UNIVERZITET U BEOGRADU

ELEKTROTEHNIČKI FAKULTET

Valentina V. Timčenko

DETEKCIJA NAPADA U RAČUNARSKIM MREŽAMA ZASNOVANA NA ANALIZI STRUKTURE SAOBRAĆAJA PRIMENOM KOMBINOVANIH ALGORITAMA MAŠINSKOG UČENJA

Doktorska disertacija

Beograd, 2022.

UNIVERSITY OF BELGRADE

SCHOOL OF ELECTRICAL ENGINEERING

Valentina V. Timčenko

NETWORK ATTACKS DETECTION BASED ON TRAFFIC FLOWS ANALYSIS USING HYBRID MACHINE LEARNING ALGORITHMS

Doctoral Dissertation

Belgrade, 2022.

Podaci o mentoru i članovima komisije

Mentor:
dr Slavko Gajin, vanredni profesor,
Univerzitet u Beogradu - Elektrotehnički fakultet

Članovi komisije:

dr Dragan Milićev, redovni profesor,
Univerzitet u Beogradu - Elektrotehnički fakultet

dr Pavle Vuletić, vanredni profesor,
Univerzitet u Beogradu - Elektrotehnički fakultet

dr Miroslav Marić, redovni profesor,
Univerzitet u Beogradu - Matematički fakultet

Datum usmene odbrane:

ZAHVALNICA

Jedna lepa izreka kaže „*Sa najtežeg uspona se pruža najlepši pogled*”. Možda sam samo inspirisana svojom velikom ljubavlju prema planinarenju, ali iz iskustva sa velikog broja uspona na planinske vrhove mogu da potvrdim da je osećaj na vrhu zaista najlepši baš onda kada je i bilo najteže popeti se. Voleti nauku, baviti se naukom, a zatim poželeti da se ta ljubav ostvari kroz rezultate, podrazumeva dugogodišnji naučno-istraživački rad. Na tom putu punom izazova i prekretnica jako je važno koga imate uz sebe. Svaka osoba koja je za ovih nekoliko godina truda i rada imala svoj uticaj na mene možda nije ni svesna, ali predstavlja kockicu mozaika bez koje ovaj rad ne bi bio isti.

Na tom putu pre svega bih volela da zahvalim velikom čoveku i stručnjaku u ovoj oblasti, svom mentoru profesoru dr Slavku Gajinu, na njegovim uvek „u centar” usmeravanjima, iskusnom sagledavanju problema sa kojima smo se bavili tokom istraživanja, savršenom razumevanju svakog koraka koji je bio potreban da se učini i podrški da svoju energiju na što efikasniji način usmerim ka cilju. Hvala puno na velikom razumevanju za moju želju da svaki istraživački zalogaj tokom zajedničkog rada bude kvalitetan, sveobuhvatan i dobra odskočna daska za svaki sledeći. Hvala na svakom podsticaju, podršci, savetu i razumevanju pri radu.

Ovo svojevrsno putovanje dugujem i podršci mnogih ljudi čije razumevanje i podsticaj na uspeh zaslužuju da budu navedeni u ovoj zahvalnici. Pre svega, hvala profesoru dr. Borislavu Đorđeviću sa kojim dugi niz godina sarađujem u naučno-istraživačkom radu u Institutu „Mihajlo Pupin”, sa kojim sam objavila veliki broj radova, ali i koji mi je u ključnim trenucima bio velika podrška i prijatelj, usmerivši me na Katedru za računarsku tehniku na Elektrotehničkom fakultetu u Beogradu. Veliku zahvalnost dugujem i svojoj dragoj koleginici dr Slavici Boštjančič Rakas, koja je sve ove godine bila prijatelj čije su mi podrška i blagotvorne reči uvek pomagale da put ka uspehu bude manje trnovit nego što inače jeste. Hvala puno i dragim kolegama iz Instituta „Mihajlo Pupin” koji su znali da kažu pravu reč u pravo vreme. Te ljude smatram pre svega svojim prijateljima, tek onda kolegama.

U moru neprospavanih noći, jurenja za rokovima, težnji da sve bude savršeno, ono najblagotvornije bilo je svetlo koje sam dobijala od svojih najmilijih, svoje porodice, onih bez kojih sve ovo ne bih uspela. Hvala vam, najmiliji moji, na svakom zagrljaju, reči ohrabrenja, držanju straha, vama je uvek bilo jasno kako dišem i kako se osećam. Hvala mojim divnim i požrtvovanim roditeljima, majci Mirjani i mom ocu Vladimiru i mojoj duši najdražoj, sestri Jeleni koja je sa mnom disala i držala me za ruku sve vreme rada na disertaciji. Hvala vam za svaku reč, zagrljaj, ljubav i podršku na koju mogu da računam od kada znam za sebe, hvala što ste celog mog života bili uz mene, u svim ključnim trenucima mi davali bezrezervnu podršku i radovali se sa mnom svakom mom uspehu. Bez vas ja ovo ne bih mogla. Disertaciju posvećujem vama i vašoj bezrezervnoj ljubavi!

Na kraju, zahvaljujem svim članovima Komisije za doktorski ispit i prihvatanje teme, Komisije za ocenu podobnosti teme i kandidata, Komisije za pregled i ocenu doktorske disertacije i Komisije za odbranu doktorske disertacije, na tome što su svoje dragoceno vreme uložili i svojim sugestijama i komentarima pomogli da ova disertacija bude kvalitetnija.

U Beogradu,
28.2. 2022.

mr Valentina Timčenko, dipl.el. inž.

POSVETA

Disertaciju posvećujem svojim roditeljima i sestri, uz veliko hvala
na nesebičnoj podršci i bezrezervnoj ljubavi!

SAŽETAK

Razvoj savremenih mrežnih okruženja se zasniva na primeni različitih tehnologija, povezivanju sa drugim tehnološki drugačijim konceptima i obezbeđivanju njihove interoperabilnosti. Tako složeno mrežno okruženje je neprekidno izloženo različitim izazovima, pri čemu je obezbeđivanje sigurnosti servisa i podataka jedan od najvažnijih zadataka. Novi zahtevi za sisteme zaštite se zasnivaju na potrebi za efikasnim praćenjem i razumevanju karakteristika mrežnog saobraćaja, a uslovljeni su stalnim porastom broja korisnika i razvojem novih aplikacija.

Razvoj rešenja u oblasti detekcije anomalija i napada je postao svojevrsni imperativ, imajući u vidu da se paralelno odvija intenzivni razvoj u oblasti sajber napada. Osim toga, promene mrežnog saobraćaja su postale sve dinamičnije, a kao poseban problem se izdvaja velika heterogenost primenjenih tehnologija i korisničkih uređaja. Iako dostupna literatura prepoznaje veliki broj radova koji se bave analizom tokova mrežnog saobraćaja za potrebe praćenja performansi i sigurnosnih aspekata mreža, mali je broj istraživanja koja se zasnivaju na procedurama generisanja i analize profila ponašanja mrežnog saobraćaja, odnosno specifičnih komunikacionih obrazaca. U tom smislu, analiza ponašanja mreže se u sve većoj meri oslanja na razumevanje normalnih ili prihvatljivih obrazaca ponašanja na osnovu kojih je moguće efikasno otkrivanje obrazaca anomalija. Za razliku od sistema za otkrivanje napada koji se zasnivaju na analizi sadržaja svakog pojedinačnog paketa (*signature-based*), ovaj pristup je izuzetno koristan za identifikaciju nepoznatih pretnji, napada nultog dana, sumnjivog ponašanja i za sveopšte poboljšavanje performansi mrežnih okruženja.

U ovoj doktorskoj disertaciji predložena je nova metoda detekcije napada i anomalija u mrežnom okruženju koja je zasnovana na profilisanju mrežnog saobraćaja. Predložena metoda koristi samo IP (*Internet Protocol*) adrese i brojeve portova koji se prikupljaju primenom NetFlow protokola. Predloženo rešenje vrši specifičnu predobradu tokova mrežnog saobraćaja primenom proračuna entropije, primenjujući je nad određenim atributima (odlikama) instanci tokova mrežnog saobraćaja. Zatim se agregacijom izračunavaju dodatni atributi koji odražavaju komunikacionu aktivnost učesnika u posmatranom vremenskom intervalu, odnosno epohi. Daljom transformacijom generisanih atributa formiraju se karakteristični potpisi kojima se opisuju profili mrežnog saobraćaja. Metoda dalje podrazumeva grupisanje instanci mrežnog saobraćaja u skladu sa definisanim profilima, nad kojima se primenjuje unapređeni algoritam hijerarhijskog aglomerativnog klasterovanja (*Hierarchical Agglomerative Clustering,* HAC).

Disertacija sveobuhvatno sagledava problem detekcije i identifikacije anomalija i napada u savremenim mrežnim okruženjima, pri čemu je primenjen sistematski pristup rešavanju problema. Postupak polazi od osnovnih hipoteza, obavlja se analiza karakteristika tokova mrežnog saobraćaja, a zatim je predloženo novo rešenje koje se zasniva na kombinovanoj primeni različitih tehnika. Primenjene tehnike obuhvataju tehnike za predobradu tokova mrežnog saobraćaja, metode za izračunavanje entropije atributa podataka i tehnike za njihovu agregaciju. Na osnovu tako dobijenih podataka se formiraju specifični potpisi profila mrežnog saobraćaja i primenjuje se modifikovani HAC algoritam klasterovanja.

Osnovna ideja je da se omogući brza i efikasna obrada podataka koji potiču iz realnih mrežnih okruženja, pri čemu je predviđen rad sa neobeleženim podacima, nepotpunim podacima i podacima koji imaju različite dužine tokova. Predloženo rešenje se zasniva na tome da svaki tok podataka ima određeni broj informacionih i volumetrijskih atributa, dok se primenom posebnih tehnika agregacije generišu dodatni atributi ponašanja. Za svaki od njih se u procesu predobrade podataka primenjuju

tehnike agregacije slično kao kod proračuna entropije, a zatim se obrađeni atributi tumače kao poseban potpis toka komunikacije. Jedan od ciljeva istraživanja predstavljenog u disertaciji je pronalaženje metode kojom bi se obezbedilo unapređivanje entropijski zasnovanog rešenja detekcije napada primenom algoritama mašinskog učenja (*machine learning,* ML), pri čemu su obuhvaćena dva nova pristupa.

Prvi pristup se zasniva na primeni *Expectation-Maximization* (EM) algoritma nenadgledanog mašinskog učenja za analizu promene vrednosti entropija. Kroz eksperimentalno dobijene rezultate je ukazano na izvesna poboljšanja kojima ovaj algoritam doprinosi u procesu detekcije napada i anomalija. Za razliku od klasičnog pristupa analizi promene entropija, kao što su metode kliznih vremenskih prozora (*moving window*) i eksponencijalni pokretni prosek (*Exponential Moving Average*, EMA), primenom EM algoritma su se izdvojila sva veća odstupanja od normalnog saobraćaja. Takođe, EM algoritam ima viši stepen nezavisnosti od vrednosti parametra *k*. Multiplikativni parametar *k* se u entropijskoj metodi koristi za fino podešavanje margina detekcije. Zahvaljujući ovoj osobini EM algoritam ne generiše lažne alarme (*False Positive*, FP), koje su inače jedna od slabih tačaka kod primene entropijskih metoda. Rezultati ukazuju na poboljšanja koja je unela primena EM algoritma, pri čemu je u velikom broju slučajeva EM algoritam generisao veći broj klastera i u njima tačno rasporedio instance podataka, sve vreme uzimajući u obzir intenzitet i vreme pojavljivanja napada.

Drugi pristup predstavlja najznačajniji doprinos disertacije, a odnosi se na profilisanje, klasifikaciju i detekciju anomalija na nivou pojedinačnih tokova mrežnih podataka, primenom modifikovanog HAC algoritma. Specifičnom obradom podataka je generisan skup relevantnih atributa ponašanja (*behavior features*) koji se koriste i pri primeni entropijskih pristupa. Atributi se zatim dodeljuju svakoj instanci toka mrežnog saobraćaja kako bi ih dalje koristio algoritam mašinskog učenja. Zatim se primenjuje posebna obrada podataka koja podrazumeva diskretizaciju vrednosti tako dobijenih novih atributa. Vrednosti atributa se diskretizuju u vrednosti iz skupa {0, 1, 2} kojima se označavaju niska (*Low*), srednja (*Medium*) i visoka (*High*) vrednost atributa, respektivno. Ovakva markacija se dalje koristi kao karakterističan potpis komunikacionih aktivnosti, odnosno koristi se kao metod profilisanja najčešćih potpisa u okviru realnog saobraćaja kao i potpisa tipičnih anomalija. Profilisanje se obavlja primenom modifikovanog HAC uz definisanje odgovarajuće funkcije rastojanja.

Opisana metoda omogućava profilisanje svake mrežne komunikacije uz pridruživanje odgovarajućim klasterima normalnog saobraćaja ili anomalija, što osim profilisanja može da služi i za detekciju i identifikaciju anomalija. Preciznost detekcije i identifikacije anomalija je obezbeđena korišćenjem skupa komunikacionih potpisa koji se odnose na opšte modele anomalija i služe kao referentne tačke u procesu klasterovanja. Tokovi koji su blisko grupisani sa ovim tačkama se smatraju odgovarajućom anomalijom. Na osnovu uvida u dostupnu naučnu literaturu, predloženo rešenje predstavlja nov i originalan metod profilisanja i detekcije anomalija mrežnog saobraćaja.

Sveobuhvatnom eksperimentalnom analizom predloženog rešenja za različite scenarije primene dobijen je skup rezultata koji ukazuju na visok stepen efikasnosti i praktične primenljivosti rešenja u realnim mrežnim uslovima.

Ključne reči: detekcija anomalija i napada, algoritmi klasterovanja, entropija, mašinsko učenje.

Naučna oblast: Elektrotehnika i računarstvo

Uža naučna oblast: Računarska tehnika i informatika

UDK broj:

ABSTRACT

The development of the modern network environments, their application, and the dynamics of their interoperability with other technologically different concepts, is based on the application and compatibility of different heterogeneous technologies. Such a complex network environment is constantly exposed to various operational challenges, where ensuring the security and safety of services and data represents one of the most important tasks. The constant increase in the number of users and the intensive development of new applications that require high bandwidth has defined new requirements for security systems, which are based on monitoring and effectively understanding network traffic characteristics. In the light of the increasingly intensive development in the field of cyberattacks, persistent dynamic changes in network traffic, as well as the increased heterogeneity of the used technologies and devices, the development of solutions in the field of anomaly and attack detection has become a kind of imperative. Although the available literature recognizes a large number of papers dealing with the analysis of network traffic flows for the needs of the monitoring of the performance and security aspects of networks, just a few studies are based on the procedures for generating network traffic behavior profiles, or specific communication patterns. In this sense, network behavior analysis relies on an understanding of normal or acceptable behavior patterns, which would allow for the effective detection of unusual, anomalous behavior patterns. Unlike the intrusion detection systems that are based on the packet payload or signature (*signature-based*), this approach is extremely useful not only for the identification of unknown threats, zero-day attacks, and suspicious behavior, but also for the improvement of the overall network performance.

This dissertation proposes a new method for attacks and anomalies detection, which is based on the profiling of the network traffic that uses only IP addresses and port numbers collected via the NetFlow protocol. The proposed solution relies on a specific preprocessing of the network traffic flows by applying entropy calculation over certain attributes of the traffic flow instances. Then, by the means of the aggregation techniques, some additional attributes are calculated, reflecting the communication activity of the participants in the observed time interval - epoch. By the means of the additional transformation of the generated attributes, several characteristic signatures are formed, describing the network traffic profiles. Further, with the application of the enhanced hierarchical clustering algorithm, the traffic instances are grouped according to the defined profiles.

The dissertation encompasses a comprehensive overview of the issues in the field of the detection and identification of anomalies and attacks in modern network environments and applies a systematic approach to solving the issues starting from the defined hypotheses, analyzing the characteristics of network traffic flows, and then proposing a new solution based on the combination of different techniques. It includes the pre-processing of network traffic flows, entropy calculation of attribute values, their aggregation, generation of specific network traffic profile signatures, and the application of a modified hierarchical agglomerative clustering (*HAC*) algorithm.

The basic idea is to enable fast and efficient processing of real network environment data, in the case of working with unlabeled, incomplete, and different flow lengths. The proposed solution is based on the assumption that each data flow includes certain information and volumetric attributes, while the application of special aggregation techniques generates additional attributes, the so-called behavioral attributes. Similar to the entropy-based techniques, in this case, the aggregation is applied over each

data flow, while this way preprocessed attributes are then interpreted as a separate signature of the communication flow. One of the dissertation goals is to find a method that would ensure the enhancement of the entropy-based techniques with the application of different machine learning algorithms, and it relies on the proposal of two new approaches.

The first approach is based on the application of the Expectation-Maximization (EM) unsupervised algorithm for the needs of the analysis of the entropy values variations, whose development and application, through experimentally obtained results, indicated the improvement of the detection results. Unlike the classical approach to the analysis of the entropy values changes, such as the moving windows and Exponential Moving Average (EMA) techniques, the EM algorithm has isolated specific deviations from the normal traffic and its efficiency does not depend on a specific multiplier parameter *k*, which is used in the entropy method to fine-tune detection margins. Also, EM easily clusters the instances without generating the false positive (FP) alarms, which is one of the entropy technique's major weaknesses. The application of the EM algorithm provides improvements, and in many cases the EM algorithm has generated a larger number of clusters while accurately distributing the instances in them, all the time taking into consideration the attack intensity and timing.

The second proposed approach represents the most significant contribution of the dissertation and is based on the profiling, classification, and detection of the anomalies on the flow level based on the application of the modified HAC algorithm. The application of several specific data processing techniques provides the generation and selection of a set of relevant behavioral attributes that are used in the application of entropy-based approaches and then assigned to each instance of network traffic flow, which further allows their use by machine learning algorithms. This approach applies a special data processing, which implies discretization of the values of the new attributes. Attribute values are discretized into categories with values 0, 1, and 2, denoting low, medium, and high values of the considered attribute, respectively. This labeling is used as a characteristic signature of the communication activities, and is used as a method of profiling the most common signatures within real traffic and signatures of typical anomalies, which is provided by the proposed modified hierarchical agglomerative clustering and defining the appropriate distance function.

The described method enables the profiling of each network communication by joining the appropriate clusters of normal traffic or anomalies, which in addition to profiling can also be used to detect and identify anomalies. The accuracy in the process of detecting and identifying anomalies is ensured by the use of a set of communication signatures that refer to general models of anomalies and serve as reference points in the clustering process, with flows closely grouped with these points considered an appropriate anomaly. Based on the available scientific literature, the proposed solution represents a new and original method of profiling and detection of network traffic anomalies. A comprehensive experimental analysis of the proposed solution for different application scenarios has provided a set of results that indicate a high-efficiency degree and practical applicability of the proposed solution in real network conditions.

Keywords: Anomaly and Attack Detection, Clustering Algorithms, Entropy, Machine learning

Scientific field: Electrical and Computer Engineering

Research area: Computer Engineering and Informatics

UDC number:

SPISAK SKRAĆENICA

A

ACK	Acknowledge
APT	Advanced Persistent Threat
AI	Artificial Intelligence

C

CIC	Canadian Institute for Cybersecurity
COD	Clustering with Obstacle

D

DoS	Denial of Service
DDoS	Distributed Denial of Service
DNS	Domain Name System
DT	Decision Trees

E

EMA	Exponential Moving Average
ENISA	European Union Agency for Cybersecurity
EM	Expectation-Maximization
ESS	Error Sum of Squares

F

FG	Flow Generator
FP	False Positive
FTP	File Transfer Protocol

H

HAC	Hierarchical Agglomerative Clustering
HIDS	Host based Intrusion Detection System
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure

I

ICMP	Internet Control Message Protocol
IDE	Integrated Development Environment
IoT	Internet of Things
IDS	Intrusion Detection System
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export

K

KDD	Knowledge Discovery and Data Mining
k-NN	k-Nearest Neighbor

L

LW	Lance-Williams
LDAP	Lightweight Directory Access Protocol
LOF	Local Outlier Factor

M

ML	Machine Learning

N

NIST	National Institute of Standards and Technology
NADS	Network Anomaly Detection System
NIDS	Network Intrusion Detection System
NTP	Network Time Protocol

R

R2L	Remote to Local
RF	Random Forest
ROC AUC	Receiver Operator Characteristics Area Under the Curve

S

SOM	Self Organizing Maps
SSH	Secure Shell
SSE	Sum of Squared Errors
SVM	Support Vector Machine
SYN	Synchronize

T

TCP	Transmission Control Protocol

U

U2R	User to Root
UDP	User Datagram Protocol
UPGMC	Unweighted Pair-Group Method with Centroid Averaging

W

WEKA	Waikato Environment for Knowledge Analysis

SPISAK SLIKA

SPISAK TABELA

SADRŽAJ

1. UVOD

Savremeni okviri razvoja novih tehnologija uslovljeni su diktatom snažnog potrošački orijentisanog tržišta i težnjom za prilagođavanjem potreba za servisima, brzim protocima informacija, prenosu velikih količina podataka, njihovom čuvanju i obradi. Napredne tehnologije u velikoj meri zavise od njihove interoperabilnosti, mehanizama za prevazilaženje problema uzrokovanih heterogenošću, kao i potrebom rada u realnom vremenu. Za moderna mrežna okruženja je postalo karakteristično da se generišu velike količine podataka različitih formata i obima, što direktno implicira veću osetljivost mrežnog saobraćaja na nove generacije i oblike napada, ranjivosti i anomalija.

Uporedo sa dinamičnim razvojem tehnologija, razvijaju se i različiti oblici napada. Napadi su većinom orijentisani ka onemogućavanju pristupa resursima i servisima i kompromitovanju informacija i poverljivih/privatnih podataka. Za zaštitu od napada su nekada bile dovoljne mrežne zaštitne barijere (*firewalls*), koje su uz primenu baze poznatih napada (*signature-based*) uspešno branile mrežu od spoljašnjih napada. Međutim, takva rešenja su se pokazala nedovoljno efikasnim u okvirima kontinualnog integrisanja novih tehnologija. Mnoge savremene tehnologije dodatno zahtevaju podršku za mobilnost i za što jednostavnijom integracijom u okviru savremenih konceptualnih rešenja, kao što su računarstvo u oblaku (*Cloud Computing*), obrada velikih podataka (*Big Data*) i internet stvari (*Internet of Things*, IoT). Nedavni izveštaji tvrde da će do kraja 2022. godine biti više od 29 milijardi uređaja povezanih na Internet, dok će više od 60% biti povezano u nekom obliku IoT okruženja, dok najnovija istraživanja ukazuju na to da su takva predviđanja već uveliko premašena [1]. Ipak, mnoga poslovna okruženja je takva situacija zatekla nespremnima, jer pored visokih zahteva za protokom mrežnog saobraćaja, neophodno je uvesti odgovarajuća rešenja zaštite razmene podataka i infrastrukture, kao i obezbediti odgovarajući nivo privatnosti korisnika. Industrijska praksa i naučna istraživanja pokazuju da se tradicionalne metode zaštite moraju podržati sofisticiranim tehnikama koje će objediniti inteligentno i efikasno detektovanje anomalija i napada.

Sa druge strane, razvoj u oblasti mrežnih napada sve vreme u korak prati razvoj sigurnosnih rešenja, pa su tako napadi postali sofisticiraniji dajući prednost različitim oblicima distribuiranih napada uskraćivanjem usluge (*Denial of Service*, DoS i *Distributed Denial of Service*, DDoS), napadima nultog dana (*zero-day attacks*), *botnet* napadima i drugim naprednim formama napada (*Advanced Persistent Threat*, APT). Sve je češća potreba za udaljenim pristupom računarskim resursima i servisima, nezavisno od lokacije i karakteristika uređaja koje korisnik upotrebljava, tako da rešenja za pravovremeno otkrivanje anomalija i napada postaju posebno bitna karika u bezbednom funkcionisanju mrežnog sistema. Samim tim, u naučno-tehnološkim krugovima postoji stalna potreba da se istražuju tehnike i metode kojima bi se odgovorilo na sve novonastale situacije, a koje su proizvod aktivnosti čitavog spektra različitih anomalija mrežnog saobraćaja, napada i njihovih varijacija.

Agencija Evropske Unije za sajber bezbednost (*European Union Agency for Cybersecurity*, ENISA) je 2020. godine u svom godišnjem izveštaju ukazala na najnovije promene u oblasti mrežnih napada, naglašavajući problem sve učestalijih aktivnosti velikog broja sajber-kriminalnih grupa [2]. NexusGuard je 2019. godine sa posebnom zabrinutošću ukazao na veliki procenat pojačanih DNS (*Domain Name System*) DDoS vektorskih napada, HTTP (*Hypertext Transfer Protocol*) plavljujućih i TCP SYN (*Transmission Control Protocol SYNchronize*) napada [3]. Istraživanja su ukazala na intenzivno dejstvo pojačanih napada zanovanih na mehanizmima refleksije, enkripcije i pojavi novih,

složenijih vektora napada. Utvrđeno je da je 79,7% svih distribuiranih DoS napada iz kategorije SYN Flood, a da ih po učestalosti prate napadi primenom dinamičnih veb (*Web*) servisa, pojačani i reflektovani napadi i viševektorski DDoS napadi. Ove aktivnosti su najčešće usmerene ka povećanoj efikasnosti unutrašnjih napada, jačanju dejstva aktivnosti zlonamernog softvera, *botnet* napada, kao i zloupotrebi prikupljenih korisničkih i autorizacionih podataka. Stalno pojavljivanje novih bezbednosnih pretnji, napada nultog dana i učestala upotreba tehnika kriptografije u generisanju saobraćaja, utiču na potrebu za razvojem inteligentnih sigurnosnih sistema. Međutim, uprkos ubrzanom razvoju još uvek ne postoji jedinstveno sigurnosno rešenje koje bi sveobuhvatno podržalo sve bezbednosne zahteve u svakom od mogućih mrežnih okruženja.

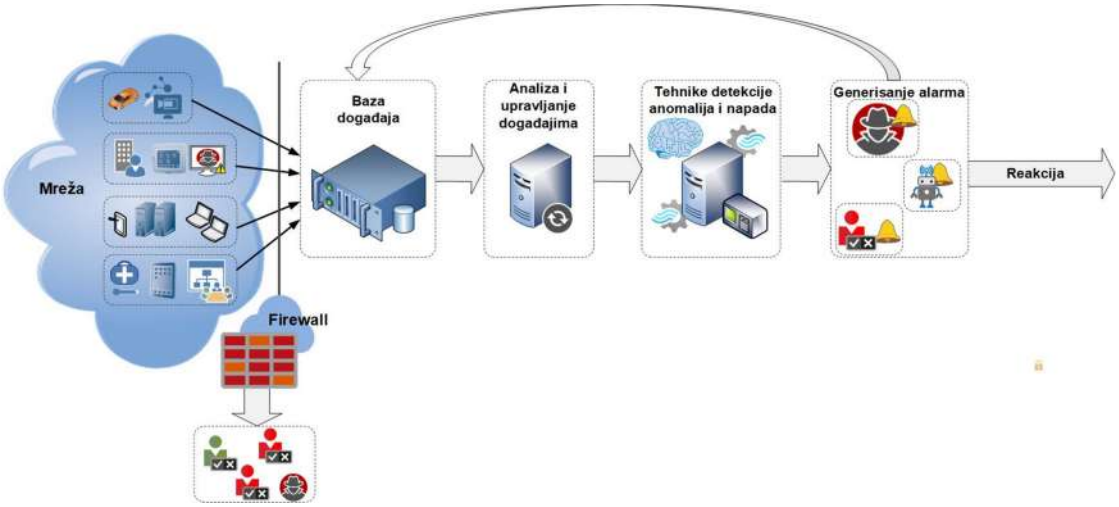
Firewall rešenja obezbeđuju zaštitu lokalne mreže od spoljašnjih napada, propuštajući samo dozvoljeni mrežni saobraćaj. Kriptografijom se obezbeđuje izvestan stepen sigurnosti konekcija u komunikaciji, dok se mere kontrole pristupa prvenstveno koriste za autentifikaciju korisnika. Međutim, tako zadate zaštitne mere su samo donekle primenljive pri odbrani od spoljašnjih napadača, dok je mreža i dalje prilično ranjiva iznutra. Zaštitu na tom nivou su omogućila IDS (*Intrusion Detection System*) rešenja koja se primenjuju za nadgledanje mrežnog saobraćaja i detekciju unutrašnjih i spoljašnjih napada.

