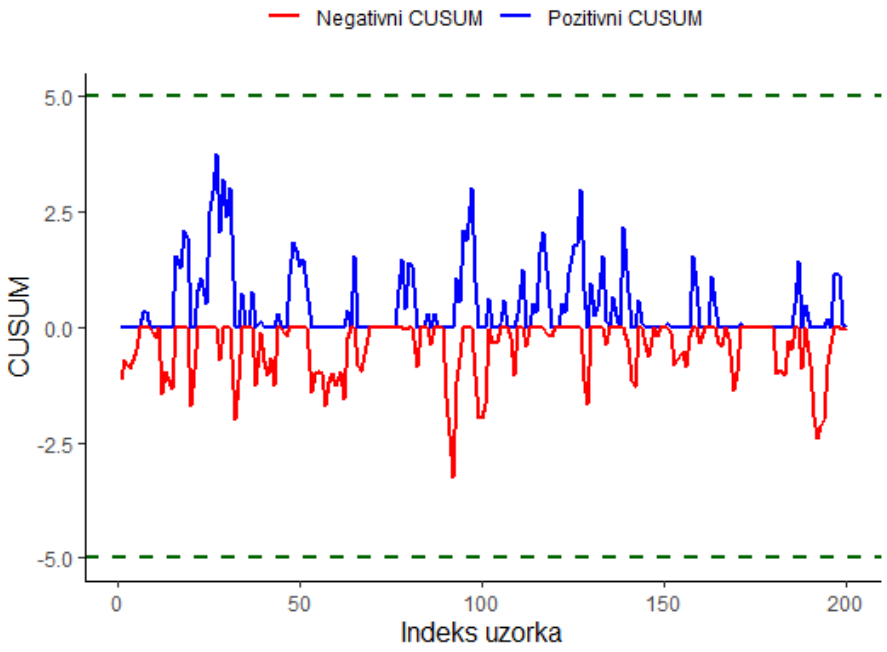
Kako smo već naveli CUSUM je zapravo srednja vrednost sume odstupanja od referentne vrednosti μ, koja predstavlja periodično ažuriranu vrednost u realnom vremenu. Odatle sledi da ako je S_i vrednost i-te kumulativne sume, a x_n je vrednost promenjive x u trenutku n, i μ je srednja vrednost odstupanja od referentne vrednosti, onda je formula za izračunavanje kumulativne sume S_i sledeća:

$$S_i = \sum_{i=1}^{n}(x_1 - \mu) = (x_n - \mu) + S_{i-1} \tag{3}$$

- S_i - vrednost kumulativne sume za parametar i,
- x_n - vrednost posmatrane promenjive u trenutku n,
- μ - srednja vrednost odstupanja od referentne vrednosti.

Na slici 5 može se videti kako izgleda grafikon za neke proizvoljne vrednosti. Plavom bojom prikazane su pozitivne, a crvenom bojom negativne CUSUM vrednosti, dok su donja i gornja granična vrednost obeležena zelenom isprekidanom linijom. Indeks uzorka je prikazan na X-osi i predstavlja vremenski interval u sekundama, dok je na Y-osi prikazana CUSUM vrednost.

Algoritam CUSUM je odabran za predloženo rešenje jer je već dokazan kao dobra metoda za primenu u IDS sistemima što se može videti u pregledu dosadašnjih istraživanja [34], [9], [35], [36], [37], [38], [22].



Slika 5: Primer CUSUM grafikona sa graničnim vrednostima

3.1.4 TMR

Razvoj informaciono komunikacionih tehnologija (IKT) dostigao je nivo koji omogućava njihovu primenu i implementaciju u složenim i ranjivim sistemima i domenima, a gde su potrebni visoka pouzdanost, sigurnost, dostupnost i stabilnost. Takvi sistemi se uglavnom nazivaju visokopouzdani ili sistemi otporni na greške. Sistemi otporni na greške su sistemi koji nastavljaju da obavljaju svoje funkcije čak i u veoma nepovoljnim uslovima, zahvaljujući sposobnosti da tolerišu pojedinačne kvarove [58, 40].

Nekoliko faktora uticalo je na razvoj i širenje koncepta sistema otpornih na greške. Pre svega iz razloga što moderni sistemi postaju sve složeniji jer se sastoje od velikog broja povezanih komponenti, što usložnjava ceo sistem, a time se povećava mogućnost kvarova. Tu je i faktor razvoja elektronskih sistema koji su manje pouzdani od mehaničkih i zahtevaju dodatne mere za povećanje pouzdanosti.

Kada su u pitanju sistemi otporni na greške, jedan od uobičajenih metoda za povećanje pouzdanosti sistema je korišćenje redundanse. Redundansa predstavlja dodavanje resursa, informacija ili vremena iznad nivoa potrebnog za normalan rad sistema, i ta redundansa može biti hardverska, softverska, informaciona i vremenska [40].

Hardverska redundansa je fizičko umnožavanje hardvera radi detekcije i tolerancije grešaka i deli se na tri tipa: pasivnu, aktivnu i hibridnu. U pasivnoj hardverskoj redundansi koristi se princip većinskog odlučivanja, gde se na primer trostruka modularna redundansa (TMR) koristi tako što se hardver utrostruči i greška se prikriva većinskim odlučivanjem. Ipak, glavna slabost TMR-a je mehanizam za odlučivanje, jer ako on prestane da radi, pouzdanost celog sistema pada na nivo pouzdanosti tog mehanizma. Aktivna hardverska redundansa funkcioniše detekcijom, lokalizacijom i popravkom grešaka, omogućavajući sistemima da tolerišu privremene greške dok se ne stabilizuju. Hibridna redundansa, kombinacija aktivne i pasivne, koristi prikrivanje grešaka uz istovremenu detekciju i popravku kako bi se sistem stabilizovao.

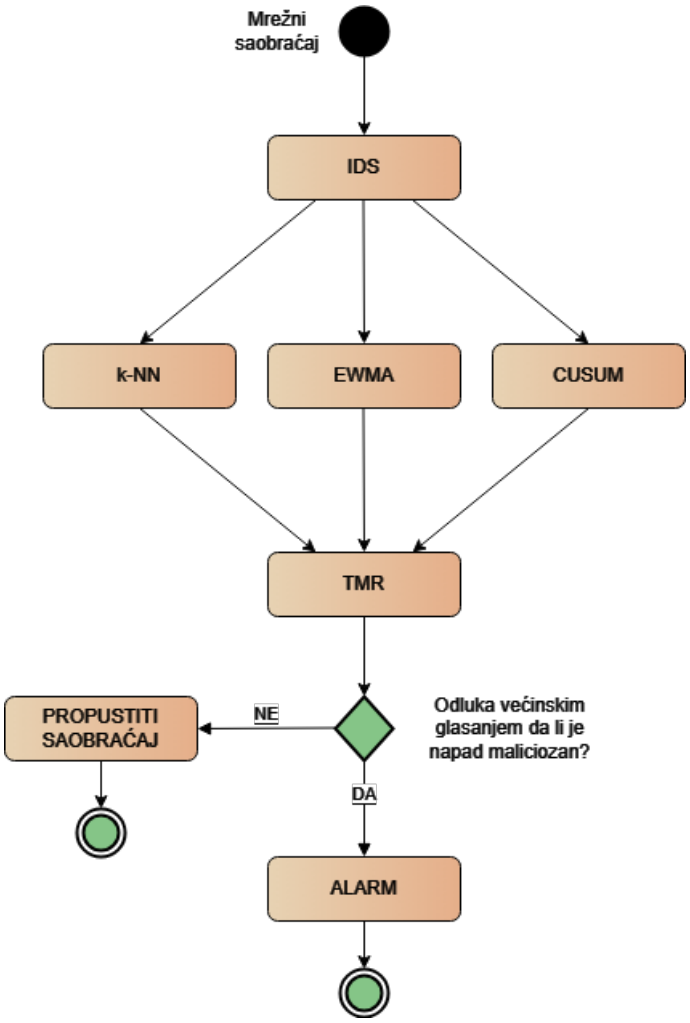
Softverska redundansa uključuje tehnike detekcije i tolerancije grešaka implementirane direktno u softveru, bez potrebe za umnožavanjem programa. Primeri uključuju dodatne komande za proveru sistema i male programske procedure za periodično testiranje memorije. Ovaj tip redundanse je korišćen u predloženom rešenju.

Informaciona redundansa podrazumeva dodavanje dodatnih informacija, kao što su kodovi za detekciju i korekciju grešaka. Kodiranje transformiše originalne podatke u kodove pomoću pravila kodiranja, dok dekodiranje vraća podatke u prvobitni oblik. Kodovi za detekciju grešaka omogućavaju detekciju grešaka u podacima, dok kodovi za korekciju omogućavaju njihovo ispravljanje. Ključni parametar u karakterizaciji ovih kodova je Hemingova distanca, koja označava broj pozicija na kojima se dve binarne reči razlikuju. Ova distanca određuje koliko grešaka kod može da ispravi ili da detektuje.

Vremenska redundansa se koristi za obezbeđivanje dodatnog vremena za izvršenje sistema, čime se omogućava detekcija i korekcija grešaka bez dodatnih hardverskih resursa. U aplikacijama gde je vreme manje ograničavajuće od hardvera, vremenska redundansa predstavlja praktično rešenje, jer smanjuje troškove i zahteve za fizičkim resursima koji utiču na težinu, zapreminu, energiju i cenu sistema.

Kombinacijom ovih različitih vrsta redundansi, sistemi mogu povećati otpornost na greške, što je naročito važno za kritične primene gde je kontinuitet rada neophodan.

TMR ima primenu i u IDS sistemima gde je otpornost na greške veoma značajna. UML (eng. Unified Modeling Language) dijagram stanja na slici 6 prikazuje kako izgleda proces kombinovanja algoritama k-najbližih suseda, eksponencijalno ponderisanog pokretnog proseka i kumulativne sume. Dijagram ilustruje primenu TMR metoda u IDS sistemu za analizu mrežnog saobraćaja. Mrežni saobraćaj prvo ulazi u IDS sistem, gde se analizira korišćenjem tri algoritma: KNN, EWMA i CUSUM. Rezultati analize ovih algoritama prosleđuju se TMR sistemu, koji donosi odluku na osnovu većinskog glasanja. Ako se većinskim glasanjem utvrdi da je saobraćaj maliciozan, pokreće se alarm, dok se u suprotnom saobraćaj propušta. Dijagram jasno pokazuje način na koji se TMR metod koristi za povećanje pouzdanosti detekcije malicioznih aktivnosti u mreži.



Slika 6: TMR primena u IDS sistemu

Isti koncept bi se mogao primeniti i na n-modularnu redudansu ali ne bi postojala značajnija poboljšanja u odnosu na predloženi metod, dok bi performanse zasigurno bile lošije.

3.1.5 IDS

Detekcija nepravilnosti se može izvršiti na mnogo načina. Cilj je da se napad detektuje što je to ranije moguće, da se o tome obavesti korisnik sistema koji je žrtva napada i da se smanji broj lažnih pozitiva na minimum, odnosno da se poveća preciznost. U predloženom rešenju koriste se KNN, EWMA i CUSUM algoritmi za detekciju napada a zatim se kombinuju u algoritam TMR kako bi se dobili tačniji rezultati [1].

Ovaj metod razmatra klasifikaciju rezultata dobijenih primenom nabrojanih algoritama i to u dve klase, pozitivne i negativne rezultate, što u ovom slučaju znači da li je napad tačno ili netačno detektovan.

Mogući ishodi klasifikacije su prikazani u tabeli 1.

Tabela 1: Prikaz matrice za klasifikaciju predviđanja

		Odgovor IDS-a	
		+	−
Upad	+	TP (pravi pozitiv)	FN (lažni negativ)
	−	FP (lažni pozitiv)	TN (pravi negativ)

U tabeli 1, neka je N broj članova i predstavlja sumu promenjivih TP, FN, FP i TN. Matrica prikazana u tabeli 1 zove se 2x2 matrica. Kako je prikazano u tabeli moguća su samo 4 različita rezultata, pravi pozitivi (TP), lažni pozitivi FP), pravi negativi (TN) i lažni negativi (FN) [59]. U tabeli je znakom + označeno da li se upad dogodio odnosno da li je IDS detektovao napad. Sa znakom − je označeno ako se upad nije dogodio odnosno IDS nije detektovao napad. Možemo ove vrednosti posmatrati kao celobrojne pozitivne vrednosti. Na osnovu rezultata iz tabele 1 za klasifikaciju, mogu se razmatrati četiri parametra klasifikacije a to su tačnost (eng. accuracy), preciznost (eng. precision), odziv (eng. recall) i F1 mera performansi za klasifikaciju koji se računaju na sledeći način:

$$\text{Tačnost} = \frac{TP + TN}{N} \tag{4}$$

$$\text{Preciznost} = \frac{TP}{TP + FP} \tag{5}$$

$$\text{Odziv} = \frac{TP}{TP + FN} \tag{6}$$

$$\text{F1} = 2 \times \frac{\text{Preciznost} \times \text{Odziv}}{\text{Preciznost} + \text{Odziv}} \tag{7}$$

Jedna od metoda grafičkog prikaza efikasnosti algoritma jeste iscrtavanje (ROC) (operativne karakteristike primaoca eng. Receiver Operating Characteristics) krive [59]. ROC kriva se prikazuje kao odnos između TPR (osetljivosti eng. True positive rate) i FPR (učestalosti lažnih alarma eng. False positive rate) i te vrednosti se računaju na sledeći način:

$$TPR = \frac{TP}{TP + FN}. \tag{8}$$

$$FPR = \frac{FP}{FP + TN}. \tag{9}$$

ROC kriva se često koristi za analizu rezultata jednog klasifikacionog procesa. U slučaju binarne klasifikacije, ROC kriva u dvodimenzionalnom koordinatnom sistemu predstavlja, pri različitim pragovima klasifikacije, na osi O_x stopu lažnih pozitiva, a na osi O_y stopu pravih pozitiva, što je sinonim za parametar odziva.

Površina ispod ROC krive (AUC eng. Area Under Curve) pruža zbirnu meru performansi za sve moguće pragove klasifikacije, a efikasan algoritam zasnovan na sortiranju može nam pružiti informacije o kvalitetu razmatrane klasifikacije. AUC vrednost se kreće od 0 do 1, pri čemu model čija su predviđanja 100 posto netačna ima AUC vrednost 0, dok model sa 100 posto tačnim predviđanjima ima AUC vrednost 1.

Kako bi detekcija bila precizna i pravovremena potrebno je odrediti prag detekcije. U IDS sistemima se najčešće koristi adaptivni prag. Adaptivni prag je metoda koja se koristi u algoritmima detekcije nepravilnosti ili napada kako bi se automatski prilagodio prag detekcije na osnovu trenutnog stanja mreže ili sistema [59]. To omogućava sistemu da se efikasno prilagodi dinamičkim promenama u mrežnom saobraćaju, smanjujući lažne alarme i povećavajući preciznost detekcije.

Adaptivni prag se koristi u statističkim tehnikama detekcije nepravilnosti u mrežnom saobraćaju. Ova metoda analizira mrežni saobraćaj i prilagođava prag za alarmiranje na osnovu sledećih parametara:

- Istorijskih podataka gde se prethodni uzorci i trendovi u mrežnom saobraćaju za postavljanje praga.
- Promena u realnom vremenu odnosno detekcija trenutnih odstupanja u mrežnom saobraćaju koja odstupaju od očekivanih vrednosti i obrazaca.
- Kombinacije statističkih i probabilističkih modela kao što su Gaussian modeli za detekciju verovatnoće nepravilnosti.

Prednosti adaptivnog praga uključuju njegovu mogućnost da smanji lažno pozitivne alarme u situacijama kada dolazi do legitimnih povećanja saobraćaja (npr. u špicu ili tokom posebnih događaja, praznika i drugo) i bolju detekciju stvarnih pretnji kada nepravilnosti pređu prag koji je prilagođen na osnovu trenutnih uslova.

3.2 Analizirani skupovi podataka

Za validaciju rezultata predloženog rešenja potrebno je koristiti skupove podataka koji su pogodni za razvijanje i testiranje IDS sistema. Odabrani skupovi podataka služe za istraživanje i razvoj sistema za detekciju i analizu mrežnih napada, pružajući realistične scenarije mrežnog saobraćaja sa podacima o različitim vrstama mrežnih napada. Njihova svrha je unapređenje sigurnosnih rešenja kroz simulaciju stvarnih pretnji u kontrolisanom mrežnom okruženju. U nastavku su opisana 3 skupa podataka koji su korišćeni za obučavanje, testiranje i validaciju.

3.2.1 CIC-IDS2017

Skup podataka CIC-IDS2017 [60], je kreirao Kanadski institut za sajber bezbednost (CIC eng. Canadian Institute for Cybersecurity) u svrhu istraživanja i evaluacije IDS sistema. Mrežni saobraćaj je generisan pomoću alata CICFlowMeter, koji su razvili istraživači sa instituta, i koji pruža različite statistike kao što su trajanje sesije, protok paketa, broj bajtova, itd. Skup sadrži preko 2.8 miliona instanci prikupljenih tokom pet dana. Skup sadrži 79 kolona, od kojih je 78 numeričkih karakteristika.

Ovaj skup podataka sadrži različite vrste napada kao što su DDoS, brute-force

napadi (SSH i RDP), web napadi (SQL injection, XSS), botnet aktivnosti, napadi pomoću skeniranja portova i napadi zlonamernim softverom (eng. malware).

- SSH - Napad koji podrazumeva automatizovani pokušaj pristupa koristeći veliki broj različitih kombinacija korisničkih imena i lozinki kako bi se pristupilo SSH serveru. Cilj je da se odrede tačni pristupni parametri i da se ostvari neovlašćeni pristup sistemu.
- RDP - Napad na RDP podrazumeva pokušaje pogađanja pristupnih parametara koristeći ranjivosti u RDP implementaciji, ili koristeći ukradene podatke kako bi se stekao neovlašćeni pristup udaljenom računaru. Takvi napadi se neretko završavaju kompromitovanjem sistema i podataka.
- SQL Injection - Sigurnosna ranjivost u aplikacijama koja omogućava napadaču da izvrši zlonamerne SQL naredbe kako bi rukovao bazama podataka.
- XSS - Napad koji omogućava napadačima da unesu zlonamerni kod u internet stranice kako bi ukrali podatke korisnika ili izveli druge zlonamerne radnje.

Skup podataka je podeljen po danima od ponedeljka 3. jula 2017. godine pa do petka 7. jula 2017. godine gde je svakoga od navedenih pet dana generisan jedan ili više gorepomenutih napada.

U tabeli 2 prikazani su generisani napadi po danima.

Za potrebe testiranja i evaluacije predloženog rešenja odabran je peti dan, odnosno saobraćaj generisan 7. jula 2017. godine kada su zabeležene botnet aktivnosti u generisanom saobraćaju. Korišćenje botnet mreže je razlog zašto je odabran peti dan, jer to ukazuje da je napad izvršen sa većeg broja računara i da se radi o napadu preplavljivanja mrežnih resursa.

3.2.2 CIC-DDoS2019

Skup podataka CIC-DDoS2019 [61], je kreirao Kanadski institut za sajber bezbednost (CIC eng. Canadian Institute for Cybersecurity), predstavlja vredan resurs za proučavanje DDoS napada koji predstavljaju ozbiljnu pretnju bezbednosti računarskih mreža. Iako postoje brojne statističke metode za detekciju DDoS napada, izazov ostaje napraviti detektor koji može da radi u realnom vremenu i koji ima nisko računarsko opterećenje.

Ovaj skup podataka sadrži različite scenarije DDoS napada izvedene na mrežama u kontrolisanom okruženju i uključuje podatke o mrežnom saobraćaju, protokolima i ponašanju napada. CIC-DDoS2019 skup podataka omogućava istraživačima da

Tabela 2: Tipovi napada u CIC-IDS2017 skupu podataka

Dan	**Tip napada**	**Period napada**
03. jul 2017.	Mrežni saobraćaj bez napada	
04. jul 2017.	Brute-force (FTP)	09:20 – 10:20
	Brute-force (SSH)	14:00 – 15:00
05. jul 2017.	DoS Slowloris	09:47 – 10:10
	DoS Slowhttptest	10:14 – 10:35
	DoS Hulk	10:43 – 11:00
	DoS GoldenEye	11:10 – 11:23
06. jul 2017.	Web napad – brute-force	09:20 – 10:00
	Web napad – XSS	10:15 – 10:35
	Web napad – sql injection	10:40 – 10:42
	Infiltration – Meta exploit Windows Vista	14:19
		14:20 – 14:21
	Infiltration – cool disk – MAC	14:53 – 15:00
	Infiltration – Windows Vista	15:04 – 15:45
07. jul 2017.	Botnet ARES	10:02 – 11:02
	Port scan	13:55 – 14:35
		14:51 – 15:29
	DDoS LOIT	15:56 – 16:16

analiziraju različite tipove DDoS napada, kao što su UDP, TCP, ICMP i drugi, i da razviju efikasnije metode za detekciju i odbranu. U tabeli 3 prikazano je 7 DDoS napada koji su izvedeni prvoga dana, kao i 12 tipova napada koji su izvedeni drugoga dana. Skup sadrži oko 80 mrežnih karakteristika.

Skup podataka je koristan za obučavanje algoritama mašinskog učenja koji su osnova modernih sistema za detekciju napada, i nudi mogućnost za razvoj rešenja sa boljom preciznošću u prepoznavanju zlonamernog saobraćaja. Na taj način, istraživači mogu da testiraju različite pristupe i identifikuju najbolje metode za detekciju pretnji, što je od ključnog značaja za unapređenje bezbednosti u digitalnim mrežama.

Ovaj skup podataka za razliku od skupa CIC-IDS2017 sadrži isključivo podatke o DDoS napadima. Za potrebe testiranja i evaluacije predloženog rešenja korišćena su dva fajla koja sadrže zapise generisanog mrežnog saobraćaja sa UDP napadima iz dva različita dana. U oba slučaja se radi o napadima preplavljivanja mrežnih resursa

Tabela 3: Tipovi napada u CIC-DDoS2019 skupu podataka

Dan	**Tip napada**	**Period napada**
Prvi dan	PortMap	09:43 – 09:51
	NetBIOS	10:00 – 10:09
	LDAP	10:21 – 10:30
	MSSQL	10:33 – 10:42
	UDP	10:53 – 11:03
	UDP-Lag	11:14 – 11:24
	SYN	11:28 – 17:35
Drugi dan	NTP	10:35 – 10:45
	DNS	10:52 – 11:05
	LDAP	11:22 – 11:32
	MSSQL	11:36 – 11:45
	NetBIOS	11:50 – 12:00
	SNMP	12:12 – 12:23
	SSDP	12:27 – 12:37
	UDP	12:45 – 13:09
	UDP-Lag	13:11 – 13:15
	WebDDoS	13:18 – 13:29
	SYN	13:29 – 13:34
	TFTP	13:35 – 17:15

koji su pogodni za testiranje predloženog metoda.

3.2.3 IoT

Skup podataka „IoT Network Intrusion“ [62] je kreiran u akademske svrhe simulacijom različitih tipova mrežnih napada u okruženju Internet stvari (IoT). U eksperimentu su korišćeni tipični pametni kućni uređaji: pametni zvučnik (SKT NUGU - NU 100) i Wi-Fi kamera (EZVIZ C2C Mini 0 Plus 1080P). Oni su zajedno sa nekoliko laptop računara i pametnih telefona povezani su na istu bežičnu mrežu.

Ovaj skup podataka sadrži 42 datoteke sa snimljenim mrežnim paketima (PCAP datoteke) u različitim vremenskim tačkama. Paketi su snimljeni korišćenjem bežičnog adaptera u monitor modu, pri čemu su zaglavlja uklonjena pomoću alata Aircrack-ng [63]. Većina napada, osim onih iz kategorije Mirai

botneta, simulirana je korišćenjem alata kako što je Nmap. U slučaju Mirai botneta, napadi su generisani na laptop računaru i potom modifikovani da izgledaju kao da potiču sa IoT uređaja.

Kratak opis datoteka, odnosno napada u skupu može se videti u tabeli 4.

Od navedenih datoteka korišćene su datoteke *benign-dec.pcap* koja sadrži pakete mrežnog saobraćaja bez napada, dok je datoteka *mirai-udpflooding-1-dec.pcap* koja sadrži pakete normalnog mrežnog saobraćaja i tipičnog Mirai UDP flooding napada koji je korišćen za obučavanje. Datoteka *benign-dec.pcap* je korišćena za vizuelizaciju saobraćaja koji ne sadrži napade odnosno za poređenje sa drugim podacima koji sadrže napade. Za testiranje i validaciju korišćena je datoteka *dos-synflooding-1-dec.pcap* koja sadrži pakete mrežnog saobraćaja DoS napada korišćenjem SYN zahteva. U oba slučaja radi se o datotekama koje sadrže napade preplavljivanja mrežnih resursa gde dolazi do naglog porasta u broju paketa, i to je razlog zašto su baš ove datoteke odabrane za obučavanje i testiranje.

Tabela 4: Tipovi napada u IoT Network Intrusion skupu podataka

Datoteka	**Opis**
benign-dec.pcap	saobraćaj bez napada
mitm-arpspoofing-n(1-6)-dec.pcap	saobraćaj bez napada i MITM (ARP preplavljivanje) napadi
dos-synflooding-n(1-6)-dec.pcap	saobraćaj bez napada i DoS (SYN preplavljivanje) napadima
scan-hostport-n(1-6)-dec.pcap	saobraćaj bez napada i skeniranjima (host i port scan) napadima
scan-portos-n(1-6)-dec.pcap	saobraćaj bez napada i skeniranjem (port i OS scan) napadima
mirai-udpflooding-n(1-4)-dec.pcap	saobraćaj bez napada i tipičnim Mirai napadima (UDP preplavljivanje)
mirai-ackflooding-n(1-4)-dec.pcap	(ACK preplavljivanje)
mirai-httpflooding-n(1-4)-dec.pcap	(HTTP preplavljivanje)
mirai-hostbruteforce-n(1-5)-dec.pcap	saobraćaj bez napada i inicijalnom fazom Mirai malvera, uključujući otkrivanje hostova i Telnet brute-force napada

4. Rezultati - studija slučaja

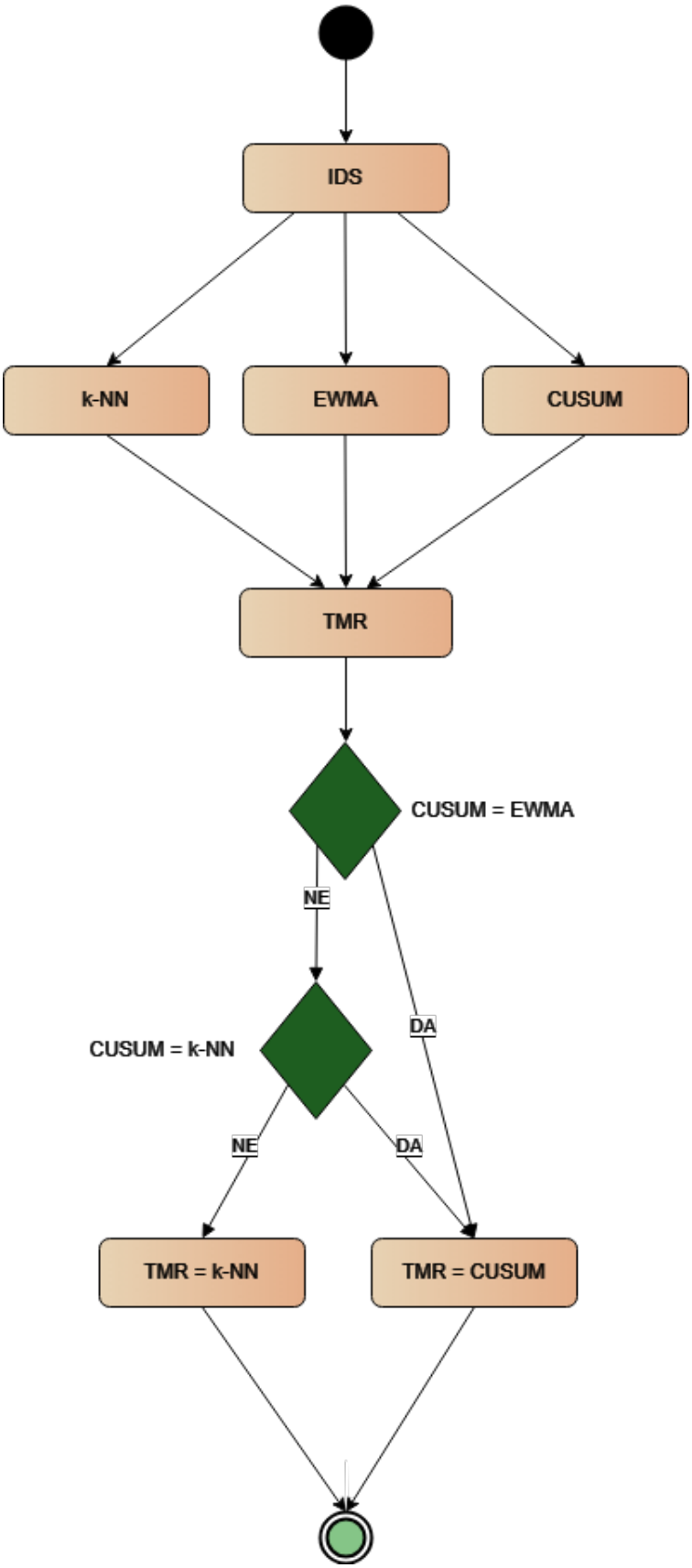
Ovo poglavlje je posvećeno rezultatima disertacije. U prvom odeljku je data arhitektura predloženog rešenja, potom sledi njegova implementacija i studija slučaja zasnovana na razvijenom rešenju. Ključni delovi rešenja su ilustrovani karakterističnim delovima programskog koda. Poslednji odeljak donosi konačne rezultate i zaključna razmatranja zaokružuju ovo poglavlje.

4.1 Arhitektura predloženog rešenja

Predloženo rešenje funkcioniše na sledeći način: rezultati dobijeni primenom algoritama kumulativne sume (CUSUM), eksponencijalno ponderisanog pokretnog proseka (EWMA) i algoritma k-najbližih suseda (KNN) se kombinuju i prosleđuju u sistem trostruke modularne redundanse (TMR). Ovaj sistem zatim donosi konačnu odluku o tome da li je potrebno aktivirati alarm na osnovu analize dobijenih podataka [1].

Kada mrežni saobraćaj stigne do IDS sistema, prvo se formiraju vremenske serije. U ovom rešenju, vremenske serije su kreirane na intervalima od jedne sekunde. Tokom svakog tog intervala, potrebno je izbrojati broj paketa koji su poslati u mreži. Nakon što se kreiraju vremenske serije i prebroje paketi unutar njih, primenjuju se tri odabrana algoritma: algoritam kumulativne sume, eksponencijalno ponderisani pokretni prosek i k-najbliži susedi. Svaki od ovih algoritama pojedinačno pruža indikaciju da li je analizirani saobraćaj maliciozan ili ne. Dobijene vrednosti iz sva tri algoritma zatim se koriste kao ulazni parametri za algoritam trostruke modularne redundanse, koji donosi konačnu odluku o tome da li posmatrani saobraćaj predstavlja napad, na osnovu zadatih parametara.

Veliki značaj u detekciji ima i odabir algoritama koji su korišćeni u kombinaciji sa algoritmom trostruke modularne redundanse. Iz tog razloga su tri navedena algoritma odabrana jer su već dokazani kao pouzdani u detekciji mrežnih napada. Ova tri algoritma se mogu čak i dodatno optimizovati za bolje performanse [1]. Prilikom kreiranja ovog rešenja nisu izvršene modifikacije izvornih algoritama jer svakako i u svom izvornom obliku su dovoljno dobri da bi pokazali efikasnost predložene metode. Čak i kada jedan od njih zakaže prilikom detekcije, predloženo rešenje će to nadomestiti sa druga dva algoritma i dokazati efikasnost ovog metoda.



Slika 7: TMR - prikaz sistema većinskog odlučivanja

U prikazu algoritma 1 i slike 7 može se videti da se izlazne vrednosti algoritama CUSUM, EWMA i KNN porede kako bi se pronašle dve jednake vrednosti. Moguće izlazne vrednosti su 0 i 1 koje ukazuju da li je napad detektovan ili ne. U prvoj iteraciji porede se izlazne vrednosti CUSUM i EWMA algoritma, ako su te dve vrednosti jednake onda je izlazna vrednost trostruke modularne redundanse ista kao i u slučaju CUSUM algoritma. Ako su različite, sledeće poređenje se radi između CUSUM i KNN algoritma koje će i dati konačni rezultat. Ako je izlazna vrednost KNN algoritma jednaka izlaznoj vrednosti CUSUM algoritma onda je izlazna vrednost trostruke modularne redundanse ista kao i u slučaju CUSUM algoritma. Ako je vrednost različita, uzima se izlazna vrednost EWMA ili KNN algoritma kao izlazna vrednost trostruke modularne redundanse. EWMA ili KNN vrednosti se uzimaju u ovom slučaju jer su obe vrednosti različite od CUSUM vrednosti, a to je upravo ono što i treba da se dogodi, da većinsko glasanje odlučuje odnosno 2 glasa prema 1.

Algoritam 1: Primena TMR algoritma za okidanje alarma u IDS sistemu

Ulaz: Ulaz-CUSUM, Ulaz-EWMA, Ulaz-KNN.

Izlaz: IZLAZNA VREDNOST-TMR.

Izvrši ALGORITAM-CUSUM (*IZLAZNA VREDNOST-CUSUM*)

Izvrši ALGORITAM-EWMA (*IZLAZNA VREDNOST-EWMA*)

Izvrši ALGORITAM-KNN (*IZLAZNA VREDNOST-KNN*)

```
if IZLAZNA VREDNOST-CUSUM = IZLAZNA VREDNOST-EWMA then
    IZLAZNA VREDNOST-TMR = IZLAZNA VREDNOST-CUSUM;
else
    if IZLAZNA VREDNOST-CUSUM = IZLAZNA VREDNOST-KNN then
        IZLAZNA VREDNOST-TMR = IZLAZNA VREDNOST-CUSUM;
    else
        IZLAZNA VREDNOST-TMR = IZLAZNA VREDNOST-EWMA;
```

4.2 Implementacija predloženog rešenja

Predloženo rešenje je isprogramirano u Python programskom jeziku. Python je odabran zbog svoje lakoće korišćenja kao i zbog brojnih biblioteka otvorenog koda za rukovanje mrežnim saobraćajem, između ostalog i korišćeni algoritmi su jedna od tih opcija, kao i veliki broj biblioteka za alarmiranje koje je jedna od ključnih karakteristika u svakom IDS sistemu. Python biblioteke koje se koriste su sledeće:

- Pandas [65] je Python biblioteka koja se koristi uglavnom za rukovanje podacima i njihovu analizu. Omogućava jednostavan rad sa skupovima

podataka u bilo kom formatu (npr. Excel, CSV, SQL), prevodeći ih u takovzane okvire koji predstavljaju tabelarnu, odnosno matričnu strukturu podataka. Pandas biblioteka sadrži i EWMA algoritam koji se koristi u predloženom rešenju

- Detecta [66] je Python biblioteka namenjena za detekciju promena i analizu vremenskih serija. Koristi se kada je potrebno identifikovati trenutke u kojima dolazi do naglih promena u podacima kao što su na primer skokovi u srednjoj vrednosti. Ova biblioteka uključuje i CUSUM algoritam koji se koristi u predloženom rešenju

- SciKit [67] je Python biblioteka za mašinsko učenje i zasnovana je na bibliotekama NumPy [68] i SciPy [69]. Koristi se za kreiranje modela mašinskog učenja, analizu podataka i predviđanje (predikciju). Pruža alate za klasične algoritme mašinskog učenja, a jedan od tih je i KNN algoritam koji se koristi u predloženom rešenju.

- Matplotlib [70] je Python biblioteka koja se koristi za vizualizaciju podataka. Omogućava kreiranje i prikaz različitih grafikona kako i optimizaciju njihovog prikaza. Ova biblioteka je odabrana za prikaz grafikona zbog lake kontrole oznaka, boja i legendi kao i mogućnosti čuvanja grafikona kao slike.

Pregled koda 1 pokazuje praktičnu primenu predloženog metoda u programskom jeziku Python. Nakon inicijalnog učitavanja datoteke koja sadrži prethodno obrađene podatke o napadu, podešavaju se granične vrednosti kao i dodatni parametri za CUSUM i EWMA algoritme. Zatim se pozivaju funkcije za izračunavanje vrednosti za svaki od algoritama pojedinačno kao i za iscrtavanje grafikona. Poslednja stavka jeste čuvanje dobijenih rezultata u CSV fajl. Ono što nije prikazano ovde jeste faza obučavanja KNN algoritma koja se izvršava u drugoj datoteci.

Programski kod 1: Python skripta

```
import pandas as pd
from ewma import calculate_ewma
from cusum import calculate_cusum
from knn import calculate_knn
from draw_plots import draw_alarm_plots

FILE_NAME = 'FINAL_data.csv'
THRESHOLD_CUMSUM = 100
THRESHOLD_EWMA = 100
DRIFT = 20
WINDOW_SIZE_EWMA = 20

data = pd.read_csv('data_files/' + FILE_NAME)
draw_alarm_plots(data, 'Attack', FILE_NAME)

names = [calculate_knn(data),
        calculate_ewma(data, threshold=THRESHOLD_EWMA,
            window_size=WINDOW_SIZE_EWMA),
        calculate_cusum(data, threshold=THRESHOLD_CUMSUM, drift=DRIFT)]

for name in names:
    draw_alarm_plots(data, name, FILE_NAME)

data['TMR Alarm'] = 0

for i in range(0, len(data['TMR Alarm'])):
    if((data[names[0]].at[i] == 1 and data[names[1]].at[i] == 1) or
            (data[names[0]].at[i] == 1 and data[names[2]].at[i] == 1) or
            (data[names[1]].at[i] == 1 and data[names[2]].at[i] == 1)):
        data['TMR Alarm'].at[i] = 1

draw_alarm_plots(data, 'TMR Alarm', FILE_NAME)
data.to_csv('results/'+FILE_NAME)
```

Za rukovanje podacima korišćen je i R statistički paket koji služi za obradu skupova podataka odnosno za kreiranje vremenskih serija koje se koriste u daljem procesu. Svi podaci koji su prikazani su prvobitno obrađeni korišćenjem sistema R i njegovih biblioteka, pa su nakon toga podaci struktuirani u CSV format obrađeni sa Python skriptom kako bi se dobili konačni rezultati. R biblioteke koje se koriste su sledeće:

- Ggplot2 [71] je R biblioteka često korišćena za vizualizaciju podataka u R-u. Korisna je za prikaz raznih tipova grafikona, a neki od njih se mogu i videti na slikama 4 i 5.
- Stringr [72] je R biblioteka za rukovanje tekstualnim podacima (eng. strings), pruža jednostavne funkcije za operacije kao što su dopisivanje, razdvajanje, zamena i pretraživanje sa podrškom za regularne izraze (eng. RegEx).
- Frequency [73] je R biblioteka koja se koristi za analizu učestalosti elemenata u podacima, pomaže u kreiranju tabel učestalosti kako i u vizualizaciji ponovljenih vrednosti u skupovima podataka. Najčešće se koristi u analizi tekstualnih podataka.
- Dplyr [74] je jedna od najbitnijih biblioteka za rukovanje podacima u R-u. Omogućava jednostavne i efikasne operacije kao što su filtriranje, sortiranje, grupisanje i agregacija podataka.
- Data.table [75] je vrlo efikasna R biblioteka za rad sa velikim skupovima podataka. Pruža efikasne funkcije za filtriranje, grupisanje i agregaciju podataka, pri čemu nudi sintaksu sličnu upitnim jezicima nad bazama podataka, sa fokusom na brzinu i memorijsku optimizaciju.

R skripta 2 pokazuje obradu datoteke koja sadrži podatke o napadu. Tom prilikom se kreiraju vremenske serije u intervalima od po jedne sekunde, i takođe se sumira broj mrežnih paketa u zavisnosti da li su maliciozni ili ne. Na osnovu tih podataka se određuje da li se u jednoj vremenskoj seriji dogodio napad ili ne. Takođe isrtava se i grafikon koji vizualizuje tok mrežnog saobraćaja. Cilj ove obrade jeste da se obradom kreira datoteka spremna za korišćenje u Python skripti 1.