Od kada je Doroti Dening [4] razvila i predstavila prvi model sistema detekcije napada IDS opšte namene, naučno-istraživačka zajednica intenzivno radi na razvoju, testiranju i implementaciji brojnih IDS rešenja. Pri tome se vodi računa o specifičnim mrežnim uslovima, korisničkim zahtevima, nameni sistema u koji se implementira kao i resursima koji su dostupni za pravilno funkcionisanje. Ta preteča današnjih IDS sistema je zasnovana na modelu ekspertskog sistema za detekciju napada u realnom vremenu, a koji je trebalo da obezbedi otkrivanje napada na sistem, kao i drugih oblika ugrožavanja bezbednosti u tada najmodernijim računarskim sistemima. Sistem se zasnivao na hipotezi da se napadi i potencijalna ugrožavanja sistema mogu detektovati praćenjem sistemskih zapisa (logova) koji se odnose na neuobičajene (abnormalne) načine korišćenja sistema. Model je predvideo korišćenje profila kojima se opisivalo ponašanje subjekata u odnosu na objekte u smislu metrike i statističkih modela, kao i pravila kojima bi se na osnovu prikupljenih informacija sticalo znanje o ponašanju i omogućila detekcija sumnjivih oblika ponašanja. S obzirom na to da je idejno ovaj sistem trebalo da bude sistem opšte namene, jedan od osnovnih ciljeva tokom razvoja bilo je obezbeđivanje njegove funkcionalne autonomije u odnosu na bilo koji sistem ili njegov deo, nezavisnost od okruženja, korišćenih aplikacija, postojećih ranjivosti sistema ili vrste napada kojem bi bio izložen, čime bi se obezbedio sveobuhvatni okvir ekspertskog sistema za detekciju napada opšte namene. U međuvremenu su se tehnologije razvijale, sistemi usložnjavali, broj korisnika je naglo porastao, a različitosti na nivou korišćenih podataka i njihovih formata su postale jedan od osnovnih problema pri analizi saobraćaja koji se razmenjuje u mrežama.

Savremeni NIDS/NADS (*Network Intrusion Detection System/Network Anomaly Detection System*) sistemi za otkrivanje napada u mreži se mogu definisati kao kombinacija softverskih i/ili hardverskih komponenata koje nadgledaju računarske sisteme i aktiviraju alarm kada dođe do napada. Dinamična i složena priroda današnjih mrežnih napada praktično je povukla mogućnost korišćenja tradicionalnih IDS rešenja, intenzivirajući razvoj metoda detekcije koje su prilagodljive, fleksibilne i primenljive na moderna mrežna okruženja i velike protoke podataka.

IDS treba da bude pouzdan, robustan i otporan na napade, pri čemu bi trebalo da bude u stanju da se brzo oporavi od napada i nastavi da ispravno funkcioniše. S obzirom na to da se današnji mrežni

sistemi, osim po razlikama u veličini, razlikuju po svojoj nameni, operativnom sistemu koji koriste, količini memorijskih resursa, kao i broju i tehnološkoj opremljenosti korisnika, predloženi IDS treba da bude otporan na veliki broj različitih scenarija napada, pouzdan u procesu detekcije, uz minimalan broj generisanih lažnih alarma. Opšti prikaz sistema za detekciju napada je dat na slici 1.1.



Slika 1.1 Opšti prikaz rada IDS sistema

U opštem smislu, IDS sistemi se mogu razmatrati sa različitih aspekata [5]. Literatura prepoznaje nekoliko podela, u zavisnosti od: (1) tipa napadača (spoljašnji, unutrašnji); (2) pozicije izvora informacija koje se koriste za rad IDS sistema (*host-based* IDS, NIDS, hibridni, *application-based*); (3) načina pristupa analizi podataka (*misuse-based*, *anomaly-based*, *specification-based*); (4) pozicije u sistemu koji štiti (centralizovan, distribuiran, hijerarhijski); (5) od odziva (aktivan, pasivan); (6) dinamike analize (*real-time*, *offline*); (7) postupka validacije (simulacija, teorijski pristup, empirijske metode, hipotetički pristup); (8) prirode podataka (*packet-based*, *flow-based*). Sveobuhvatni pregled i opis različitih kategorija IDS sistema je dat u [6–14]. Za potrebe istraživanja predstavljenog u disertaciji primenjen je *anomaly-based* pristup detekciji napada.

IDS zasnovani na detekciji anomalija se oslanjaju na definisani „profil normalnog saobraćaja", koji se kreira na osnovu ponašanja regularnog mrežnog saobraćaja, koji se prati tokom dužeg vremenskog perioda. Međutim, usklađenost/neusklađenost sa normalnim ponašanjem je samo jedan od uslova za efikasnu i tačnu detekciju napada ili anomalija. Pojava naprednijih oblika napada i njihovih varijacija uslovila je da se razvoj IDS sistema zasniva na unapređivanju tehnika generisanja profila normalnog saobraćaja, uzimajući u obzir evoluciju i promene koje bi on mogao da pretrpi tokom vremena, kao i promenljive granice na osnovu kojih se normalno ponašanje razlikuje u odnosu na anomalije. Osim toga, potrebno je redovno otkrivanje i otklanjanje defekata korišćenih skupova podataka, koji mogu dovesti do različitih nepredvidivih problema u procesu detekcije. Zahvaljujući takvom pristupu, ove metode mogu da prepoznaju i nepoznate oblike napada. Osnovni nedostatak ovakvih IDS sistema je potencijalno visok broj generisanih lažnih alarma, pri čemu nije svako odstupanje od profila normalnog saobraćaja obavezno napad ili anomalija, već može pripadati novom legitimnom obrascu ponašanja. Upravo iz tog razloga, veliki broj savremenih IDS rešenja obuhvata zajedničku primenu *anomaly-based* i *misuse-based* pristupa kako bi se ravnomerno iskoristile njihove

prednosti. Postoji nekoliko osnovnih grupa algoritama za otkrivanje anomalija. Algoritmi po kategorijama se razlikuju na osnovu informacija koje koriste u procesu analize i tehnika otkrivanja odstupanja od profila normalnog ponašanja, a mogu biti: (1) statističke metode (*statistical methods*); (2) metode zasnovane na pravilima (*rule-based*); (3) metode zasnovane na udaljenosti (*distance-based*); (4) metode profilisanja (*profiling*); (5) pristupi zasnovani na modelu (*model-based*). Referentna literatura pruža detaljne informacije o svakoj od navedenih grupa metoda [14–21].

Metode profilisanja (*profiling*) predstavljaju skup tehnika koje podrazumevaju generisanje profila normalnog ponašanja za različite vrste mrežnog saobraćaja, korisnike i aplikacije, dok se svako odstupanje od tako generisanih profila smatra napadom [22]. Inicijalno se prikupljaju informacije o različitim obrascima ponašanja saobraćaja u mreži, a koji se odnose i na ponašanje u kontekstu korišćenja različitih mrežnih servisa. Ovako definisani obrasci se zatim u realnom vremenu porede sa generisanim sekvencama i utvrđuje se da li one već postoje u skupu poznatih sekvenci ponašanja. Ukoliko se utvrdi da ne postoje, sistem aktivira odgovarajući alarm. Ove metode mogu da obuhvataju i tehnike rudarenja podataka, a pojedini pristupi su heuristički zasnovani. Pokazalo se da je za profilisanje i definisanje profila normalnog ponašanja mrežnog saobraćaja korisna primena tehnika analize obrazaca povezivanja *(association pattern analysis)*. Ova tehnika se najčešće primenjuje za potrebe obeležavanja normalnih tokova saobraćaja na osnovu kojih je kasnije moguće razlikovanje lažnih od stvarnih alarma i za obezbeđivanje skupa osnovnih informacija vezano za konekcije visokog nivoa u mreži, a koje je sistem za detekciju anomalija rangirao kao izrazito sumnjive [23]. Time je moguće definisati potpise novih napada i proširivati baze podataka sistema za detekciju napada koji su zasnovani na potpisima.

Pristupi zasnovani na modelima primenjuju različite tipove modela kako bi okarakterisali normalno ponašanje sistema koji se nadgleda. U zavisnosti od prirode podataka, tehnike profilisanja se razvijaju u dve grane: tehnike koje se zasnivaju na analizi paketa (*packet-based*) i tehnike zasnovane na analizi tokova podataka (*flow-based*) [24], [25].

U detekciji anomalija na bazi paketa, detektor analizira redom pristigle pakete mrežnog saobraćaja sa ciljem detekcije anomalije. Međutim, ovakav pristup je procesorski, vremenski i memorijski izuzetno zahtevan, pogotovo u kontekstu velikih protoka saobraćaja, gde bi analiza svakog pojedinačnog paketa, u realnom vremenu, bila gotovo nemoguća. Kako bi se rešio problem velikog broja paketa koje je potrebno analizirati u jedinici vremena, u većini ovih rešenja se primenjuje tehnika uzorkovanja. Primenom ovih tehnika, IDS u tačno određenim intervalima vremena uzima pakete na analizu, propuštajući veliki broj paketa bez provere. Time se potencijalno gubi na tačnosti i preciznosti, ali se dobrom izbalansiranošću dužina vremenskih intervala i broja uzorkovanih paketa dobija sistem koji sa zadovoljavajućim nivoom pouzdanosti daje odgovarajući rezultat detekcije. Upravo je precizno određivanje granularnosti jedan od izazova vezanih za proces uzorkovanja. Ukoliko se uzorkovanje odvija češće nego što je optimalno, IDS bi ispitivao nepotrebno veliki broj paketa, čime bi se usporio već dovoljno složen proces detekcije i identifikacije anomalija. Sa druge strane, ako se uzorkovanje dešava ređe nego što bi trebalo, rezultat bi bio nedostatak važnih informacija i nemogućnost detekcije anomalija. U otkrivanju anomalija zasnovanom na tokovima podataka, umesto pojedinačnih paketa IDS analizira tokove saobraćaja koji se uspostavljaju i razmenjuju između izvorišnih i odredišnih čvorova. Kao i u slučaju pri razmeni paketa, IDS pri svom radu može da obuhvati sve tokove, ili može da se ograniči na manji broj tokova koji se dobija primenom metoda uzorkovanja.

Jedan od glavnih izazova u procesu detekcije napada i anomalija mrežnog saobraćaja jeste to kako osmisliti metod za precizno i brzo razlikovanje instanci anomalija od instanci normalnog

saobraćaja. Sve je učestalija primena aplikacija koje su mrežno povezane, a za čije pravilno funkcionisanje je neophodno da se obezbedi odgovarajući protok saobraćaja kao i metode zaštite koje bi radile na osnovu tako utvrđenih različitih obrazaca ponašanja mrežnog saobraćaja. Time bi se omogućila primena pristupa zasnovanog na profilisanju mrežnog saobraćaja na osnovu znanja o specifičnim obrascima ponašanja mrežnog saobraćaja (*traffic behavior profiling approach*). Međutim, razlike koje postoje između instanci normalnog mrežnog saobraćaja i instanci anomalija su često neprecizne i teško uočljive. Osim toga, anomalije su obično sporadični događaji, tako da ne postoji adekvatan skup označenih podataka koji bi mogao da se koristi za obuku i učenje o njima, niti postoji skup podataka za validaciju i dalje istraživanje modela. U praksi je broj instanci anomalija najčešće ozbiljno neuravnotežen u korist broja instanci normalnog saobraćaja, a u nekim slučajevima instance anomalija uopšte nisu dostupne, dok je poseban izazov otkrivanje anomalija i napada kada se u obzir uzima veliki broj različitih strukturalnih i dinamičkih aspekata obrazaca ponašanja mrežnog saobraćaja. Razvoj novih rešenja je snažno usmeren ka sofisticiranim tehnikama detekcije anomalija i napada, među kojima su i tehnike zasnovane na entropiji i primeni različitih algoritama mašinskog učenja.

U kontekstu efikasne primene za potrebe zaštite realnog mrežnog saobraćaja u realnom vremenu, od značaja su tehnike koje imaju mogućnost analize podataka o strukturi mrežnog saobraćaja, a koji se lako prikupljaju primenom NetFlow, IPFIX (*Internet Protocol Flow Information Export*) ili sličnih protokola.

Jedna od karakteristika po kojima se pristup predložen u ovoj tezi razlikuje od ostalih jeste ta da su prikupljene instance tokova saobraćaja podeljene u vremenske epohe odgovarajuće dužine, a koje se zatim agregiraju prema pojedinačnim atributima i kao takve (instance) dalje koriste za izračunavanje dodatnih, relevantnih atributa (*features*). Nad ovim podacima je moguće generisati vremenski niz (*time-series*) vrednosti entropija svakog atributa, pri čemu svaka vrednost odgovara izračunatoj entropiji u jednoj epohi. Ova tehnika pruža širu sliku karakteristika mrežnog saobraćaja u vremenu, uz mogućnost jasnog pregleda i lakog uočavanja promena ponašanja. Međutim, iako je metoda memorijski i procesorski intenzivna, složenost procedure agregacije je linearno proporcionalna protoku mrežnog saobraćaja.

Istraživanjem predstavljenim u ovoj disertaciji je pokazano da se primenom postupka agregacije nad podacima iz ovih skupova podataka mogu dobiti specifični izvedeni atributi koji zajedno sa postojećim atributima mogu da obezbede dovoljno informacija za uspešno izračunavanje entropije. Ipak, tehnike zasnovane na entropiji imaju neke inherentne slabosti, jer su efikasne samo u slučajevima kada se struktura mrežnog saobraćaja značajno menja tokom napada, a neefikasne u slučaju napada ili anomalija čije su komunikacione karakteristike slične karakteristikama normalnog, legitimnog mrežnog saobraćaja [26]. Osim toga, kod tehnika zasnovanih na entropiji, prilikom uočavanja anomalija nedostaje direktna informacija o uzroku napada, što se mora dodatno analizirati. Samim tim, jedan od pokretača ideje na kojoj se zasniva ova disertacija je bila potreba za generisanjem rešenja koje bi obuhvatilo prednosti tehnika zasnovanih na entropiji, a primenom određenih metoda mašinskog učenja značajno unapredilo efikasnost i preciznost otkrivanja anomalija i napada različitih tipova i intenziteta. Primena algoritama mašinskog učenja nije nov pristup, ali njihovo kombinovanje sa drugim pristupima može da poboljša kvalitet i proširi mogućnosti primene rešenja. Razvoj ideje je ukazivao na potrebu hibridnog pristupa analizi instanci mrežnog saobraćaja, kako bi se sa više stepeni slobode vršila detekcija i najupornijih, najsofisticiranijih oblika anomalija, pri čemu je primena nenadgledanih oblika algoritma mašinskog učenja dala sveobuhvatnost pristupu i veću otpornost rešenja na različite oblike napada i anomalija.

Metode mašinskog učenja, bez obzira na to da li su zasnovane na nadgledanom ili nenadgledanom pristupu, razlikuju se u mnogim aspektima od tehnika zasnovanih na proračunu entropije. Tehnike mašinskog učenja koje se zasnivaju na analizi pojedinačnih tokova podataka (*flow level*) obezbeđuju odgovarajući rezultat koji se tumači kroz procese detekcije, odnosno klasifikacije ili klasterovanja. Međutim, problem koji se nameće je da se standardni NetFlow atributi, kao što su izvorišne i odredišne IP adrese i brojevi portova, ne mogu koristiti jer bi doveli do preopterećanja modela (*overfitting*), a koji bi zatim učio o karakteristikama napadača umesto o karakteristikama samog napada [27]. Takve okolnosti su dalje navele na potrebu da se razmatra generisanje novih atributa, a koji su se pokazali kao veoma korisni u procesu detekcije anomalija i napada: veličina paketa, veličina TCP prozora, TCP oznake (*flags*), vreme povratnog puta (*round trip time*), njihove minimalne, srednje i maksimalne vrednosti i vrednosti standardnih devijacija. Glavni problem sa ovim atributima je da oni nisu generički dostupni jednostavnim eksportovanjem informacija o tokovima mrežnog saobraćaja sa rutera, već je potrebno izvršiti ekstrakciju pojedinačnih podataka i zatim obaviti proračune nad sirovim tokovima mrežnog saobraćaja, što značajno otežava proceduru i podrazumeva primenu dodatnih metoda obrade podataka.

Osim toga, treba imati u vidu da se nadgledane tehnike mašinskog učenja mogu primenjivati isključivo ako se radi sa označenim instancama podataka, a da bi napad mogao da bude detektovan, neophodno je da i određeni broj primera instanci napada bude uključen i označen u okviru obučavajućeg skupa podataka. Prednost nadgledanog pristupa je mogućnost izračunavanja određenih korisnih metrika kojima se procenjuje efikasnost algoritama. Većina takvih metrika je izvedena iz matrice konfuzije i vrednosti dobijenih za broj tačnih/pogrešnih (*True*/*False*) pozitivnih/negativnih (*Positive*/*Negative*) instanci. Među najčešće primenjivanim izvedenim metrikama se ističu: preciznost (*Precision*), tačnost (*Accuracy*), opoziv (*Recall*), F-mera (*F-measure*) i karakteristika ROC AUC *(Receiver Operator Characteristics Area Under the Curve)* krive. Međutim, uprkos svim ovim prednostima rada sa označenim instancama, evidentna je njihova nepraktičnost kada se radi sa mrežnim saobraćajem koji se generiše i razmenjuje u realnom vremenu, u stvarnom mrežnom okruženju i koji nije označen. Sa druge strane, tehnike nenadgledanog mašinskog učenja ne zahtevaju označene podatke, ali mogu da budu izuzetno neskalabilne zahvaljujući složenim računarskim procesima, koji su obično u rangu $O(n^2)$ ili $O(n^3)$ vremenske složenost, pri čemu je n broj instanci podataka [28].

U ovoj disertaciji je kroz različite celine predstavljen naučno-istraživački doprinos u ovoj oblasti, a koji se ogleda kroz predlog nove metode detekcije napada i anomalija primenom kombinovanog pristupa koji obuhvata elemente korišćene kod proračuna entropije za generisanje novih atributa i primenu modifikovanog HAC algoritma mašinskog učenja. Glavni doprinos rada se zasniva na tome da se atributi, koji se tradicionalno koriste za izračunavanje entropije kao metrike visokog nivoa za opisivanje karakteristika mrežnog saobraćaja, generišu za svaku instancu toka mrežnog saobraćaja, a zatim se novogenerisani atributi dalje tumače kao poseban potpis obrasca ponašanja mrežnog saobraćaja i koriste za potrebe profilisanja mrežnog saobraćaja kao ulazni podaci za rad optimizovanog HAC algoritma. Otkrivanje i klasifikacija anomalija su obezbeđeni korišćenjem komunikacionih potpisa opštih modela anomalija koji se koriste kao referentni u procesu grupisanja, a tokovi koje je moguće grupisati ovim grupama tačaka se smatraju odgovarajućom anomalijom.

U slučaju analize mrežnog saobraćaja, od suštinske važnosti je obratiti pažnju na strukturu podataka koji se analiziraju. Za potrebe istraživanja predstavljenog u disertaciji, analiza je posebno obavljena nad sirovim podacima slobodno dostupnih skupova podataka koji su odabrani za potrebe evaluacije rešenja, a zatim je analiza obavljena nad podacima koji su dobijeni modifikacijama,

adaptacijama i proširivanjem početnog skupa podataka. Proces modifikacije početnog skupa podataka se zasniva na specifičnoj predobradi podataka primenom metoda agregacije, slično kao kod metoda računanja entropija kojima se dobijaju novi atributi (u disertaciji nazvani „atributi ponašanja") kao i eliminacijom iz proračuna onih atributa koji ne doprinose učenju ili efikasnoj primeni analiziranih algoritama.

1.1 Ciljevi i značaj istraživanja

Ciljevi ostvareni tokom istraživanja se mogu predstaviti na sledeći način:

(1) Dat je predlog principa konstruisanja novog modela sistema detekcije anomalija i napada na bazi analize dodatno izvedenih parametara komunikacionih tokova mrežnog saobraćanja kombinovanom primenom metoda proračuna entropije i algoritama mašinskog učenja.

(2) Uvedena je modifikacija skupova podataka, koja je podrazumevala da se skupovi očiste od neispravnih instanci. Skupovi su zatim obogaćeni sintetički generisanim instancama kojima su simulirane tipske anomalije u mrežnom saobraćaju. Na osnovu toga su generisani novi skupovi podataka obradom podataka primenom softverskih alata za računanje entropije distribucije podataka o karakteristikama.

(3) Definisan je novi pristup analizi tokova mrežnog saobraćaja zasnovan na primeni agregacije, a zatim primeni diskretizacije odgovarajućih vrednosti dobijenih atributa ponašanja, na osnovu koje je omogućeno generisanje odgovarajućih potpisa. Za tako dobijene potpise je utvrđeno da su relevantni indikatori prisustva instanci saobraćaja koje mogu da se povežu sa odgovarajućim komunikacionim modelima.

(4) Ostvarena je obrada, implementacija i testiranje odabranih algoritama mašinskog učenja nad modifikovanim i novim skupovima podataka.

(5) Definisane su karakteristike i unešene neophodne modifikacije HAC algoritma nenadgledanog mašinskog učenja, koji je zatim verifikovan kroz odgovarajuću eksperimentalnu analizu.

Značaj predstavljenog istraživanja se ogleda kroz definisanje i primenu novog pristupa i sistema za koji je kroz eksperimentalnu analizu utvrđeno da može da obezbedi veći nivo sigurnosti u uslovima realnog korišćenja mrežnih usluga. Visok nivo bezbednosti u mreži je od posebnog značaja naročito u slučajevima potrebe za hitnim intervencijama i sistemima posebne namene. Tada je od najveće važnosti da se pravovremeno (skoro u realnom vremenu) i potpuno otkrivaju maliciozne aktivnosti i anomalije, otklanjaju otkrivene ranjivosti sistema, utvrdi tip sigurnosnih pretnji za tu specifičnu mrežnu infrastrukturu, vrstu saobraćaja ili nivo uspostavljene zaštite.

1.2 Polazne hipoteze

Osnovne hipoteze na kojima se zasniva istraživanje:

(1) *Postoji mogućnost da se predloži novi metod analize i profilisanja mrežnog saobraćaja zasnovan samo na osnovnim informacijama o učesnicima u komunikacijama (IP adrese i portovi), a koji bi se koristio za detekciju anomalija kao indikacije napada.*

Izbor metoda detekcije napada i anomalija u velikoj meri zavisi od karakteristika dostupnih podataka. Nove metode mašinskog učenja se u velikoj meri oslanjaju na detaljnije, granularnije pretprocesiranje ulaznih podataka, ulaženje dublje u strukturu podataka i prepoznavanje specifičnih obrisa profila saobraćaja, kao i na poređenje karakteristika atributa instanci saobraćaja sa osnovnim karakteristikama prisutnim kod normalnog saobraćaja. Tom prilikom se često kombinuje više metoda kako obrade podataka tako i mašinskog učenja, pri čemu se u tom domenu potenciraju kombinovani pristupi zasnovani na primeni metoda grupnog učenja (*ensemble*), grupisanja (*clustering*), polu-nadgledanog učenja i drugi.

(2) *Predloženi metod može da omogući detekciju poznatih i nepoznatih napada i anomalija.*

Metode otkrivanja napada na osnovu zapisa iz sadržaja paketa (*signature-based IDS*) su efikasne samo za poznate napade, dok ovakav pristup ne može da se primeni za detekciju novih napada, tzv. napada nultog dana, kao i napada i anomalija čiji je sadržaj šifrovan. Potrebna je primena sofisticiranih i brzih metoda detekcije nepravilnosti i neusaglašenosti sa već naučenim osobinama sličnih napada, čime se obezbeđuje pravovremeno izolovanje takvog saobraćaja i smanjuje njegovo maliciozno dejstvo.

(3) *Predloženi model je nezavisan od tipa napada, broja napadača, trenutka u kojem dolazi do napada ili anomalije, kao i karakteristika generisanog saobraćaja anomalije/napada.*

Prilikom razvoja modela za detekciju napada i anomalija, potrebno je uzeti u obzir potencijalnu primenu u različitim mrežnim okruženjima, pri čemu je cilj obezbediti skalabilnost modela u kontekstu povećanja broja učesnika u komunikaciji, promene profila trenutno ispitivanog saobraćaja, povećanja protoka i količine informacija koje je potrebno obraditi, kao i aktivnog ispitivanja i primenu trenutno najpovoljnijeg algoritma mašinskog učenja.

(4) *Postoji mogućnost definisanja skupa kombinovanih algoritama mašinskog učenja za efikasan rad u sistemu sa strukturalno različitim ulaznim podacima.*

Pristup kombinovanog mašinskog učenja u kontekstu ove teze je predviđen kroz primenu metoda različitih algoritama nadgledanog i nenadgledanog mašinskog učenja i njihovog kombinovanja sa metodom zasnovanom na entropiji. Inicijalno je predviđena analiza rešenja primenom kompozitnih klasifikatora (*ensemble classifiers*), SVM i *Random Forest* (RF) algoritama, a zatim je istraživanje usmereno na primenu algoritama grupisanja (*clustering*), pri čemu je posebna pažnja posvećena primeni nenadgledanih algoritama mašinskog učenja: *Expectation-Maximization* algoritma i modifikovanog hijerarhijskog aglomerativnog algoritma klasterovanja. Predviđeno je da se ove različite metode mogu kombinovati u procesu predobrade podataka, pri nadgledanom i nenadgledanom mašinskom učenju.

U obradi teme doktorske disertacije, pored opštih metoda naučnog istraživanja, primenjene su metode modelovanja, funkcionalne analize i simulacije, pri čemu su analizirani različiti oblici sigurnosnih pretnji [29-39].

1.3 Organizacija teze po poglavljima

Ova teza je organizovana na sledeći način.

Poglavlje 2 daje prikaz problema koji se istražuju u ovoj oblasti, kao i detaljan pregled referenci koje su obeležile najznačajnije pristupe rešavanju problema, sa posebnim osvrtom na radove koji se konkretno bave sličnom problematikom predstavljenom u ovoj disertaciji.