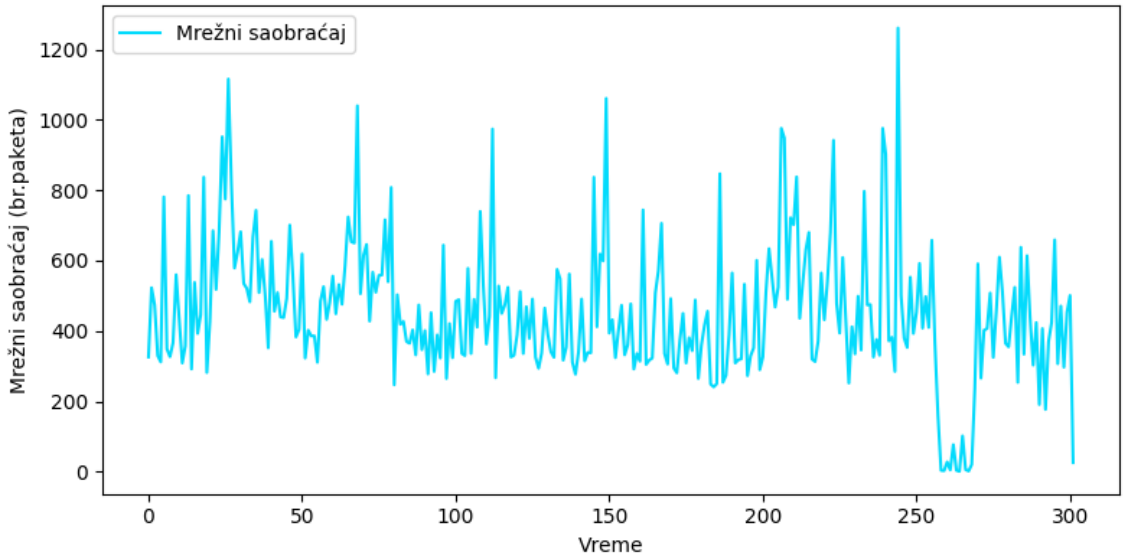
Programski kod 2: R skripta

```
setwd('C:/Users/User/Desktop')
library(ggplot2)
library(lattice)
library(stringr)
library(frequency)
library(dplyr)
ds <- read.csv("UDP_attack.csv", stringsAsFactors=TRUE, header=T)

ds$Time <- as.numeric(as.POSIXct(ds$Time))
minimum = min(ds$Time, na.rm = FALSE)
ds$Time = ds$Time - minimum
Tmax = ((floor(max(ds$Time, na.rm = TRUE)) + 5)/10)*10
ds_Packets = data.frame(ds$Time, 1, 1, ds$Label, 0, 0)
colnames(ds_Packets)=c("Time", "Time1", "nrPack", "Label", "UDP",
    "Attack")
ds_Packets$UDP <- ifelse(ds_Packets$Label %in% c("UDP"), 1, 0)
ds_Packets$Attack <- ifelse(ds_Packets$Label %in% c("MSSQL", "BENIGN"),
    1, 0)
ds_Packets$Time1 = (ds_Packets$Time %/% 1) * 1
ds_final = aggregate(ds_Packets$nrPack, by=list(ds_Packets$Time1),
    FUN=sum, na.rm=TRUE)
ds_final2 = aggregate(ds_Packets$UDP, by=list(ds_Packets$Time1), FUN=sum,
    na.rm=TRUE)
ds_final3 = aggregate(ds_Packets$Attack, by=list(ds_Packets$Time1),
    FUN=sum, na.rm=TRUE)
colnames(ds_final)=c("Time", "Packets")
colnames(ds_final2)=c("Time", "Attack")
colnames(ds_final3)=c("Time", "NotAttack")
finalDS <- data.frame("Time" = ds_final$Time,
                "Packets" = ds_final$Packets,
                "Attack" = ifelse(ds_final2$Attack > ds_final3$NotAttack,
                    1, 0))

plot(finalDS$Time, finalDS$Packets, main = "Packets/Time",
     xlab = "Time", ylab = "Number of Packets" , xlim=c(0,Tmax), type =
         "l",
     frame = FALSE)
write.csv(finalDS,file="FINAL_data.csv")
```

Sve navedene biblioteke za R i Python su korisne za obradu i vizualizaciju velikih skupova podataka. Mrežni saobraćaj koji se koristi obično sadrži veliku količinu podataka koje je potrebno efikasno obraditi u realnom vremenu u slučaju IDS sistema.

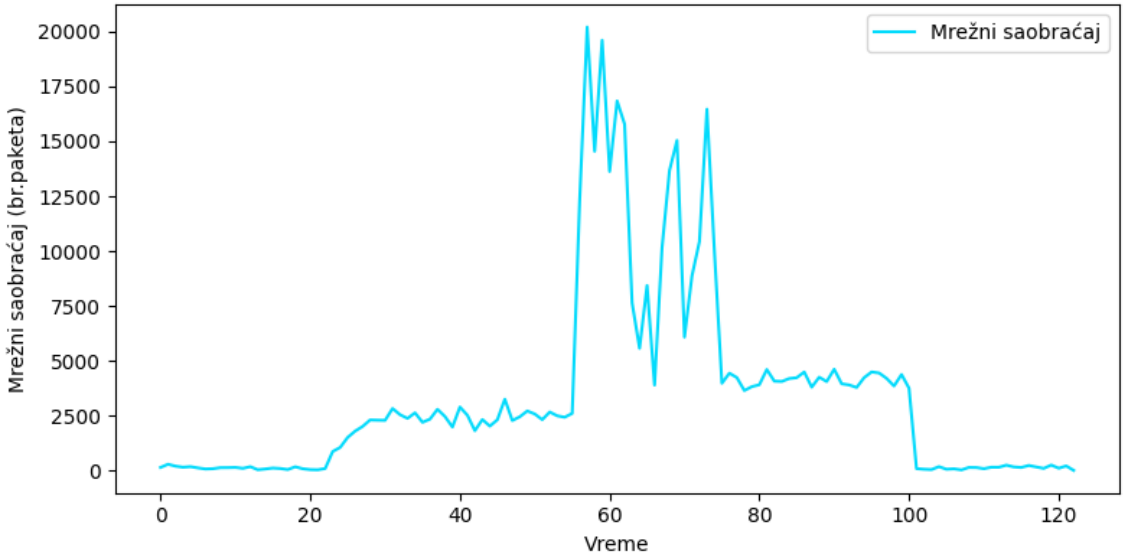
4.2.1 Modelovanje saobraćaja

Na slici 8 je prikazan mrežni saobraćaj koji ne sadrži napad. Za ovaj uzorak normalnog mrežnog saobraćaja je iskorišćen skup podataka „IoT Network Intrusion“ [62] a naziv datoteke koja je obrađena u svrhu prikaza podataka je *bening-dec.pcap*.



Slika 8: Mrežni saobraćaj bez napada

Na slici 9 je prikazan mrežni saobraćaj koji sadrži napad tipa UDP flooding. Na prikazanom grafikonu jasno se može uočiti razlika između uobičajenog mrežnog saobraćaja i saobraćaja koji je generisan kao posledica napada. Razlika u broju paketa je velika, vrednost broja paketa po sekundi ide i do 20000 što je značajno više od uobičajenog broja paketa. Za ovaj uzorak mrežnog saobraćaja koji sadrži napad iskorišćen je skup podataka „IoT Network Intrusion“ [62] a naziv datoteke koja je obrađena u svrhu prikaza podataka je *mirai-udpflooding-1-dec.pcap*.



Slika 9: Mrežni saobraćaj sa napadom tipa UDP flooding

Kod modelovanja saobraćaja može se diskutovati i o koherentnosti podataka. Kada se izvrši detaljnija analiza mrežnog saobraćaja te se umesto posmatranja broja paketa u vremenu, posmatra broj paketa po konekciji, dolazi se do zaključka da je broj IP adresa odnosno konekcija takođe veoma bitan faktor u određivanju da li je došlo do napada ili ne [1]. Posmatrajući uobičajeni mrežni saobraćaj u odnosu na mrežni saobraćaj koji sadrži napad uočava se da je broj IP konekcija veći ali da je broj paketa po konekciji manji kod DDoS napada. To je iz razloga što se koristi distribuirana mreža za izvođenje napada, odnosno veliki broj računara sa različitih lokacija a samim tim i različitih IP adresa. Kod regularnih konekcija obično se događa razmena većeg broja paketa između dve mreže ili računara, dok kod napada to nije slučaj.

4.3 Konačni rezultati

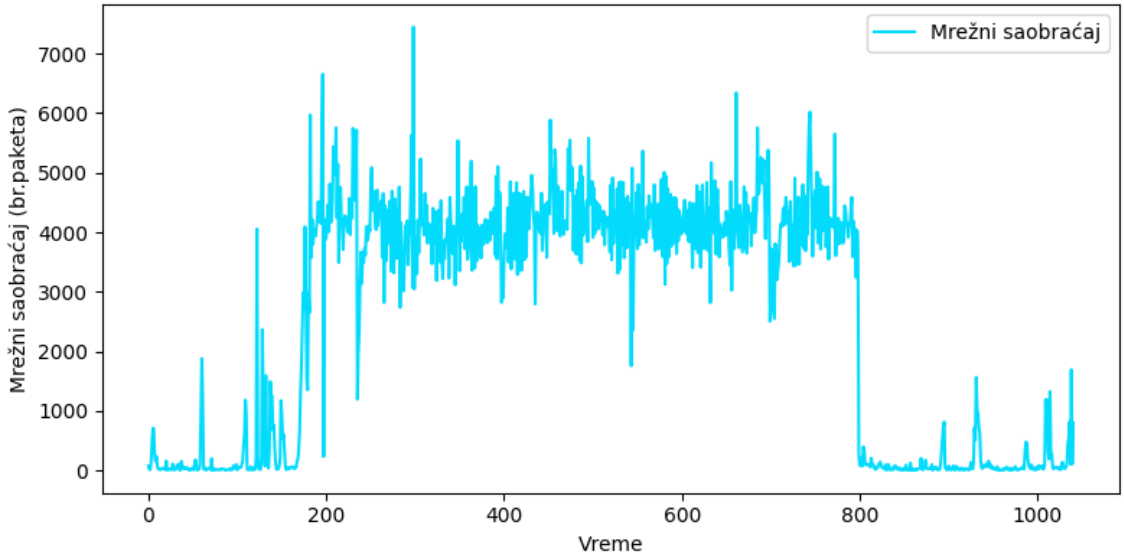
Tri algoritma EWMA, CUSUM i KNN su testirani na različitim skupovima podataka, a kako bi se pokazale prednosti predloženog rešenja. Za testiranje i validaciju rezultata korišćena su 3 skupa podataka iz kojih su iskorišćene četiri datoteke sa snimljenim mrežnim saobraćajem koje sadrže napade. Kako bi se izvršilo poređenje kreirane su vremenske serije od po jedne sekunde i obeležene su vremenske serije kada se napad dogodio [1].

Nakon obeležavanja vremenskih serija kada se napad dogodio izmerene su vrednosti za tačnost, preciznost, F1 meru i odziv za svaki od tri odabrana algoritma, kako bi se algoritmi uporedili međusobno i kako bi se pokazala njihova efikasnost na datim podacima. Na kraju su dobijeni rezultati kombinovani sa algoritmom TMR kako bi se dobio najbolji mogući rezultat. Za svaki skup podataka je ponovljen isti proces i kreirani su odgovarajući grafikoni kako bi se pokazalo prethodno navedeno.

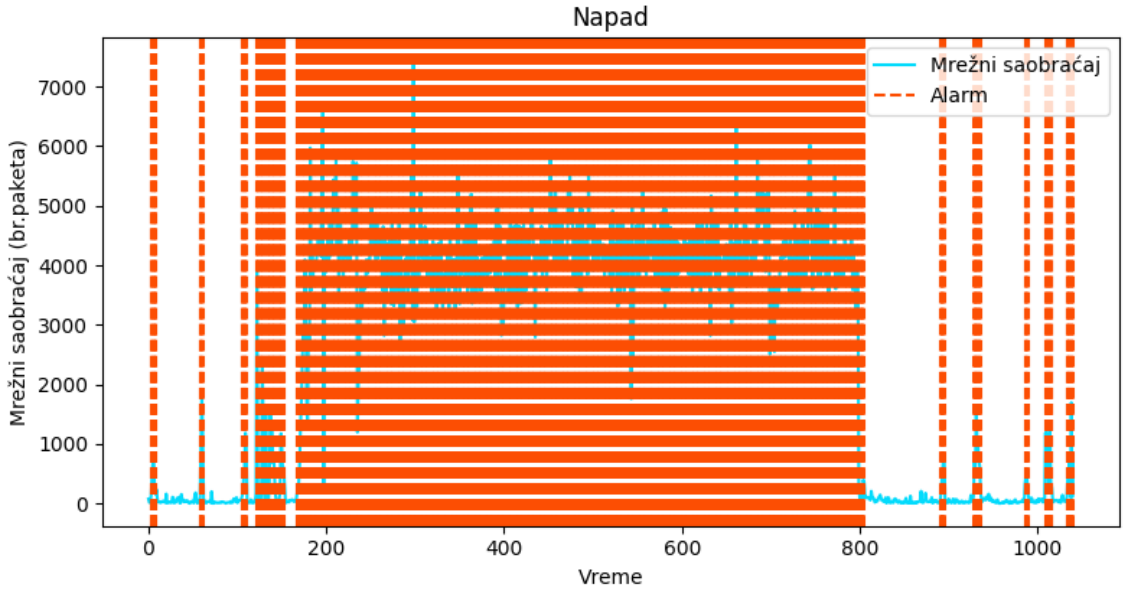
Za dobijanje vrednosti za tačnost, preciznost, F1 meru i odziv prethodno je bilo potrebno odrediti prag detekcije. Prag u IDS sistemima se određuje analizom ulaznih podataka koji sadrže kako normalne tako i maliciozne mrežne aktivnosti. Neophodno je najpre odrediti mere odstupanja od uobičajenog obrasca ponašanja, poput učestalosti događaja ili obrazaca u mrežnom saobraćaju. Statističkom analizom tih podataka, definiše se prag koji razdvaja normalni mrežni saobraćaj od saobraćaja koji sadrži napad. Prilikom analize korišćenih skupova podataka definisan je prag za svaki skup podataka ponaosob na osnovu pređašnjeg iskustva kao i potreba predloženog rešenja. Ti pragovi su zatim testirani i validirani nad korišćenim podacima u cilju dobijanja optimalnih rezultata.

Prva datoteka koja je obrađena je iz skupa podataka CIC-IDS2017 [60] pod nazivom *Friday-WorkingHours.pcap*.

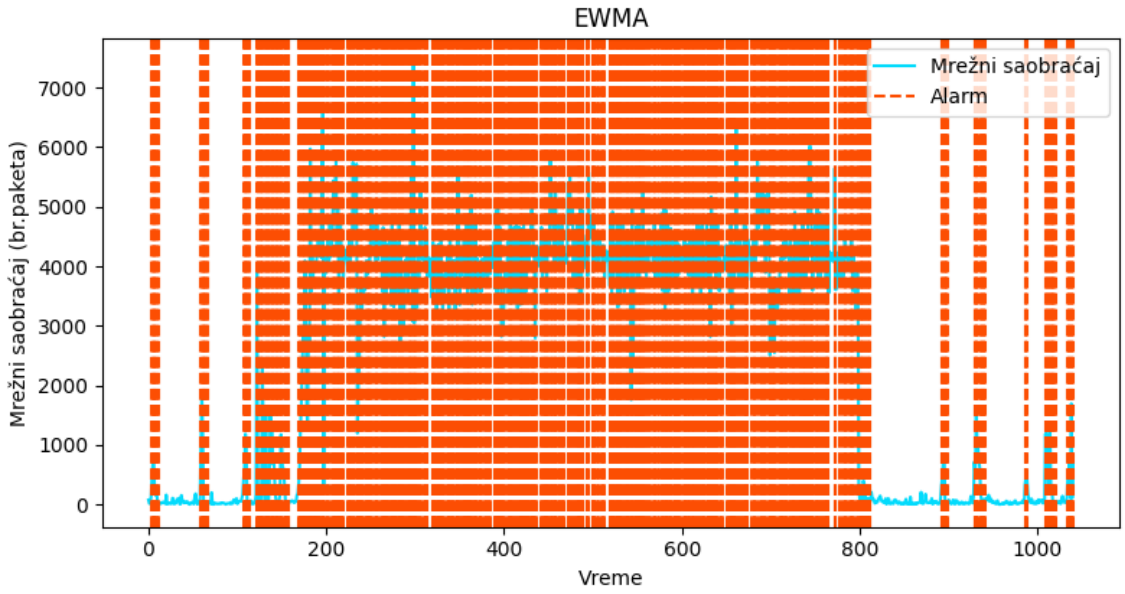
Na slici 10 se može videti grafikon napada, dok se na slici 11 vidi isti grafikon ali sa napadom označenim crvenom bojom. Zatim slede grafikoni na slikama 12, 13 i 14 i to redom za EWMA, CUSUM i KNN algoritme koji predstavljaju funkcionisanje navedenih algoritama na ovom konkretnom skupu podataka. Poslednji grafikon je prikazan na slici 15 koji prikazuje kako TMR funkcioniše na zadatom skupu, dok su u tabeli 5 prikazani i dobijeni numerički rezultati.



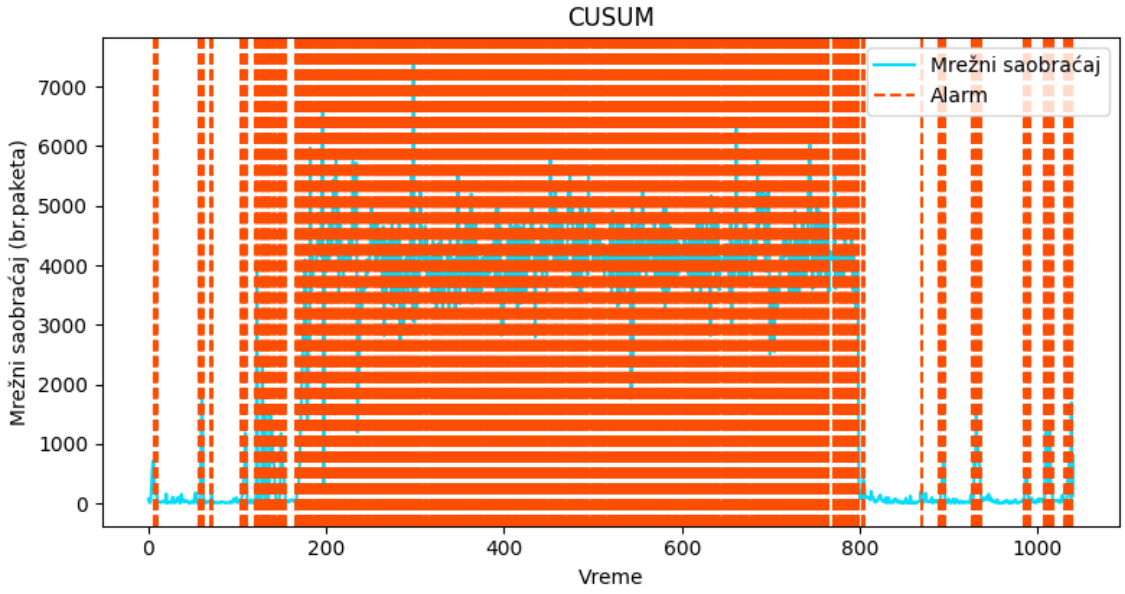
Slika 10: Friday-WorkingHours - Mrežni saobraćaj sa napadom



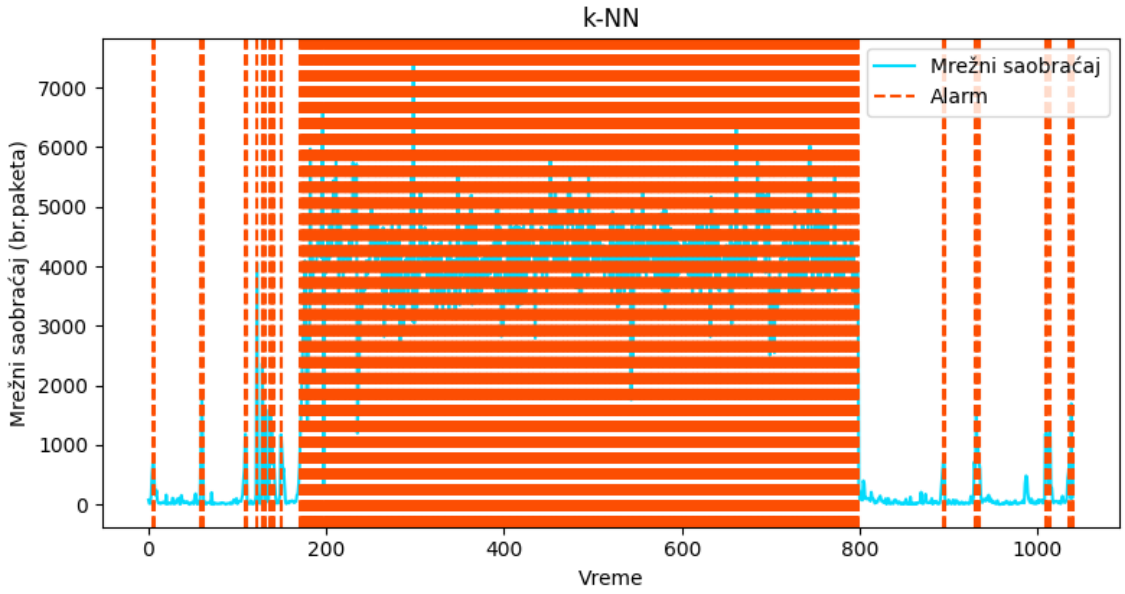
Slika 11: Friday-WorkingHours - Obeležen napad



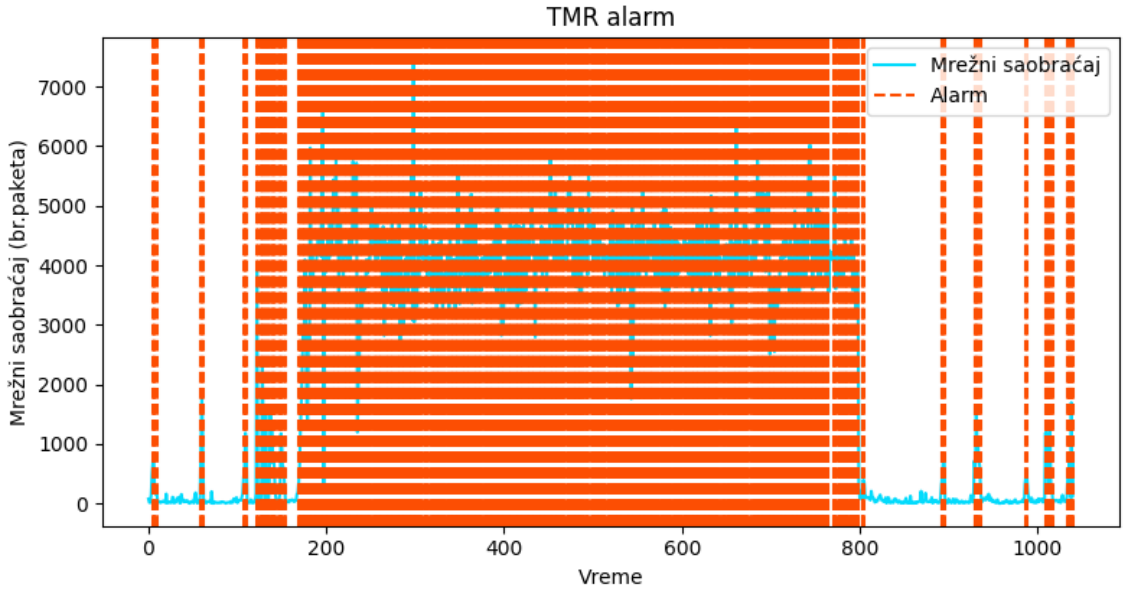
Slika 12: Friday-WorkingHours - Primenjen EWMA algoritam (za vrednost praga 150, i vrednost težinskog faktora α 0.20)



Slika 13: Friday-WorkingHours - Primenjen CUSUM algoritam (za vrednost praga 150, i vrednost odstupanja 25)



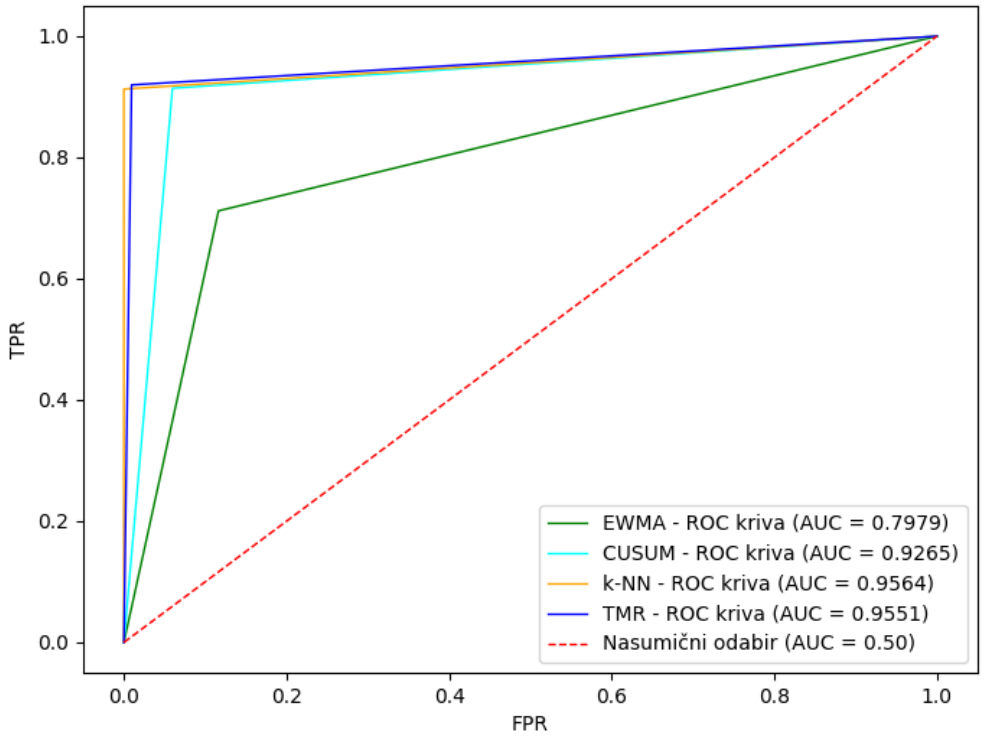
Slika 14: Friday-WorkingHours - Primenjen KNN algoritam



Slika 15: Friday-WorkingHours - Primenjen TMR algoritam

Tabela 5: Friday-WorkingHours evaluacija rezultata

TMR			
TP	665	**Tačnost**	0,9414
TN	315	**F1**	0,9561
FP	3	**Preciznost**	0,9955
FN	58	**Odziv**	0,9197
-	-	**ROC (AUC)**	0,9551
CUSUM			
TP	660	**Tačnost**	0,9212
TN	299	**F1**	0,9415
FP	19	**Preciznost**	0,9720
FN	63	**Odziv**	0,9128
-	-	**ROC (AUC)**	0,9265
EWMA			
TP	515	**Tačnost**	0,7646
TN	281	**F1**	0,8078
FP	37	**Preciznost**	0,9329
FN	208	**Odziv**	0,7123
-	-	**ROC (AUC)**	0,7979
KNN			
TP	660	**Tačnost**	0,9394
TN	318	**F1**	0,9544
FP	0	**Preciznost**	1
FN	63	**Odziv**	0,9128
-	-	**ROC (AUC)**	0,9564



Slika 16: Friday-WorkingHours - ROC krive sa iskazanim AUC vrednostima

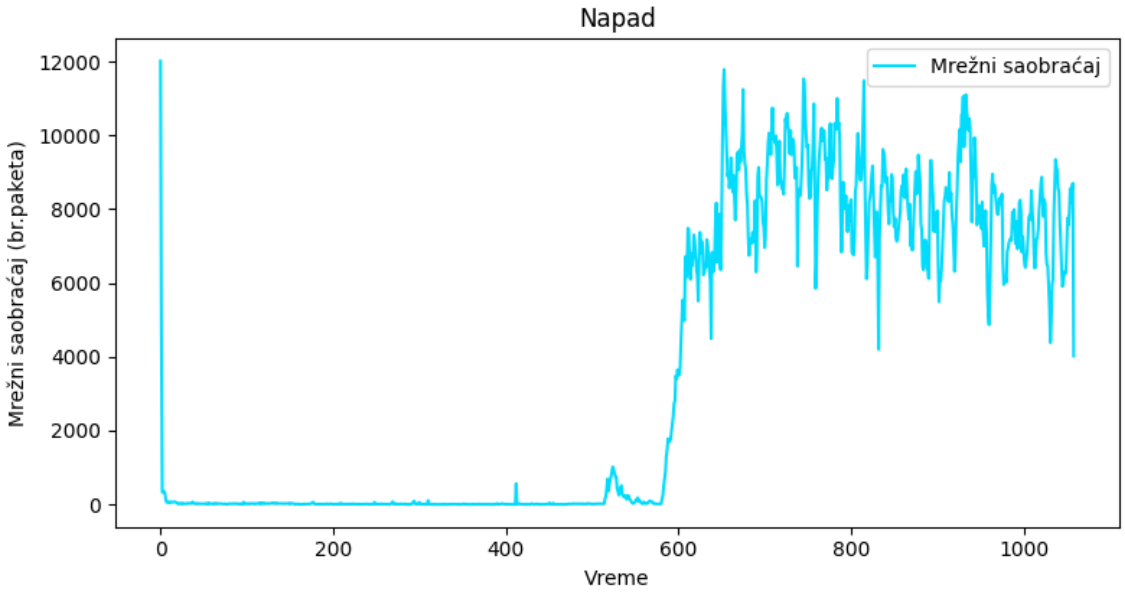
Na slici 16 prikazane su ROC krive za algoritme EWMA, CUSUM, KNN i za predloženi TMR metod nad obrađenom datotekom Friday-WorkingHours. U ovom primeru AUC vrednost za TMR je manje za 0.0013 od vrednosti za KNN.

Prag detekcije od 150 je postavljen na osnovu broja paketa u sekundi u trenutku kada napad počinje. Identifikovana je tačka gde vrednosti značajno odstupaju od broja paketa normalnog saobraćaja. Normalni broj paketa u sekundi se nalazi u opsegu od 1 do 100, a tokom napada naglo raste na preko nekoliko hiljada. Prag je definisan kao vrednost koja je za 50% veća od gornje granice normalnog broja paketa. Vrednost odstupanja od 25 za CUSUM algoritam je postavljena na osnovu analize normalnih oscilacija podataka, tako da se razlikuju uobičajene varijacije od većih promena. Takođe težinski faktor α od 0,20 je postavljen tako da balansira između brzine reakcije na promene i stabilnosti. Sve vrednosti su validirane testiranjem nad podacima.

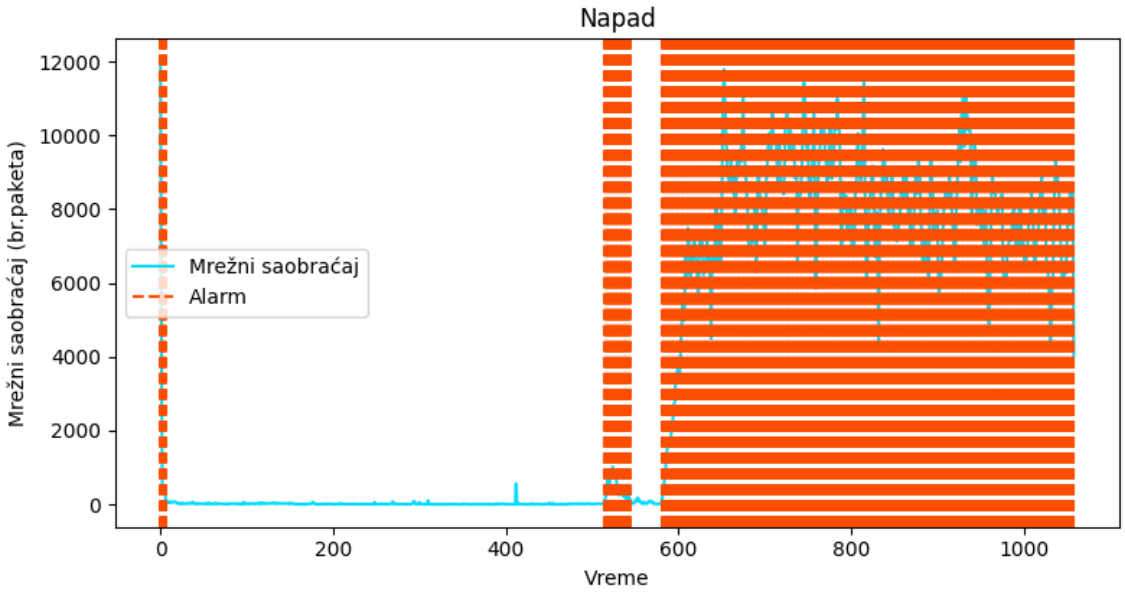
Sledeći napad koji je obrađen je iz skupa podataka CIC-IDS2019 [61] i nalazi se u datoteci pod nazivom *UDP.csv*.

Na slici 17 se može videti grafikon napada, dok se na slici 18 vidi isti grafikon ali

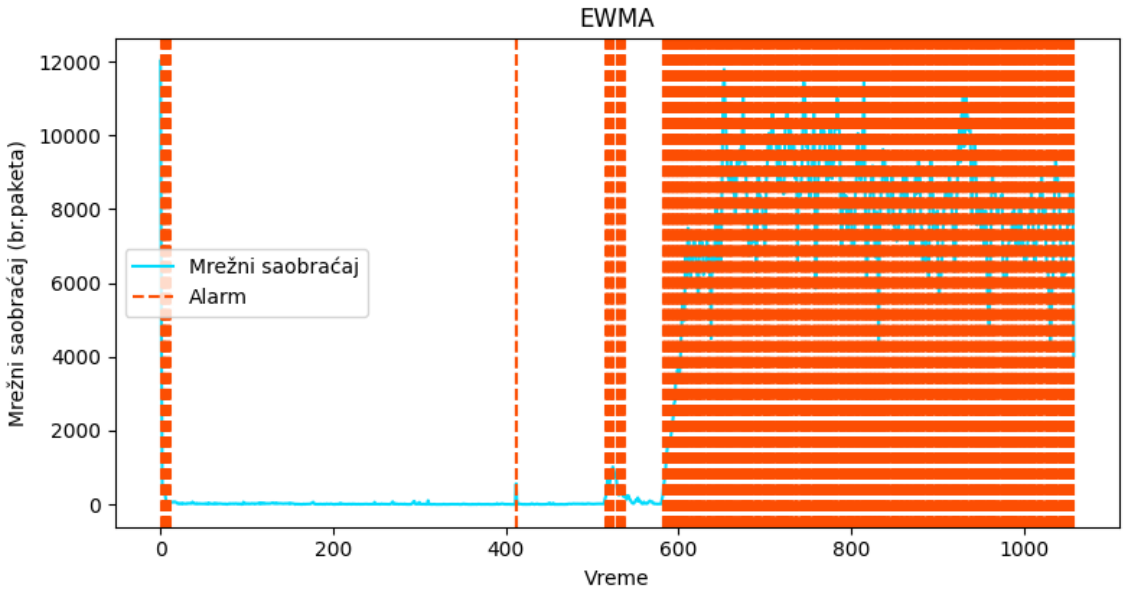
sa napadom označenim crvenom bojom. Zatim slede grafikoni na slikama 19, 20 i 21 i to redom za EWMA, CUSUM i KNN algoritme koji predstavljaju funkcionisanje navedenih algoritama na ovom konkretnom skupu podataka. Poslednji grafikon je prikazan na slici 22 koji prikazuje kako TMR funkcioniše na zadatom skupu, dok su u tabeli 6 prikazani i dobijeni numerički rezultati.



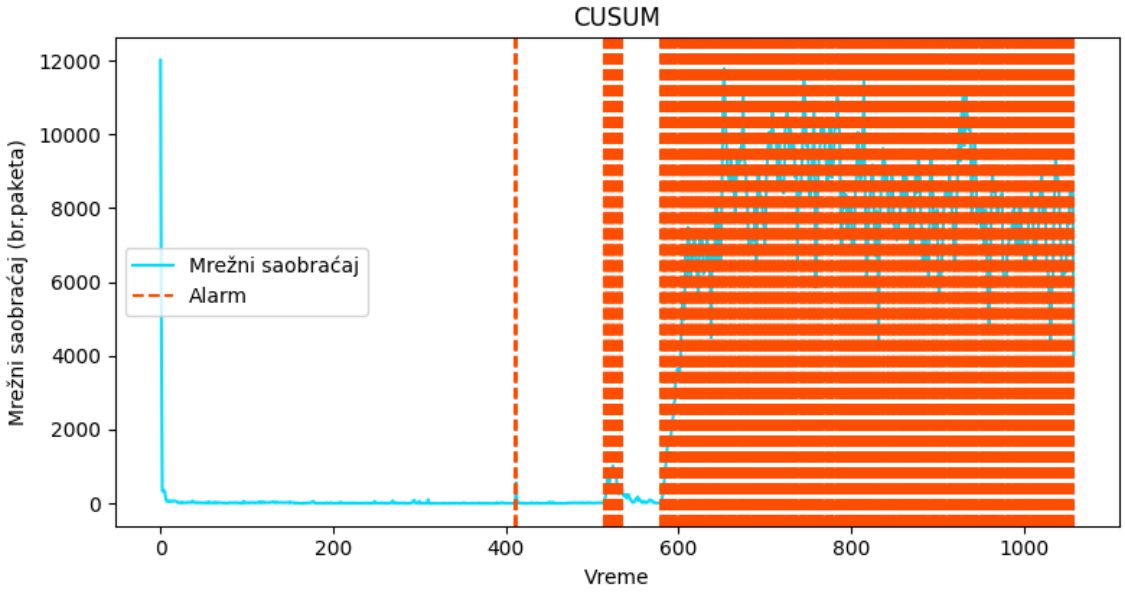
Slika 17: UDP - Mrežni saobraćaj sa napadom



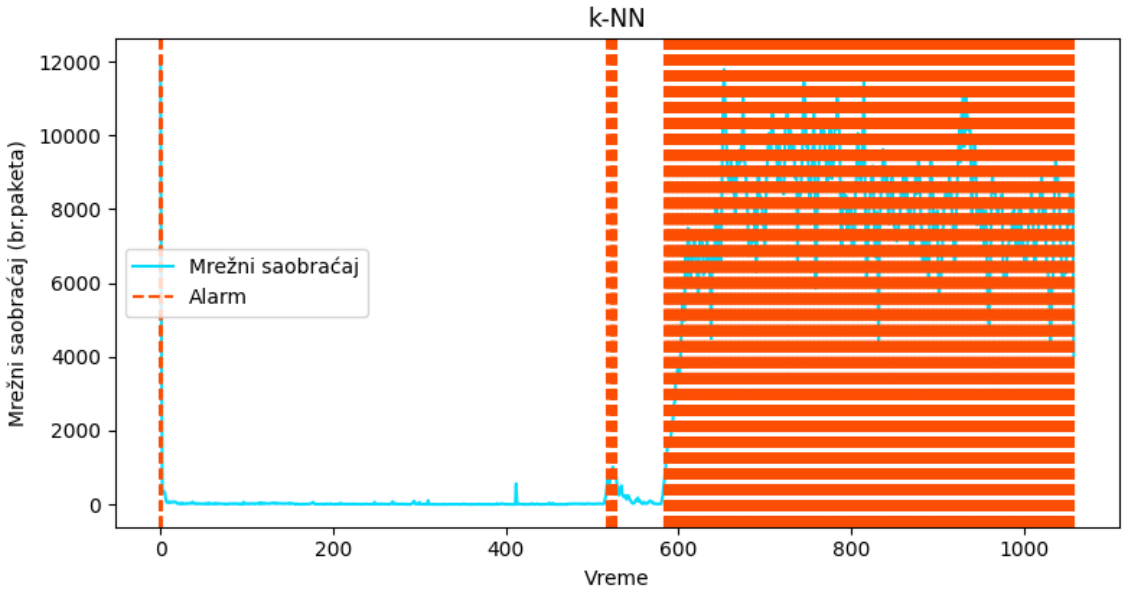
Slika 18: UDP - Obeležen napad



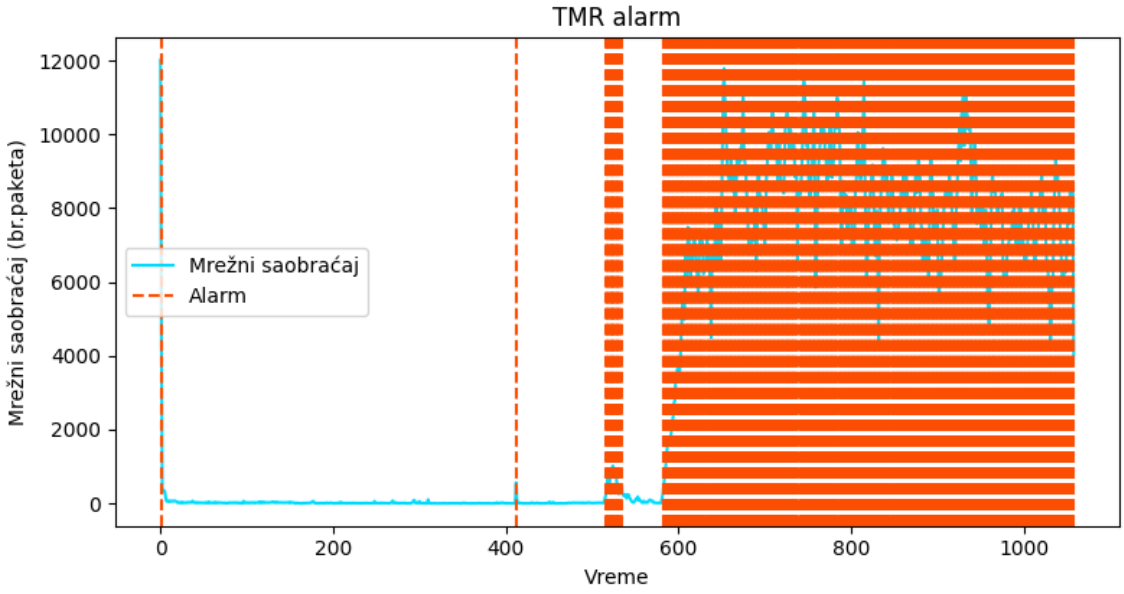
Slika 19: UDP - Primenjen EWMA algoritam (za vrednost praga 100, i vrednost težinskog faktora α 0.30)



Slika 20: UDP - Primenjen CUSUM algoritam (za vrednost praga 136, i vrednost odstupanja 30)