U poglavlju 3 su date definicije napada i anomalija i izložen je kratak opis kategorija i vrsta napada u savremenim mrežnim okruženjima.

U poglavlju 4 je uveden koncept mašinskog učenja i dat je sveobuhvatan prikaz različitih kategorija algoritama i metoda mašinskog učenja uz kratak opis najkarakterističnijih tehnika. Posebna pažnja je posvećena tehnikama mašinskog učenja koje su primenjene u okviru predloženog rešenja sistema za detekciju anomalija i napada. U posebnim odeljcima su dati opisi algoritama nenadgledanog mašinskog učenja koji su analizirani, unapređeni i primenjeni u okviru predloženog rešenja.

Poglavlje 5 je posvećeno entropijski zasnovanim metodama koje se koriste u nekim rešenjima sistema za detekciju napada i anomalija, a koje su primenjene u procesu predobrade podataka korišćenih za potrebe istraživanja predstavljenog u ovoj disertaciji.

U poglavlju 6 su predstavljeni korišćeni softverski alati i okruženja za potrebe pretprocesiranja podataka i primene modifikovanih algoritama mašinskog učenja u okviru predloženog rešenja sistema detekcije anomalija i napada.

Poglavlje 7 je u potpunosti posvećeno predloženom originalnom rešenju sistema za detekciju napada i anomalija i primeni modifikovanih algoritama nenadgledanog mašinskog učenja. Ovo poglavlje je podeljeno u nekoliko celina, u skladu sa fazama istraživanja. U prvom delu je predstavljena arhitektura predloženog sistema i metodologija njegovog razvoja. Detaljno su obrazloženi koncept rešenja, struktura podataka, predstavljena je arhitektura na kojoj se zasniva predloženo rešenje i data je taksonomija komunikacionih modela na osnovu koje je dalje razvijano predloženo rešenje. U drugom delu poglavlja su sistematično predstavljeni ostvareni istraživački rezultati zasnovani na primeni *Expectation-Maximization* algoritma mašinskog učenja. Rezultati ostvareni u toj fazi istraživanja su dali smernice daljeg razvoja rešenja. U ovom poglavlju je zatim predstavljen najvažniji deo ovog istraživanja, kroz detaljan, sveobuhvatan i sistematičan prikaz primene predložene metode diskretizacije vrednosti generisanih atributa i formiranje specifičnih potpisa ponašanja tokova podataka, koji su zatim korišćeni u primeni modifikovanog HAC algoritma mašinskog učenja, za potrebe pouzdane i efikasne detekcije anomalija i napada.

Na osnovu predloženog originalnog rešenja sistema za detekciju napada i anomalija, u poglavlju 8 su predstavljeni rezultati dobijeni na osnovu detaljno izložene eksperimentalne procedure, na osnovu kojih je izvršena validacija predložene metode.

U poglavlju 9 su predstavljena zaključna razmatranja.

U prilogu 1 je dat spisak publikovanih radova koji su proistekli kao rezultat istraživanja predstavljenog u ovoj disertaciji.

2. PREGLED ISTRAŽIVANJA U OBLASTI

Jedan od najjačih pokretača naučno-istraživačkog rada i tehnološkog razvoja u oblasti novih tehnologija i heterogenih okruženja su hiperaktivni, izuzetno zahtevni i tehnološki osvešćeni korisnici, koji zahtevaju pouzdano, efikasno, sadržajno i sigurno okruženje. Sa druge strane, sve je raširenije prisustvo IoT zasnovanih tehnološki povezanih okruženja, usidrenih u nekom od dostupnih koncepata računarstva u oblaku (*Edge Computing*, *Fog Computing*) za potrebe čuvanja i obrade različitih količina podataka, u realnom ili blisko realnom vremenu. Takve okolnosti pružaju plodno tle za pojavu različitih bezbednosnih problema, motivišući naučnu zajednicu da radi na iznalaženju pouzdanijih i efikasnijih rešenja sistema za detekciju mrežnih anomalija i napada. U oba slučaja važno je obezbediti odgovarajući mehanizam za njihovo otkrivanje.

Dostupna literatura obiluje istraživačkim radovima koji se bave različitim pristupima problemu obezbeđivanja sigurnosti u mrežnom okruženju. Prethodnica danas dostupnih rešenja je svoje predloge uglavnom zasnivala na primeni nekog od *host-based* IDS (HIDS) oblika zaštite, koji prate određeni uređaj odnosno host. Takva zaštita je bila prilično ograničena, a pojavom sve većih mrežnih okruženja postala je i neodrživa.

Prvi mrežni sistemi detekcije anomalija i napada NADS/NIDS su bili zasnovani na primeni baze znanja o prethodno naučenim napadima (*misuse-based*). Međutim, vremenom su takvi sistemi postali neefikasni u kontekstu pojave novih napada ili varijacija postojećih napada za koje nije bilo moguće prepoznavanje. Bilo je neophodno napraviti pomeraj ka sistemima koji će ući dublje u suštinu problema, učiti o specifičnostima ponašanja takvih pojava u mreži, analizirati strukturu podataka, utvrđivati razlike koje se pojavljuju u odnosu na uobičajeno mrežno ponašanje i na osnovu njih reagovati u skladu sa definisanim procedurama (*anomaly-based*). Širok spektar različitih tehnologija i mrežnih struktura je uslovio potrebu za razvojem i primenom IDS sistema zasnovanih na skupu specifičnih *custom-made* pravila i algoritama na osnovu kojih se vrši detekcija i identifikacija napada i anomalija. Pri tome, sistem se smatra bezbednim ukoliko je ispunjeno trojstvo računarske bezbednosti: poverljivost, integritet i dostupnost [40].

Naučno-tehnološka istraživanja su već neko vreme orijentisana na rad u oblasti razvoja tehnika za izdvajanje različitih profila ponašanja mrežnog saobraćaja. Ovaj pristup se zasniva na analizi obrazaca ponašanja mrežnog saobraćaja (*traffic patterns*), na osnovu čega je dalje omogućeno prepoznavanje sličnih obrazaca. Rešenja su većinom definisana u skladu sa strukturom mrežnog saobraćaja, profilima ponašanja mrežnog saobraćaja i rutinama u ponašanju. Neka rešenja koriste *benchmarking* okruženja u vidu specifičnih redovno ažuriranih skupova podataka koji se koriste za analizu na osnovu koje se sa većom pouzdanošću prate dalje promene uslova posmatranog mrežnog saobraćaja [29], [41]. Ipak, osnovni problem je što većina studija cilja samo na određenu grupu anomalija, ili analizira vrlo specifične strukture podataka i okruženja.

Uprkos velikom broju različitih pristupa ovom problemu najsavremenije tehnike detekcije napada su vrlo često zasnovane na korišćenju tokova podataka mrežnog saobraćaja. Iako se ponekad smatraju manje tačnim i preciznim u poređenju sa algoritmima zasnovanim na analizi paketa mrežnog saobraćaja u slučaju kada se kombinuju sa nekim dodatnim tehnikama mogu efikasno da obezbede i tačnije rezultate. U prilog tome, najnovije istraživačke inicijative ukazuju na tendenciju ka finijoj granulaciji sistematskih procedura koje koriste rešenja za detekciju anomalija, čime se promoviše

iscrpna predobrada informacija, a zatim primena različitih algoritama mašinskog učenja [42], [36], [37]. Osim toga, intenzivirano je istraživanje u oblasti primene tehnika dubokog učenja, pri čemu je fokus na otkrivanju napada nultog dana i detekciji izuzetaka (*outliers*) [43–47].

Jedan od pravaca razvoja sistema za detekciju napada i anomalija podrazumeva primenu sofisticiranih statistički zasnovanih metoda analize tokova podataka mrežnog saobraćaja. U tom kontekstu, dominantno je prisutan koncept zasnovan na proračunu raspodele entropije podataka, a zatim analize tako obrađenih podataka. Kada se primenjuje za potrebe detekcije anomalija i napada, entropija se kao mera može koristiti za predstavljanje nivoa slučajnosti u raspodeli podataka mrežnog saobraćaja [48]. Tehnike zasnovane na entropiji su se pokazale izuzetno efikasnim u okolnostima gde je prisutan anomalan saobraćaj visokog intenziteta, ukazujući na značajne skokove u raspodeli podataka kada se pojave anomalije i ne ostavljajući takve događaje nedetektovanim [49]. Pri primeni entropijski zasnovanih metoda detekcije, glavni oslonac su efekti inherentnih karakteristika entropije mrežnog saobraćaja. Tako su, u slučaju instanci normalnog saobraćaja, izračunate vrednosti entropije uglavnom konstantne, sa nekim sporadičnim, manjim odstupanjima, dok se pojavom instanci anomalnog mrežnog saobraćaja vrednosti entropije za određene atribute tog saobraćaja značajno menjaju. Tako je u radu [50] predloženo rešenje detekcije *botnet* malvera (*malware*) primenom proračuna entropije profila malicioznog mrežnog saobraćaja. Iako ova studija tvrdi da su pri detekciji vrhova i repova raspodela entropija napada parametrizovani oblici proračuna entropije, Rényi i Tsallis [51], [52], dominantno bolji u odnosu na standardnu Šenonovu entropiju, istraživanja koja su rađena i za potrebe ove disertacije pokazuju da se takvi zaključci ne mogu generalizovati i da zavise od primenjenih metoda detekcije, karakteristika podataka i izbora atributa obuhvaćenih analizom [27], [39].

Tokovi podataka mrežnog saobraćaja se u pojedinim studijama smatraju nedovoljno detaljnim izvorima informacija. Ipak, brojna druga istraživanja pokazuju da analiza zasnovana na tokovima podataka omogućava brži odziv na promene, nije previše zahtevna po pitanju mrežnih resursa i daje dovoljno kvalitetan odgovor na događaje u mreži, što je naišlo na odobravanje među brojnim istraživačima. Međutim, da bi istraživanja mogla da se obavljaju, neophodno je imati dovoljan broj kvalitetnih, slobodno dostupnih skupova podataka, što je motivisalo istraživače da generišu svoje skupove podataka [53]. *Sperotto* skup podataka je prvi skup podataka zasnovan na označenim instancama tokova mrežnog saobraćaja. Odmah nakon što je objavljen, pojedini istraživački timovi su ga koristili i prilagođavali svojim oblastima rada [54]. Tako je Winter ovaj skup prilagodio za istraživanja metode potpornih vektora (*Support Vector Machine*, SVM) [55]. Prekretnica je možda ipak bila pojava dva skupa, CTU-13 i UNSW-NB15, kojima je obuhvaćeno normalno ponašanje mrežnog saobraćaja savremenih mrežnih okruženja, kombinovano sa savremenim sintetizovanim instancama napada [56], [57]. UNSW-NB15 je jedan od najsveobuhvatnijih, modernih skupova podataka o mrežnom saobraćaju koji pokriva širok spektar napada i anomalija. U literaturi je često korišćen kao *benchmarking* okruženje za analizu atributa mrežnog saobraćaja i evaluaciju tehnika redukovanja broja analiziranih atributa zasnovanih na primeni algoritama mašinskog učenja. CTU-13 je skup podataka koji je orijentisan ka *botnet* saobraćaju. Sadrži 13 grupacija instanci koje odgovaraju različitim oblicima malvera koji se može pronaći u realnom mrežnom okruženju [58], [59]. U [60] autori su koristili CICIDS2017 za procenu četiri različita algoritma koji se mogu koristiti za izbor relevantnih atributa podataka mrežnog saobraćaja. Cilj studije je bila dalja analiza IDS rešenja sa tako definisanim suženim skupom atributa i primena nadgledanih algoritama mašinskog učenja [61]. Neki autori su ovaj skup koristili za razmatranje tehnika koje se primenjuju kod preteranog uzorkovanja podataka

(*oversampling*), tehnika za izbor optimalnog skupa atributa i redukciju broja atributa iz dostupnog skupa podataka. Primenom ovih tehnika se omogućava efikasno pretprocesiranje podataka i njihova primena za generisanje rešenja zasnovanih na *ensemble* algoritmima mašinskog učenja [62]. Za potrebe istraživanja predstavljenog u ovoj disertaciji preuzeti su CTU-13 i CICIDS2017 skupovi podataka, a zatim su modifikovani za dalji rad.

Tokom istraživačkog rada predstavljenog u ovoj disertaciji jedan od koraka bio je primena postupka agregacije nad podacima u cilju generisanja skupa izvedenih atributa koji bi zajedno sa postojećim atributima obezbedili dovoljno informacija za uspešno izračunavanje entropije. Međutim, uprkos svojoj efikasnosti u slučajevima kada se struktura mrežnog saobraćaja značajno menja tokom napada, primena proračuna entropije je pokazala slabosti i neefikasnost u slučajevima analize instanci tokova napada ili anomalija koje su sličnih komunikacionih karakteristika normalnom mrežnom saobraćaju [26]. Samim tim, glavna prekretnica u naučno-istraživačkom radu na kojoj se zasniva ova disertacija bila je potreba za kreiranjem sveobuhvatnog rešenja koje bi integrisalo modifikovane metode i tehnike mašinskog učenja, a sa druge strane u potpunosti iskoristilo prednosti tehnika zasnovanih na entropiji. Počev od niza eksperimenata koji su podrazumevali primenu različitih algoritama nadgledanog mašinskog učenja (*ensemble*, SVM, stablo odlučivanja i metoda detekcije izuzetaka), tok istraživanja je vodio ka ispitivanju mogućnosti primene nekog od metoda koji bi mogao da se primeni i nad neoznačenim podacima, a koji bi bio efikasan i pouzdan u procesu detekcije. Razvoj ideje je ukazivao na potrebu primene nekog od nenadgledanih algoritama mašinskog učenja, konkretno algoritama klasterovanja, dok je kombinovanim pristupom analizi instanci mrežnog saobraćaja obezbeđen veći stepen slobode u detekciji i identifikaciji šireg spektra napada i anomalija. Upravo je primena nenadgledanih oblika algoritama mašinskog učenja dala tu sveobuhvatnost pristupu i obezbedila veću otpornost predloženog rešenja na različite oblike napada i anomalija.

U korist ovakvog pristupa je veliki broj različitih istraživanja koja se bave primenom mehanizama zaštite, posebno u slučajevima naglo povećanog obima napada i novih oblika već poznatih napada (npr. distribuirani IoT DoS). Jedan od ključnih momenata u određivanju usmeravanja toka istraživanja u ovoj oblasti bila je pojava vrlo razornih IoT *botnet* napada. Među prvima, Mirai IoT napad je 2016. godine izazvao značajnu štetu mnogim svetski poznatim sajtovima, kao što su PayPal, Netflix, Visa i Amazon [63]. Pojavila su se IDS rešenja koja su IoT orijentisana, pri čemu neka koriste prikupljena znanja o napadima i primenjuju tehnike *MapReduce*, klasterovanja i tehnike glasanjem [64]. U istraživanju predstavljenom u [65], autori ukazuju na prednosti veštački obučenih tehnika u obezbeđivanju sigurnosti mreža i mrežnih sistema, dok neka istraživanja novijeg datuma predlažu primenu IoT-NADS rešenja u oblaku, zasnovanih na specifičnom obliku kombinovanog *ensemble* i dubokog mašinskog učenja [40]. Sa druge strane, u nekim studijama novijeg datuma se primenjuju metode granularnog učenja i računarstva za rešavanje problema u oblasti veštačke inteligencije (*Artificial Intelligence*, AI) i mašinskog učenja (ML) [66].

Istraživanjem predstavljenim u ovoj disertaciji je pokazano da je potrebno nastaviti sa intenzivnim istraživanjem metoda primene različitih algoritama nenadgledanog mašinskog učenja, upravo zbog njihove mogućnosti rada u realnom vremenu, sa potpuno neoznačenim podacima.

U [67] autori koriste tokove podataka mrežnog saobraćaja za potrebe analize različitih tehnika analize mrežnog saobraćaja. Rezultati ukazuju na to da se analizom raspodele vrednosti različitih atributa instanci mrežnog saobraćaja mogu dobiti korisni podaci o strukturi instanci anomalija mrežnog saobraćaja, na osnovu kojih je kasnije moguća lakša detekcija njihovog prisustva. Pristup se zasniva na

primeni proračuna entropije u procesu sumarizacije instanci mrežnih tokova, pri čemu se dobijaju raspodele vrednosti atributa mrežnog saobraćaja na osnovu kojih je dalje bilo moguće smislenije grupisanje anomalija. Međutim, uprkos izuzetnom bogatstvu u broju i raznovrsnosti studija koje se bave oblašću detekcije anomalija mrežnog saobraćaja, vrlo malo njih daje dovoljno primenljive rezultate vezane za primenu nenadgledanih algoritama mašinskog učenja, a posebno nisu u dovoljnoj meri zastupljeni algoritmi klasterovanja za koje se pokazalo da su od velike važnosti kada se radi sa retkim i neoznačenim instancama mrežnog saobraćaja [68].

Algoritmi hijerarhijskog klasterovanja omogućavaju koncizno sumiranje podataka, obezbeđujući različit stepen granularnosti, što omogućava njihovu primenu u slučajevima kada postoje ograničenja dostupne memorije, kao što je slučaj pri radu sa tokovima podataka (*data streams*) [69]. Pojavom nekoliko skalabilnih hijerarhijski zasnovanih algoritama klasterovanja, BIRCH i CURE, omogućen je efikasniji rad sa velikim skupovima podataka [70], [71], a većina algoritama klasterovanja koji se primenjuju za obradu podataka zadatih u obliku vremenskih serija se praktično zasnivaju na nekom obliku hijerarhijske strukture [71], [72]. Za razliku od algoritama klasterovanja zasnovanih na proračunu rastojanja između instanci podataka [73], hijerarhijske forme algoritama klasterovanja se sve više primenjuju za potrebe primene u aplikacijama koje funkcionišu u realnom vremenu [74–77].

Hijerarhijski aglomerativni algoritmi (HAC) predstavljaju jednu od najbrže razvijanih grupa algoritama nenadgledanog mašinskog učenja [78–82]. Izbor kriterijuma povezivanja (*linkage criterion*) ima snažan uticaj na ostvarive performanse klasterovanja određenog algoritma, tako da se brojna istraživanja bave mogućnostima optimizacije i generalizacije kriterijuma povezivanja kako bi se omogućio efikasniji rad sa manjim brojem generisanih klastera [83], [84]. U [85] autori kombinuju HAC i dinamičko *k-NN* (*k-nearest-neighbor*) za potrebe generisanja liste *k* najbližih suseda za svaki kreirani klaster, čime se obezbeđuje skraćivanje vremena računanja koje je inače neophodno u slučaju primene Vardove (*Ward*) metode povezivanja [86]. Neke studije predlažu proračun novih, kombinovanih metrika sličnosti koje se zasnivaju na kombinovanju postojećih mera sa novim parametrima, poput koeficijenta rekonstrukcije. Osnovna ideja je da se obezbedi veća robusnost pri radu sa podacima koji obiluju šumom i izuzecima (*outliers*), gde je neophodno što preciznije izračunavanje udaljenosti parova instanci pri HAC klasterovanju [87].

Iako su u mnogim situacijama efikasne, pomenute tehnike imaju nekoliko nedostataka, tako da su razvijene posebne metode hibridnog klasterovanja. Na primer, jedan takav pristup se zasniva na primeni tehnika ispravljanja pogrešno klasifikovanih instanci podataka pri hijerarhijskom grupisanju, a koji se oslanja na kombinaciju hijerarhijskog i *k-means* klasterovanja [88]. Inicijalno, ova metoda obavlja hijerarhijsko klasterovanje podataka na osnovu kojeg se donosi odluka o postavljanju lokacija i početnom broju instanci podataka u svakom od klastera. Zatim se primenjuje *k-means* algoritam sa tako definisanim početnim parametrima. Međutim, iako zasnovan na dobrim hipotezama, ovaj metod je primenljiv samo za rad sa numeričkim tipom podataka. Sličan pristup je zastupljen u još nekim studijama, gde je primenjeno dvostepeno hibridno klasterovanje. Osnovna ideja je da se inicijalno dobijaju male grupe klastera, pri čemu u toj fazi korisnik bira da li će primeniti hijerarhijsko ili *k-means* klasterovanje, a zatim se u drugoj fazi vrši ponovno klasterovanje tako dobijenih malih klastera, ali isključivo primenom hijerarhijskih metoda klasterovanja [89], [90].

S obzirom na to da se istraživanje predstavljeno u ovoj disertaciji jednim svojim delom zasniva na izračunavanju vrednosti entropije atributa podataka u vremenskim epohama, koje se oslanja na agregaciju određenog broja instanci tokova podataka za koje se dalje izračunava entropija, jedan od inicijalnih koraka je bio pronalaženje referenci koje bi dale okvirne informacije o sličnim pristupima.

Tako je u [22] analizirana primena pristupa zasnovanog na profilisanju ponašanja mrežnog saobraćaja u realnom vremenu sa ciljem detekcije anomalija i napada. Pristup je fokusiran na podatke o mrežnom saobraćaju koji su zadati na nivou veze (*link-level*), a koji su u cilju otkrivanja specifičnih obrazaca ponašanja obrađeni tehnikama zasnovanim na proračunu entropije i metodama rudarenja podataka [91]. Međutim, iako je to istraživanje zasnovano na primeni agregacije tokova mrežnog saobraćaja, ono u obzir uzima samo dva dodatna atributa, veličinu paketa i brzinu prenosa paketa, zasnivajući se na zaglavlju paketa i informacijama o vremenu sa ciljem da se poveća otpornost rešenja na pojavu lažno pozitivnih alarma. Druga bitna razlika je to što autori koriste jednosmerne tokove agregiranog mrežnog saobraćaja, dok je istraživanje predstavljeno u ovoj disertaciji zasnovano na formiranju dvosmernih tokova podataka, čime su dobijene dodatne informacije, a omogućeno je jasno prepoznavanje inicijatora komunikacije (prepoznatog po izvorišnoj IP adresi i broju porta) i odredišnog uređaja koji šalje odgovore u okviru komunikacije. U [92] je dat pristup koji se zasniva na primeni agregacije nad dvosmernim tokovima podataka. Autori su primetili prednosti primene agregacije u cilju dobijanja konkretnijih informacija vezano za neke specifične oblike napada, za čije efikasnije detektovanje su primenom agregacije generisali dva nova atributa, *number of flows* i *source ports delta*, a zatim primenili veštačke neuralne mreže. Za razliku od pristupa predstavljenog u ovoj disertaciji, autori se nisu bavili entropijski zasnovanim pretprocesiranjem podataka, već su agregaciju primenjivali nad sirovim instancama tokova podataka, čime je onemogućeno korišćenje svih prednosti entropijski zasnovanih metoda kao i fino podešavanje parametara algoritma kojima bi se na efikasniji način vršila detekcija napada i anomalija. Pristup predstavljen u ovoj disertaciji omogućava veću primenljivost i pokriva detekciju šireg spektra potencijalnih napada i anomalija, pri čemu je ključan doprinos primena diskretizacije dobijenih vrednosti entropija za 34 novogenerisana atributa nakon primenjene agregacije korišćenjem autentičnog algoritma generisanja ključeva agregacije.

Osim toga, u literaturi se može naći svega nekoliko skupova podataka koji su zasnovani na instancama sa malim brojem atributa kojima se predstavlja kardinalnost pojavljivanja nekog drugog atributa u određenom broju vremenski uzastopnih instanci podataka, kao što je, na primer, broj pojavljivanja iste izvorišne IP adrese u poslednjih 100 instanci podataka [93–95]. Takvi atributi reflektuju izvesnu zavisnost drugih atributa u vremenu, a kako većina napada koji su analizirani pomoću takvih skupova podataka za svoju aktivnost koristi vremenski interval duži od 2 sekunde, autori ovih skupova podataka su produžili vremenski interval u kojem se nadgleda rad mreže i umesto njega koriste prozor konekcije (*connection window*) koji je zadat da ima veličinu od 100 konekcija (instanci). Tako, u slučaju UNSW-NB15 skupa podataka, autori ističu postojanje ovih posebno generisanih atributa koje su nazvani „atributi veze" (*connection features*), a koji su generisani na osnovu 100 uzastopnih instanci tokova zadatih u vremenu [96]. U slučaju starijeg, prevaziđenog KDD99 skupa podataka, ovi atributi su definisani kao karakteristike „saobraćaja" (*traffic features*). Fokus je na atributima kojima se opisuje „isti domaćin" i „ista usluga", dok su u skupu podataka Kyoto 2006+ samo dva atributa kreirana ovom logikom [93], [94].

Glavni doprinos ove disertacije je predlog novog, sveobuhvatnog rešenja za profilisanje mrežnog saobraćaja i detekciju anomalija i napada, a koji na najbolji način koristi prednosti oba primenjena pristupa, pristupa zasnovanog na entropiji i pristupa primenom metoda nenadgledanog mašinskog učenja. Za razliku od svih postojećih metoda, predloženo rešenje primenjuje analizu atributa dobijenih primenom proračuna entropije nad svakom instancom toka mrežnog saobraćaja, a zatim ih koristi za potrebe profilisanja saobraćaja, analizu i detekciju anomalija i napada primenom nenadgledanog algoritma klasterovanja. Ovim novim pristupom se postiže visokokvalitetno profilisanje

tokova podataka i detekcija anomalija, koristeći samo osnovne atribute tokova podataka. Predloženi metod je posebno važan za praktičnu primenu u stvarnom mrežnom okruženju jer se zasniva na radu sa podacima koji su dobijeni jednostavnom primenom NetFlow protokola ili nekim sličnim protokolom, a za njegovu primenu nije neophodno obučavanje sistema skupom označenih podataka.

3. ANOMALIJE I NAPADI U MREŽNOM OKRUŽENJU

Prenos podataka u različitim mrežnim infrastrukturama, pod različitim uslovima, specifičnim komunikacionim obrascima i dostupnim servisima predstavlja jedan živ proces koji je podložan različitim uticajima, ometanjima i nepravilnostima. Praksa i dostupna stručna literatura kategorišu različite probleme u prenosu mrežnog saobraćaja na dve osnovne grupe: anomalije i napade.

3.1 Anomalije

Anomalije mrežnog saobraćaja se mogu definisati kao ponašanja i promene u strukturi mrežnog saobraćaja koje odudaraju od ponašanja definisanog kao legitimno za date uslove. Anomalije se u mrežnom saobraćaju mogu javiti iz više razloga, a osnovna podela je na anomalije koje su striktno vezane za ostvarene performanse i anomalije koje doprinose direktnom ugrožavanju sigurnosti u mreži. Anomalije koje su definisane na osnovu kritičnih promena pojedinih performansi mrežnog saobraćaja se uglavnom javljaju kao anomalije izazvane lavinskim slanjem paketa (*broadcast storms*), prolaznim zagušenjima mrežnog saobraćaja ili sporadičnim otkazima rada nekog servera. Sa druge strane, mnogo ozbiljnije u kontekstu održivosti rada mreže i opšte sigurnosti su anomalije koje imaju veze sa ugrožavanjem bezbednosti, jer je tada uglavnom u pitanju umešanost nekog malicioznog entiteta koji pokušava da sakupi informacije o ponašanjima elemenata mreže, prevarom preuzme kredencijale odgovarajućih korisnika mreže, preplavljuje mrežu nekorisnim i nepotrebnim saobraćajem, permanentno ugrožava dostupnost mrežne infrastrukture ili nekog servisa, ili onemogućava dalji pristup nekom elementu mreže. Ovaj oblik anomalija je u korelaciji s terminom napada, jer se uglavnom zasniva na zlonamernim aktivnostima.

Posebna podela tipova anomalija zasniva se na karakteristikama izlaznih informacija koje se dobijaju nakon primene odgovarajućeg rešenja za detekciju anomalija, a predstavljaju se kao: (1) tačkaste anomalije, (2) kontekstualne anomalije i (3) kolektivne anomalije [11], [40], [97], [98]. Tačkasta anomalija nastaje kada određeno zapažanje odstupa od legitimnog profila ponašanja i u statističkom smislu se tumači kao izuzetak (*outlier*). Kontekstualne (uslovne) anomalije se javljaju u slučaju kada instanca podataka može da se smatra anomalijom u nekom određenom kontekstu. Međutim, čest je slučaj da instanca podataka sa atributima ponašanja koji u nekom kontekstu određuju anomalno ponašanje, u drugom kontekstu odgovara normalnom ponašanju. Ako je grupa povezanih instanci podataka po prirodi anomalna u odnosu na ceo skup instanci podataka, u pitanju je kolektivna anomalija. Tada pojedinačne instance podataka u grupi kolektivne anomalije možda i nisu same po sebi instance anomalije, međutim njihovo zajedničko pojavljivanje u vidu grupe deluje kao anomalija. Ipak, istraživanja su trenutno najživlja u oblasti razvoja metoda analize izuzetaka (*outlier*). Prema Hawkinsu, izuzetak se može definisati kao „zapažanje koje toliko odstupa od drugih zapažanja da izaziva sumnju da je generisano drugačijim mehanizmom" [99]. Ovaj specifičan pristup identifikaciji podataka koji su izrazito različiti, odnosno nesaglasni sa preostalim podacima, objašnjen je u nekoliko studija. U dostupnoj naučnoj literaturi pojedini autori navode šest kategorija tehnika detekcije anomalija: tehnike zasnovane na klasifikaciji, na najbližim susedima, na klasterovanju (grupisanju), statističke tehnike, tehnike zasnovane na teoriji informacija i tehnike zasnovane na teoriji spektra [18]. Više detalja o rezultatima koji su tokom ovog istraživanja dobijeni primenom analize izuzetaka se može naći u [49].

3.2 Napadi

Američki nacionalni institut za standarde i tehnologiju (*National Institute of Standards and Technology*, NIST) definiše detekciju napada [100] kao „proces praćenja događaja koji se dešavaju u računarskom sistemu ili mreži i njihovo analiziranje na naznake napada, a koji su definisani kao pokušaji ugrožavanja poverljivosti, integriteta, dostupnosti ili zaobilaženja primenjenih sigurnosnih mehanizama posmatranog računara ili mreže".

U opštem smislu, napad predstavlja bilo koji skup radnji koje narušavaju integritet, poverljivost ili dostupnost mrežnih usluga i resursa. Može se definisati kao svaka zlonamerna aktivnost u mrežnom okruženju, neovlašćeni pristup ili zloupotreba informacija. Problem detektovanja napada se oslanja na kontinuirano praćenje mrežne aktivnosti, utvrđivanje pravila po kojima se pojavljuje neki nepoželjni maliciozni događaj ili identifikaciju neobičnog ponašanja koje se tumači kao anomalija. Svako odstupanje od normalnog ponašanja se smatra sumnjivim i treba ga analizirati kako bi se pravilno klasifikovao kao normalan ili zlonameran događaj.

Kako bi što preciznije svoje dejstvo usmerili na ciljani sistem i njegove slabe tačke, napadi se najčešće obavljaju u četiri osnovne kategorije: izviđanje, skeniranje, eksploatacija i trajni pristup [101].

U kontekstu izviđanja, napadi se javljaju kao napadi analize saobraćaja i napadi društvenog inženjeringa (na primer društvene mreže). Ova kategorija napada svoje dejstvo zasniva na prikupljaju privatnih i poverljivih informacija vezanih za mrežu i korisnike. Napad koji se zasniva na procesima analize mrežnog saobraćaja primenjuje metode preslušavanja i analize paketa koji se prenose, kako bi se izvukle informacije o strukturi mreže, načinu povezivanja različitih elemenata mreže i otkrivanju privatnih podataka poput korišćenih IP adresa i portova. Napadi socijalnog inženjeringa koriste informacije vezane za interakciju između korisnika kako bi se došlo do poverljivih informacija vezanih za autorizaciju i autentifikaciju.

Druga kategorija napada odgovara fazi skeniranja koje se primenjuje sa ciljem neometanog otkrivanja detalja o aktivnim uređajima u okviru mrežnog okruženja. Posebno se izdvajaju skeniranja IP adresa, skeniranja po portovima, skeniranja po servisima i skeniranja za potrebe otkrivanja različitih oblika ranjivosti. Princip je najčešće taj da se napadač prvo fokusira na skeniranje IP adresa, na osnovu kojih se identifikuju uređaji koji su povezani na mrežu, a zatim se za svaki tako otkriveni uređaj obavlja posebno skeniranje korišćenih portova i utvrđivanje koji portovi su otvoreni i aktivni za dalje funkcionisanje. Na osnovu ovih podataka, napadač se dalje usmerava na utvrđivanje specifičnih servisa koji se koriste u mreži, da bi zatim otkrivao potencijalne nedostatke, ranjivosti i probleme u komunikaciji koje bi mogao da na maliciozan način iskoristi za svoje potrebe.

Treća kategorija odgovara fazi kada se napadač aktivno posveti malicioznoj eksploataciji i iskorišćavanju ranjivosti elemenata mreže i ciljnog sistema. U okviru ove grupe napada se nalaze različiti oblici crva, virusa, napada uskraćivanjem servisa (DoS i DDoS), *brute force* napadi, napadi usmereni na dostupnost sistema (*availability*), njegov integritet (*integrity*) i poverljivost (*confidentiality*), dok je u značajnoj meri u fokusu ugrožavanje privatnosti korisnika i njegovih privatnih podataka.

Četvrta karakteristična kategorija se odnosi na procedure kojima napadač održava svoje prisustvo i pokušava da stekne trajni pristup određenom delu mreže ili uređaju, koristeći se nekim od *backdoor* alata [101].

Opšta podela napada je na spoljašnje i unutrašnje napade. Spoljašnji napadači koriste različite tehnike prodora u sistem (pristup sa spoljne mreže ka unutrašnjoj), lažnog predstavljanja, probijanja *firewall* barijera i pristupnih lista. Međutim, mnogo su opasniji unutrašnji napadi jer ih izvode korisnici koji su upoznati sa unutrašnjom arhitekturom i mrežom sistema, te često imaju i dozvolu da pristupe sistemu i nekim od njegovih resursa. Uobičajeno se maskiraju i prijavljuju sa kredencijalima drugih korisnika koji imaju pristup specifičnim delovima mreže i osetljivim mrežnim podacima, a poznati su i napadi takozvanih tajnih unutrašnjih napadača koji imaju mogućnost da svoju aktivnost i identitet sakriju od sistema i neopaženo zloupotrebljavaju pristup mrežnim resursima. Bezbednosni napadi se obično odvijaju u skladu sa klijent-server modelom, ali sa intenziviranim vrednostima nekih komunikacionih karakteristika kao što su intenzitet saobraćaja, broj napadača, mogućnost presretanja i krađe enkriptovanih podataka. Pri tome, mrežnim napadom se smatra svaki proces kojim se kompromituje bezbednost mreže u rasponu od sloja veze podataka (*data link layer*) do sloja aplikacije (*application layer*). Mrežni napadi su zasnovani na primeni različitih metoda za manipulisanje radom mrežnih protokola. Drugi vid mrežnog napada se ogleda kroz nelegalno korišćenje korisničkih naloga i privilegija, onemogućavanje legitimnim korisnicima da pristupe mrežnim uslugama i resursima, kao i da skupom aktivnosti utiču na manipulacije, brisanja i unošenje grešaka u rad mrežnih resursa i propusni opseg mreže.

U [102] je data taksonomija različitih oblika napada sa fokusom na sajber napade, kategorišući ih na osnovu vektora napada, uticaja na operativnost sistema, načina odbrane, informacionog doprinosa i ciljanog elementa u mreži. U [103] je dat pregled sajber napada sa fokusom na mrežni aspekt, ali je ukazano i na najnovije trendove u toj oblasti. Sa druge strane, u [12] je dat jedan od najmerodavnijih pregleda napada u mrežnom okruženju. Dopunjena lista napada koji su izloženi u toj studiji daje nekoliko osnovnih kategorija napada: (1) napadi odbijanjem servisa; (2) napadi skeniranjem; (3) napadi krađom kredencijala; (4) *Botnet* napadi; (5) R2L (*Remote to Local*) napadi; (6) U2R (*User to Root*) napadi; (7) pasivni napadi; (8) aktivni napadi; (9) fizički napadi; (10) ucenjivački napadi (*Ransomware*); (11) napadi nultog dana; (12) virusi, crvi i Trojanci.

Detaljan prikaz i karakteristike ovih vrsta napada su predstavljeni u referentnoj literaturi [30], [102–106].

Istraživanje i rezultati predstavljeni u okviru ove disertacije se u velikoj meri zasnivaju na ispitivanju metoda detekcije različitih formi napada odbijanjem servisa, napada skeniranjem, napada grubom silom i *botnet* napada. U sledećih nekoliko odeljaka je dat prikaz osnovnih karakteristika ovih vrsta napada.

3.3 Napad odbijanjem servisa

Napad odbijanjem servisa predstavlja svaki pokušaj sprečavanja legitimnog rada nekog servera koji pruža uslugu kao što su veb, e-*mail*, DNS, NTP (*Network Time Protocol*), a ostvaruje se generisanjem značajno većeg obima saobraćaja čime se premašuje dostupan propusni opseg, ili je zasnovan na generisanju mnogo većeg broja zahteva za uspostavljenjem servisa nego što to server ili sistem može da podrži. Ovaj oblik napada se javlja u formi *host-based*, *network-based*, a najčešće u distribuiranom obliku (DDoS) napada [102]. DDoS podrazumeva simultano DoS dejstvo većeg broja napadača u cilju bržeg i efikasnijeg ostvarivanja cilja maliciozne aktivnosti. U savremenim sistemima i tehnološkim okolnostima, DDoS se najčešće javlja u formi sajber napada velikim brojem *botnet* napadača. Opšta podela DoS/DDoS napada koja je od interesa u kontektu ove disertacije se zasniva na

klasifikaciji prema iskorišćenosti ranjivosti, pri čemu se DDoS mogu pojaviti kao napadi izazvani poplavama (*flood attacks*), kao pojačani napadi (*amplification attacks*) ili kao napadi koji se zasnivaju na iskorišćavanju karakteristika protokola (*protocol exploits*). Ove tri kategorije DDoS napada su detaljnije izložene u okviru ovog odeljka. Osim toga, pojedine DDoS kategorije napada se zasnivaju na generisanju neispravnih, odnosno oštećenih paketa (*malformed packets*) [106].

3.3.1 DDoS napadi pojačanjem

DDoS napadi pojačanjem (*amplification attacks*) koriste servise koji se obezbeđuju radom odgovarajućih servera, poput DNS ili NTP, a koji funkcionišu kao serveri otvorenog tipa (nisu pravilno zaštićeni određenom konfiguracijom) [105]. Posrednički uređaji koji se koriste kao pojačivači napada se nazivaju reflektorima, a takvu ulogu može da ima bilo koji uređaj sa dodeljenom IP adresom i koji na prijem nekog paketa odgovaraju slanjem odgovarajućeg odgovora. Samim tim, DNS, veb i NTP serveri i ruteri mogu da imaju ulogu reflektora, čija je funkcionalnost da na kratke upite šalju obimne odgovore, tako da u slučaju kada se adresa pošiljaoca lažira, takvi obimni odgovori se zapravo preusmeravaju ka žrtvi napada.

Napad reflektorima zahteva skup unapred određenih reflektora, a njihove lokacije mogu biti distribuirane u okviru mreže. Poseban aspekt ovakvog napada se manifestuje kroz činjenicu da su reflektovani paketi zapravo paketi normalnog saobraćaja sa dodeljenim legitimnim IP adresama i ne mogu da se filtriraju na osnovu mehanizama dostupnih u procesu rutiranja saobraćaja. U principu, napadač šalje pakete koji zahtevaju da reflektori pošalju adekvatne odgovore. Paketi su modifikovani tako da su unesene lažne izvorišne adrese, podešene na adresu žrtve. Samim tim, reflektori šalju odgovore na adresu žrtve. U slučaju velikog broja reflektora moguće je obezbediti da reflektovani paketi preplave žrtvu i onemoguće bilo kakav oblik njenog komuniciranja. Reflektore je jednostavno identifikovati na osnovu izvorišnih IP adresa koje su upisane u okviru paketa koji stižu na adresu žrtve, ali je reflektoru teško da identifikuje napadača koji inicira napad, jer saobraćaj koji se šalje ka reflektoru nema unešenu izvorišnu adresu napadača, već žrtve. Napad se izvodi tako što napadač generiše i šalje serveru veliki broj kratkih upita/zahteva koristeći se lažnom izvorišnom IP adresom, a kao odgovor na upite serveri generišu saobraćaj značajno većeg obima. Napadač može da pošalje pakete direktno ili korišćenjem različitih agenata za slanje paketa kako bi povećao obim napada. Pojedini oblici ovih napada funkcionišu na osnovu dodatnog infiltriranja napadača tako što u okviru korišćenih elemenata mreže instaliraju softver za ovakve aktivnosti. Među poznatim oblicima ovog tipa napada su *Smurf* i *Fraggle* napadi [30].

3.3.2 DDoS napadi izazvani poplavama

U DDoS napadima izazavnim poplavama (*flood attacks*) napadači generišu i šalju velike količine mrežnog saobraćaja ka potencijalnoj žrtvi napada u cilju zagušenja propusnog opsega i onemogućavanja funkcionisanja odabranog dela sistema ili mreže. Efekat ovakvog napada može da bude usporavanje rada ciljnog sistema, a najozbiljniji oblik napada dovodi do pada sistema zasićenjem njegovog dostupnog propusnog opsega i nemogućnosti korišćenja dostupnog opsega za potrebe uspostavljanja konekcija legitimnih zahteva ka servisu. Ovaj vid napada se najčešće javlja u formi ICMP (*Internet Control Message Protocol*) *flood* i UDP (*User Datagram Protocol*) *flood* napada, gde se na primer u UDP flood napadu veliki broj UDP paketa sistematski šalje ka slučajno odabranim ili precizno definisanim portovima na odredišnom serveru ili korisniku čiji rad se time onemogućava. Kada odredišni server primi tako poslate UDP pakete, pokušaće da identifikuje aplikaciju koja se javlja

na odredišnom portu. Kada postane jasno da ne postoji aplikacija koja čeka na portu, server će generisati ICMP paket sa porukom „port je nedostupan" (*port unreachable*) na lažno generisanu adresu izvorišta komunikacije [30]. Sa povećanjem broja ovako generisanih paketa i poslatih odgovora napadaču, odredišni server će se prezasititi zahtevima i time će njegova funkcionalnost biti kompromitovana i potencijalno onemogućena. Slična situacija se javlja i u slučaju ICMP flood napada, pri čemu se kao osnov napada zloupotrebljava sistem slanja *Echo* poruka putem ICMP protokola. Tako tokom samog napada napadači šalju žrtvi ogroman broj ICMP *Echo Reply* paketa, takozvanih *ping* paketa, koji zahtevaju da žrtva pošalje odgovor čime dokazuje da je aktivna. Kada napadač koristi lažnu izvorišnu adresu, žrtva će slati veliki broj odgovora, što može dovesti do zasićenja komunikacije [30].

3.3.3 DDoS napadi zasnovani na iskorišćavanju protokola

Napadi zasnovani na iskorišćavanju karakteristika protokola (*protocol exploits*) zloupotrebljavaju neke od karakterističnih funkcionalnosti protokola ili neku od primećenih manjkavosti u radu protokola. Cilj ove grupe napada je da se na osnovu poznatih nefunkcionalnosti korišćenog protokola iscrpe resursi na strani žrtve, a jedan od tipičnih primera je TCP SYN napad. Ovaj napad je karakterističan po tome što zloupotrebljava inherentne slabosti korišćene *three-way-handshake* procedure TCP protokola koja se obavlja u cilju uspostavljanja konekcije između korisnika i nekog servera usluge. Server, nakon što primi inicijalni SYN paket (sinhronizuj/pokreni) odnosno zahtev od korisnika, uzvraća sa SYN/ACK (*SYNchronize/ACKnowledge*) (sinhronizuj/potvrdi) paketom i čeka da klijent pošalje konačnu potvrdu u vidu ACK paketa. Ova jednostavna procedura se zloupotrebljava tako što napadač započinje napad slanjem velikog broja SYN paketa, a nakon što primi odgovore, ne odgovara na njih i time u suštini ostavlja server da čeka na nepostojeće ACK pakete potvrde [104]. Uzimajući u obzir to da server ima ograničen broj konekcija koje može da uspostavi, SYN flood će onemogućiti serveru da obrađuje bilo koje druge, legitimne zahteve za uspostavljanjem veze jer je server već zasićen zahtevima na koje ne dobija potvrdne odgovore.

3.4 Napad skeniranjem

Ova grupa napada skenira mrežu i njenih učesnika (*Probe/Scanning attack*) kako bi se identifikovale korišćene IP adrese i prikupile različite informacije vezane za operativni sistem, usluge, konfiguraciju sistema, mreže ili za konkretnog korisnika (*Information gathering attacks*) [32], [107–111]. Na osnovu sakupljenih informacija napadač može da generiše odgovarajuću bazu podataka o sistemu i njegovim ranjivostima na nivou sigurnosti i bezbednosti, a koje može da kasnije zloupotrebi primenom nekog od invanzivnih, aktivnih napada.

Osnovna karakteristika ovih napada je da deluju tiho, vrlo često u pozadini pre nego što dođe do neke ozbiljnije pretnje sigurnosti sistema, a obično se javljaju u obliku skeniranja portova (*Port scanning*) i skeniranja mreže (*Network scanning*). Napadi mrežnog skeniranja funkcionišu tako što skeniranjem zapravo primenjuju procedure pretrage uređaja u napadnutoj mreži, tako što generišu tokove mrežnog saobraćaja sa jedne izvorišne IP adrese i najčešće proizvoljnog izvorišnog porta, ka nekom fiksnom odredišnom portu preko kojeg se dopire do velikog broja korisnika u okviru mreže. Sa druge strane, napadi skeniranjem portova utvrđuju koji su portovi otvoreni na određenom uređaju, tako što generišu veliki broj tokova mrežnog saobraćaja ka različitim odredišnim portovima i fiksnom odredišnom IP adresom.

3.5 Napad grubom silom

Napad grubom silom (*Brute force attack*) se zasniva na nizu pokušaja pristupa sistemu ili korisničkom nalogu primenom sistema eliminacije iz predefinisanih ili slučajnih lozinki, a sve u cilju njenog dešifrovanja [112]. Napad može da se odvija i na daljinu, a zasniva se na kombinovanju mogućih ASCII znakova. Tako na primer, kada se host nalazi sa otvorenim TCP portom koji zahteva autentifikaciju, kao što je port 22 za SSH ili 3389 za Microsoft Remote Desktop, napadač može da otkriva kredencijale primenom napada grube sile, pokušavajući da primeni često korišćene reči i izraze koje se koriste i u napadu rečnikom (*Dictionary attack*). Profil ovog napada je okarakterisan velikim brojem kratkih tokova mrežnog saobraćaja koji se sastoje od jednog ili dva paketa, a koji se prenose između dve fiksne IP adrese, koristeći više izvorišnih portova i jedan odredišni port.

3.6 *Botnet* napad

Botnet je napad zasnovan na aktivnosti botova, specifičnih oblika računarskih robot-aplikacija, koji daljinski usklađuju svoje aktivnosti putem komande i kontrole na osnovu čega dalje upravljaju velikim brojem hakovanih, otetih računarskih sistema. *Botnet* mrežu čini veliki broj kompromitovanih računara koji mogu na određenu komandu da sprovode neku malicioznu radnju – obično DDoS ili *spam* napad. Iako se uglavnom kontrolišu daljinski, ovi napadi mogu efektivno da se izvršavaju i samostalno [9], [31], [58].

4. MAŠINSKO UČENJE

Procvat u oblasti veštačke inteligencije (*Artificial Inteligence*, AI) i njene primene u različitim oblastima istraživanja jednim delom je podržan intenziviranim razvojem algoritama mašinskog. U opštem smislu tehnike mašinskog učenja su metode kojima se sistem obučava o različitim aspektima ponašanja, a na osnovu kojih, u zavisnosti od načina realizacije, metode mašinskog učenja mogu da pomognu pri donošenju određenih odluka.

4.1 Definicija mašinskog učenja

Jedan od najčešće citiranih opisa termina mašinskog učenja je dao Tom Mitchell [113], [114]: „Kaže se da računarski program uči iz iskustva *I*, u odnosu na klasu zadatka *Z* i meru performansi *P* ukoliko se njegove performanse *P* prilikom izvršavanja zadatka *Z* poboljšavaju zahvaljujući usvojenom znanju o iskustvu *I*.” U kontekstu funkcionisanja nekog algoritma mašinskog učenja, ovako definisan pristup se može tumačiti kao složeni skup metoda kojima je moguće na osnovu zadatih informacija (informacije sakupljene u dužem vremenskom periodu, informacije koje se sakupljaju u realnom vremenu, korisnička baza podataka ili podaci iz nekog drugog izvora informacija) utvrditi karakteristično znanje odnosno iskustvo *I*, na osnovu kojeg je moguće obaviti prepoznavanje sličnih informacija, obaviti klasifikaciju ili klasterovanje zadataka *Z* (u zavisnosti od osnovnog tipa algoritma mašinskog učenja), a zatim izračunati skup mera performansi *P* za tako dobijen rezultat.

Nijedan algoritam mašinskog učenja ne može da bude univerzalno primenljiv u svakoj situaciji, u svakom mrežnom okruženju ili za sve potencijalne potrebe. Odabir odgovarajućeg modela zavisi od karakteristika podataka koji se obrađuju, potreba za radom sa podacima u realnom vremenu, kao i veličine i karakteristika sistema za koji se primenjuje.

4.2 Primena mašinskog učenja

Osnovni uslov kvalitetnog rada bilo kog algoritma mašinskog učenja je dostupnost velike količine podataka koji su relevantni za oblast rada sistema u kojem će algoritam biti primenjen. Takav skup podataka će algoritmu mašinskog učenja da obezbedi kvalitetan izvor informacija o karakterističnim podacima koji se razmenjuju, infrastrukturi mreže, specifičnim servisima, korisničkim rutinama i drugo. U novijoj taksonomiji, oblast veštačke inteligencije se zasniva na razvoju dve kategorije algoritama: algoritmi mašinskog učenja i algoritmi dubokog učenja (*deep learning*). Vrlo često se u praksi ove dve oblasti međusobno dopunjuju i kombinuju u cilju obuhvatanja svih njihovih pojedinačnih prednosti i što efikasnijeg krajnjeg rešenja. Različiti su pristupi kategorisanju algoritama mašinskog učenja, pri čemu svaki potencira neki od konkretnih pravaca njegovog razvoja i zavisi od oblasti primene [103], [115–120]. Osim osnovnih kategorija nadgledanog, nenadgledanog i polunadgledanog učenja, postoje i kategorije tehnika koje se zasnivaju na obučavanju sa podsticajem i kombinovane tehnike.

Za potrebe istraživanja predstavljenog u ovoj disertaciji primenjivano je nekoliko algoritama iz oblasti nadgledanog i nenadgledanog mašinskog učenja. Za te konkretne kategorije algoritama je u sledećim odeljcima dat detaljan opis. Kratak opis ostalih kategorija i grupa algoritama je dat u sledećih nekoliko pasusa, a detaljne informacije se mogu pronaći u referentnoj literaturi.

Poseban tip algoritama mašinskog učenja spada u kategoriju polunadgledanog učenja (*semi-supervised*) koje obezbeđuje oznake preslikavanja za jedan manji deo skupa podataka nad kojim se obavlja analiza, dok za veći deo skupa podataka i dalje ne postoji funkcija preslikavanja [120]. Osnovni cilj ovakvog učenja je da se iskoriste neobeleženi ulazni podaci radi boljeg obučavanja modela. Izuzetno su korisni u praksi jer u mnogim slučajevima nije lako obezbediti dovoljne količine podataka sa obeleženim izlazom.

Sa druge strane, metode mašinskog učenja sa podsticajem (*reinforcement learning*) se zasnivaju na učenju na osnovu ulaznih podataka koji karakterišu aktivnosti određene grupe učesnika, takozvanih agenata, dok je podrška učenju obezbeđena kroz odgovarajući signal podrške [121]. Signal podrške se uzima u obzir na kraju nekog specifičnog skupa akcija pojedinog učesnika u komunikaciji i oslikava željeni ili nepoželjni ishod ponašanja učesnika, a koji se zatim koristi pri korigovanju daljeg rada agenata. Učenje sa podsticajem je problem sa kojim se suočava agent koji uči kako da se ponaša kroz niz interakcija tipa „pokušaj-greška" u dinamičkom okruženju.

Kombinovane metode mašinskog učenja se primenjuju u slučajevima kada je optimalno i najefikasnije da se kombinuje više različitih tehnika mašinskog učenja. Cilj je da se kombinovanjem metoda ublaže slabosti i nedostaci svakog od primenjenih modela i istovremeno iskoriste njihove pojedinačne prednosti u cilju poboljšanja ukupne efikasnosti i sposobnosti učenja tako kombinovanog modela [122]. U okviru ove kategorije algoritama mašinskog učenja razvija se i posebna kategorija višeklasifikatorskih kompozitnih algoritama, odnosno ansambl (*ensemble*) algoritama koji su primenjivani u inicijalnom delu istraživanja vezanom za disertaciju [123]. Ostale metode u okviru kombinovanih metoda mašinskog učenja su detaljno analizirane u referentnoj literaturi [124].

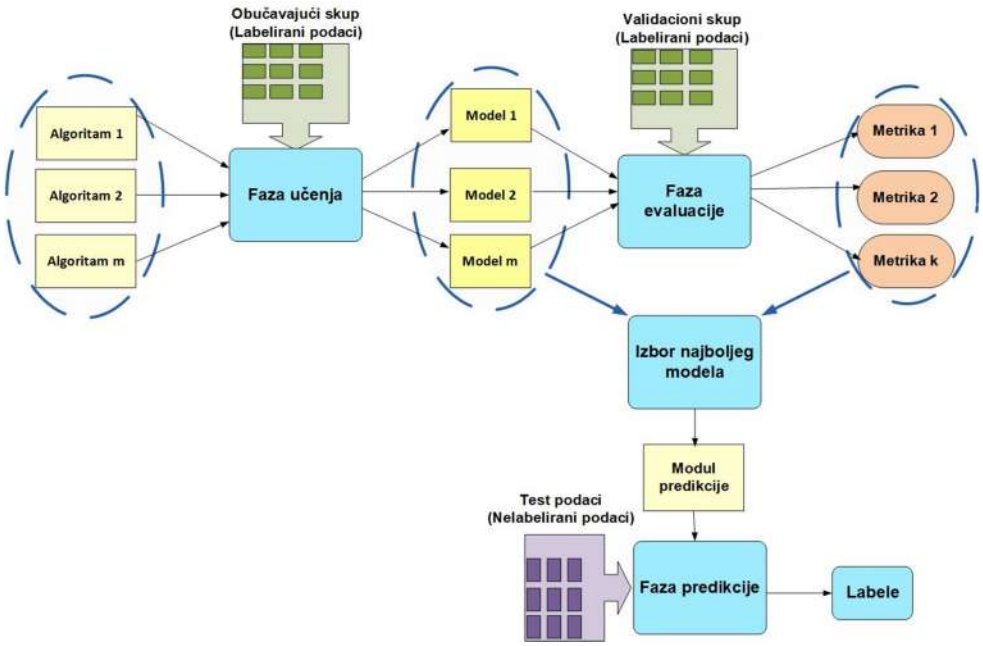
U sledećim poglavljima su predstavljeni algoritmi koji su korišćeni za potrebe ovog istraživanja.