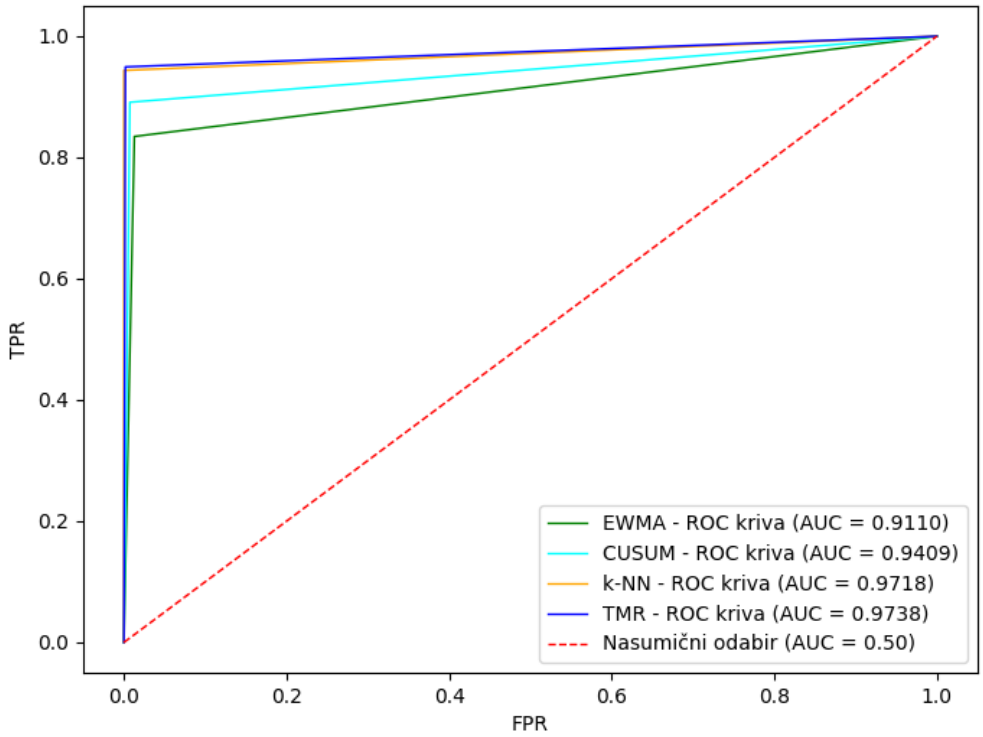
Slika 21: UDP - Primenjen KNN algoritam



Slika 22: UDP - Primenjen TMR algoritam

Tabela 6: UDP evaluacija rezultata

TMR			
TP	489	**Tačnost**	0,9745
TN	549	**F1**	0,9731
FP	1	**Preciznost**	0,9979
FN	26	**Odziv**	0,9495
-	-	**ROC (AUC)**	0,9738
CUSUM			
TP	458	**Tačnost**	0,9423
TN	540	**F1**	0,9375
FP	4	**Preciznost**	0,9913
FN	57	**Odziv**	0,8893
-	-	**ROC (AUC)**	0,9409
EWMA			
TP	430	**Tačnost**	0,9131
TN	537	**F1**	0,9033
FP	7	**Preciznost**	0,9839
FN	85	**Odziv**	0,8349
-	-	**ROC (AUC)**	0,9110
KNN			
TP	486	**Tačnost**	0,9726
TN	544	**F1**	0,9710
FP	0	**Preciznost**	1
FN	29	**Odziv**	0,9436
-	-	**ROC (AUC)**	0,9718



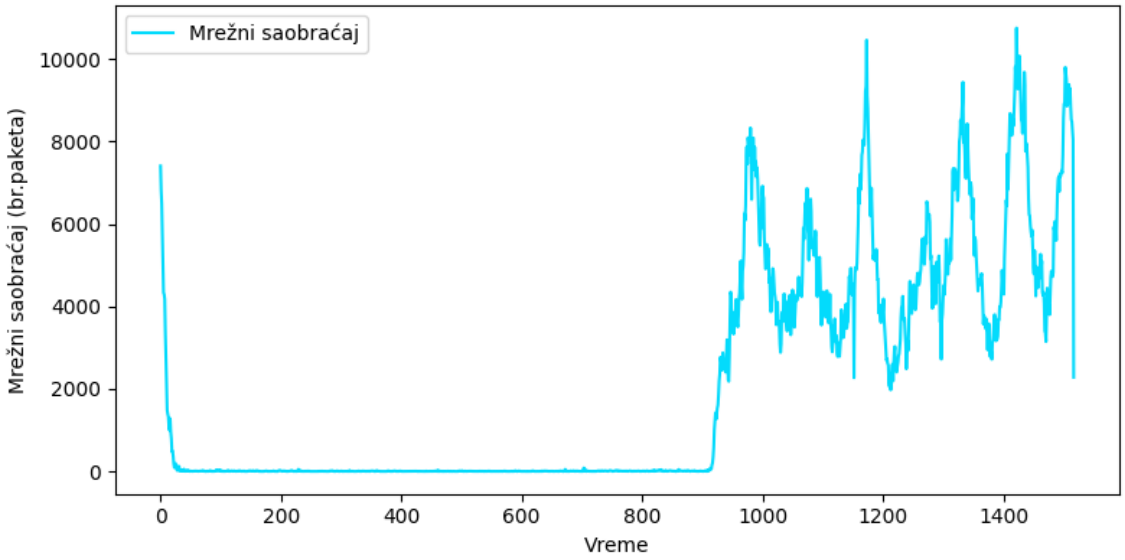
Slika 23: UDP - ROC krive sa iskazanim AUC vrednostima

Na slici 23 prikazane su ROC krive za algoritme EWMA, CUSUM, KNN i za predloženi TMR metod primenjen nad UDP napadom. U ovom primeru AUC vrednost za TMR je bolja od ostalih algoritama.

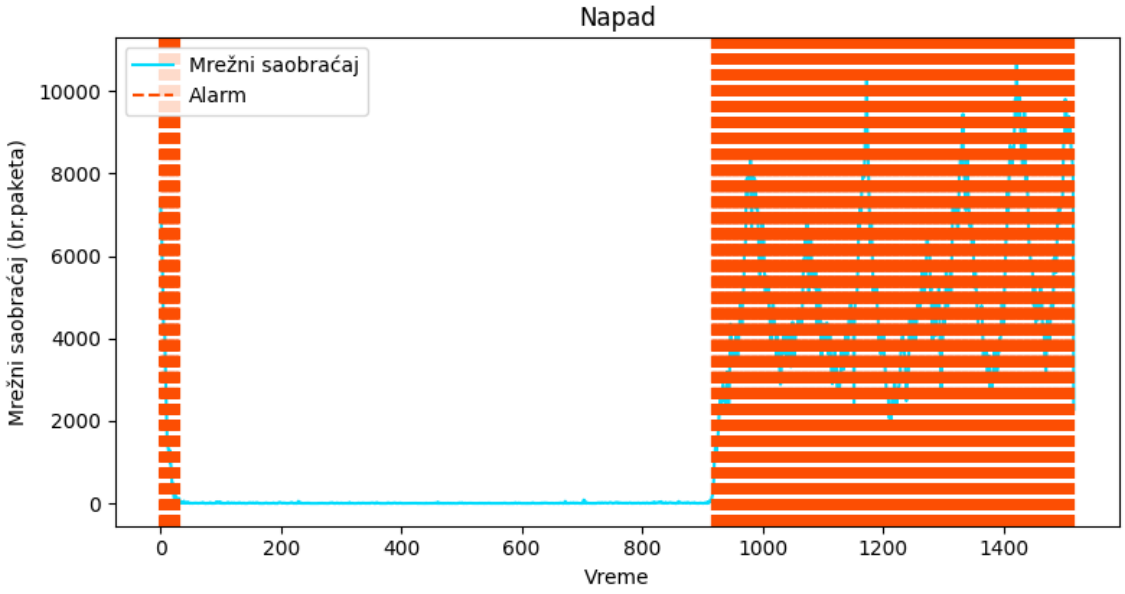
Pragovi detekcije od 100 i 136 su postavljeni na osnovu broja paketa u sekundi u trenutku kada napad počinje. Pragovi su različiti u ovom slučaju jer je testiranjem potvrđeno da se dobijaju bolji rezultati za CUSUM ako je prag 136. Obe vrednosti praga su odabrane tako da vrednosti koje značajno odstupaju od broja paketa normalnog saobraćaja budu veće. Normalni broj paketa u sekundi se nalazi u opsegu od 1 do 80 sa manjim odstupanjima, a tokom napada naglo raste i na preko 10.000. Prag je definisan kao vrednost koja je veća od gornje granice normalnog broja paketa. Vrednost odstupanja od 30 za CUSUM algoritam je postavljena na osnovu analize normalnih oscilacija podataka, tako da se razlikuju uobičajene varijacije od većih promena. Takođe težinski faktor α od 0,30 je postavljen tako da balansira između brzine reakcije na promene i stabilnosti. Sve vrednosti su validirane testiranjem nad podacima.

Sledeći napad koji je obrađen je iz skupa podataka CIC-IDS2019 [61] i nalazi se u datoteci pod nazivom *DrDoS_UDP.csv*.

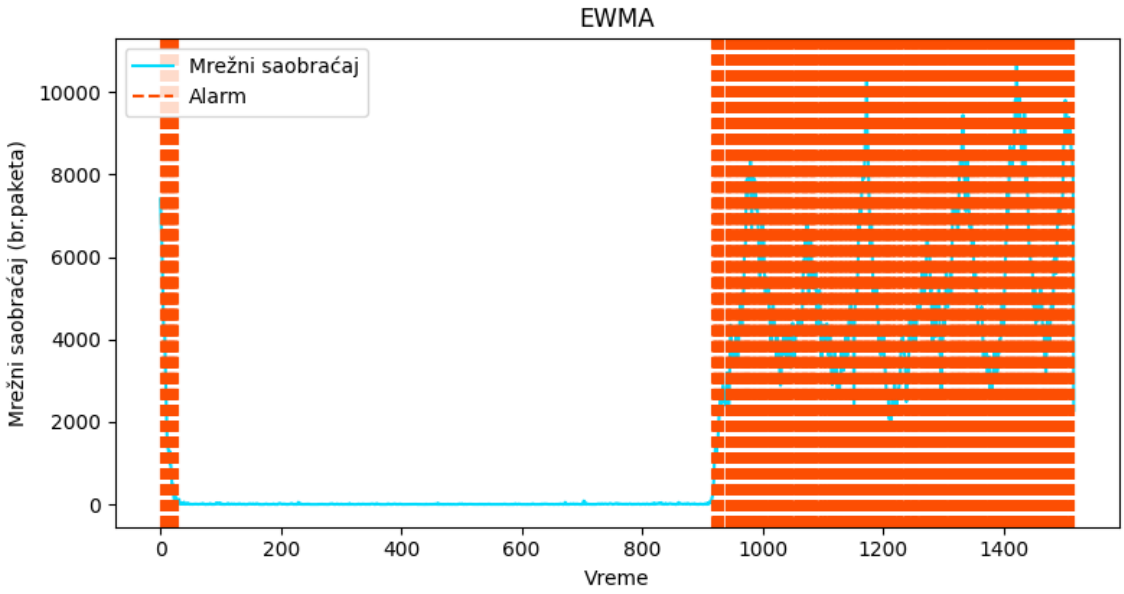
Na slici 24 se može videti grafikon napada, dok se na slici 25 vidi isti grafikon ali sa napadom označenim crvenom bojom. Zatim slede grafikoni na slikama 26, 27 i 28 i to redom za EWMA, CUSUM i KNN algoritme koji predstavljaju funkcionisanje navedenih algoritama na ovom konkretnom skupu podataka. Poslednji grafikon je prikazan na slici 29 koji prikazuje kako TMR funkcioniše na zadatom skupu, dok su u tabeli 7 prikazani i dobijeni numerički rezultati.



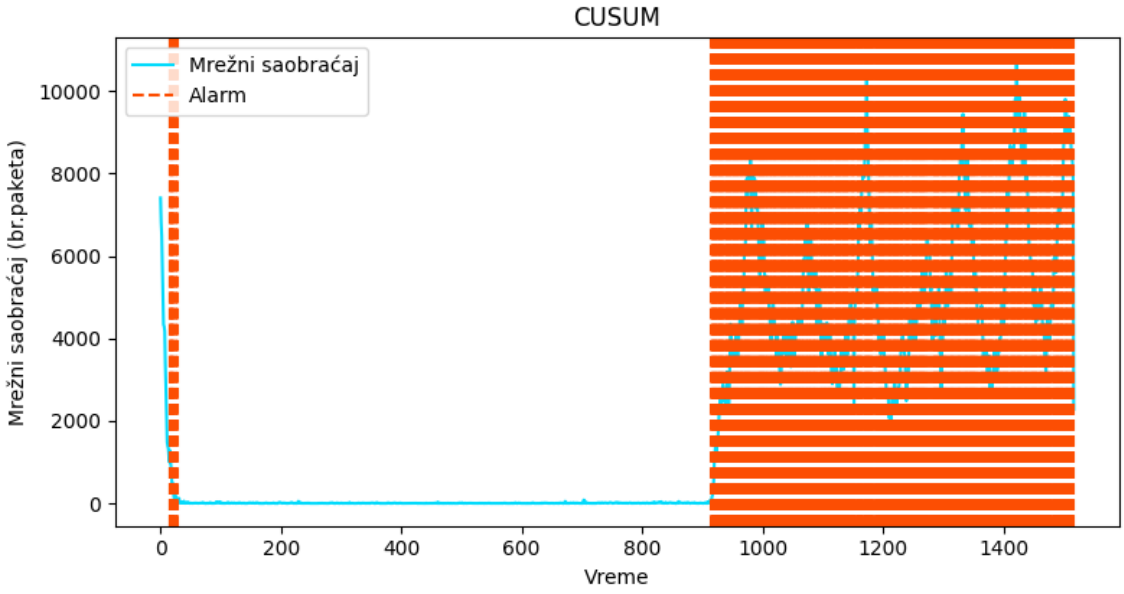
Slika 24: DrDoS_UDP - Mrežni saobraćaj sa napadom



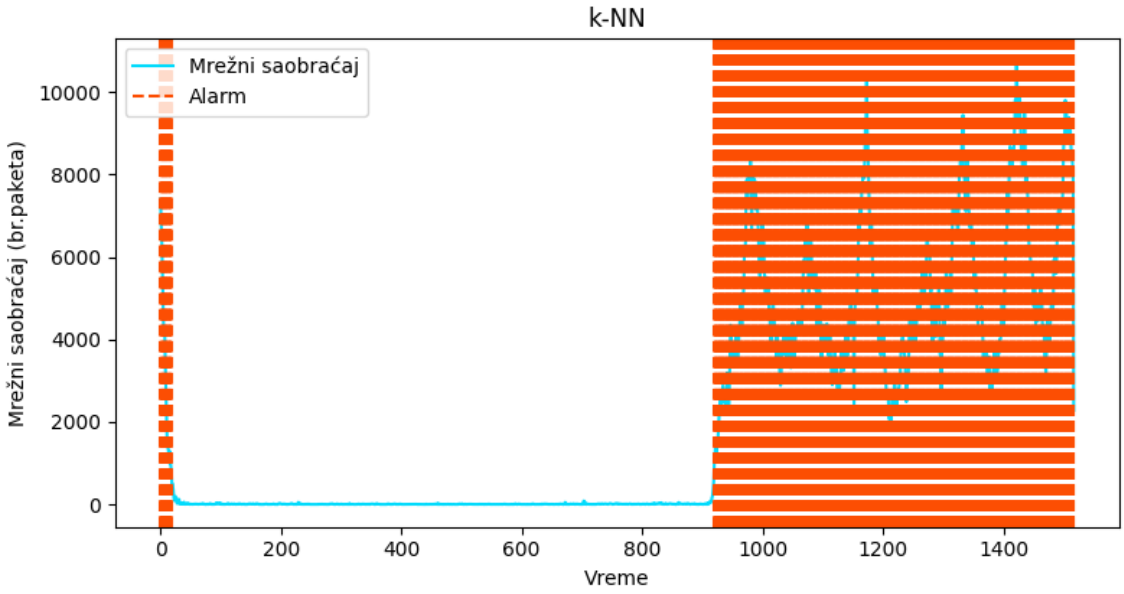
Slika 25: DrDoS_UDP - Obeležen napad



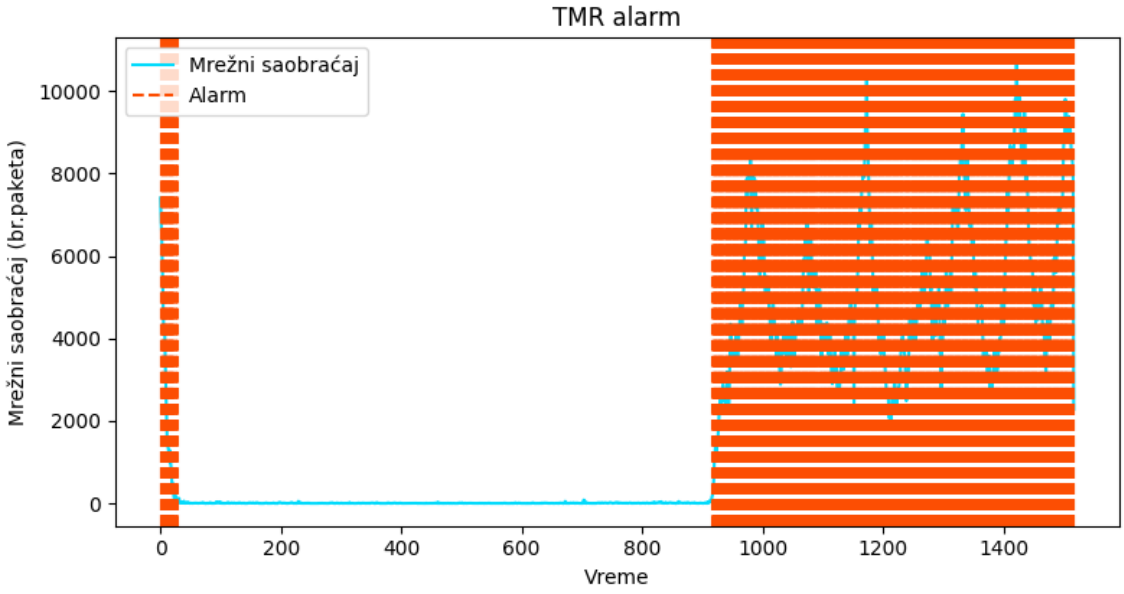
Slika 26: DrDoS_UDP - Primenjen EWMA algoritam (za vrednost praga 100, i vrednost težinskog faktora α 0.25)



Slika 27: DrDoS_UDP - Primenjen CUSUM algoritam (za vrednost praga 100, i vrednost odstupanja 20)



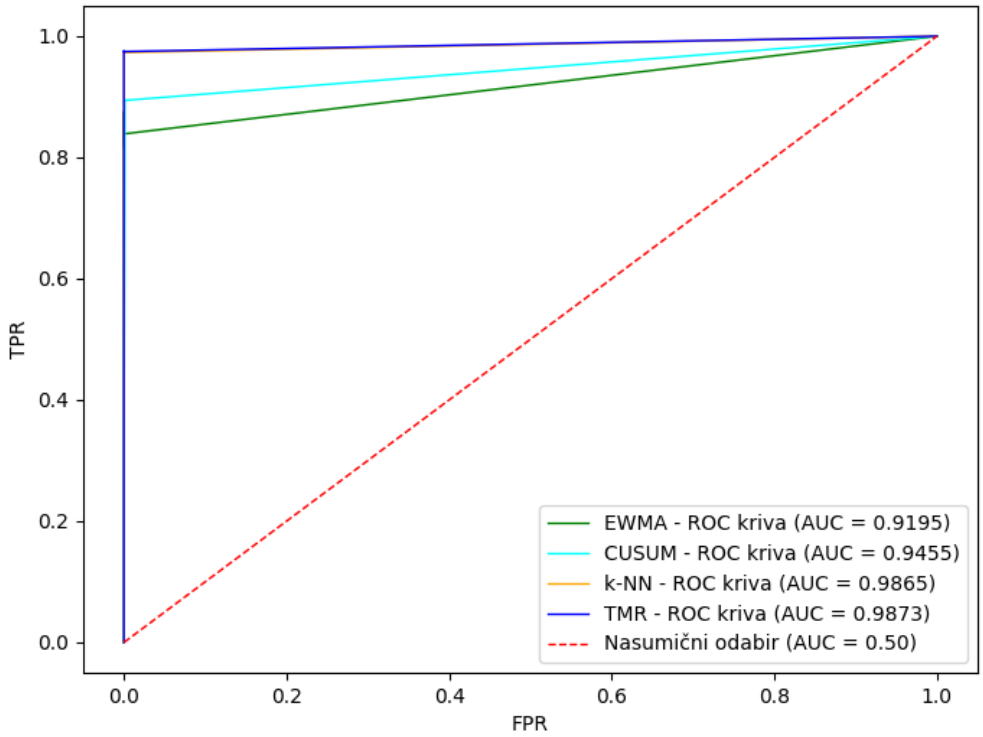
Slika 28: DrDoS_UDP - Primenjen KNN algoritam