4.3 Metode nadgledanog mašinskog učenja

4.3.1 Osnovne karakteristike

Algoritmi koji se zasnivaju na nadgledanom obliku mašinskog učenja funkcionišu na osnovu podataka koji su zadati u formi obučavajućeg skupa, pri čemu su svi podaci označeni i prethodno je poznato kojoj klasi treba da pripadaju. Na osnovu njih algoritam uči kako da za date ulazne podatke obezbedi odgovarajuću klasifikaciju izlaznih podataka.

Nadgledani algoritmi mašinskog učenja zahtevaju sveobuhvatan obučavajući skup podataka koji služi kao primarni ulaz za generisanje klasifikatora, pri čemu je važno da taj skup bude kompletan u smislu obuhvatanja svih karakterističnih primera instanci podataka i neophodno je da algoritam bude sposoban da efikasno razlikuje klase podataka. Iako se smatraju povoljnim u smislu predstavljanja diskretnog skupa pravila ili stabala odlučivanja za identifikaciju aplikacija, nadgledani algoritmi ne obezbeđuju kompletno rešenje za izazove na koje nailazi klasifikacija. Naime, potrebno je da obučavajući skup, kao i skup za testiranje budu kvalitetno generisani i zasnovani na tzv. osnovnim istinitim podacima (*ground truth*). Nadgledanim učenjem se obezbeđuje optimalna funkcija mapiranja ulaznih podataka ka izlaznim. Na slici 4.1 je predstavljen tok nadgledanog mašinskog učenja.



Slika 4.1 Princip rada nadgledanog algoritma mašinskog učenja

Nenadgledani algoritmi mašinskog učenja se dodatno kategorišu kao algoritmi za klasifikaciju i algoritmi regresije. Svaka od ovih kategorija se grana na nekoliko podvrsta koje imaju specifične metode implementirane u procesu učenja i detekcije.

Klasifikacija se koristi za učenje modela (klasifikatora) iz skupa označenih instanci podataka (koje se nazivaju instance za obuku). Proces klasifikacije se izvodi kroz faze obuke, validacije i testiranja. U fazi obuke model klasifikatora se obučava koristeći veliki broj označenih instanci podataka za učenje i predviđanje u okviru obučavajućeg skupa. Zatim se vrši validacija primenom skupa za validaciju kojom se podešavaju parametri modela mašinskog učenja radi bolje preciznosti krajnjeg modela. U fazi testiranja se koriste instance iz test skupa, na koje se primenjuje generisan model i na osnovu kojeg se vrši klasifikovanje instanci u jednu od klasa korišćenjem naučenog modela. Primenom algoritma klasifikacije se u opštem slučaju test instance klasifikuju kao normalne ili abnormalne (anomalije), dok sama klasifikacija u većini slučajeva podržava rad i sa višeklasnim podacima [123], [125].

Regresija je statistička metoda kojom se pronalazi odnos između zavisne promenljive i jedne ili više nezavisnih promenljivih [126], [127]. Modeli koji su bliskiji primeni tehnika zasnovanih na nekom obliku regresije se mogu tumačiti kao modeli koji pripadaju linearnoj regresiji, logističkoj regresiji, posebnom obliku primene potpornih vektora, stabala odlučivanja, neuralnih mreža, *stohastic gradient descent* metoda, *ensemble* algoritama i drugih.

Jednostavna regresija podrazumeva da zavisna promenljiva zavisi samo od jedne promenljive, dok se višestruka regresija odnosi na slučaj kada zavisna promenljiva zavisi od više nezavisnih promenljivih. Linearna regresija se odnosi na slučaj kada je zavisnost promenljivih linearna. U tom slučaju je potrebno pronaći linearnu funkciju kojom se predviđa vrednost zavisne promenljive kao funkcija nezavisne promenljive (relacija 4.1):

$$y = \beta_0 + \beta_1 x + \varepsilon \tag{4.1}$$

gde je y zavisna promenljiva, x je nezavisna, objašnjavajuća (prediktorska) promenljiva, β_0 predstavlja slobodni član, β_1 predstavlja koeficijent smera, dok je ε slučajna greška, odnosno rezidual. Za slučajnu grešku se pretpostavlja da ima očekivanje jednako 0. Ona predstavlja razliku između ocenjene vrednosti regresione funkcije i njene stvarne vrednosti. Promenljiva *x* nije slučajna i u praksi se ona najčešće zadaje, dok se *y* meri i predstavlja odziv.

Višestruka linearna regresija utvrđuje odnos između zavisne promenljive *Y* i više nezavisnih promenljivih, pri čemu se njihova međuzavisnost opisuje relacijom 4.2:

$$Y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + .. + \beta_p x_p + \varepsilon \tag{4.2}$$

Pri čemu su x_1, x_2 , x_3, ,.., x_p nezavisne promenljive; β_0, β_1,.., β_p su parametri modela regresije, a ε je slučajna greška. Kada se ovakav model primeni na slučajnom uzorku $(x_{i1}, x_{i2}, \dots, x_{ip})$ od n instanci podataka ($i = 1, .. n$), tada se ovaj model može opisati u matričnom obliku (relacija 4.3):

$$\mathbf{Y} = \boldsymbol{X}\beta + \varepsilon, \text{ pri čemu je: } \mathbf{Y} = \begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_n \end{bmatrix}, \mathbf{X} = \begin{bmatrix} 1 & x_{11} & \cdots & x_{1p} \\ 1 & x_{21} & & x_{2p} \\ \vdots & & \ddots & \vdots \\ 1 & x_{n1} & \cdots & x_{np} \end{bmatrix}, \beta = \begin{bmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_p \end{bmatrix}, \varepsilon = \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_p \end{bmatrix} \tag{4.3}$$

Logistička regresija (binarni logistički regresioni model) je jedan specifičan oblik linearne regresije u kojem je zavisna promenljiva binarnog tipa (može da uzima samo dve vrednosti, vrlo retko više), dok nezavisne promenljive mogu biti kategorijalne, numeričke ili neka njihova kombinacija. Zavisna promenljiva će jednom ishodu da dodeljuje vrednost 1, dok će drugom dodeljivati vrednost 0.

Regresione metode su vrlo primenljive u rešavanju problema predviđanja, pri čemu proces obučavanja prolazi kroz sve podatke i pronalazi regresionu funkciju sa minimalnom greškom predviđanja. S obzirom na to da se algoritmi mašinskog učenja najčešće primenjuju nad velikim brojem podataka, potrebno je osim minimalne greške obezbediti i brz odziv. Kako bi se obezbedio brži rad regresionog algoritma, primenjuje se metoda silaznog gradijenta (*gradient descent*) kojom se obezbeđuje minimizacija odstupanja između vrednosti ciljne funkcije i hipoteze na datim primerima. Metodom silaznog gradijenta se vrši ažuriranje vrednosti promenljivih β u cilju pronalaženja minimalne vrednosti greške, pri čemu procedura započinje nekim inicijalnim vrednostima parametara, zatim se one iterativno menjaju sve dok se ne pronađu vrednosti kojima se zadaje optimalna regresiona funkcija. Pri tome, metoda ne prolazi kroz sve instance skupa podataka kojih može biti veliki broj, već vrši izbor instanci na preskok i one se posmatraju kao uzorak na kom se testira vrednost greške. Tehnika silaznog gradijenta koristi specifičnu vrednost koraka sa kojim vrši gradijentno spuštanje u svakoj iteraciji, a potrebno je da to spuštanje bude glatko i u što manjim koracima.

Među karakterističnim kategorijama algoritama nadgledanog mašinskog učenja se ističu: (1) metode potpornih vektora SVM; (2) stabla odlučivanja (*Decision Trees*, DT); (3) neuralne mreže (*Neural Networks*); (4) slučajne šume (*Random Forest, RF*); (5) Bayes-ove metode (*Bayesian methods*); (6) metode *k* najbližih suseda (*k-Nearest Neighbors*) i druge.

Detaljan prikaz ovih metoda je predstavljen u referentnoj literaturi: *Decision Trees* [128], *Neural Networks* [129–132], *Random Forest* [133], [134], *Bayesian methods* [135] i *k-NN* [136].

Tokom istraživanja predstavljenog u ovoj disertaciji, u jednoj od početnih faza je ispitivana mogućnost primene nadgledanih algoritama mašinskog učenja. Tako su u kontekstu predloženog rešenja ispitivane mogućnosti primene *ensemble* algoritama, a ostvareni rezultati su predstavljeni u [123]. Zatim je izvršen niz eksperimenata u kojima su korišćeni algoritmi iz grupe metoda potpornih vektora [125], [137]. Rezultati analize *RF* i *Näive-Bayes* algoritama prikazani su u [27], [125].

4.4 Metode nenadgledanih algoritama mašinskog učenja

4.4.1 Osnovne karakteristike

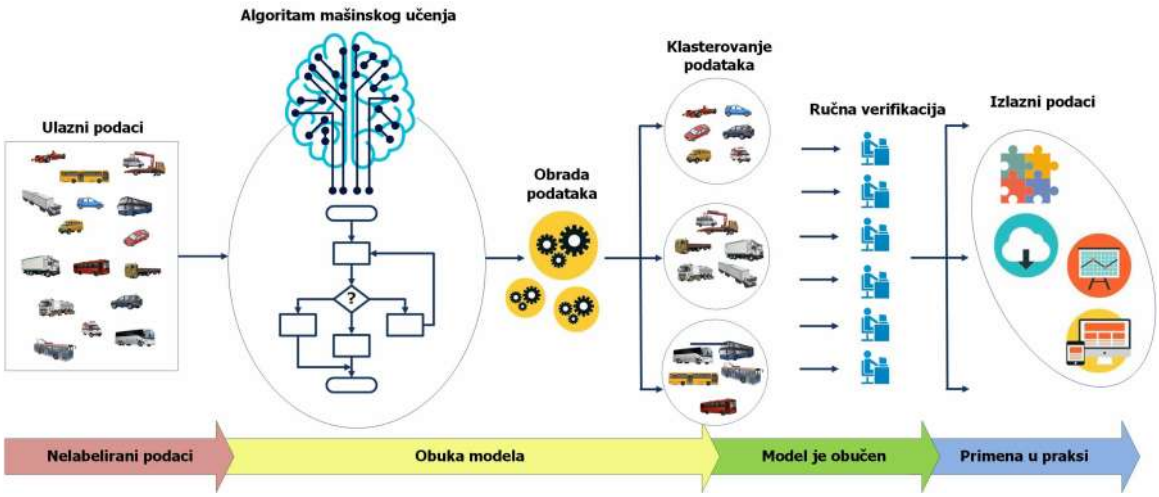
Nenadgledano mašinsko učenje se zasniva na radu sa ulaznim podacima za koje nisu zadate odgovarajuće izlazne vrednosti, tako da je neophodno pronaći neku pravilnost u strukturi i statistici podataka kako bi se mogao predvideti izlaz. Samim tim ovi algoritmi se zasnivaju na utvrđivanju karakteristika strukture dostupnih podataka i definisanju zakonitosti po kojima se određene strukture pojavljuju u nekim specifičnim situacijama na osnovu kojih se razmatrane instance podataka grupišu u grupe koje se nazivaju klasteri. Algoritmi nenadgledanog mašinskog učenja se vrlo često primenjuju u situacijama u kojima je potrebno da se na osnovu dostupnih podataka formira model ponašanja, a zatim da se novim instancama dodeljuju oznake o pripadnosti specifičnim klasterima. Grupisanje u klastere (*clustering*) je osnovni tip algoritma koji se koristi u kontekstu nenadgledanog mašinskog učenja. Podaci se svrstavaju u klastere kojima se maksimizuje neki kriterijum sličnosti, odnosno minimizuje se neki kriterijum različitosti. Najčešće se kombinuje sa nekom od metoda smanjenja dimenzionalnosti čime se redukuje skup atributa nad kojim se obavlja analiza, a koji zadržava inicijalne glavne obrasce i varijacije u skupu početnih promenljivih (atributa).

4.4.2 Tehnike klasterovanja

Klasterovanje predstavlja osnovnu kategoriju algoritama u oblasti nenadgledanog mašinskog učenja [138]. Ove tehnike su svoj inicijalni razvoj doživele još 60-tih godina prošlog veka kada je njihova primena uglavnom bila za potrebe bioloških sistematizacija i istraživanja, da bi zatim razvojem statistike ova grupa algoritama imala mnogo konkretniju primenu u različitim oblastima.

Generalno, klasterovanje se može definisati kao skup tehnika mašinskog učenja za efikasno pronalaženje unutrašnje strukture u određenom skupu podataka na takav način da se slični objekti ili instance grupišu i time odvajaju od drugih, različitih objekata. Rezultat ovih metoda daje odvojene instance normalnih podataka u poseban klaster, dok anomalije izdvaja u poseban klaster ili klastere, u zavisnosti od toga koliko ima anomalija i koliko ima različitih kategorija anomalija [139].

Klasterovanje je jedan od najvažnijih metoda za otkrivanje korisnih informacija pri učenju zasnovanom na višedimenzionalnim podacima, pri čemu se identifikuju uzorci ili grupe sličnih instanci u okviru skupa podataka od interesa (skupovi podataka, realni mrežni saobraćaj ili logovi podataka koji se čuvaju za dalju forenzičku analizu). Na slici 4.2 je predstavljen tok primene algoritma klasterovanja.



Slika 4.2 Princip rada nenadgledanog algoritma mašinskog učenja [27], [140]

Takođe, primena algoritama klasterovanja poželjna je u slučajevima kada se odlaže obrada postojećeg obučavajućeg skupa sve dok se na ulazu ne pojavi instanca koja je nepoznata i za koju je potrebno obaviti sve faze obrade, a u samoj fazi klasterovanja se uključuju prethodno sakupljene instance. Algoritmi klasterovanja su primenljivi u prirodnim naučnim oblastima, gde je potrebno generisati različite oblike taksonomija. U biologiji se ovi algoritmi primenjuju za rad sa podacima koje je inače teško drugačije razvrstavati, na primer: klasa, familija i vrsta kojoj pripada neka životinja ili biljka. Zanimljiva je primena u kontekstu dugoročnog i kratkoročnog predviđanja klimatskih prilika, seizmoloških informacija, kao i drugih kategorija istraživanja prirodnih pojava, a zatim primena dobijenih rezultata u cilju odbrane od naglih promena vremena, poplava, cunamija, zemljotresa, vulkanskih erupcija i drugih prirodnih katastrofa. Noviji društveno-ekonomski tokovi su uslovili i intenzivnu primenu ovih metoda u kontekstu funkcionisanja društvenih mreža kao i u istraživanjima vezanim za tržište robe i usluga. Na osnovu takvih istraživanja bi preduzeća na efikasniji način plasirala svoj reklamni sadržaj korisnicima od interesa, na način prilagođen različitim ciljnim grupama, a koje su određene nakon analize podataka vezanih za njihova interesovanja, godište, mesto stanovanja, nivo obrazovanja i drugo.

Među tehnikama iz ove kategorije posebno se mogu izdvojiti grupe algoritama koje u svojoj osnovi imaju metode klasterovanja podataka na osnovu rastojanja između instanci (*distance-based*) (na primer *k-means*, *k-medoids*, *fuzzy C means*), hijerarhijskog klasterovanja, metode detekcije izuzetaka, odnosno odudarajućih instanci (*outlier detection*), Gausovi mešani modeli (*Gaussian Mixture models*), skriveni Markovljevi modeli (*Hidden Markov models*) kao i niz metoda za redukovanje dimenzionalnosti.

Klasterovanje objedinjuje metode i tehnike rada sa neoznačenim podacima, a kojima se obavlja analiza podataka vezanih za stvarne, realne scenarije u kojima je ručno označavanje podataka neisplativno i skupo. Vrlo često je ekspertsko znanje, koje je neophodno kako bi se olakšalo ručno označavanje, nedostupno ili nedovoljno kvalitetno. Izuzetna rasprostranjenost veb aplikacija, porast broja mobilnih uređaja, mrežnih uređaja i senzora, kao i sve veći obim podataka koje je potrebno analizirati, imaju mnogo veći rast u odnosu na dinamiku razvoja računarskih mogućnosti i resursa. U takvim okolnostima klasterovanje postaje prikladnija opcija u odnosu na metode nadgledanog učenja.

Algoritmi klasterovanja se mogu klasifikovati na osnovu karakteristika podataka koje analiziraju i u tom slučaju se mogu posmatrati kao statistički ili konceptualni:

- Statistički zasnovani algoritmi klasterovanja (*statisticaly based*) svoje tehnike rada zasnivaju na primeni različitih statističkih metoda, a koriste se u slučaju u kom se raspolaže samo numeričkim podacima.
- Konceptualni algoritmi klasterovanja (*conceptualy based*) su orijentisani na kategorijalni tip podataka, odnosno u osnovi primenjuju tehnike za ispitivanje zajedničkih osobina podataka, koje zatim uzimaju u obzir prilikom daljeg generisanja klastera podataka.

Druga podela se fokusira na potencijalno preklapanje klastera, u smislu:

- tvrdog klasterovanja (*hard clustering*)
- mekog klasterovanja (*soft clustering*)

U kontekstu ovakve podele metoda klasterovanja, kod metoda koje pripadaju *hard* klasterovanju svaka tačka u inicijalnom skupu će u rezultatu biti klasterovana tačno u jedan klaster, bez preklapanja. Sa druge strane, kod *soft* klasterovanja se koriste takozvane *fuzzy* tehnike kojima se vrši proračun verovatnoća pripadnosti tačke različitim klasterima, odnosno, tačke inicijalnog skupa podataka nisu jednoznačno dodeljene nekom konkretnom klasteru, već sa nekim proračunatim verovatnoćama mogu da pripadaju različitim klasterima [141].

Najčešća podela tehnika klasterovanja je na: (1) metode zasnovane na raščlanjivanju (*partition-based methods*); (2) metode zasnovane na modelu (*model-based methods*); (3) metode zasnovane na gustini podataka (*density-based*); (4) metode zasnovane na umrežavanju (*grid-based);* (5) metode zasnovane na ograničenjima (*constraint-based*); (6) metode zasnovane na povezivanju (*link-based*); (7) metode zasnovane na čestim obrascima ponašanja (*frequent pattern-based*); (8) metode analize izuzetaka (*outlier analysis*); (9) hijerarhijski zasnovane metode (*hierarchical methods*).

Veći deo istraživanja predstavljenog u ovoj disertaciji zasniva se na primeni algoritama klasterovanja. U ovom delu je dat pregled samo najosnovnih karakteristika nekih metoda klasterovanja, dok je u nastavku poglavlja dat detaljniji pregled karakteristika metoda klasterovanja koje su osnov istraživačkog rada i naučnog doprinosa rešenja predstavljenog u ovoj disertaciji, *Expectation-Maximization* (EM) algoritma i modifikovanog HAC algoritma.

Metode zasnovane na raščlanjivanju (*partitioning-based*) se zasnivaju na principima kontruisanja jedne optimalne podele tačaka po klasterima, a zatim se za tako definisan broj klastera vrši inicijalno raspoređivanje tačaka iz skupa podataka. U sledećim iteracijama se tako raspoređeni podaci premeštaju iz klastera u klaster u zavisnosti od vrednosti različitih primenjenih metrika optimizacije, a u cilju dobijanja poboljšanog klasterovanja. Predstavnici ove kategorije algoritama su: *k-means*, *k-medoids*, *k-means++* i *CLARANS*. U referentnoj literaturi je dat prikaz najvažnijih metoda iz ove kategorije [142], [143]. Za potrebe istraživanja predstavljenog u ovoj disertaciji, *k-means* algoritam je korišćen u fazi kada su rađena inicijalna ispitivanja hibridnog pristupa problemu detekcije napada i anomalija, kao i tokom dela istraživanja u kom su ispitivane različite mogućnosti primene klasterovanja podataka zadatih u vidu vremenski serija [49], [137].

Metode zasnovane na modelu (*model-based*) primenjuju hipotezu određenog modela nad svakim od klastera, pod pretpostavkom da su podaci zadati kao mešavina niza raspodela verovatnoća, a u cilju

pronalaženja najboljeg usaglašavanja parametara izabranog modela karakteristikama podataka koji se analiziraju. Tipični predstavnici ove kategorije algoritama su *EM* [144], [145], AutoClass [146], *SOM* (*Self Organizing Maps*) [147] i klasterovanje zasnovano na konceptu neuralnih mreža, konceptualno klasterovanje – *COBWEB* i *CLASSIT* [148], [149]. Tehnika *Expectation-Maximization* je detaljno predstavljena u odeljku 4.6 ovog poglavlja.

Metode zasnovane na gustini podataka (*density-based*) se zasnivaju na primeni različitih metoda za proračun konektivnosti i funkcija gustine podataka. Najpoznatiji metodi iz ove kategorije su *DBSCAN*, *OPTICS* i *DenClue* [150–152].

Metode zasnovane na umrežavanju (*grid-based*) se zasnivaju na primeni koncepta višenivovske granularne strukture podataka, a neke metode se zasnivaju i na primeni kvantizacije i *wavelet* transformacija za potrebe generisanja klastera. Tipični predstavnici su *STING*, *WaveCluster*, *CLIQUE* [153], [154].

Metode zasnovane na ograničenjima (*constraint-based*) zasnivaju se na zadovoljavanju skupa korisničkih ili zahteva koji proističu iz karakteristika dalje primene rezultata klasterovanja (*application-specific constrains*), a najznačajniji predstavnik je *COD* (*Clustering with Obstacle*) [155].

Metode zasnovane na povezivanju (*link-based*) podrazumevaju specifičnu analizu raspoređenosti i povezanosti tačaka u okviru skupa podataka koji je na raspolaganju, a u praksi se primenjuju takozvane metode masovnih linkova SimRank [156] i LinkClus [157].

Metode zasnovane na čestim obrascima ponašanja (frequent pattern-based) razmatraju obrasce ponašanja i u zavisnosti od njihove učestalosti izvode zaključke o potencijalnoj optimizaciji u procesu klasterovanja. Koriste se metodama kojima je omogućeno klasterovanje u potprostore (*subspace-clustering*), gde se pravi izbor dimenzija u odnosu na koju će biti izvedeno klasterovanje. Osim toga, aktivno se primenjuju tehnike ekstrakcije atributa (*feature extraction*). Tipičan predstavnik je *p-Cluster* metoda, zasnovana na metodi sličnosti obrazaca (*pattern similarity*) [158].

Metode analize izuzetaka (outlier analysis) odnosno odudarajućih instanci, rade sa skupovima u kojima postoje instance koje se značajno razlikuju od ostalih i koje se po svojim karakeristikama mogu smatrati izuzecima. Tipični predstavnici (*Local Outlier Factor,* LOF i *Online Analytical Processing*) ovih metoda se vrlo često kombinuju sa nekim drugim metodama kako bi se efikasnije otkrivalo prisustvo izuzetaka [15], [159].

Hijerarhijski zasnovane metode iterativno primenjuju tehnike spajanja ili razdvajanja instanci podataka, a sve u zavisnosti od proračuna udaljenosti između elemenata skupa podataka koji se razmatra [160]. Osnovni princip je da se formira odgovarajuća arhitektura, stablo koje se naziva dendrogram, koje obuhvata niz iterativno ugnežđenih klastera podataka, pri čemu nije neophodno prethodno predvideti broj klastera koji će se generisati ali je neophodno da postoji uslov završetka rada algoritma (na primer definisanje *threshold* vrednosti). Generisanje dendrograma može biti zasnovano na primenama metoda udruživanja klastera, odnosno na aglomerativnim metodama hijerarhijskog klasterovanja (*hierarchical aglomerative clustering*), dok sa druge strane može da se zasniva i na metodi razdvajanja kada se primenjuju divizione hijerarhijske metode klasterovanja (*hierarchical divisive clustering*). U odnosu na aglomerativne tehnike, divizione tehnike se ređe primenjuju u praksi. Osnovni primeri algoritama koji se zasnivaju na primeni aglomerativne metode su Agnes [161], kao i niz algoritama kombinovanih sa *distance-based* metodama: BIRCH, ROCK i CAMALEON [69], [70], [162]. Primer primene *divisive* tehnika je algoritam Diana [163]. Tehnika hijerarhijskog

aglomerativnog klasterovanja HAC je jedna od ključnih za istraživanje predstavljeno u disertaciji i detaljno je izložena u odeljku 4.7 ovog poglavlja.

Generalno, kvalitet metode klasterovanja zavisi od toga kolika je sličnost instanci podataka koje su klasterovane unutar pojedinačnih klastera, dok je sa druge strane neophodno obezbediti nizak nivo međuklasterske sličnosti. Jedan od kriterijuma kvaliteta algoritma je sposobnost otkrivanja različitih obrazaca ponašanja na osnovu kojih će se efikasnije ostvariti klasterovanje. Kvalitetan algoritam klasterovanja treba da bude skalabilan, da može da se primenjuje u radu sa različitim tipovima atributa, da bude primenljiv za rad sa dinamičkim podacima i u uslovima prisustva šuma i izuzetaka i da može da radi sa podacima visoke dimenzionalnosti.

4.5 Procena sličnosti instanci podataka

Svaki skup podataka koji se koristi u procesu mašinskog učenja sadrži određeni broj instanci podataka koje dele neku specifičnu strukturu i karakteristike. Sličnost instanci podataka se može procenjivati primenom neke od mera sličnosti (npr. koeficijent korelacije) ili proračunom udaljenosti dve instance (*Eucledian*, *Manhattan*, *Minkowski*, srednja udaljenost). U kontekstu HAC algoritma najvažniji elementi ovih procena su određivanje odgovarajuće funkcije udaljenosti i metode grupisanja (primenjene u okviru odeljka 8.4).

4.5.1 Funkcije udaljenosti

Funkcija udaljenosti se primenjuje i u kontekstu istraživanja kojim se bavi ova disertacija. Konkretno se primenjuje na koordinate potpisa, mereći njihova međusobna rastojanja i time ukazujući na meru njihove različitosti.

Mnoge metode klasterovanja se zasnivaju na primeni proračuna udaljenosti (distance) kako bi se utvrdila sličnost ili različitost bilo kojeg para instanci podataka. Udaljenost između dva podatka x i y se označava kao $d_{x,y}$ i predstavlja preslikavanje ta dva podatka u jedan realan broj. Da bi mera udaljenosti bila validna, treba da ispunjava uslov simetričnosti i da dobija minimalnu izmerenu vrednosti odnosno da se njenom primenom obezbedi proračun rastojanja između dve instance podataka, a zatim da bi se utvrdilo koje dve instance iz analiziranog skupa imaju najmanju međusobnu udaljenost (što je relevantno za ispravan rad HAC algoritma u datom trenutku). Sa druge strane, za neke metode jedan od uslova je da bude u skladu sa uslovom nejednakosti trougla. Mera distance se tumači kao metrička mera udaljenosti u slučaju kada je zadovoljeno:

1. $d_{x,y} \geq 0,$ što odgovara uslovu nenegativnosti
2. $d_{x,y} = 0 \Rightarrow x = y \quad \forall x, y \in S$
3. $d_{x,y} = d_{y,x} \quad \forall x, y \in S,$ što odgovara uslovu simetričnosti
4. $d_{x,z} \leq d_{x,y} + d_{y,z} \quad \forall x, y, z \in S,$ što odgovara uslovu nejednakost trougla

Pri čemu je S skup podataka.

U literaturi, najčešće primenjivana je euklidska funkcija udaljenosti, *Euclidean Distance function,* d_e [164]. Za tačke skupa podataka, pri čemu svaka ima p koordinata, ovom funkcijom se rastojanje računa kao koren sume kvadrata rastojanja tačaka po koordinatama (relacija 4.4):

$$d_e = \sqrt{\sum_{i=1}^{p}(x_i - y_i)^2} \tag{4.4}$$

Manhattan Distance function, d_M, se zasniva na sumi razlika tačaka po vrednostima koordinata, za svaki par tačaka x i y, pri čemu tačke skupa podataka imaju po p koordinata i rastojanje se izračunava na sledeći način (relacija 4.5) [165]:

$$d_M = \sum_{i=1}^{p}|x_i - y_i| \tag{4.5}$$

U cilju obezbeđivanja kvalitetnijih rezultata, u ovoj tezi je korišćena *Squared Distance function*, funkcija kvadratne udaljenosti d_{sd}, kojom se rastojanje meri kao zbir kvadrata razlika u svakoj dimenziji i koje je definisano u relaciji 4.6:

$$d_{sd} = \sum_{i=1}^{p}|x_i - y_i|^2 \tag{4.6}$$

Za potrebe istraživanja predstavljenog u ovoj disertaciji, pokazuje se da bi se primenom mere zasnovane na proračunu euklidske udaljenosti, odnosno merenjem kvadratnog korena sume kvadratnog rastojanja, obezbedilo da razlika između dva sasvim različita klastera bude manje očigledna, posebno u daljoj vizuelnoj analizi odgovarajućeg dendrograma HAC algoritma.

Osim ovih mera, u praksi se često koristi *Minkowski* mera koja predstavlja izvestan vid generalizacije *Eucledean Distance* funkcije, jer koristi parametar q kojim se definiše struktura i tip mere (relacija 4.7):

$$d_{MN} = \left(\sum_{i=1}^{p}(x_i - y_i)^q\right)^{\frac{1}{q}} \tag{4.7}$$

Tako za q čija je vrednost jednaka 1, ova metrika meri takozvanu *City Block* metriku kojoj pripadaju i *Manhattan Grid*, *Taxicab* i norm L_1 distance. U slučaju kada q ima vrednost jednaku 2, ova metrika meri po principu euklidske metrike, a za vrednost q koja teži beskonačnosti, *Minkowski* metrika se odnosi na supremum L_{max} norm i L_∞ norm distance, odnosno maksimum rastojanja između bilo kojih komponenata vektora podataka [166]. U slučaju rada sa binarnim promenljivima, gde se često javlja problem isptivanja simetričnosti odnosno nesimetričnosti, primenjuje se *Jaccard* koeficijent [167].

4.5.2 Mere udaljenosti klastera

Dok funkcija rastojanja definiše rastojanje između dve tačke podataka, metode izračunavanja rastojanja pri grupisanju podataka definišu način na koji se izračunava rastojanje između dva klastera

koji sadrže proizvoljan broj tačaka podataka [80], [82], [168]. Ove udaljenosti se mere između klastera C_1 i C_2, a ne tačaka podataka.

Single-link, odnosno metoda najbližih suseda, je najjednostavniji način merenja razdaljine između klastera (relacija 4.8). U slučaju ovako definisanog merenja rastojanja između dva klastera, proračunom se traže dve najbliže instance podataka, pri čemu je jedna instanca u jednom klasteru, a druga je u drugom klasteru. Tako se za sve potencijalne parove instanci vrši proračun rastojanja i traži minimum od svih instanci iz jednog klastera i svih instanci drugog klastera, kao rastojanje između tačaka u dva različita klastera x_1 i x_2.

$$D(C_1, C_2) = \min_{x_1 \in C_1, x_2 \in C_2} D(x_1, x_2) \tag{4.8}$$

Međutim, iako je ovaj pristup jednostavan, kao rezultat može da proizvede veoma dugačke lance elemenata, s obzirom na to da se povezuju tačka sa obližnjom tačkom i na kraju će u isti klaster biti unešene dve tačke koje su veoma udaljene.

Complete-link, odnosno povezivanje najdaljih suseda je metoda kojom će dva klastera biti spojena ukoliko je udaljenost najdaljih članova iz ta dva klastera najmanja. Merenjem rastojanja se generišu klasteri koji teže sfernom obliku, sa konsistentnim prečnikom, odnosno cilj je da sve tačke u klasteru budu relativno blizu jedna drugoj. Cilj ove mere je da sve tačke budu u blizini u okviru određenog praga. Samim tim, kada se meri rastojanje između dva klastera traži se par tačaka čije je međusobno rastojanje najveće. Inicijalno se pretražuju parovi tačaka gde svaka tačka pripada drugom klasteru i traži se par koji daje maksimalno rastojanje. Zatim se u konkurenciji tako izabranih parova različitih klastera (kada se izračunaju udaljenosti) dalje traže dva najbliža klastera, što znači da se traži minimum od svih izračunatih maksimuma međusobnih rastojanja. Par klastera za koji se pronađe minimum se u nastavku procedure spaja u novi klaster (relacija 4.9):

$$D(c_1, c_2) = \max_{x_1 \in c_1, x_2 \in c_2} D(x_1, x_2) \tag{4.9}$$

Dakle, jedna opcija pretražuje lance (*single-link*), a druga (*complete-link*) traži sferne oblike pri klasterovanju.

Average-link pristup se zasniva na računanju prosečne vrednosti rastojanja svih parova tačaka između posmatranih klastera. Dva klastera će se spojiti ukoliko je prosečna udaljenost između ta dva klastera najmanja u odnosu na sve ostale prosečne vrednosti udaljenosti između različitih klastera. Za sve tačke iz jednog klastera se mere rastojanja ka svim tačkama drugog klastera, sabiraju se i tako dobijena vrednost se deli ukupnim brojem parova. Ovako izračunata mera rastojanja predstavlja izvestan vid sredine između *single-link* i *complete-link* metrika (relacija 4.10):

$$D(C_1, C_2) = \frac{1}{|C_1|}\frac{1}{|C_2|}\sum_{x_1 \in C_1}\sum_{,x_2 \in C_2} D(x_1, x_2) \tag{4.10}$$

Ovaj način merenja rastojanja podleže manjem uticaju izuzetaka (*outliers*), a osim toga nema nekih značajnijih prednosti u odnosu na ostale metrike. *Weighted average group* metoda se primenjuje

kada prilikom izračunavanja srednjih vrednosti rastojanja nemaju svi uzorci isti značaj, već se vrši ponderisanje tako što se jednom ili većem broju različitih merenih rastojanja daje veći značaj ili težina.

Centroid metrikom se mere rastojanja između proračunatih centroida svakog od razmatranih klastera, dakle ne neke konkretne instance podataka već težišta, centra klastera. Rastojanje između težišta se tumači kao rastojanje između klastera (relacija 4.11).

$$D(C_1, C_2) = D\left(\left(\frac{1}{|C_1|}\sum_{x\in C_1}\vec{x}\right), \left(\frac{1}{|C_2|}\sum_{x\in C_2}\vec{x}\right)\right) \tag{4.11}$$

Vordovom *(Ward)* metodom se proračunava ukupna varijansa oko centroida, tako da se za svaki centroid pretražuju sve tačke koje mogu da budu dodeljene tom centroidu, a računaju se odstupanja, odnosno kvadratna odstupanja tačaka od tog centroida. Tako, pre nego što se dva klastera spoje, svaki ima svoje težište, a postoje određena odstupanja tačaka od tako definisanog težišta. Funkcija povezivanja koja specificira rastojanje između dva klastera se izračunava kao povećanje zbira kvadrata greške (*Error Sum of Squares*, ESS) nakon spajanja dva klastera u jedan klaster (relacija 4.12):

$$TD_{C_1\cup C_2} = \sum_{x\in C_1\cup C_2} D\left(x, \mu_{C_1\cup C_2}\right)^2 \tag{4.12}$$

gde *TD* predstavlja ukupno rastojanje (*total distance*), a $C_1 \cup C_2$ predstavlja spajanje dva klastera. Vardova metoda se u literaturi spominje i kao metoda minimalne varijanse. Obuhvata sve klastere, a osnovni princip je da se obavi maksimiziranje homogenosti unutar klastera. Ukupna suma kvadrata unutar klastera se računa u cilju utvrđivanja koja se dva klastera dalje spajaju u svakom koraku algoritma. Suma kvadrata greške (*Sum of Squared Errors*, *SSE*) je definisana kao (relacija 4.13):

$$SSE = \sum_{i=1}^{k}\sum_{j=1}^{m_i}\left(x_{ij} - \bar{x_i}\right)^2 \tag{4.13}$$

pri čemu je x_{ij} j-ta instanca u *i*-tom klasteru, *k* je broj klastera, $\bar{x_i}$ predstavlja centar *i*-tog klastera, a m_i je broj instanci u *i*-tom klasteru.

Imajući primer dva različita klastera sa svojim instancama, svaki klaster ima svoje težište, a od svake tačke klastera može da se meri rastojanje do tog težista. Ukupno odstupanje se koristi za dalje odlučivanje koji klasteri će se spajati. Novonastali klaster koji je zasnovan na dva izabrana klastera će imati svoje novo težiste i tada je potrebno meriti rastojanja između svih tačaka tog novog klastera i njegovog težista. Meri se ukupno rastojanje, i ono što teorija pokazuje je da prilikom merenja ukupnog novog odstojanja, ona rastu, odnosno, prilikom svakog novog spajanja klastera instance podataka završavaju dalje od težišta novog klastera. Suma će uvek biti veća, a izbor algoritma je da u svakoj iteraciji poredi te izračunate udaljenosti i bira par klastera čijim spajanjem se dobija najmanje povećanje varijanse.

Vardova metoda obezbeđuje visoku tačnost u poređenju sa drugim metodama, pri čemu prilikom klasterovanja nije potrebno unapred definisati broj klastera. Osnovne mane metode se uglavnom zasnivaju na velikoj složenosti sa povećanjem broja instanci koje je potrebno uzeti u obzir prilikom proračuna, kao i osetljivost na prisustvo instanci koje odskaču svojom vrednošću od većine instanci (*outlier*s).

U praksi se često koristi *Lance-Williams* (LW) algoritam koji omogućava implementaciju svih ovih algoritama primenom samo jednog algoritma [85], [169]. *Lance-Williams* rekurzivna formula ažurira matricu udaljenosti na osnovu udaljenosti izračunatih u prethodnoj iteraciji.

Pojednostavljeno, *Lance-Williams* algoritam se smatra sveobuhvatnim metodom kojim je moguće implementirati bilo koju od prethodno opisanih metoda i primenjen je za potrebe istraživanja predstavljenog u okviru disertacije. Zasniva se na vrednostima iz matrice udaljenosti *D*, a kojom se računaju sva međusobna rastojanja između pojedinačnih klastera, definisanih za ove potrebe kao klaster *i,* (C_i), i klaster *j*, (C_j).

D={$D_{i,j}$: rastojanje između C_i i C_j za svako i, j koje uzima vrednosti 1, …, N}

Procedura započinje sa matricom udaljenosti $D_{i,j}$ gde za svaku instancu klastera C_i i C_j postoje izračunata rastojanja među njima, na neki od prethodno opisanih načina. Algoritam će imati $N-1$ iteracija jer se u okviru svake iteracije spajaju dva klastera. Tako na primer, ako se utvrdi par klastera koji su najbliži, C_i i C_j koji imaju minimalno rastojanje, algoritam će ih spojiti i tako novogenerisani klaster uvrstiti u svoj skup klastera, a pojedinačne klastere C_i i C_j će izbrisati iz daljeg proračuna. Za svaki preostali klaster, C_x, koji nije jedan od dva upravo spojena, algoritam će da ažurira rastojanja, odnosno u matricu rastojanja će uneti rastojanje od klastera C_x do novogenerisanog klastera $C_{i\cup j}$. Takođe, brišu se iz matrice rastojanja prethodno izračunata rastojanja od C_x do C_i i od C_x do C_j, i unosi se izračunato rastojanje između C_x i $C_{i\cup j}$. Na primer, u slučaju *single-link* pristupa, kada imamo tri klastera C_i, C_j, C_x, proračun *Lance-Williams* algoritma je jednostavan jer se uzima minimalno od dva razmatrana rastojanja - između C_x i C_i i rastojanja između C_x i C_j. Tako, ako je rastojanje između C_x i C_j manje od rastojanja između C_x i C_i, to znači da postoji element u C_j koji je bliži nekom elementu u C_x, nego što je to najbliži element u C_i blizak po rastojanju nekom elementu u C_x, tako da se uzima minimum ovih intraklaster rastojanja i ono postaje novo rastojanje između C_x i $C_{i\cup j}$. Dakle, vrlo mala promena ažuriranjem udaljenosti u matrici može da proizvede velike razlike u rezultatima.

U opštem smislu se algoritam predstavlja na sledeći način (relacija 4.14):

$$D_{x,i+j} = \alpha_i D_{x,i} + \alpha_j D_{x,j} + \beta D_{i,j} + \gamma \left| D_{x,i} - D_{x,j} \right| \tag{4.14}$$

Na osnovu ovakve polazne formule, za *single-link* za koji inače važi da je rastojanje trećeg klastera C_x od novonastalog klastera $C_{i\cup j}$ rastojanje je dato kao u relaciji 4.15:

$$D_{x,i+j} = min\{D_{x,i}, D_{x,j}\} \tag{4.15}$$

Sada, za proračun u *Lance-Williams* formuli se uzima rastojanje od C_x do C_i, rastojanje od C_x do C_j i rastojanje od C_i do C_j, dakle rastojanja između svih postojećih klastera. Na te udaljenosti se

postavljaju težinski faktori, a težine su zapravo date na osnovu nekoliko konstanti koje se priključuju na odgovarajući način u jednačinu, čime se dobijaju drugačiji algoritmi za klasterovanje.

Opšta formula LW rekurentne formule obuhvata različite metode grupisanja. U slučaju *Average Clustering* metode, odnosno metode grupisanja na osnovu proseka, ona ima sledeći oblik (relacija 4.16):

$$D(C_{1\cup2}, C_x) = \frac{\left(n_1 D(C_1, C_x) + n_2 D(C_2, C_x)\right)}{n_1 + n_2} \tag{4.16}$$

gde su C_1 i C_2 klasteri sa ukupnim brojem n_1 odnosno n_2 tačaka podataka, a koji su upravo spojeni u jedan novi klaster $C_{1\cup2}$, dok C_x predstavlja bilo koji od preostalih klastera koji u ovoj iteraciji nisu spojeni sa nekim drugim klasterom. U prethodoj iteraciji, matrica rastojanja je već sadržala rastojanja između svakog od parova klastera aktuelnih u tom koraku, uključujući i rastojanja ka klasteru C_1 i klasteru C_2, izraženih sa $D(C_1, C_x)$ i $D(C_2, C_x)$ u odnosu na svaki od preostalih klastera. Vrednosti parametara α_i, α_j, β i γ za različite algoritme koje LW formula obuhvata su zadate u tabeli 4.1:

Tabela 4.1 Primena LW metode za računanje različitih metrika rastojanja klastera

Metoda	$\boldsymbol{\alpha_i}$	$\boldsymbol{\alpha_j}$	$\boldsymbol{\beta}$	$\boldsymbol{\gamma}$
Single link	0.5	0.5	0	-0.5
Complete link	0.5	0.5	0	0.5
Average group link	$\frac{n_i}{n_i + n_j}$	$\frac{n_j}{n_i + n_j}$	0	0
Weighted average group	0.5	0.5	0	0
Centroid	$\frac{n_i}{n_i + n_j}$	$\frac{n_i}{n_i + n_j}$	$\frac{-n_i \cdot n_j}{\left(n_i + n_j\right)^2}$	0
Ward's	$\frac{n_i + n_k}{n_i + n_j + n_k}$	$\frac{n_j + n_k}{n_i + n_j + n_k}$	$\frac{-n_k}{n_i + n_j + n_k}$	0

Dakle, u slučaju primene *single-link* metode, kombinuju se sve izmerene razdaljine sa konstantama koje imaju vrednosti 0.5 za osnovna rastojanja novog klastera i nekog koji je preostao (posmatraju se rastojanja između C_x i C_i i između C_x i C_j), dok se prethodno međusobno rastojanje između dva spojena klastera (C_i i C_j) ne uzima u obzir, odnosno konstantom β koja ima vrednost 0 se taj član formule anulira. Zatim se vrednoću -0.5 za konstantu γ množi apsolutna vrednosti rastojanja izračunatih za udaljenost između C_x i C_i i između C_x i C_j. Rezultat je minimum rastojanja između C_x i C_i i rastojanja između C_x i C_j što je intuitivno i jasno kada je u pitanju *single-link* pristup (relacija 4.17).

$$D_{x,i+j} = \frac{1}{2}\left(D_{x,i} + D_{x,i} - \left|D_{x,i} - D_{x,j}\right|\right) \tag{4.17}$$

Jasno je da je dobijen minimum, jer postoje rastojanja $D_{x,i}$ i $D_{x,j}$ i jedno od njih je maksimalno, a drugo je minimum od ta dva, a vrednost zadata apsolutnom vrednošću razlike je praktično apsolutna vrednost razlike između tih minimum i maksimum vrednosti. Kada se od maksimuma oduzme razlika maksimuma i minimuma, rezultat je minimum.

Lance-Williams formula je jako dobar pristup za implementaciju različitih funkcija agregacije. Primenom ove metode moguće je modelovati niz različitih funkcija agregacije samo unošenjem odgovarajućih vrednosti konstanti kao parametara linearne kombinacije za svaki od ovih pristupa. Osim toga, jasno je da je složenost (cena) izvršavanja ovog algoritma sa ovim pristupom kubna, odnosno, inicijalno se izvodi N iteracija spajajući po dva klastera u svakom koraku, a zatim se pretražuju parovi klastera i nalazi onaj par sa najmanjom razdaljinom čime će se ostvariti N^2 koraka, a zatim se za svaki od preostalih klastera izvodi N koraka ažuriranja distance.

4.6 Algoritam maksimizacije očekivanja

U kontekstu istraživanja predstavljenog u ovoj disertaciji, jedan deo analize je podrazumevao primenu algoritma maksimizacije očekivanja (*Expectation-Maximization algorithm*) (poglavlje 8). EM algoritam se odnosi na meko klasterovanje, a zasniva se na proračunu gustine verovatnoće određenih veličina, kako bi se sa većom pouzdanošću podatak pridružio odgovarajućem klasteru. Pri tome ne postoje striktna ograničenja između klastera, već se za svaki podatak primenom EM algoritma izračunavaju verovatnoće pripadnosti svakom od generisanih klastera [145], [170]. EM je algoritam iterativnog tipa koji nakon početne inicijalizacije ciklično prolazi kroz fazu očekivanja (*expectation*, *E-faza*) i fazu maksimizacije (*maximization*, *M-faza*), a ceo postupak se ponavlja sve dok algoritam ne dostigne konvergenciju rezultata. U okviru *E-faze* se obavlja estimacija parametara, dok se u okviru *M-faze* vrši njihova optimizacija kako bi se što bolje prilagodili podacima nad kojima se algoritam primenjuje.

EM algoritam se dobro kombinuje sa modelom Gausovih mešavina (*Gaussian mixture model*). Gausova raspodela (*Gaussian distribution*) p je zadata relacijom (4.18) i zasniva se na vrednostima srednje vrednosti μ i standardne devijacije σ:

$$p(x \mid <\mu,\sigma>) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{4.18}$$

Za svaku Gausovu raspodelu se proračunavaju parovi (μ, σ). Tako, ukoliko se posmatra x_n tačaka podataka koji proističu sa dva izvora v i w, za svaki klaster C postojaće odgovarajuća raspodela za koju je potrebno proračunati vrednosti μ i σ. Procedura započinje inicijalizacijom dva slučajno pozicionirana para Gausovih promenljivih μ i σ, tako što se računaju vrednosti μ i σ Gausovih izvora podataka v i w. Verovatnoća da tačka x_i pripada izvoru v je definisana relacijama u Bayesovoj (4.19) i Gausovoj formi (4.20):

$$p(v \mid x_i) = \frac{P(x_i \mid v)P(v)}{P(x_i \mid v)P(v) + P(x_i \mid w)P(w)} \tag{4.19}$$

$$p(x_i \mid v) = \frac{1}{\sqrt{2\pi\sigma_v^2}} exp\left(-\frac{(x_i - \mu_v)^2}{2\sigma_v^2}\right) \tag{4.20}$$

Zatim algoritam ulazi u *E-fazu* računajući parove μ, σ za različite raspodele svake instance x_i i proverava za dva zadata izvora da li je veća verovatnoća generisanja ukoliko je instanca pristigla sa izvora *v* ili ukoliko je pristigla sa izvora *w*. U *M-fazi* se vrši maksimizacija izračunatih vrednosti parova μ, σ i vrši se njihova optimizacija kako bi se što bolje prilagodili podacima.

Ono što ovaj algoritam čini primenljivijim od nekih drugih metoda je izuzetna snalažljivost u radu sa nepotpunim podacima (koji su čest slučaj u realnim sistemima).

4.7 Hijerarhijsko klasterovanje

Hijerarhijsko klasterovanje (*hierarchical clustering*) je od velikog značaja za potrebe analitike podataka, posebno zbog eksponencijalnog rasta količine podataka koji se prenose savremenim mrežnim okruženjima, a koji su vrlo često neoznačeni. Hijerarhijski metod se zasniva na formiranju grafičkog prikaza rezultata klasterovanja, koji je dat u vidu stabla povezivanja, dendrograma. Postoje dva osnovna pristupa hijerarhijskom klasterovanju, aglomerativni i divizioni hijerarhijski metod. Oba metoda inicijalno računaju udaljenosti svih pojedinačnih instanci podataka, a zatim obavljaju klasterovanje metodom spajanja, što je tipičan pristup kod aglomerativnog klasterovanja, ili razdvajanjem, što je karakteristično za divizioni pristup hijerarhijskom klasterovanju. Dendrogram, kao izlazni rezultat primene ove grupe algoritama, se može koristiti za razumevanje opšte slike vezane za situaciju u razmatranom mrežnom saobraćaju, kao i teže uočljivih međurelacija u podacima.

4.7.1 Hijerarhijsko aglomerativno klasterovanje

Hijerarhijsko aglomerativno klasterovanje (HAC) predstavlja metod koji polazi od toga da se svaka instanca podataka inicijalno smatra posebnim klasterom, takozvanim singlton (*singleton*) klasterom. Zatim se primenom odabrane metode merenja rastojanja procenjuje bliskost između različitih singlton klastera i utvrđuju oni koji su najbliži, koji se u sledećem koraku spajaju i u daljoj proceduri razmatraju kao jedan novi, poseban klaster. Dva spojena singlton klastera se zatim brišu i ne razmatraju u daljem toku klasterovanja. Poslednji korak ovakvog postupka je da se generiše jedan sveobuhvatni klaster koji bi obuhvatao sve inicijalno uključene instance podataka. U pitanju je takozvani *bottom-up* metod kojim se dendrogram gradi u formi „odozdo nagore".

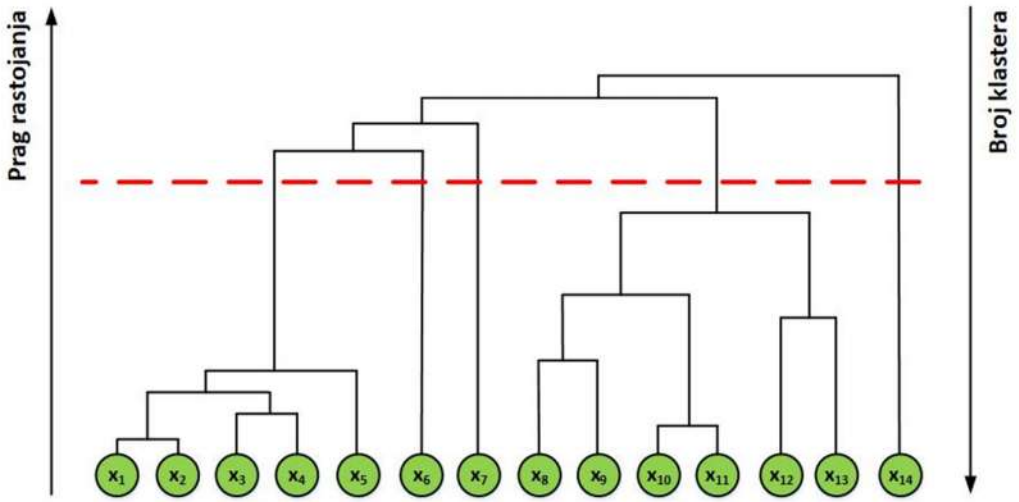
Aglomerativno hijerarhijsko grupisanje se zasniva na analizi strukturalnih sličnosti/razlika između instanci podataka koje je potrebno klasterovati. Definisanje sličnosti ili različitosti između instanci podataka zavisi od karakteristika, prirode i strukture analiziranih podataka.

Osnovna ideja je da se osigura da podaci koji su bliski (slični) budu klasterovani u isti klaster. S obzirom na to da je aglomerativno klasterovanje zasnovano na principu pregrupisavanja „odozdo nagore", sama procedura započinje tako što imajući na raspolaganju skup *S* sa *N* pojedinačnih instanci, za svaku od instanci podataka algoritam generiše klaster koji sadrži samo tu jednu tačku podataka: $C_i = \{x_i\}$. Zatim se iterativno prolazi kroz skup podataka i pretražuje par instanci podataka koje su najbliže jedna drugoj: $\min_{i,j} D(C_i, C_j)$.

Ovo rastojanje već nakon prve iteracije prestaje da bude rastojanje između dve instance podataka, već se definiše kao rastojanje između dva klastera. Razmatrajući po dva klastera C_i i C_j meri se rastojanje između njih, uočavaju se svi mogući parovi, a traži se par klastera koji su najbliži i koji se zatim spajaju u novi klaster $C_{i\cup j}$. Ovaj novi klaster obuhvata sve instance podataka koje su pripadale klasteru C_i i one koje su pripadale klasteru C_j i koje su sada spojene u novi klaster. Sledeći korak je da se iz dalje procedure iz skupa *S* izbrišu pojedinačni klasteri C_i i C_j, a skupu *S* se dodaje novoformirani klaster $C_{i\cup j}$.