Slika 29: DrDoS_UDP - Primenjen TMR algoritam

Tabela 7: DrDoS_UDP evaluacija rezultata

TMR			
TP	618	**Tačnost**	0,9894
TN	884	**F1**	0,9872
FP	0	**Preciznost**	1
FN	16	**Odziv**	0,9747
-	-	**ROC (AUC)**	0,9873
CUSUM			
TP	566	**Tačnost**	0,9545
TN	883	**F1**	0,9425
FP	1	**Preciznost**	0,9982
FN	68	**Odziv**	0,8927
-	-	**ROC (AUC)**	0,9455
EWMA			
TP	532	**Tačnost**	0,9328
TN	884	**F1**	0,9125
FP	0	**Preciznost**	1
FN	102	**Odziv**	0,8391
-	-	**ROC (AUC)**	0,9195
KNN			
TP	617	**Tačnost**	0,9888
TN	884	**F1**	0,9864
FP	0	**Preciznost**	1
FN	17	**Odziv**	0,9731
-	-	**ROC (AUC)**	0,9865

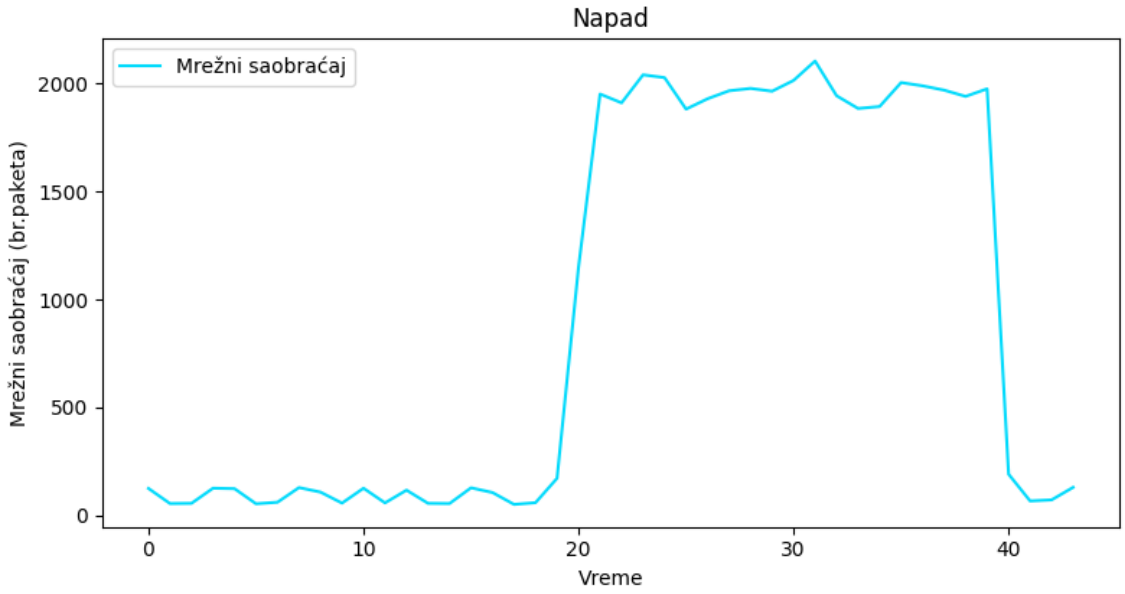


Slika 30: DrDoS_UDP - ROC krive sa iskazanim AUC vrednostima

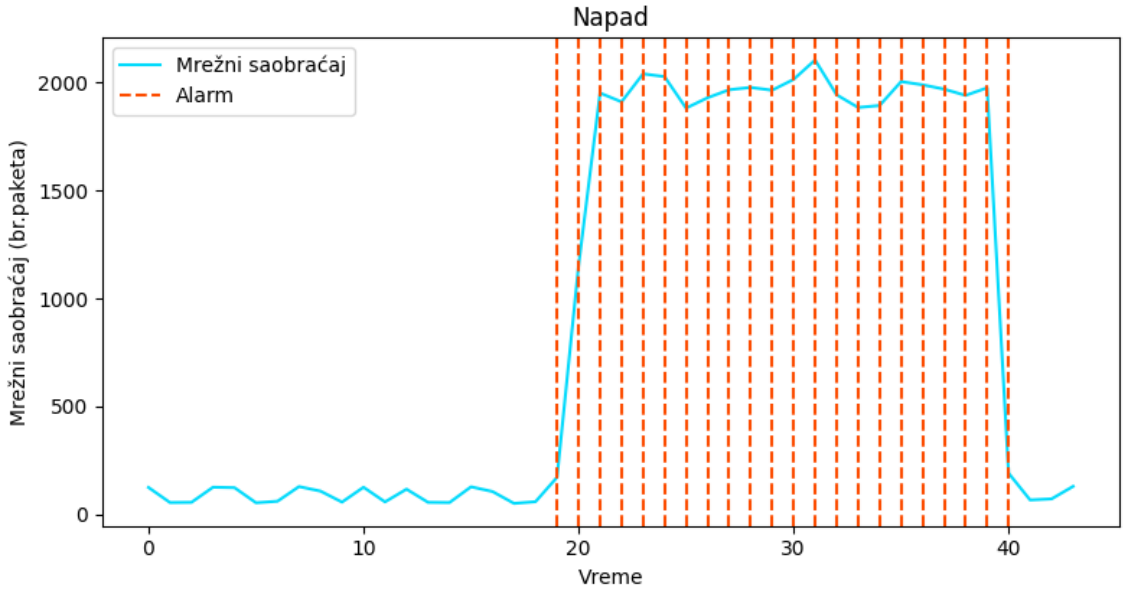
Na slici 30 prikazane su ROC krive za algoritme EWMA, CUSUM, KNN i za predloženi TMR metod u slučaju DrDoS napada. U ovom primeru AUC vrednost za TMR je bolja od ostalih algoritama.

Prag detekcije od 100 je postavljen na osnovu broja paketa u sekundi u trenutku početka napada. Identifikovana je tačka gde vrednosti značajno odstupaju od broja paketa normalnog saobraćaja. Normalni broj paketa u sekundi se nalazi u opsegu od 1 do 80 sa manjim odstupanjima, a tokom napada naglo raste na preko nekoliko hiljada. Prag je definisan kao vrednost koja je za veća od gornje granice normalnog broja paketa. Vrednost odstupanja od 20 za CUSUM algoritam je postavljena na osnovu analize normalnih oscilacija podataka, tako da se razlikuju uobičajene varijacije od većih promena. Takođe težinski faktor α od 0,25 je postavljen tako da balansira između brzine reakcije na promene i stabilnosti. Sve vrednosti su validirane testiranjem nad podacima.

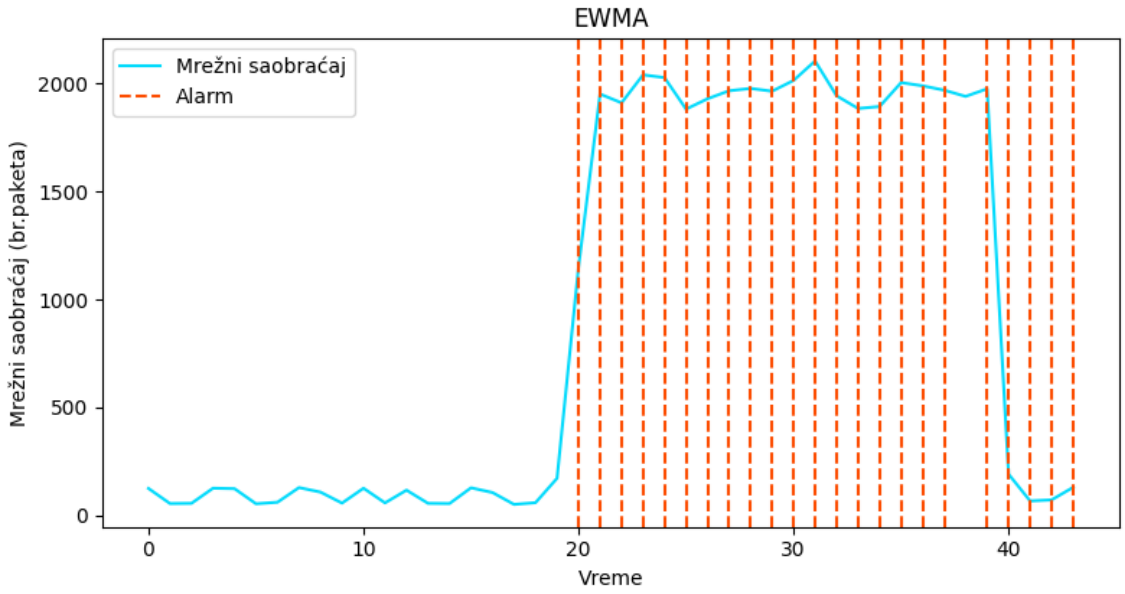
Sledeći napad koji je obrađen je iz skupa podataka IoT Network Intrusion [62] i nalazi se u datoteci pod nazivom *dos-synflooding-1-dec.pcap*.



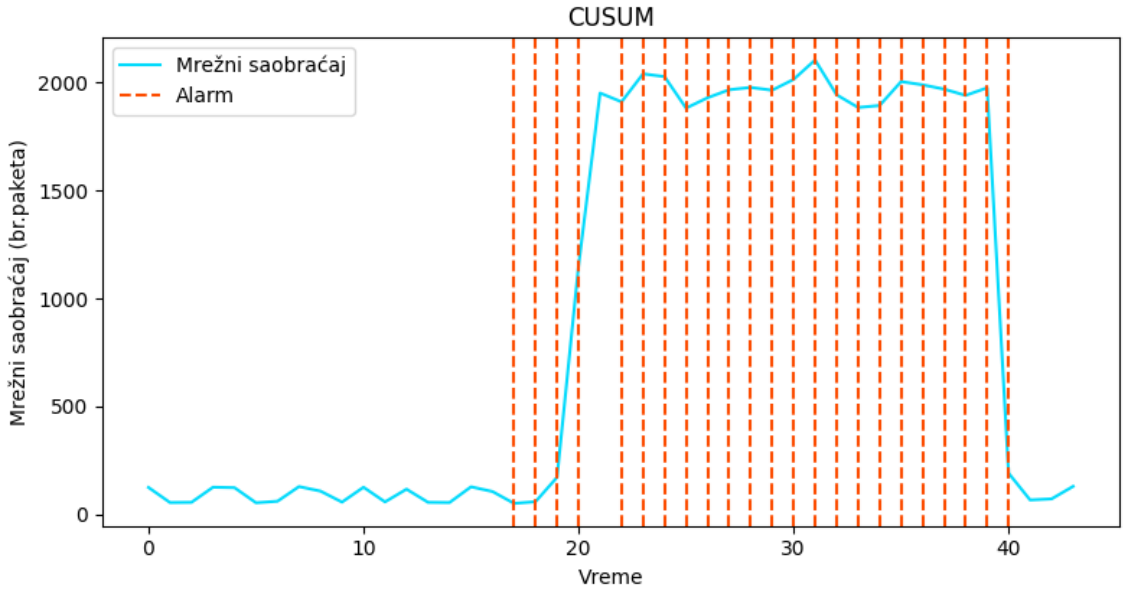
Slika 31: DoS synflooding - Mrežni saobraćaj sa napadom



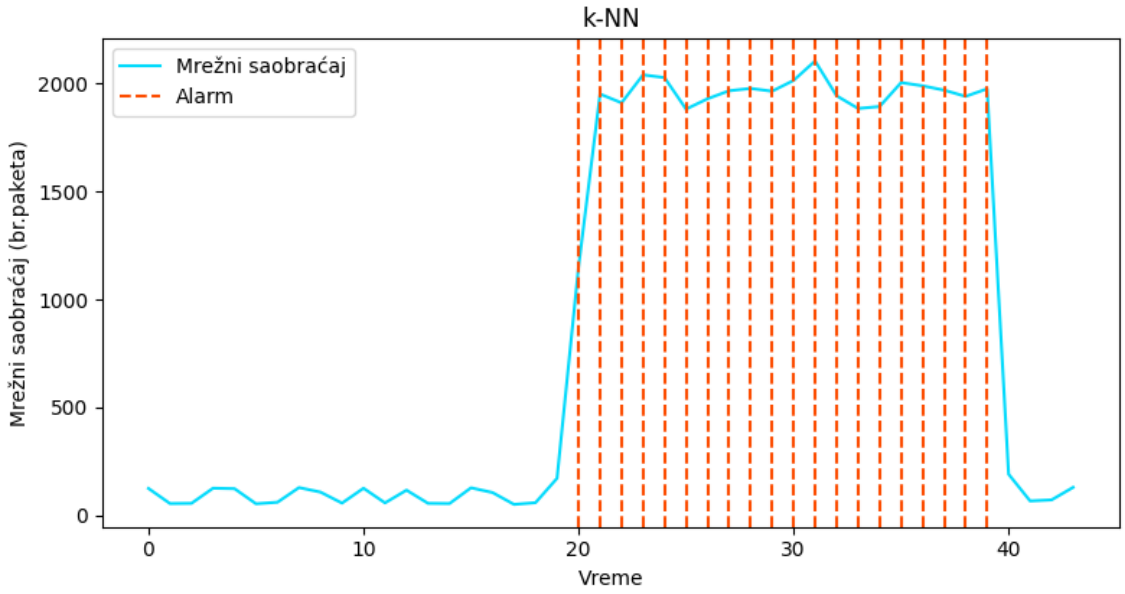
Slika 32: DoS synflooding - Obeležen napad



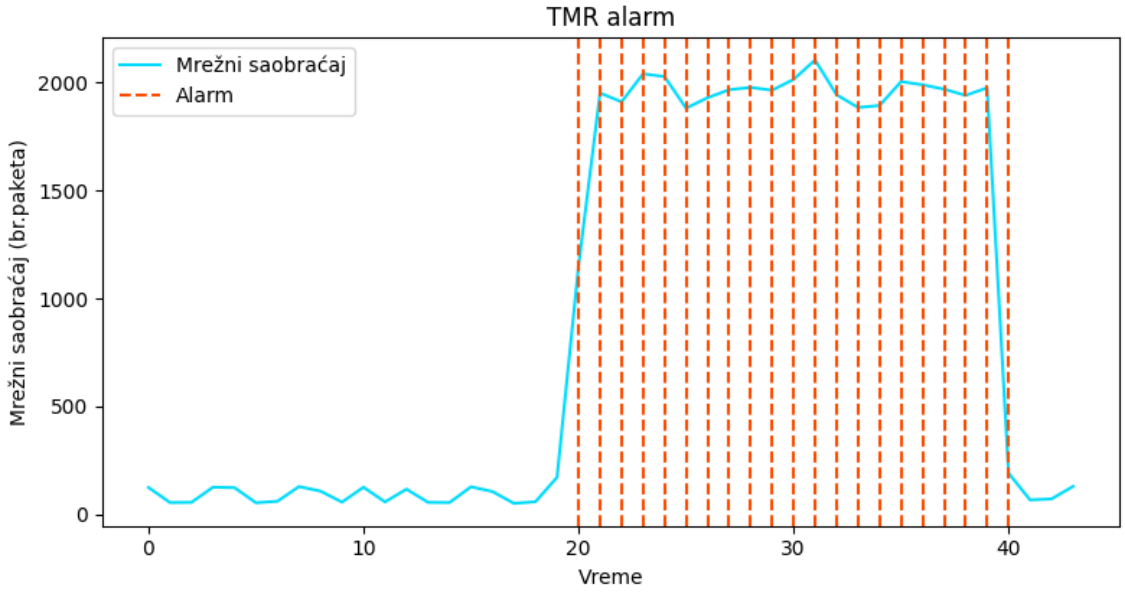
Slika 33: DoS synflooding - Primenjen EWMA algoritam (za vrednost praga 100, i vrednost težinskog faktora α 0.14)



Slika 34: DoS synflooding - Primenjen CUSUM algoritam (za vrednost praga 100, i vrednost odstupanja 4)



Slika 35: DoS synflooding - Primenjen KNN algoritam

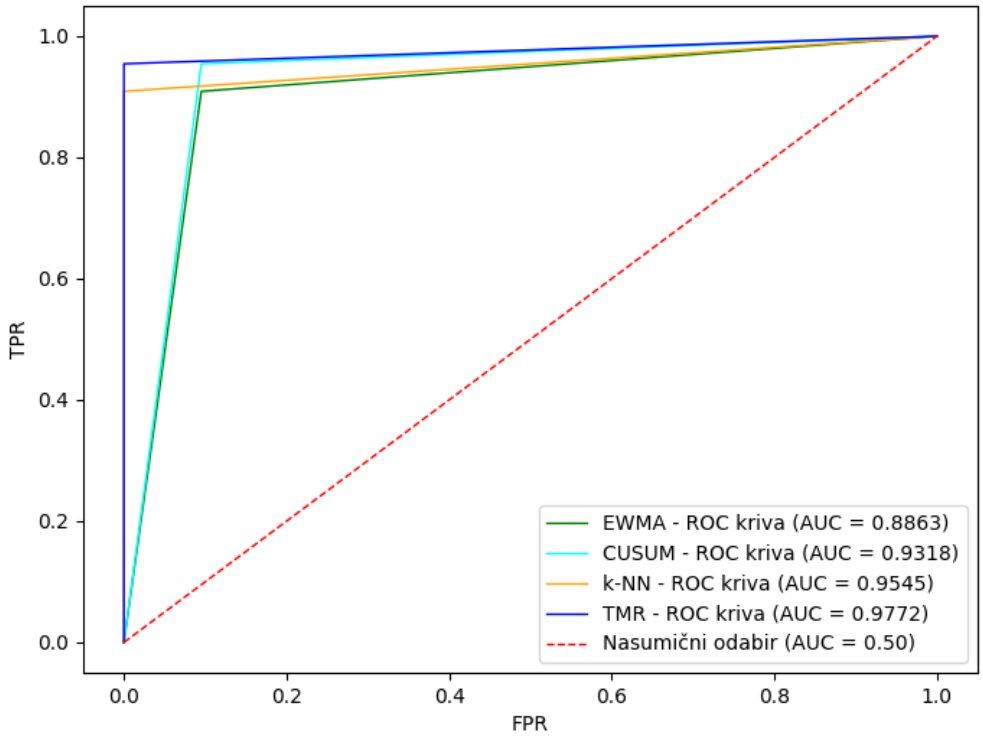


Slika 36: DoS synflooding - Primenjen TMR algoritam

Na slici 31 se može videti grafikon napada, dok se na slici 32 vidi isti grafikon ali sa napadom označenim crvenom bojom. Zatim slede grafikoni na slikama 33, 34 i 35 i to redom za EWMA, CUSUM i KNN algoritme koji predstavljaju funkcionisanje navedenih algoritama na ovom konkretnom skupu podataka. Poslednji grafikon je prikazan na slici 36 koji prikazuje kako TMR funkcioniše na zadatom skupu, dok su u tabeli 8 prikazani i dobijeni numerički rezultati.

Tabela 8: DoS synflooding evaluacija rezultata

TMR			
TP	21	**Tačnost**	0,9772
TN	22	**F1**	0,9767
FP	0	**Preciznost**	1
FN	1	**Odziv**	0,9545
-	-	**ROC (AUC)**	0,9772
CUSUM			
TP	21	**Tačnost**	0,9318
TN	20	**F1**	0,9333
FP	2	**Preciznost**	0,9130
FN	1	**Odziv**	0,9545
-	-	**ROC (AUC)**	0,9318
EWMA			
TP	20	**Tačnost**	0,8863
TN	19	**F1**	0,8888
FP	3	**Preciznost**	0,8695
FN	2	**Odziv**	0,9090
-	-	**ROC (AUC)**	0,8863
KNN			
TP	20	**Tačnost**	0,9545
TN	22	**F1**	0,9523
FP	0	**Preciznost**	1
FN	2	**Odziv**	0,9090
-	-	**ROC (AUC)**	0,9545



Slika 37: DoS synflooding - ROC krive sa iskazanim AUC vrednostima

Na slici 37 prikazane su ROC krive za algoritme EWMA, CUSUM, KNN i za predloženi TMR metod u slučaju obrađenog DoS synflooding napada. Na grafikonu su navedene i AUC vrednosti kako bi se uočila efikasnost svakog metoda pojedinačno. U ovom slučaju AUC vrednost za TMR je bolja od ostalih algoritama.

Prag detekcije od 100 je postavljen na osnovu broja paketa u sekundi u trenutku kada napad počinje. Ovaj skup podataka je drugačiji u odnosu na 3 prethodna, jer se sastoji od 22 vremenske serije. Iz tog razloga je prag postavljen niže nego uobičajeno kako bi se napad pravovremeno detektovao. Prag je definisan kao vrednost koja je skoro jednaka gornjoj granici normalnog broja paketa. Vrednost odstupanja od 4 za CUSUM algoritam je manja nego uobičajeno iz razloga manjeg broja vremenskih serija. Takođe težinski faktor α od 0,14 je postavljen na manju vrednost nego što je to uobičajeno [31], a kako bi se dobili relevantni rezultati. Sve vrednosti su validirane testiranjem nad podacima, čak i u ovom slučaju gde je relativno mali uzorak mrežnog saobraćaja može se videti poboljšanje u rezultatima dobijenim predloženom metodom.

Predloženo rešenje je testirano i validirano na različitim skupovima podataka što se potvrđuje rezultatima dobijenim u tabelama 5, 6, 7 i 8. Ovo rešenje daje

bolje rezultate u odnosu na rezultate svakog od algoritama pojedinačno za sledeće parametre: tačnost, F1 mera, preciznost i odziv. Vrednosti koje su navedene u tabelama su između 0 i 1 i predstavljaju izraženi procenat podeljen sa 100. U dva slučaja u tabelama 5 i 6 se može uočiti da algoritam TMR za parametar preciznosti daje rezultat koji nije najbolji (KNN daje bolji rezultat) ali se taj rezultat od najboljeg razlikuje u minimalnom procentu (manje od 0.5) od najboljeg rezultata.

Na grafikonu za ROC krive su navedene i AUC vrednosti kako bi se uočila efikasnost svakog metoda pojedinačno. Vrednosti FPR i TPR su iskazane u brojčanim vrednostima od 0 do 1 što predstavlja procentualnu vrednost podeljenu sa 100.

Sagledani parametri tačnost, F1 mera i odziv su bolji ili jednaki primenom trostruke modularne redundanse od sva tri korišćena algoritma pojedinačno. Takođe prikaz ROC krivih je potvrdio da su dobijeni rezultati bolji odnosno da je predloženi metod efikasniji.

5. Diskusija

Peto poglavlje je posvećeno diskusiji rezultata, koja počinje sa uporednim rezultatima, za čim sledi unakrsna validacija rezultata i konačno primena TMR metode u IDS sistemu.

5.1 Uporedni rezultati

U tabeli 9 su dati, objedinjeni uporedni rezultati za 4 testirana napada: Friday, UDP, DrDoS UDP i DoS synflood. Za svaki su od napada iskazane mere za tačnost, preciznost, F1 meru i odziv. Takođe rezultati su podeljeni i po primenjenim metodama.

Pregledom rezultata u tabeli 9 dokazano je da predloženo rešenje daje bolje rezultate od tri odabrana algoritma pojedinačno. U poređenju rezultata dobijenih za TMR sa rezultatima KNN algoritma može se primetiti da su razlike neznatne i da za parametar preciznosti u dva slučaja KNN čak daje i marginalno bolje rezultate. Sa druga dva algoritma CUSUM i EWMA to nije slučaj, posebno u slučaju EWMA algoritma koji daje najlošije rezultate od sva tri analizirana. Iako ti rezultati u proseku prelaze vrednost od 90 procenata, oni su najlošiji u poređenju sa druga dva algoritma. Pokazano je da predloženo rešenje radi očekivano i da daje poboljšane rezultate u odnosu na odabrane algoritme.

Pragovi detekcije za korišćene skupove podataka su određeni tako da balansiraju između broja detekcija lažnih pozitiva (FP) i lažnih negativa (FN). Za svaki od skupova je isprobrano nekoliko različitih vrednosti praga dok nisu dobijene optimalne vrednosti prikazane u ovom poglavlju.

Tabela 9: Objedinjeni rezultati za 4 testirana napada

TMR				
	Friday	UDP	DrDoS UDP	DoS synflood
Tačnost	0,9414	0,9745	0,9894	0,9772
F1	0,9561	0,9731	0,9872	0,9767
Preciznost	0,9955	0,9979	1	1
Odziv	0,9197	0,9495	0,9747	0,9545
CUSUM				
	Friday	UDP	DrDoS UDP	DoS synflood
Tačnost	0,9212	0,9423	0,9545	0,9318
F1	0,9415	0,9375	0,9425	0,9333
Preciznost	0,9720	0,9913	0,9982	0,9130
Odziv	0,9128	0,8893	0,8927	0,9545
EWMA				
	Friday	UDP	DrDoS UDP	DoS synflood
Tačnost	0,7646	0,9131	0,9328	0,8863
F1	0,8078	0,9033	0,9125	0,8888
Preciznost	0,9329	0,9839	1	0,8695
Odziv	0,7123	0,8349	0,8391	0,9090
KNN				
	Friday	UDP	DrDoS UDP	DoS synflood
Tačnost	0,9394	0,9726	0,9888	0,9545
F1	0,9544	0,9710	0,9864	0,9523
Preciznost	1	1	1	1
Odziv	0,9128	0,9436	0,9731	0,9090

5.2 Unakrsna validacija rezultata

Kao dodatna potvrda tačnosti dobijenih rezultata prikazanih u tabeli 9 urađena je i unakrsna validacija nad skupom podataka CIC-DDoS2019 [61] i to nad datotekom *DrDos_UDP.csv*. Rezultati unakrsne validacije su prikazani u tabeli 10. Kako bi se uradila unakrsna validacija datoteka *DrDos_UDP.csv* je nakon obrade R skriptom i kreiranje vremenskih serija, podeljena u 6 jednakih datoteka, nakon čega je izvršeno testiranje nad svakom od tih 6 datoteka posebno [1]. Na kraju su dobijeni slični rezultati kao i prilikom testiranja i evaluacije celokupne datoteke. Može se primetiti da su pojedina polja prazna, odnosno da nema rezultata. To je zbog činjenice da, na primer, nisu postojali pravi pozitivi, što je dovelo do deljenja nulom. U takvim slučajevima, ta polja su isključena iz računanja proseka.

Nedostatak metode TMR je vreme obrade podataka, jer obrada podataka za tri algoritma umesto jednog iziskuje dodatne resurse. Benefit tačnijih rezultata bi trebalo da opravda to vreme dodatno utrošeno za detekciju. Predložena metoda može biti korišćena u realnim sistemima uz minimalne adaptacije.

Koristeći TMR postignut je balans između tri korišćena algoritma. Na primer, CUSUM algoritam ne okida alarm ako broj paketa krene da opada tokom napada, dok je sa EWMA algoritmom problem ako napad dugo traje i nema većih oscilacija u broju paketa koji pristižu. U tom slučaju ako nema oscilacija EWMA algoritam će to ponašanje prepoznati kao legitimni saobraćaj. Kao što se može primetiti KNN algoritam daje najbolje rezultate od tri korišćena ali ne i dovoljno dobre da nadmaši rezultate dobijene korišćenjem TMR metode.

U tabeli 10 prikazan je DrDoS UDP napad podeljen u 6 jednakih setova. Nakon primene 4 metoda TMR, CUSUM, EWMA i KNN nad svakim od setova, iskazane su mere za tačnost, preciznost, F1 meru i odziv.

Tabela 10: Unakrsna validacija - DrDoS UDP

-	1. set	2. set	3. set	4. set	5. set	6. set	Prosek
TMR							
Tačnost	0,9723	1	1	0,9881	0,9802	0,9841	0,9874
F1	0,8771	-	-	0,9841	0,9900	0,9920	0,9608
Preciznost	1	-	-	1	1	1	1
Odziv	0,7812	-	-	0,9687	0,9802	0,9841	0,9286
CUSUM							
Tačnost	0,9169	1	1	0,9805	0,8972	0,8853	0,9466
F1	0,5116	-	-	0,9735	0,9458	0,9392	0,8425
Preciznost	1	-	-	0,9892	1	1	0,9973
Odziv	0,3437	-	-	0,9583	0,8972	0,8853	0,7711
EWMA							
Tačnost	0,9841	1	1	0,9209	0,8102	0,8695	0,93083
F1	0,9333	-	-	0,8837	0,9851	0,9302	0,9106
Preciznost	1	-	-	1	1	1	1
Odziv	0,8750	-	-	0,7916	0,8102	0,8695	0,8366
KNN							
Tačnost	0,9486	1	1	0,9841	1	1	0,9832
F1	0,7450	-	-	0,9787	1	1	0,9309
Preciznost	1	-	-	1	1	1	1
Odziv	0,5937	-	-	0,9583	1	1	0,8880

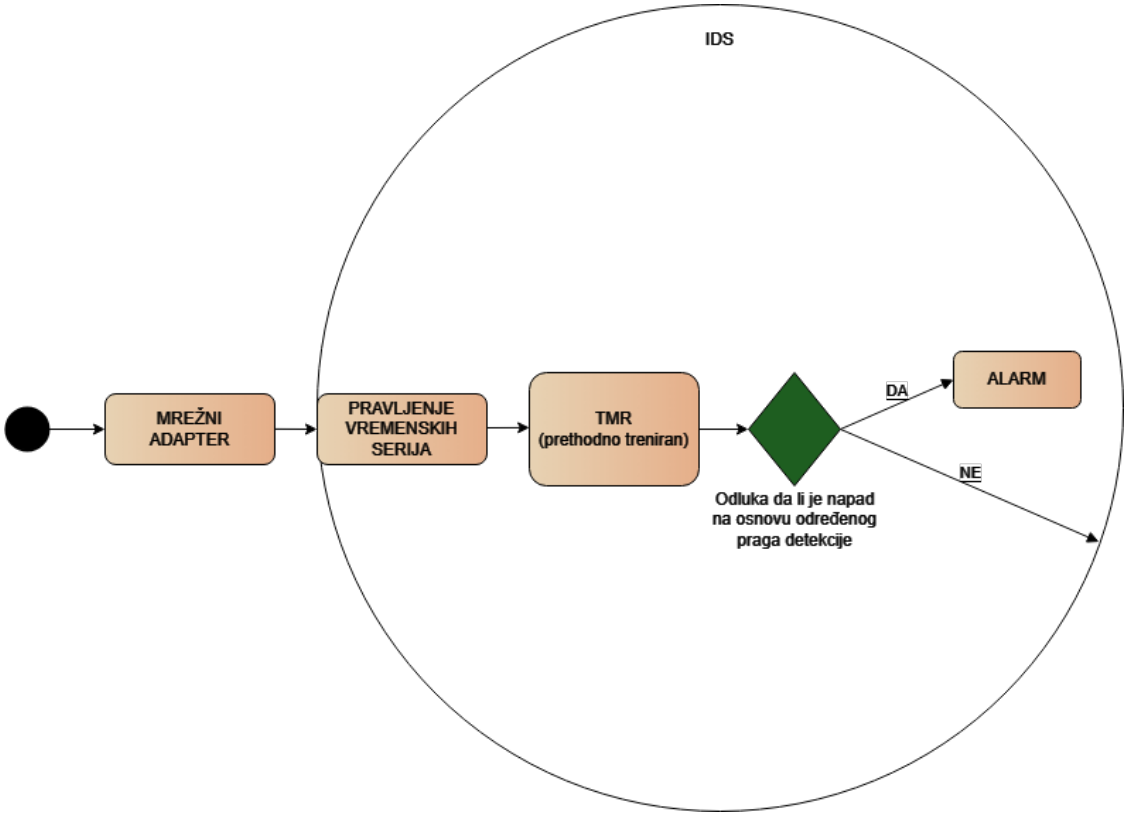
Poredeći dobijene rezultate sa rezultatima predstavljenim u radovima (Elsayed i dr. 2020) [76], (Lima i dr. 2019) [77] i (Muhammad i dr. 2021) [78], a koji su koristili iste skupove podataka za evaluaciju i testiranje i to konkretno CIC-IDS2017 [60] i CIC CIC-DDoS2019 [61], uočava se da vrednosti dobijene predloženom metodom iznose uglavnom preko 95%, dok u nekim slučajevima i značajno više, što je približno rezultatima iz pomenutih radova. Poređenje rezultata TMR metode sa rezultatima drugih pristupa u ovom slučaju nije u potpunosti validno. Na primer, ako se odaberu tri algoritma koji pojedinačno ne daju dobre rezultate, krajnji rezultat TMR metode takođe će biti slabiji. Međutim, i u takvoj situaciji, TMR metoda će ostvariti nešto

bolje rezultate u odnosu na svaki pojedinačni algoritam. Razlika možda neće biti značajna, ali će rezultati ipak biti bolji, što i jeste suština predloženog rešenja.

5.3 Primena TMR metode u IDS sistemu

TMR metod je primenjiv u realnim uslovima IDS sistema, koristeći pomenute biblioteke u kombinaciji sa odgovarajućom Python bibliotekom za snimanje ili posmatranje mrežnog saobraćaja, kao što je Scapy [79]. TMR metod se može prilagoditi da obrađuje pristigle mrežne pakete u realnom vremenu. Umesto R skripti koje su korišćenje u ovoj disertaciji, jer je rešenje testirano na već postojećim podacima, Python skripta se može optimizovati da pravi vremenske serije dok je direktno povezana na mrežni adapter.

Ilustracija primene TMR metoda u IDS sistemu je prikazana na slici 38 gde se primećuje važnost primene predloženog rešenja u jednom takvom sistemu. Ključna komponenta IDS sistema jeste određivanje praga i donošenje odluke da li se radi o napadu ili ne, što je u ovom slučaju i pokazano.



Slika 38: Primena TMR metoda u IDS

U prikazanom slučaju radi se o mrežno baziranoj detekciji upada (NIDS) gde

se radi na identifikaciji mrežnog saobraćaja koji odstupa od uobičajenog obrasca ponašanja. Kao što se može videti IDS sistem ne blokira saobraćaj, već on ima pasivnu ulogu. IDS sistem prikuplja, identifikuje i registruje operacije i alarmira [59].

Predloženo rešenje zahteva prethodnu obuku za detekciju različitih vrsta napada. Proces obuke se sprovodi tako što se TMR metoda primenjuje na postojeće uzorke mrežnog saobraćaja koji sadrže poznate napade. Tokom obuke koriste se različiti parametri detekcije za svaki od algoritama uključenih u proces kako bi se postigli optimalni rezultati. Cilj ovog postupka je precizno određivanje promenljivog praga detekcije, koji je prilagođen specifičnim vrstama napada i obrascima ponašanja mrežnog saobraćaja. Na ovaj način, rešenje se usklađuje sa karakteristikama različitih napada i povećava njegova tačnost i pouzdanost u realnim uslovima.

6. Zaključak

U ovoj disertaciji predložen je pristup određivanju praga detekcije koristeći trostruku modularnu redundansu u IDS sistemima kako bi se najpre detektovali, a zatim i sprečili DDoS napadi. U savremenom dobu, gde su mrežni sistemi konstantno izloženi potencijalnim pretnjama i napadima, neophodno je obezbediti neprekidnu, 24/7 zaštitu informacionih sistema. Pored zaštite, ključna funkcionalnost modernih IDS sistema jeste pravovremeno alarmiranje koje omogućava brzo reagovanje na sumnjive aktivnosti ili pokušaje narušavanja bezbednosti. Ova kombinacija stalne zaštite i pouzdane funkcije alarmiranja predstavlja osnovu za očuvanje integriteta, poverljivosti i dostupnosti mrežnih resursa, što je od presudnog značaja za savremeno poslovanje i svakodnevne digitalne aktivnosti. U predloženom rešenju, gde su tri algoritma kombinovana kako bi se dobio najbolji mogući rezultat, kao što je prikazano u tabeli 9, korišćenjem TMR postignuti su najbolji rezultati za tačnost, F1 meru i odziv dok preciznost ima veoma visoku vrednost u poređenju sa svakim od ta tri algoritma pojedinačno i sa konačnim rezultatom TMR-a. U tabeli 10, svi parametri tačnost, F1 mera, preciznost i odziv su imali najbolje rezultate, što pokazuje da je ovaj pristup ispravan i da daje bolje rezultate. Korišćenjem TMR-a, pokazano je da dolazi do poboljšanja rezultata istovremenim korišćenjem analiziranih algoritama u poređenju sa njihovim pojedinačnim rezultatima. Takođe, umesto trostruke modularne redundanse, može se koristiti n-modularna redundansa, gde je n bilo koji neparan broj veći od 2.

Najvažniji aspekt predloženog rešenja, koji je vredno istaći, jeste njegova sposobnost da obezbedi efikasnu i preciznu detekciju, prilagođenu različitim vrstama mrežnih napada.

Primenjena unapređenja:

- Korišćenje redundanse za postizanje boljih rezultata kombinovanjem postojećih algoritama;
- Kombinovanje EWMA, CUSUM i KNN algoritma u jedan TMR;

Prednosti:

- Bolji rezultati nego kod svakog algoritma pojedinačno;
- Jednostavna implementacija u Python-u.

Nedostatak predloženog rešenja je potencijalno vreme izvršavanja za TMR, jer

se koriste tri algoritma čiji se rezultati moraju prvo izračunati. U najboljem slučaju, TMR bi bio brz koliko i najsporiji od ova tri algoritma, a sa modernim operativnim sistemima sa više niti to je verovatno i najčešći slučaj, tako da to nije veliki gubitak u performansama ukoliko se uzmu u obzir bolji rezultati. Ovo rešenje se takođe može koristiti u realnim sistemima sa određenim ograničenjima performansi i kombinovati se sa drugim softverskim rešenjima koja mogu biti deo sistema za sprečavanje upada. To je jedan od razloga zašto je odabrana trostruka modularna redundansa, a ne n-modularna redundansa – dobitak u rezultatima ne može biti značajno bolji nego primenom TMR, ali bi vreme izračunavanja zasigurno bilo duže. Još jedan od nedostataka je i to što efikasnost predloženog rešenja zavisi od inicijalnog odabira algoritama koji će se koristiti. Performanse bi mogle varirati u zavisnosti od efikasnosti tih algoritama pojedinačno, kao i u zavisnosti od korišćenih skupova podataka za obuku.

Predloženo rešenje sa TMR se može integrisati u već postojeće sisteme za otkrivanje upada u korporativnim, državnim ili IoT mrežama. Najbolji efekat bi se postigao primenom u mrežnim okruženjima koja su osetljiva na DDoS napade kao što su na primer bankarski ili zdravstveni sistemi. Takođe predloženo rešenje bi se dalje moglo optimizovati povremenim testiranjem sa najnovijim skupovima podataka.

Autor planira da se dalje bavi proučavanjem postojećih algoritama za detekciju napada kako bi se osigurali najbolji mogući rezultati sa TMR metodom. Iz dobijenih rezultata se može uočiti da postoji prostora za poboljšanje, kao i da se može razmotriti i još neki od algoritama koji se koriste za IDS. Takođe opcije za alarmiranje je potrebno istražiti dodatno, s obzirom da to nije bila tema ove disertacije ali je značajan deo IDS sistema. Predloženo rešenje je moguće proširiti i na druge vrste napada, poput napada na aplikativnom nivou ili napada unutar mreže. Takođe, mogu se primeniti i adaptivni sistemi koji bi automatski podešavali parametre TMR algoritma u realnom vremenu. To bi se najpre postiglo primenom veštačke inteligencije za donošenje odluke o vrednosti tih parametara pomoću dubokog učenja.

Literatura

[1] Ivan Babić, Aleksandar Miljković, Milan Čabarkapa, Vojkan Nikolić, Aleksandar Đorđević, Milan Ranđelović, and Dragan Ranđelović. Triple Modular Redundancy Optimization for Threshold Determination in Intrusion Detection Systems. *Symmetry*, 13(4), 2021. https://www.mdpi.com/2073-8994/13/4/557.

[2] Shi Pu. Choosing parameters for detecting ddos attack. In *2012 International Conference on Wavelet Active Media Technology and Information Processing (ICWAMTIP)*, pages 239–242, Chengdu, China, 17-19 December 2013. IEEE.

[3] Keunsoo Lee, Juhyun Kim, Ki Hoon Kwon, Younggoo Han and Sehun Kim. DDoS attack detection method using cluster analysis. *Expert systems with applications*, 34(3):1659–1665, 2008.

[4] DDoS Attack Types and Mitigation Methods. `https://www.imperva.com/learn/ddos/ddos-attacks`.

[5] A. Sanmorino and S. Yazid. Ddos attack detection method and mitigation using pattern of the flow. In *Proceedings of the 2013 International conference of Information and communication technology (ICoICT)*, Bandung, Indonesia, 20-22 March 2013. IEEE. 12-16.

[6] S. Shanbhag and T. Wolf. Accurate anomaly detection through parallelism. *IEEE Network*, 23:22–28, 2009.

[7] P. Machaka, A. Bagula, and F. Nelwamondo. Using exponentially weighted moving average algorithm to defend against DDoS attacks. In *Proceedings of the 2016 Pattern Recognition Association of South Africa and Robotics and Mechatronics International Conference (PRASA-RobMech)*, pages 1–6, Stellenbosch, South Africa, 30 November - 2 December 2016. New Jersey, USA, Piscataway.

[8] H. Wang, D. Zhang, and K. G. Shin. Change-Point Monitoring for the Detection of DoS Attacks. *Transactions on Dependable and Secure Computing*, 1:193–208, 2004.

[9] R.R. Özçelik, I.; Brooks. Cusum-entropy: an efficient method for DDoS attack detection. In *Proceedings of the 2016 4th International Istanbul Smart Grid Congress and Fair (ICSG)*, pages 1–5, Istanbul, Turkey, 20–21 April 2016. IEEE.