Ovaj postupak se ponavlja dok ne preostane samo jedan klaster koji sadrži sve instance podataka. Ukupno će biti izvršeno *N-1* iteracija, pošto se u svakom koraku uzimaju dva klastera i spajaju u jedan. Na taj način se u svakom koraku brojčano gubi jedan klaster. Rezultat ove metode je hijerarhijsko stablo klastera, dendrogram. Za pokretanje algoritma je inicijalno neophodno da se definiše metrika udaljenosti koja će se primenjivati u proračunima. Naime, neophodno je da se u svakom koraku meri rastojanje između svih elemenata skupa podataka koji se razmatra, tako da u prvom koraku gde su definisani samo singlton klasteri, kojih ima *N*, neophodno je da se izračunaju rastojanja između svakog singlton klastera i svih ostalih singlton klastera, što čini složenost $O(N^2)$ ukupnih poređenja. Za svako poređenje će biti potrebno *d* operacija, jer je potrebno u obzir uzeti i broj atributa, tako da je to cena generisanja matrice udaljenosti.

Matrica udaljenosti se izračunava samo jednom, a zatim se u svakoj iteraciji algoritma ova matrica ažurira. Dakle, biće *N* koraka ovog algoritma, a zatim će svaki put biti potrebno da se nalazi par najbližih klastera, što podrazumeva N^2 koraka [168]. Na slici 4.3 je dat primer funkcionisanja hijerarhijskog aglomerativnog algoritma. Za potrebe proračuna rastojanja korišćena je najjednostavnija mera rastojanja, *single-link distance*.



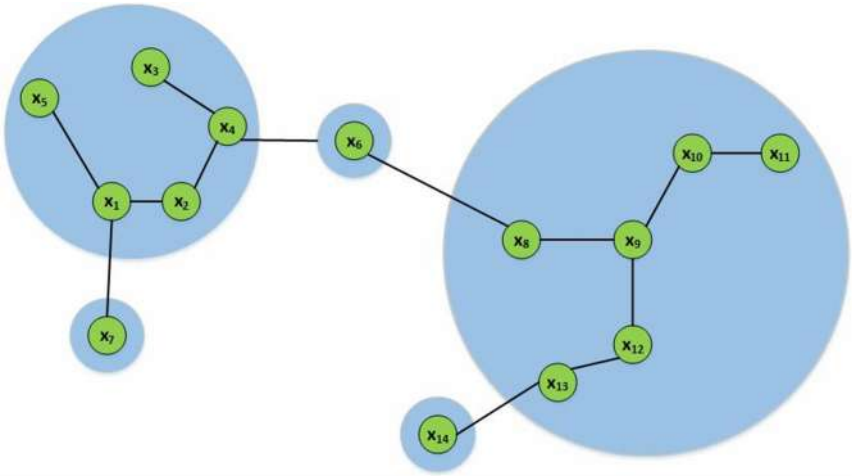
Slika 4.3 Primer izvršavanja hijerarhijskog aglomerativnog algoritma klasterovanja

Dakle, zadate su tačke koje su zatim na grafikonu inicijalno poređane. Svaka od njih (x_1, x_2, ..., x_{12}, x_{13}, x_{14}) je singlton klaster, tako da algoritam pretražuje skup u potrazi za parom klastera koji su najbliži. U ovom slučaju su najbliži x_1 i x_2, tako da ih algoritam povezuje, što se vidi na slici 4.3, a ta

dva singlton klastera prestaju da budu singlton i postaju jedan klaster, $\{x_1, x_2\}$. Dakle, u stablu dendrograma se povezuju čvorovi x_1 i x_2 i postavlja se visina tog spoja koja predstavlja rastojanje između x_1 i x_2 u prostoru (koliko su udaljeni jedan od drugog). Algoritam dalje pretražuje klastere kako bi pronašao sledeći najbliži par. U ovom slučaju je to par x_{10} i x_{11}, tako da algoritam iscrtava vezu između njih koja se postavlja na malo veću udaljenost nego prethodni par, jer je rastojanje nešto veće nego što je kod bilo kod x_1 i x_2. Zatim se procedura ponavlja u potrazi za sledećim parom, gde algoritam utvrđuje da je par x_3 i x_4 prvi sledeći par sa najbližim rastojanjem. Zatim se utvrđuje da rastojanje između $\{x_1, x_2\}$ i $\{x_3, x_4\}$ definiše novi najbliži par pa se time spajaju klasteri $\{x_1, x_2\}$ i $\{x_3, x_4\}$. Zatim se u sledećim iteracijama ponavlja ovaj postupak sa ostalim singltonima i klasterima. Svaki put kada dođe do spajanja dva klastera, iscrtava se još jedan novi luk u okviru dendrograma i postavlja na visinu definisanu rastojanjem koje postoji između novopronađenog para klastera, odnosno rastojanje spajanja je uvek sve veće. Procedura se nastavlja sve dok ne dođe da spajanja svih instanci podataka u jedan veliki klaster, pri čemu će sve grane biti povezane u dendrogram i time omogućiti prikaz hijerarhijske strukture podataka, odnosno njihove organizacije. Na osnovu postavljenog praga se preseca dendrogram na nekom rastojanju, pri čemu svaki čvor koji je obuhvaćen delom dendrogama do samog praga postaje klaster. Na predstavljenom primeru jedan klaster će sadržati elemente x_1, x_2, x_3, x_4, x_5 dok je x_6 klaster sam za sebe, x_7 je klaster sam za sebe, dok su se sa druge strane formirali klasteri sa x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, a klaster x_{14} je klaster sam za sebe (slika 4.3 i slika 4.4). U zavisnosti od uslova i primene dobijenih rezultata, dendrogram se može preseći na mestu koje je optimalno za konkretnu sitaciju.

Osim na osnovu dendrograma, definisanje optimalnog broja klastera može da se izvede i iscrtavanjem rastojanja u odnosu na broj klastera, nakon čega se primenjuje vizuelna pretraga praznina, ili se primenjuje metoda proračuna maksimuma drugog izvoda i slično [168].

Jedan od metoda za računanje optimalnog broja klastera je takozvana metoda lakta (*elbow method*), kojom se izračunava suma kvadrata grešaka na svakom klasteru, zatim se iscrtava grafički prikaz tih suma na osnovu kojih se traži promena nagiba sa strmih delova na delove sa blagim nagibom (ili bez nagiba), a koji su obično u obliku sličnom laktu. Za potrebe istraživačkog rada predstavljenog u ovoj disertaciji, hijerarhijski aglomerativni pristup klasterovanja predstavlja osnov predloženog rešenja i njegove primene.



Slika 4.4 Rezultat klasterovanja primenom hijerarhijskog aglomerativnog algoritma

4.7.2 Hijerarhijsko klasterovanje deljenjem

Hijerarhijsko klasterovanje deljenjem (*hierarchical division clustering*) predstavlja metodu koja polazi od pretpostavke da su sve instance podataka inicijalno deo jednog velikog, zajedničkog klastera. Zatim se primenom određenih metoda razdvajanja vrši segmentacija takvog klastera na dva manja. Svaka iteracija vrši dalje segmentiranje, sve dok se segmentacijom ne stigne do situacije kada je svaka instanca podataka raspodeljena u po jedan poseban klaster. Ovaj metod se naziva *top-down*, odnosno „odozgo nadole". Najveći izazov pri radu sa ovom grupom algoritama jeste izbor sledećeg klastera kandidata za razdvajanje, a uobičajeni pristup je primenom metoda *size-priority* kojima se vrši odabir klastera najveće veličine za razdvajanje. Takav pristup daje prioritet kreiranju klastera koji su izbalansirani po veličini. Implementacija ove grupe algoritama se vrlo često zasniva na primeni metode usrednjavanja sličnosti (*average similarity*) [171]. Osim toga, važno je voditi računa o koheziji klastera, odnosno treba imati u vidu da za klaster sa datom prosečnom sličnošću može postojati više različitih oblika. Tako, izduženi klaster (ili klaster koji se sastoji od dva dobro odvojena potklastera) može imati istu prosečnu sličnost kao i sferni klaster. Vrlo često se koriste algoritmi zasnovani na konceptu sličnosti, poput *MinMaxCut* algoritma [172] koji je zasnovan na *Min-Max* principu klasterovanja, koji podrazumeva da se podaci grupišu u klastere tako da se sličnost između različitih klastera svede na minimum, dok se sličnosti unutar svakog klastera maksimalno povećavaju. Tako se za potrebe ispunjavanja ovog cilja uvode različite metode za merenje stepena težine pri razbijanju klastera na dva dela, pri čemu se kohezijom klastera smatra najmanja vrednost funkcije *MinMaxCut* kada je klaster podeljen na dva potklastera. U praksi se divizioni metod hijerarhijskog klasterovanja ređe primenjuje od aglomerativnog pristupa hijerarhijskom klasterovanju.

5. ENTROPIJSKI ZASNOVANE METODE

Savremeni principi razvoja metoda detekcije anomalija i napada se svojim velikim delom zasnivaju na analizi mrežnog saobraćaja, sa ciljem što efikasnije upotrebe korisnih informacija sakupljenih u tokovima mrežnog saobraćaja. Posebnim metodama analize moguće je iz ekstrahovanih tokova mrežnog saobraćaja precizno izdvajati tokove normalnog saobraćaja od onih koji pripadaju neuobičajenom mrežnom saobraćaju. Takve metode se u velikoj meri zasnivaju na definisanju graničnih vrednosti različitih statističkih karakteristika saobraćaja i generisanju odgovarajućih alarma u slučajevima kada one prelaze definisane vrednosti. Zbog svoje jednostavnosti prikupljanja statističkih podataka o mrežnoj komunikaciji sa mrežnih uređaja putem NetFlow ili sličnog protokola, otkrivanje mrežnih anomalija na osnovu analize ponašanja obrazaca saobraćaja je prepoznato kao koristan metod savremene bezbednosne analitike i rešenja zaštite. Tehnike koje su zasnovane na proračunu entropije se mogu primenjivati za potrebe detekcije anomalija i napada, koristeći se jakom korelacijom koja je utvrđena između atributa kojima su opisane izvorišna/odredišna adresa i odgovarajući portovi, posebno u slučaju korišćenja dvosmernih tokova podataka.

5.1 Osnovne karakteristike

Entropija se definiše kao mera neizvesnosti i slučajnosti nekog stohastičkog procesa. U kontekstu analize mrežnog saobraćaja, može se pretpostaviti kao stepen varijanse različitih profila (obrazaca ponašanja) atributa koji na neki način odražava mrežni saobraćaj pri čemu obezbeđuje mehanizme za praćenje efekata promene karakteristika saobraćaja pri promeni vrednosti atributa podataka. Ove varijacije u vrednostima entropije predstavljaju značajnu indikaciju postojanja anomalije ili napada.

U literaturi i praksi je poznato nekoliko pristupa za izračunavanje entropije. Najopštiji i najosnovniji pristup računanju entropije je Šenonov (*Shannon*) metod, dok su se razvojem u ovoj oblasti u međuvemenu pojavili i drugi, specifični oblici poput *Rényi* i *Tsallis* entropija [51], [52], [173]. Šenonova entropija je definisana relacijom (5.1):

$$H_S(X) = \sum_{i=1}^{N} p(x_i)\ \log_a \frac{1}{p(x_i)} \tag{5.1}$$

Pri tome N predstavlja ukupni broj elemenata obuhvaćenih distribucijom podataka, $p(x_i)$ predstavlja verovatnoću pojave elementa x_i u distribuciji, a koja se izračunava kao odnos doprinosa elementa x_i sa vrednošću m_i u ukupnoj sumi svih vrednosti, M (relacija 5.2):

$$p(x_i) = \frac{m_i}{M},\ M = \sum_{i=1}^{N} m_i \tag{5.2}$$

Šenonova entropija se oslanja na kompromis između postignutih uticaja iz glavnog dela distribucije i repa distribucije, a što se može bolje kontrolisati korišćenjem parametarizovanih entropijskih generalizacija, *Rényi* i *Tsallis* varijantama proračuna entropije. *Tsallis* $H_T(X)$ i *Rényi* $H_R(X)$ entropije su parametrizovane parametrom skaliranja α i zadate relacijama (5.3) i (5.4), respektivno:

$$H_T(X) = \frac{1}{1-\alpha}\left(\sum_{i=1}^{N} p(x_i)^{\alpha} - 1\right) \quad (5.3)$$

$$H_R(X) = \frac{1}{1-\alpha}\log_b\left(\sum_{i=1}^{N} p(x_i)^{\alpha}\right) \quad (5.4)$$

Pored toga, u kontekstu primene entropijski zasnovanih metoda detekcije napada i anomalija korisno je primeniti specifičan faktor skaliranja za normalizaciju entropije na vrednost 1 za potpuno randomizovanu distribuciju. Prema ovom postupku, faktor skaliranja koji se primenjuje za Šenonovu i *Rényi* entropiju je dat kao $1/\log_b N$, dok je za *Tsallis* entropiju definisan kao $(1-\alpha)/(N^{1-\alpha}-1)$. Primenom Šenonove metode entropije dobijaju vrednosti u opsegu od 0 do 1, što je slučaj i sa *Rényi* i *Tsallis* metodom u slučaju kada parametar α ima pozitivnu vrednost. U slučaju negativne vrednosti parametra α ove metode će generisati vrednosti entropije veće od 1 [27].

5.2 Primena entropije u sistemima detekcije napada i anomalija

Jedna grupa istraživanja je došla do zaključka da su *Rényi* i *Tsallis* pristup dominantno efikasniji u odnosu na Šenonov, zasnivajući svoje tvrdnje na rezultatima koji ukazuju na bolju detekciju pikova ili repova u dobijenim raspodelama entropija podataka [48], [50]. Iskustvo u korišćenju *Rényi* i *Tsallis* metoda pokazuje da se optimalne performanse mogu dobiti za fiksnu vrednost parametra α u opsegu od -2 do +2 [27]. Istraživanje predstavljeno u ovoj disertaciji se jednim svojim delom zasniva i na primeni i analizi entropijski zasnovanih metoda, pri čemu je ispitivana i prethodno navedena generalizacija vezano za opseg optimalnih vrednosti parametra α [27], [49], [140], [174]. Na osnovu eksperimenata i analize rezultata obuhvaćenih disertacijom može se zaključiti da je u opštem slučaju prethodno opisana generalizacija neosnovana, te da su rezultati izloženi u tim studijama u velikoj meri zavisili od specifičnosti skupa korišćenih tehnika detekcije, izbora podataka koji će se analizirati i odabira karakteristika koje se dalje koriste za eksperimente. Pretpostavljena je mogućnost korišćenja granice tolerancije kako bi se proširila margina varijacije entropije u skladu sa faktorom (parametrom) množenja *k*, a koji podešava opseg prihvatljivih vrednosti. Dakle, sve vrednosti entropije koje su van granica margine (ispod donje granice ili iznad više granice) se smatraju anomalnim, što izaziva alarm. Detaljniji rezultati i analiza su predstavljeni u poglavlju 7.

Detekcija anomalija mrežnog saobraćaja zasnovana na entropiji se u mnogim aspektima potpuno razlikuje od metoda mašinskog učenja, što otežava, pa čak i onemogućava direktno poređenje njihovih performansi.

Informacije o komunikacionim tokovima se sa mrežnih rutera jednostavno dobijaju korišćenjem IPFIX protokola ili sličnih industrijskih standarda, kao što su NetFlow, JFlow, NetStream i drugi. Originalni tokovi su jednosmerni, a dalja predobrada je potrebna da se oni konvertuju u dvosmerne tokove koji pružaju više informacija za precizno otkrivanje anomalija.

Entropija se izračunava po epohi za svaku distribuciju podataka generisanu procesom agregacije, čime se dobija veliki broj vremenskih serija entropija podataka (jedna vrednost atributa po epohi). Značajna promena u raspodeli podataka koja se javlja kao posledica promena aktivnosti u tokovima mrežnog saobraćaja kao rezultat ima naglu promenu entropije. Ove promene se mogu detektovati korišćenjem nekog od mehanizama zasnovanih na definisanju vremenskih prozora ili primenom

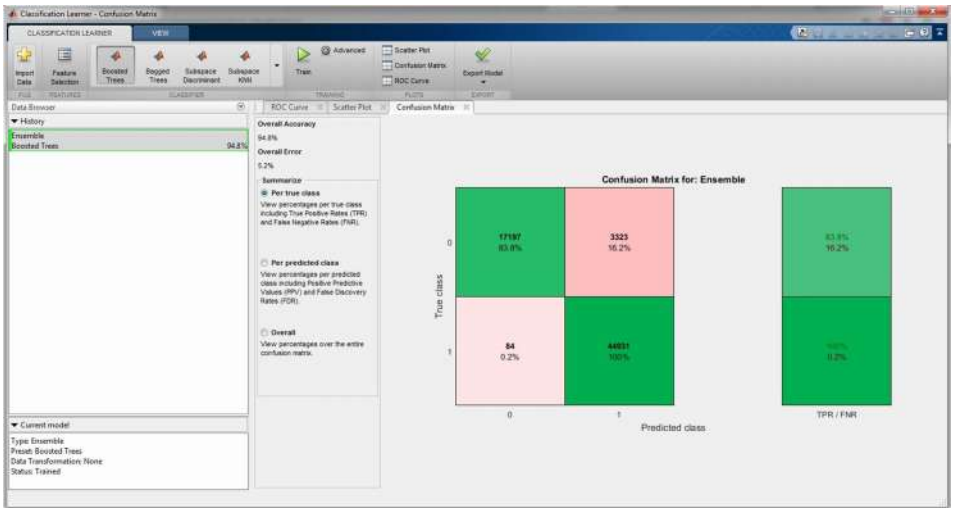
eksponencijalnog pokretnog proseka, odnosno EMA algoritma [175], koji se zasniva na izračunavanju margine prihvaćenih vrednosti. Tačnije, primenom EMA tehnike na vrednosti entropije i na vrednost standardne devijacije se dobija margina prihvatljivih varijacija vrednosti entropija. U slučaju kada izračunata vrednost entropije pređe definisanu marginu, sistem takav događaj prepoznaje kao anomaliju i generiše odgovarajući alarm. Ove anomalije su indikacija bezbednosnih pretnji i stoga je potrebna dalja analiza koja bi ispitala izvorišni razlog pojave napada ili anomalije (*root cause analysis*), a koja bi podrazumevala obradu i analizu neobrađenih instanci tokova saobraćaja kako bi se izvukle informacije o napadačima, žrtvi napada i metodi napada. Postoji niz tehnika kojima se ova analiza može dodatno poboljšati [27], [39].

6. SOFTVERSKI ALATI I RAZMATRANO OKRUŽENJE

Za potrebe razvoja specifičnog rešenja detekcije napada i anomalija u mrežnom okruženju predstavljenog u ovoj tezi bilo je neophodno obezbediti radno okruženje koje će moći da pruži sve uslove za primenu različitih metoda mašinskog učenja, podrži rad sa velikim skupovima podataka (veličine i do nekoliko miliona instanci podataka) održavajući korišćene skupove podataka konzistentnim i upotrebljivim za ceo tok istraživanja, kao i da na efikasan način generiše neophodan skup rezultata i omogući njihovu kvalitetnu računarsku i grafičku analizu. Istraživački rad je trajao celim tokom doktorskih studija, pri čemu je sve vreme vođeno računa da se koriste najnovije verzije odabranih softverskih alata. Paralelno sa tim su razvijene posebne softverske komponente koje su omogućile da se ovo istraživanje adekvatno obavi, da se dođe do konkretnih rezultata i ukaže na sve naučno-istraživačke doprinose predloženog rešenja.

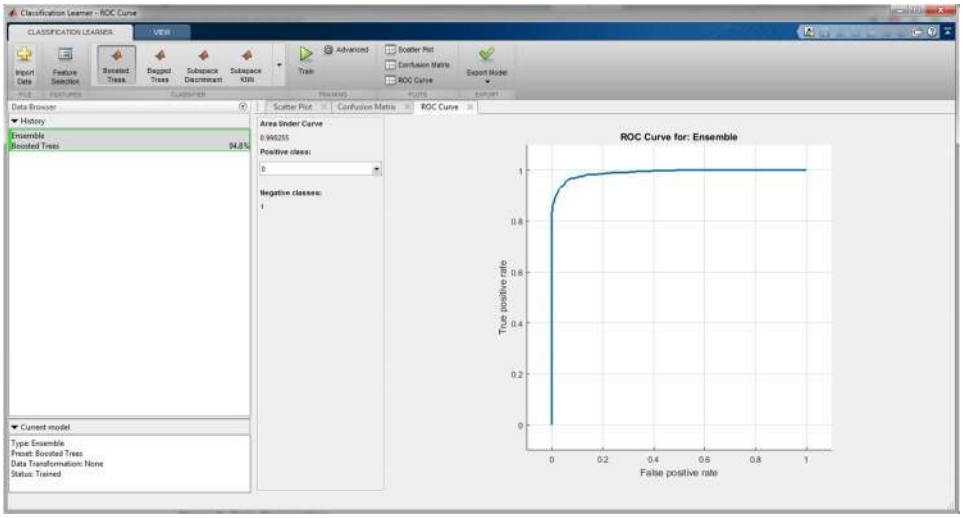
6.1 Softversko okruženje MATLAB

Za potrebe naučno-istraživačkog rada predstavljenog u ovoj tezi, u jednom delu istraživanja je korišćeno MATLAB okruženje [176]. Zahvaljujući širokom spektru ugrađenih funkcija, MATLAB predstavlja interaktivno i fleksibilno okruženje za razvoj različitih algoritama, pretprocesiranja i procesiranja ulaznih podataka, primenu različitih numeričkih proračuna, analizu podataka i njihovu vizuelizaciju. Njegov rad je zasnovan na primeni višeg programskog jezika Matlab, koji je često efikasniji i brži od tradicionalnih programskih jezika poput C++ jezika. MATLAB omogućava da se na sveobuhvatan način obrađuju podaci zadati u različitim formatima: tekst, tabelarno zadati podaci (*Excel*), slike, audio, video i XML podaci.



Slika 6.1 Primer izračunavanja vrednosti matrice konfuzije u MATLAB okruženju

Na slikama 6.1 i 6.2 su predstavljeni primeri grafičkog korisničkog interfejsa MATLAB platforme, a koji su bili od interesa i toku istraživanja. U ovom konkretnom slučaju prikazana je vizuelizacija rezultata dobijenih pri simulaciji *Boosted Tree* algoritma mašinskog učenja, jednog od tipičnih predstavnika *ensemble* algoritama.



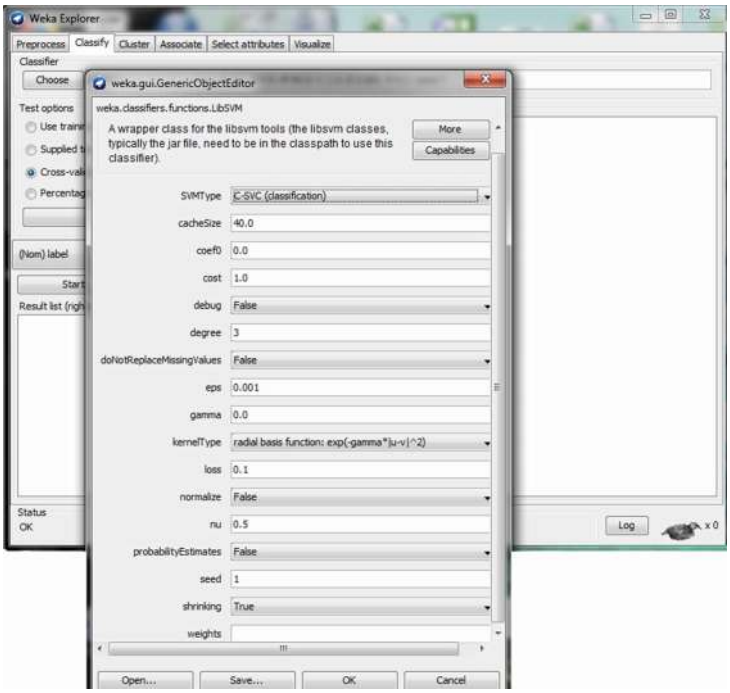
Slika 6.2 Primer izračunavanja vrednosti ROC AUC krive u MATLAB okruženju

Za potrebe ovog istraživanja MATLAB je već u inicijalnoj fazi korišćen kao osnovno okruženje za simulaciju i analizu različitih algoritama mašinskog učenja. U radu koji je objavljen na međunarodnoj konferenciji ICCP2017 predstavljeni su rezultati rada sa nekoliko najkarakterističnih algoritama iz kategorije *ensemble* klasifikatora, nad podacima iz UNSW-NB15 skupa podataka [95], [123].

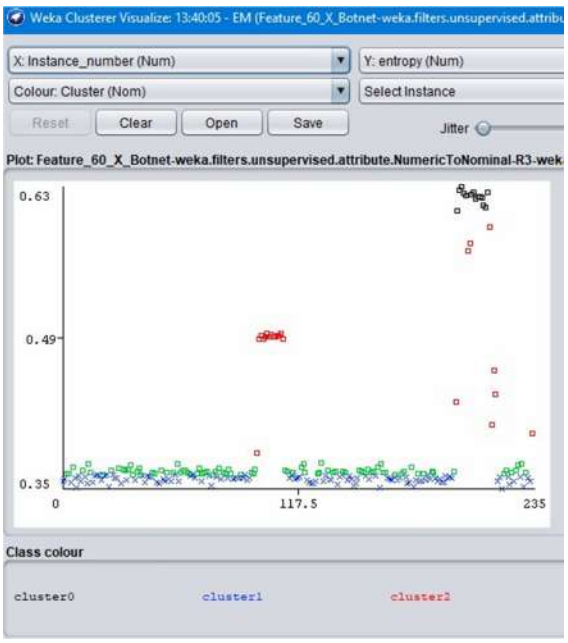
Osim toga, MATLAB je korišćen za potrebe eksperimentalne analize modifikovanog skupa podataka CTU-13, koji je prečišćen, modifikovan i dodatno obogaćen instancama sintetički generisanih oblika napada. Rezultati dobijeni ovim istraživanjem su predstavljeni u okviru rada publikovanog na međunarodnoj konfenciji, pri čemu je tada u okviru ovog istraživanja po prvi put uveden koncept kombinovane primene entropijski zasnovanih tehnika detekcije napada i metoda mašinskog učenja [137], [177].

6.2 Softversko okruženje WEKA

WEKA (*Waikato Environment for Knowledge Analysis,* Univ. Waikato, Novi Zeland) je moderan softverski alat, otvorenog Java koda i jedan od najčešće primenjivanih alata za potrebe istraživanja u oblasti veštačke inteligencije i mašinskog učenja [178–180]. Predviđen je za rad sa različitim formatima podataka, utvrđivanje njihove strukture i karakteristika kao i za merenje perfomansi u kontekstu primene različitih algoritama mašinskog učenja. WEKA podržava niz različitih formata podataka: .arff, .names, .data, .csv, .json, .libsvm, .m, .dat, .bsi, .xrff, a podrazumeva različite mogućnosti obrade podataka: pretprocesiranje, klasifikaciju, klasterovanje, primenu asocijativnih pravila, izbor atributa koji će se koristiti u eksperimentalnom delu istraživanja, kao i vizuelizaciju dobijenih rezultata. U okviru WEKA okruženja je omogućena direktna primena dostupnih algoritama iz koda koji je pisan na programskom jeziku Java. Na slikama 6.3 i 6.4 je prikazan primer rada i vizuelnog prikaza specifičnih rezultata u grafičkom korisničkom interfejsu WEKA okruženja.