[10] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang. A survey of distributed denial-of-service attack,prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, 13, 2017.

[11] Google Mitigates Largest DDoS Attack in Its History. `https://www.bitdefender.com/en-us/blog/hotforsecurity/google-mitigates-largest-ddos-attack-in-its-history`. Accessed on 8th October 2024.

[12] Masovni sajber napadi na sajt i IT infrastrukturu MUP-a. `https://www.srbija.gov.rs/vest/676312/masovni-sajber-napadi-na-sajt-i-it-infrastrukturu-mup-a.php`.

[13] Famous DDoS attacks. `https://www.cloudflare.com/learning/ddos/famous-ddos-attacks`. Accessed on 7th October 2024.

[14] J. David and C. Thomas. DDoS Attack Detection Using Fast Entropy Approach on Flow- Based Network Traffic. In *Proceedings of the 2nd International Symposium on Big Data and Cloud Computing Challenges*, pages 30–36, VIT University, Chennai, India, 12-13 March 2015. Procedia Computer Science.

[15] D. Patel, K. Srinivasan, C.-Y. Chang, T. Gupta, and A. Kataria. Network Anomaly Detection inside Consumer Networks—A Hybrid Approach. *Electronics*, 9:923, 2020.

[16] R. E. Lyons and W. Vanderkulk. The use of triple-modular redundancy to improve computer reliability. *IBM journal of research and development*, 6:200–209, 1962.

[17] J. A. Abraham and D. P. Siewiorek. An algorithm for the accurate reliability evaluation of triple modular redundancy networks. *IEEE Transactions on Computers*, 100:682–692, 1974.

[18] Ansam Khraisat, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, 2, 2019.

[19] C. Douligeris and A. Mitrokotsa. Ddos Attacks and Defense Mechanisms: a classification. In *Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology*, pages 190–193, Darmstadt, Germany, 17 December 2003. IEEE.

[20] Ilemona S. Atawodi. A Machine Learning Approach to Network Intrusion Detection System Using K Nearest Neighbor and Random Forest. Master's thesis, The University of Southern Mississippi, Hattiesburg, Mississippi, US, May 2019.

[21] T. Zhang. Cumulative sum algorithm for detecting SYN flooding attacks. *Xinxiang College*, 12 2012.

[22] P. Machaka, A. McDonald, F. Nelwamondo, and A. Using Bagula. Using the Cumulative Sum Algorithm against Distributed Denial of Service Attacks in Internet of Things. In Thu Dau Mot and Vietnam, editors, *Proceedings of the International Conference on Context-Aware Systems and Applications*, pages 66–72. IEEE, 24-25 November 2019.

[23] Santosh K. M.;Isaac and E. Defending DDoS Attack using Stochastic Model based Puzzle Controller. *IJCSNS International Journal of Computer Science and Network Security*, 13:100–105, 2013.

[24] Ece Öztürk Kiyak, Behnam Ghasemkhani, and Derya Birant. High-Level K-Nearest Neighbors (HLKNN): A Supervised Machine Learning Model for Classification Analysis. *Electronics*, 12(18), 2023.

[25] Shichao Zhang, Zhenyun Deng, Debo Cheng, Ming Zong, and Zhu Xiaoshu. Efficient kNN Classification Algorithm for Big Data. *Neurocomputing*, 195, 02 2016.

[26] Giuseppe Nuti. An Efficient Algorithm for Bayesian Nearest Neighbours. *Methodology and Computing in Applied Probability*, 21(3):967–989, 2018.

[27] Harshita Patel and G. S. Thakur. An Improved Fuzzy K-Nearest Neighbor Algorithm for Imbalanced Data Using Adaptive Approach. *IETE Journal of Research*, 2018.

[28] Hamid Parvin and Hosein Alizadeh and Behrouz Minaei-Bidgoli. MKNN: Modified K-Nearest Neighbor. In *Proceedings of the World Congress on Engineering and Computer Science 2008 (WCECS)*, pages 22–24, San Francisco, USA, 2008. World Congress on Engineering and Computer Science.

[29] P. Čisar, S. Čisar, S. Bošnjak, and S. Marav. EWMA algorithm in network practice. *International Journal of Computers, Communications and Control*, 5(2):156–167, 2010.

[30] P. Čisar and S. Maravić Čisar. EWMA Statistics and Fuzzy Logic in Function of Network Anomaly Detection. *Facta Universitatis, Series: Electronics and Energetics*, 32(2):249–265, 2019.

[31] S. Bošnjak P. Čisar and S. Maravić Čisar. EWMA-based threshold algorithm for intrusion detection. *Computing and Informatics (International journal)*, 29:1089–1101, 2010.

[32] P. Čisar and S. Maravić Čisar. Optimization methods of EWMA Statistics. *Acta Polytechnica Hungarica*, 8(5):73–87, 2011.

[33] N. Abbas, A. U. Haq, and M. S. Qazi. Enhancing the Performance of EWMA Charts. *Ibisuva Research Publications*, 2011.

[34] D. Sklavounos, A. Edoh, and M. Plytas. A Statistical Approach Based on EWMA and CUSUM Control Charts for R2L Intrusion Detection. In *Proceedings of the 2017 Cybersecurity and Cyberforensics Conference (CCC)*, pages 25–30, London, UK, 21-23 November 2017. IEEE.

[35] F. Y. Leu and W. J. Yang. Intrusion Detection with CUSUM for TCP-Based DDoS. In *Proceedings of the Embedded and Ubiquitous Computing - EUC 2005 Workshops*, pages 1255–1264, Nagasaki, Japan, 6-9 December 2005.

[36] Ashraf Ali and Andrew Ware. Anomaly Based IDS Via Customised CUSUM Algorithm for Industrial Communication Systems. In *2021 3rd IEEE Middle East and North Africa COMMunications Conference (MENACOMM)*, pages 31–36, 2021.

[37] Shih-Ting Chiu and Fang-Yie Leu. Detecting DoS and DDoS Attacks by Using CuSum Algorithm in 5G Networks. In *Advances in Networked-Based Information Systems*, pages 1–9. Springer, 2020.

[38] Wei Lu and Hengjian Tong. Detecting Network Anomalies Using CUSUM and EM Clustering. In *Advances in Computation and Intelligence: 4th International Symposium, ISICA 2009*, pages 297–308. Springer, 2009.

[39] Gabriele Gualandi, Martina Maggio, and Alessandro Vittorio Papadopoulos. Optimization-based attack against control systems with CUSUM-based anomaly detection. In *2022 30th Mediterranean Conference on Control and Automation (MED)*, pages 896–901, 2022.

[40] Slobodan Nedeljković, Vojkan Nikolić, Milan Čabarkapa, Jelena Mišić, and Dragan Ranđelović. An Advanced Quick-Answering System Intended for the

e-Government Service in the Republic of Serbia. *Acta Polytechnica Hungarica*, 16(4), 2019.

[41] R. E. Lyons and W. Vanderkulk. The Use of Triple-Modular Redundancy to Improve Computer Reliability. *IBM Journal of Research and Development*, 6(2):200–209, 1962.

[42] Tooba Arifeen, Abdus Sami Hassan, and Jeong-A Lee. Approximate Triple Modular Redundancy: A Survey. *IEEE Access*, 8:139851–139867, 2020.

[43] Z. Zhang, D. Liu, Z. Wei, and C. Sun. Research on Triple Modular Redundancy Dynamic Fault-Tolerant System Model. In *Proceedings of the First International Multi-Symposiums on Computer and Computational Sciences (IMSCCS'06)*, pages 572–576, Hanzhou, Zhejiang, China, 20-24 June 2008. IEEE.

[44] P. Balasubramanian and K. Prasad. A Fault Tolerance Improved Majority Voter for TMR System Architectures. *WSEAS Transactions on Circuits and Systems*, 14:108–122, 2016.

[45] S.M. Čisar, P. Čisar, and R. Pinter. Fuzzy-Based Intrusion Detection Systems. In *Security-Related Advanced Technologies in Critical Infrastructure Protection*, pages 205–215. Springer Netherlands, 2022.

[46] P. Čisar, B. Popović, K. Kuk, S.M. Čisar, and I. Vuković. Machine Learning Aspects of Internet Firewall Data. In *Security-Related Advanced Technologies in Critical Infrastructure Protection*, pages 43–59. Springer Netherlands, 2022.

[47] P. Čisar and S.M. Čisar. Model-based Algorithm for Statistical Intrusion Detection. In *10th International Symposium of Hungarian Researchers on Computational Intelligence and Informatics*, 12-14 November 2009.

[48] P. Čisar and S.M. Čisar. *Network Statistics in Function of Statistical Intrusion Detection*, volume 313, pages 27–35. Springer Netherlands, 10 2010.

[49] Merve Ozkan Okay, Refik Samet, Ömer Aslan, and Deepti Gupta. A Comprehensive Systematic Literature Review on Intrusion Detection Systems. *IEEE Access*, PP:1–1, 11 2021.

[50] Y. Zhou and J. Li. Research of network traffic anomaly detection model based on multilevel auto-regression. In *Proceedings of the 2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT)*, pages 380–384, Dalian, China, 19-20 October 2019. IEEE.

[51] H. Rahmani, N. Sahli, and F. Kamoun. A Traffic Coherence Analysis Model for DDoS Attack Detection. In *Proceedings of the International Conference on Security and Cryptography*, pages 148–154, Milan, Italy, 7-10 July 2009. INSTICC Press.

[52] J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi. CNN-Based Network Intrusion Detection against Denial-of-Service Attacks. *Electronics*, 9:916, 2020.

[53] Yanxin Wang and Johnny S. Wong. *A hybrid intrusion detection system*. PhD thesis, Iowa State University, USA, 2004. AAI3145689.

[54] M. A. Faizal, M. M. Zaki, S. Shahrin, Y. Robiah, S. S.;Nazrulazhar Rahayu, and B. Threshold Verification Technique for Network Intrusion Detection System. *International Journal of Computer Science and Information Security*, 1, 2009.

[55] Tobias Oetiker. MRTG: The Multi Router Traffic Grapher. In *Proceedings of the Twelfth Systems Administration Conference (LISA '98)*, Boston, Massachusetts, December 6–11 1998. USENIX Association.

[56] SNORT. `https://www.fortinet.com/resources/cyberglossary/snort`.

[57] Gongde Guo, Hui Wang, David Bell, Yaxin Bi, and Kieran Greer. KNN Model-Based Approach in Classification. In Robert Meersman, Zahir Tari, and Douglas C. Schmidt, editors, *On The Move to Meaningful Internet Systems 2003: CoopIS, DOA, and ODBASE*, pages 986–996, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[58] S. Shernta and A. Tamtum. Using Triple Modular Redundant (TMR) technique in critical systems operation. *International Journal of Computer Science and Network Security*, 13:100–105, 2013.

[59] Petar Čisar. *Detekcija napada na mrežu*. Kriminalističko-policijski univerzitet, 2021. https://www.kpu.edu.rs/cms/biblioteka/nova-izdanja/7094-detekcija-napada-na-mrezu.

[60] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. In Portugal, editor, *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, 2018. https://www.unb.ca/cic/datasets/ids-2017.html.

[61] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset

and Taxonomy. In India Chennai, editor, *Proceedings of the IEEE 53rd International Carnahan Conference on Security Technology*, 2019. https://www.unb.ca/cic/datasets/ddos-2019.html.

[62] Hyunjae Kang, Dong Hyun Ahn, Gyung Min Lee, Jeong Do Yoo, Kyung Ho Park, and Huy Kang Kim. IoT network intrusion dataset, 2019.

[63] Aircrack-ng Team. Aircrack-ng: A network security suite, 2025. Accessed on 21st December 2024.

[64] OpenAI. ChatGPT (Decembar, 2025), 2025. Large language model. https://chat.openai.com.

[65] Pandas library. `https://pandas.pydata.org/pandas-docs/version/0.17.0/generated/pandas.ewma.html`. Accessed on 15th November 2020.

[66] Marcos Duarte. detecta: A Python module to detect events in data, 3 2021. https://zenodo.org/records/4598962.

[67] Scikit Learn. `https://scikit-learn.org/stable/modules/generated/sklearn.neighbors.KNeighborsClassifier.html`. Accessed on 7th February 2021.

[68] Charles R. Harris, K. Jarrod Millman, Stéfan J. van der Walt, Ralf Gommers, Pauli Virtanen, David Cournapeau, Eric Wieser, Julian Taylor, Sebastian Berg, Nathaniel J. Smith, Robert Kern, Matti Picus, Stephan Hoyer, Marten H. van Kerkwijk, Matthew Brett, Allan Haldane, Jaime Fernández del Río, Mark Wiebe, Pearu Peterson, Pierre Gérard-Marchant, Kevin Sheppard, Tyler Reddy, Warren Weckesser, Hameer Abbasi, Christoph Gohlke, and Travis E. Oliphant. Array programming with NumPy. *Nature*, 585(7825):357–362, September 2020. https://doi.org/10.1038/s41586-020-2649-2.

[69] Pauli Virtanen, Ralf Gommers, Travis E. Oliphant, Matt Haberland, Tyler Reddy, David Cournapeau, Evgeni Burovski, Pearu Peterson, Warren Weckesser, Jonathan Bright, Stéfan J. van der Walt, Matthew Brett, Joshua Wilson, K. Jarrod Millman, Nikolay Mayorov, Andrew R. J. Nelson, Eric Jones, Robert Kern, Eric Larson, C J Carey, İlhan Polat, Yu Feng, Eric W. Moore, Jake VanderPlas, Denis Laxalde, Josef Perktold, Robert Cimrman, Ian Henriksen, E. A. Quintero, Charles R. Harris, Anne M. Archibald, Antônio H. Ribeiro, Fabian Pedregosa, Paul van Mulbregt, and SciPy 1.0 Contributors. SciPy 1.0: Fundamental Algorithms for Scientific Computing in Python. *Nature Methods*, 17:261–272, 2020.

[70] J. D. Hunter. Matplotlib: A 2D graphics environment. *Computing in Science & Engineering*, 9(3):90–95, 2007.

[71] Hadley Wickham. *ggplot2: Elegant Graphics for Data Analysis*. Springer-Verlag New York, 2016. https://ggplot2.tidyverse.org.

[72] Hadley Wickham. *stringr: Simple, Consistent Wrappers for Common String Operations*, 2023. R package version 1.5.1, https://github.com/tidyverse/stringr.

[73] Alistair Wilcox. *frequency: Easy Frequency Tables*, 2021. R package version 0.4.1.

[74] Hadley Wickham, Romain François, Lionel Henry, Kirill Müller, and Davis Vaughan. *dplyr: A Grammar of Data Manipulation*, 2023. R package version 1.1.4, https://github.com/tidyverse/dplyr.

[75] Tyson Barrett, Matt Dowle, Arun Srinivasan, Jan Gorecki, Michael Chirico, Toby Hocking, and Benjamin Schwendinger. *data.table: Extension of 'data.frame'*, 2024. R package version 1.16.99, https://Rdatatable.gitlab.io/data.table, https://github.com/Rdatatable/data.table.

[76] Mahmoud Said Elsayed, Nhien-An Le-Khac, Soumyabrata Dev, and Anca Delia Jurcut. DDoSNet: A Deep-Learning Model for Detecting Network Attacks. In *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, pages 391–396, 2020.

[77] Francisco Sales de Lima Filho, Frederico A. F. Silveira, Agostinho de Medeiros Brito Junior, Genoveva Vargas-Solar, and Luiz F. Silveira. Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning. *Security and Communication Networks*, 2019(1):1574749, 2019. https://onlinelibrary.wiley.com/doi/abs/10.1155/2019/1574749.

[78] Muhammad Aamir and Syed Mustafa Ali Zaidi. Clustering based semi-supervised machine learning for DDoS attack classification. *Journal of King Saud University - Computer and Information Sciences*, 33(4):436–446, 2021. https://www.sciencedirect.com/science/article/pii/S131915781831067X.

[79] Rohith S, Rohith R, Minal Moharir, and Shobha G. SCAPY- A powerful interactive packet manipulation program. *2018 International Conference on Networking, Embedded and Wireless Systems (ICNEWS)*, pages 1–5, 2018. https://api.semanticscholar.org/CorpusID:208205894.

Stručna biografija

Ivan Babić je rođen 09.07.1990. godine u Beogradu.

Nakon završene Matematičke gimnazije u Beogradu, upisuje osnovne akademske studije Informatike i računarstva 2011. godine na Fakultetu za informatiku i računarstvo Univerziteta Singidunum u Beogradu. U oktobru 2015. godine završava osnovne studije i stiče zvanje diplomirani informatičar.

Nakon završenih osnovnih studija 2016. godine upisuje master akademske studije na Departmanu za poslediplomske studije Univerziteta Singidunum u Beogradu, smer Savremene informacione tehnologije. U oktobru 2017. godine završava master studije i stiče zvanje master informatičar.

Počinje da radi u Ministarstvu unutrašnjih poslova u martu 2017. godine, i od 01.01.2019. godine je na radnom mestu kriminalističkog inspektora za suzbijanje visokotehnološkog kriminala u Službi za borbu protiv visokotehnološkog kriminala.

U oktobru 2018. godine upisuje doktorske akademske studije informatike i računarstva na Kriminalističko-policijskom univerzitetu.

Izjava o autorstvu

Ime i prezime studenta doktorskih studija: Ivan Babić

Broj indeksa: 2R1/0001/18

Izjavljujem

da je doktorska disertacija pod naslovom:

„Optimizacija trostruke modularne redundanse za određivanje praga u sistemima za detekciju napada“

- rezultat sopstvenog istraživačkog rada;
- da disertacija u celini ni u delovima nije bila predložena za sticanje druge diplome prema studijskim programima drugih visokoškolskih ustanova;
- da su rezultati korektno navedeni i
- da nisam kršio/la autorska prava i koristio/la intelektualnu svojinu drugih lica.

U Beogradu, _____ **Potpis studenta doktorskih studija**

_____

Izjava o istovetnosti štampane i elektronske verzije doktorske disertacije

Ime i prezime studenta doktorskih studija: Ivan Babić

Broj indeksa: 2R1/0001/18

Studijski program: Doktorske studije informatike

Naslov disertacije: „Optimizacija trostruke modularne redundanse za određivanje praga u sistemima za detekciju napada“

Mentor: prof. dr Petar Čisar

Izjavljujem da je štampana verzija mog doktorskog rada istovetna elektronskoj verziji koju sam predao/la radi pohranjivanja u Digitalnom repozitorijumu Kriminalističko-policijskog univerziteta.

Dozvoljavam da se objave moji lični podaci vezani za dobijanje akademskog naziva doktora nauka, kao što su ime i prezime, godina i mesto rođenja i datum odbrane rada.

Ovi lični podaci mogu se objaviti na mrežnim stranicama digitalne biblioteke, u elektronskom katalogu i u publikacijama Kriminalističko-policijskog univerziteta.

U Beogradu, _____ **Potpis studenta doktorskih studija**

_____

Izjava o korišćenju

Ovlašćujem Univerzitetsku biblioteku „Svetozar Marković“ da u Digitalni repozitorijum Kriminalističko-policijskog univerziteta unese moju doktorsku disertaciju pod naslovom:

„Optimizacija trostruke modularne redundanse za određivanje praga u sistemima za detekciju napada“,

koja je moje autorsko delo.

Disertaciju sa svim prilozima predao/la sam u elektronskom formatu pogodnom za trajno arhiviranje.

Moju doktorsku disertaciju pohranjenu u Digitalnom repozitorijumu Kriminalističko-policijskog univerziteta u Beogradu i dostupnu u otvorenom pristupu mogu da koriste svi koji poštuju odredbe sadržane u odabranom tipu licence Kreativne zajednice (Creative Commons) za koju sam se odlučio/la.

1. Autorstvo (CC BY)
2. Autorstvo – nekomercijalno (CC BY-NC).
3. **Autorstvo – nekomercijalno – bez prerada (CC BY-NC-ND)**
4. Autorstvo – nekomercijalno – deliti pod istim uslovima (CC BY-NC-SA)
5. Autorstvo – bez prerada (CC BY-ND)
6. Autorstvo – deliti pod istim uslovima (CC BY-SA)

(Molimo da zaokružite samo jednu od šest ponuđenih licenci. Kratak opis licenci je sastavni deo ove izjave).

U Beogradu, _____ **Potpis studenta doktorskih studija**

_____

1. **Autorstvo.** Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence, čak i u komercijalne svrhe. Ovo je najslobodnija od svih licenci.

2. **Autorstvo** – nekomercijalno. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela.

3. **Autorstvo** – nekomercijalno – bez prerada. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela. U odnosu na sve ostale licence, ovom licencom se ograničava najveći obim prava korišćenja dela.

4. **Autorstvo** – nekomercijalno – deliti pod istim uslovima. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca ne dozvoljava komercijalnu upotrebu dela i prerada.

5. **Autorstvo** – bez prerada. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca dozvoljava komercijalnu upotrebu dela.

6. **Autorstvo** – deliti pod istim uslovima. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca dozvoljava komercijalnu upotrebu dela i prerada. Slična je softverskim licencama, odnosno licencama otvorenog koda.