Slika 6.3 Primer podešavanja karakteristika klasifikatora u WEKA okruženju



Slika 6.4 Primer vizuelizacije rezultata algoritma klasterovanja u WEKA okruženju

U okviru ovog istraživanja, *WEKA* je uvedena u delu istraživanja UNSW-NB15 skupa podataka i ispitivanja performansi nekoliko karakterističnih nadgledanih algoritama mašinskog učenja [125]. Zatim je istraživanje prošireno na aspekte rada sa modifikovanim CTU-13 podacima koji su zadati u

formi vremenskih serija, gde je uveden koncept izuzetaka (*outlier*) i primenjeni su nenadgledani algoritmi mašinskog učenja kombinovani sa entropijski zasnovanim metodama [137]. Ova faza istraživanja je predstavljala uvod u konkretnije analize različitih tokova mrežnog saobraćaja (realni, *botnet* i sintetički mrežni saobraćaji) i primenu specifičnih algoritama klasterovanja: *k-means* i EM algoritma [49]. Sveobuhvatnijom analizom većeg broja eksperimenata učinjeni su značajni koraci u ostvarivanju naučnih doprinosa predstavljenih u disertaciji, koji su publikovani u časopisu od međunarodnog značaja [140].

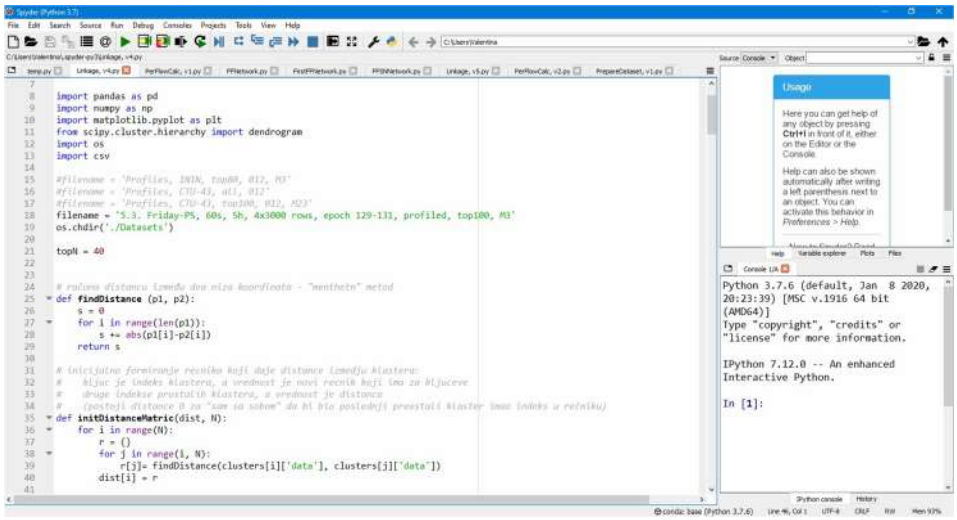
6.3 Programski jezik Python

Python je jedan od najpopularnijih programskih jezika koji se koriste u oblasti analize podataka (*data science*). Python je sintaksno jednostavan objektno orijentisan jezik koji se primenjuje za potrebe opšteg programiranja različitih aplikacija, a posebno se koristi kao pouzdano sredstvo u oblasti razvoja, testiranja i implementacije algoritama za analizu podataka [181], [182]. U odnosu na druge slične jezike, prednost Python jezika je izuzetna brzina izvršavanja, redovno ažuriranje biblioteka i funkcionalnosti, kod je izuzetno čitljiv, lako i brzo se uči, obiluje raznovrsnošću paketa, dok svojim visokim stepenom modularnosti postojećeg koda doprinosi njegovoj ponovnoj upotrebljivosti za različite potrebe. Pisanje i testiranje koda se obavlja bez potrebe za rekompilacijom koda, dok je debagovanje zasnovano na prilično jednostavnim procedurama (slika 6.5). Za potrebe analize u oblasti analize podataka preporučena je primena Python kodiranja u nekoliko razvijenih IDE (*Integrated Development Environment*) okruženja: *IDLE*, *Eclipse*, *PyCharm*, *Spyder*, *PyScripter* i druga.

Python je razvijen kroz nekoliko bitnih delova. *SciPy* predstavlja ekosistem ovog interpretiranog jezika koji se odnosi na oblasti rada vezanih za matematiku, naučna istraživanja i različite oblasti inženjerstva i tehnološkog razvoja. U njegovoj osnovi je programski jezik Python uz nekoliko paketa koji su neophodni za razvoj i testiranje u oblasti obrade podataka: *NumPy*, koji definiše različite numeričke nizove, matrične tipove i odgovarajuće operacije koje se nad njima mogu koristiti, dok je glavni objekat paketa homogeni višedimenzioni niz koji je predstavljen kao tabela elemenata (*ndarray*); *Pandas* predstavlja paket kojim su definisane različite strukture podataka za intuitivan i značajno pojednostavljen rad sa podacima, a lako se integriše u različita simulaciona okruženja pogodna za naučno-istraživački rad. Izuzetno je popularan pri radu sa tabelarno zadatim podacima, podacima koji odgovaraju uređenim/neuređenim vremenskim serijama, matricama i različitim formama podataka koji se dobijaju statističkim merenjima. Zasniva se na dve osnovne strukture podataka, *Series* za rad sa jednodimenzionalnim podacima i *DataFrame* za rad sa višedimenzionalnim podacima. Za potrebe vizuelizacije je predviđena primena *Matplotlib* biblioteke. *Scikit-learn* je neophodan modul za primenu u kontekstu analize podataka, a odgovoran je za implementaciju velikog broja različitih algoritama mašinskog učenja, uključujući algoritme klasifikacije, klasterovanja, kombinovanog učenja kao i algoritama za predobradu podataka [183].

U kontekstu istraživanja predstavljenog u ovoj tezi, glavni rezultati su ostvareni upravo primenom Python programskog jezika u *Spyder IDE* okruženju. Od posebnog značaja je bila mogućnost korišćenja *DataFrame* strukture koja ima ugrađene efikasne mehanizme grupisanja tabelarno zadatih podataka. Prilikom njegove primene, predloženi algoritam je postao efikasniji i manje složen, jer su korišćene već postojeće efikasne metode za agregaciju po više kolona (*groupby* metod), tehnike za brojanje broja pojavljivanja agregiranih redova (*size* metoda), kao i metoda za brojanje različitih elemenata (*unique* metoda). Pored toga, rezultat dobijen agregacijom automatski čuva listu indeksa odgovarajućih tokova podataka u strukturi *DataFrame*, time značajno pojednostavljujući unos

izračunatih karakteristika i izostavljajući potrebu za drugim prolazom kroz skup podataka [174]. Pokazuje se da je vreme izvršavanja algoritma nad definisanim skupom podataka od milion instanci podataka kraće u Python okruženju u odnosu na Java okruženje koje je do tada korišćeno.

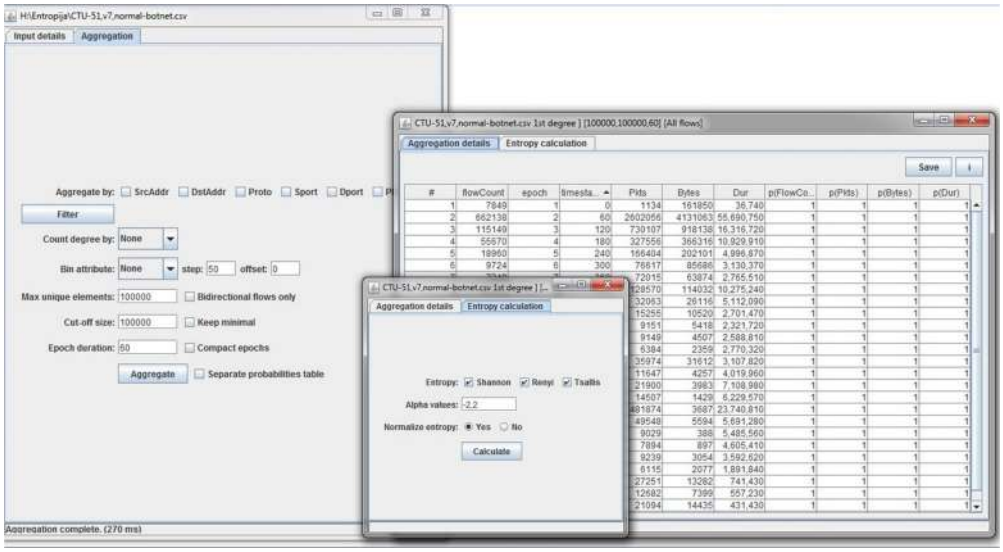


Slika 6.5 Primer dela koda pisanog u *Spyder Phyton* okruženju

6.4 Softverski alat Entropy Calculator

Za potrebe predobrade podataka entropijskim metodama [39] koje su korišćene u okviru ovog istraživanja primenjen je *Entropy Calculator*, Java softver koji je kreiran u okviru šireg istraživačkog opusa, a čija je osnovna namena u okviru ove disertacije da obavlja agregaciju, identifikuje glavne aktere u komunikaciji i izračunava odgovarajuće entropije atributa. *Entropy Calculator* je funkcionalna aplikacija koja je razvijena kroz master rad [184], a koji je korišćen i za potrebe različitih istraživačkih aktivnosti u okviru projekata Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije, kao i EUREKA programa „Sistem za detekciju anomalija u mrežnom saobraćaju na bazi analize NetFlow podataka – TRADE" (grant broj E!13304). Ovaj softver je dizajniran tako da obezbeđuje i odgovarajući jednostavan grafički korisnički interfejs, pri čemu je njegova osnovna namena da omogući agregaciju mrežnog saobraćaja prema željenim atributima i zatim izračunava entropiju. Osnovna prednost ovog softvera je mogućnost podešavanja pojedinačnih parametara analize performansi, čime se obezbeđuje optimizacija i efikasnost pri detekciji anomalija i napada. Format skupa podataka se može konfigurisati pomoću JSON meta datoteke, koja opisuje tipove karakteristika i označava ih kao identifikacione ili volumetrijske atribute. Softver podržava interaktivna ručna podešavanja parametara agregacije i obrade, ali se efikasnije korišćenje postiže masovnom obradom, gde su sva podešavanja definisana u posebnom JSON fajlu. Softver takođe obezbeđuje filtriranje podataka, definiciju serijalizovane agregacije pomoću različitih ključeva, izbor izlaznih karakteristika i tipova entropije. Analiza performansi izračunavanja entropije zasniva se na potrebnim memorijskim resursima zajedno sa potrebnim vremenom izvršenja. Osim toga, *Entropy Calculator* izvozi izračunate podatke kako bi oni mogli da se koriste za dalju obradu i analizu u ostalim modulima, poput modula za mašinsko učenje. Naime, svaki tok podataka se sastoji od nekoliko vrsta karakteristika, identifikacionih atributa i volumetrijskih atributa. Agregacija se vrši za svako jedinstveno pojavljivanje neke vrednosti

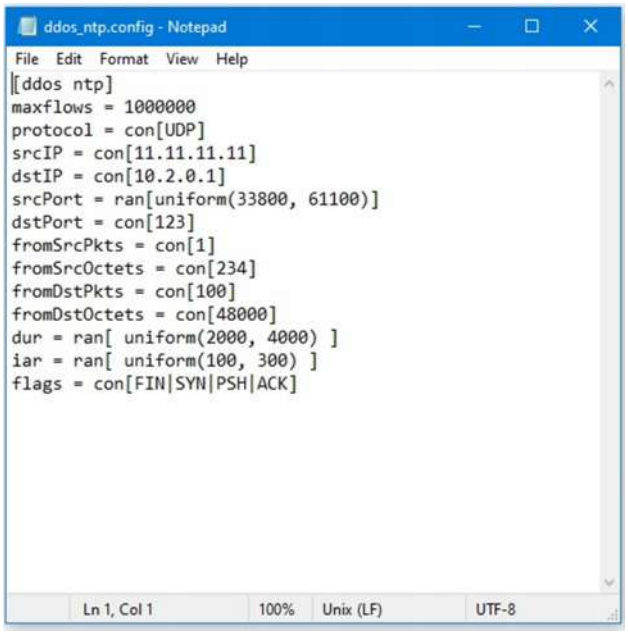
identifikacionih atributa, i to za određenu epohu, sumirajući volumetrijske podatke i računajući broj pojavljivanja vrednosti atributa ponašanja (*behavior attributes*). Za svaki atribut se proračunava entropija po epohama (zadati vremenski interval koji se uzima u obzir pri svakom prolasku). U kontekstu primene ovog alata, kroz dobijene rezultate je bitno da se uoče promene entropije izazvane anomalijama i da se na pravi način utvrdi njihova razlika u odnosu na redovne varijacije entropije. Kada je varijacija regularnih podataka manja, detekcija anomalija i napada je lakša, čak i u slučaju manje intenzivnih anomalija. U [184] je detaljno opisan rad sa podacima generisanim u okviru ove aplikacije. Na slici 6.6 je dat prikaz osnovnih prozora grafičkog korisničkog interfejsa *Entropy Calculator* aplikacije.



Slika 6.6 Grafički korisnički interfejs *Entropy Calculator* aplikacije

6.5 Softverski alat Flow Generator

Softver *Flow Generator (FG)* su razvili stručnjaci sa *Military Communication Institute C4I Systems' Department* i *AGH University of Science and Technology Department of Applied Computer Science* u Poljskoj, a kao glavni autor se navodi Berezinski [50]. *Flow Generator* je zasnovan na programskom jeziku Python i omogućava modeliranje različitih profila saobraćaja. Softver obuhvata različite modele sintetički generisanog saobraćaja uključujući DDoS (NTP, DNS, SYN), napad grubom silom, napad botovima, skeniranje portova i drugo. Na slici 6.7 je prikazan primer jednog konfiguracionog *Flow Generator* skripta koji se koristi za potrebe generisanja sintetičkih instanci mrežnog saobraćaja u slučaju napada.

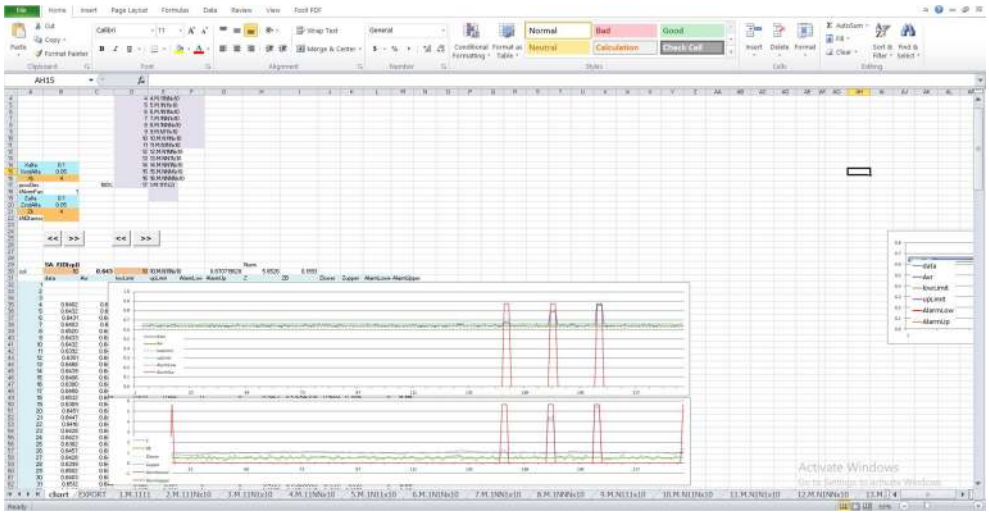


Slika 6.7 FG konfiguracioni skript za DDoS NTP napad [50]

U okviru teze je modeliranje zlonamernog saobraćaja zasnovano na primeni FG alata, koji je za potrebe istraživanja modifikovan tako da se obezbedi prilagodljivost formatu podataka.

6.6 Softverski alat Analyzer

Za potrebe sveobuhvatne analize entropijskih vrednosti u vremenu posebno je kreiran Excel fajl *Analyzer*.xlsm.



Slika 6.8 Prikaz rada *Analyzer* okruženja [140], [174]

Obuhvaćeni su podaci proračuna entropije, uključujući i standardnu devijaciju, na koje se primenjuje EMA tehnika i dobija margina prihvatljivih varijacija vrednosti entropije u vremenu. Ovaj alat je uneo sistematičnost u proces analize generisanih podataka, pri čemu na efikasan način vrši eksploataciju generisanih atributa dajući informaciju o karakterističnim parametrima. Na osnovu implementiranih različitih funkcionalnosti, ovo okruženje omogućava varijaciju pojedinih parametara i pragova koji se koriste prilikom analize distribucije entropije. Na slici 6.8 je dat prikaz primera generisanih rezultata analize u *Analyzer* okruženju.

6.7 Skupovi podataka korišćeni u istraživanju

Za potrebe analize performansi algoritama mašinskog učenja, kao i sveobuhvatnog predloženog rešenja detekcije napada i anomalija primenom kombinovanih tehnika detekcije, bilo je neophodno imati na raspolaganju adekvatne, slobodno dostupne skupove podataka koji obuhvataju savremene napade i njihove varijacije. Godinama unazad naučna zajednica je većinu svojih eksperimenata u ovoj oblasti zasnivala na korišćenju poznatog KDD99 skupa podataka i njegove poboljšane varijacije NLS-KDD [35], [93], [185]. Međutim, zastarelost instanci podataka, kao i napada koji su njima obuhvaćeni i izrazita nebalansiranost kada je u pitanju prisustvo instanci pojedinih napada, motivisalo je naučnu zajednicu da se posveti generisanju novih, modernih, sveobuhvatnih skupova podataka koji su dostupni za istraživački rad. Tokom istraživanja predstavljenog u ovoj tezi korišćeno je i dodatno modifikovano nekoliko slobodno dostupnih skupova podataka koji obiluju brojem instanci i različitim scenarijima napada i anomalija.

6.7.1 Skup podataka UNSW-NB15

UNSW-NB15 je moderan, označen skup podataka pogodan za rad u oblasti obrade podataka, kreiran u okviru *Cyber Range Lab* na Univerzitetu UNSW, Canberra, Australija [56], [95]. U pitanju je nebalansiran skup podataka koji svojim podacima obuhvata realno normalno ponašanje mrežnog saobraćaja u kombinaciji sa instancama kontrolisano sprovedenih savremenih napada. Zasnovan je na detaljnom pregledu korisnog dela paketa saobraćaja (*payload examination*), a oslanja se na 100 GB sirovog saobraćaja (*tcpdump pcap* datoteke) i paketa generisanih u *IXIA PerfectStorm* okruženju. Neobrađeni podaci se obrađuju pomoću *Argus Bro-IDS* alata, generišući 49 atributa, uključujući i oznaku klase. Ukupan saobraćaj se sastoji od 2.540.044 instanci, organizovanih sa 44 atributa, klasifikovanih u 7 grupa: *basic* (13), *content* (8), *time* (9), *additional features* (12), *attack category* (1) i *label* (1). Instance malicioznog mrežnog saobraćaja obuhvataju devet kategorija napada: *DoS*, *Fuzzers*, *Analysis*, *Backdoor*, *Shellcode*, *Worm*, *Exploits*, *Generic* i *Reconnaissance*.

6.7.2 Skup podataka CTU-13

CTU-13 je označen skup podataka zasnovan na *botnet* napadima, a obuhvata instance podataka koje pripadaju normalnom, pozadinskom i instancama *botnet* mrežnog saobraćaja. Obuhvata 13 podskupova instanci koje odgovaraju malver mrežnom saobraćaju, sakupljenih iz realnog mrežnog okruženja. Skup uključuje 7 *botnet* malvera, a ceo sadržaj skupa se zasniva na podacima o mrežnom saobraćaju ekstrahovanom u okviru *Malware Capture Facility* istraživačkog projekta, sa ciljem generisanja i dugoročnog praćenja aktivnosti *botnet* napada [57], [58]. Originalni skup podataka obuhvata oznake za: pozadinski mrežni saobraćaj, *botnet*, *command-and-control* kanale i instance normalnog saobraćaja. Pozadinski mrežni saobraćaj odgovara stvarnim događajima na mreži Češkog

tehničkog univerziteta, za koje se autori nisu oznakom odlučili da li su maliciozni ili ne. Instance se zasnivaju na 12 atributa i labeli, a dodatne modifikacije nad CTU-13 skupom podataka su primenjene kako bi se tokovi podataka pročistili od sitnih anomalija i da bi se ujednačile entropije, čime se omogućava da se jasnije istaknu sintetičke anomalije. Modifikacijom koja je primenjena za potrebe istraživanja ove teze je izvedeno nekoliko novih atributa, primenom posebnog procesa agregacije ključevima definisanim osnovnim atributima. S obzirom na to da je u pitanju blago nebalansiran skup, bila je neophodna posebna obrada podataka uz pažljiv izbor algoritama mašinskog učenja koji će se primenjivati tokom istraživanja. Glavno ograničenje u primeni skupa predstavlja neraščišćena priroda pozadinskog mrežnog saobraćaja, jer su autori naglasili da se saobraćaj sakupljao sa univerzitetskog rutera, međutim nisu date dovoljno detaljne informacije vezane za mrežnu topologiju i servise. Podaci ovog skupa su obrađeni kako bi se zadržali i koristili samo atributi koji se mogu dobiti putem NetFlow protokola. Dodatni atributi su posebno proračunati agregacijom i prebrojavanjem pojavljivanja tokom posmatrane epohe. Tako se, na primer, izračunava broj tokova u jednoj epohi koji imaju iste vrednosti pojedinih atributa (ključa agregacije).

6.7.3 Skup podataka CICIDS2017

Skup podataka CICIDS2017 je generisan kao deo istraživanja na kanadskom institutu za sajber sigurnost (*Canadian Institute for Cybersecurity*, CIC), na Univerzitetu New Brunswick. CICIDS2017 je savremen skup podataka, slobodno dostupan, zasnovan na dvosmernim tokovima mrežnog saobraćaja, svaki sa po 80 različitih atributa, a koji u velikoj meri reflektuju realnu prirodu stvarnog mrežnog saobraćaja uz realistične instance pozadinskog mrežnog saobraćaja [61].

CICIDS2017 je označen skup podataka sa modernim, ažuriranim skupom napada, koji pokriva niz uobičajenih scenarija napada, uključujući napade grubom silom, napade zasnovane na veb servisu, *botove*, napade skeniranjem, DoS/DDoS, *Heartbleed* i napade infiltracije. Ovaj skup emulira niz različitih ponašanja koja se oslanjaju na upotrebu HTTP, HTTPS (HTTP *Secure*), FTP (*File Transfer Protocol*), SSH (*Secure Shell*) i e-*mail* protokola. Predstavljen je kroz nekoliko delova, od kojih svaki čini saobraćaj sakupljen u različitim radnim danima, odnosno obuhvata 5 radnih dana (od ponedeljka do petka). Dok deo skupa koji se odnosi na sakupljene mrežne tokove tokom ponedeljka obuhvata samo normalan saobraćaj, ostali dani obuhvataju i instance koje se odnose na slučajeve različitih napada. Istraživanje predstavljeno u ovoj tezi koristi CICIIDS2017 kao jednu od okosnica evaluacije rešenja za kombinovanje tehnika entropije i mašinskog učenja u kontekstu detekcije napada i anomalija [174].

7. PREDLOŽENO REŠENJE

Korišćenje tokova mrežnog saobraćaja kao izvora podataka za sistem za detekciju napada i anomalija ima nekoliko osnovnih prednosti. Pre svega, u porastu je broj mrežnih napada (različiti oblici DDoS napada) koje nije moguće detektovati jednostavnom primenom *host*-orijentisanih sistema za detekciju napada, tako da je neophodno raspolagati podacima o dešavanjima na nivou mrežne infrastrukture. Osim toga, TCP/IP standardizacijom mrežnog saobraćaja je u velikoj meri olakšano prikupljanje, formatiranje i analiza različitih podataka heterogenih formata i intenziteta, a koji se sakupljaju sa različitih izvora u okviru posmatranog mrežnog okruženja.

Primenom metoda koje omogućavaju upotrebu korisnih informacija i sadržaja paketa koji se prenose mrežnom infrastrukturim, moguće je dobiti relevantne informacije na osnovu kojih bi se omogućila uspešna detekcija napada na pojedinačne korisnike. Međutim, nakon što se uspešno utvrdi da je došlo do napada, sam proces identifikacije napadača postaje značajno otežan jer ne postoji dovoljno informacija kojima bi se mogla povezati neka mrežna konekcija sa identitetom nekog određenog korisnika koji je učestvovao u napadu. Osim toga, u slučaju da paketi nose enkriptovan sadržaj praktično je nemoguće takav sadržaj analizirati jer su neophodni specijalizovani alati. Takođe, ako detektovani potpisi napada nisu dovoljno sveobuhvatni, moguće je da do detekcije neće ni doći jer napadači često dodatno usložnjavaju pakete koji se prenose.

U cilju pronalaženja što efikasnijeg sistema detekcije napada velika pažnja se posvećuje obimu, formatu i kvalitetu izlaznih informacija koje će se dalje koristiti za analizu. Teži se tome da sistem bude modularan kako bi se omogućila proširivost, skalabilnost, fleksibilnost i efikasnost u radu, pri čemu se u obzir uzimaju i memorijski zahtevi, potrošnja energije i propusni opseg koji sistem može da podrži u realnom vremenu.

Glavna motivacija za rad na razvoju nove metode detekcije napada i anomalija zasnovanoj na primeni nenadgledanog mašinskog učenja jeste ta da se predloži rešenje koje bi bilo primenljivo u realnim mrežnim uslovima i u realnom vremenu. Međutim, proces detekcije anomalija ili napada predstavlja samo jedan deo rešenja, dok njegova praktična implementacija zahteva planiranje i efikasnu implementaciju celog toka procesa, od procedura za prikupljanje podataka, tehnika koje se primenjuju za obradu sirovih podataka, do procesa analize, dobijanja rezultata i generisanja alarma. Rešenje izloženo u disertaciji polazi od osnovnog entropijski zasnovanog pristupa detekciji anomalija i napada, a zatim je usmereno na poboljšavanje efikasnosti razvojem i primenom skupa unapređenih algoritama nenadgledanog mašinskog učenja.

Osnovni doprinos ove disertacije je novi pristup u profilisanju i analizi ponašanja mrežnog saobraćaja i otkrivanja anomalija, zasnovan na primeni unapređenog algoritma hijerarhijskog aglomerativnog klasterovanja. Posebna pogodnost za praktičnu implementaciju je što se rešenje zasniva samo na osnovnim podacima koji se mogu prikupiti pomoću NetFlow protokola, na osnovu kojih se preračunavaju dodatni podaci.

Predloženi kombinovani pristup obuhvata primenu algoritama nenadgledanog mašinskog učenja nad podacima koji su prethodno obrađeni primenom entropijski zasnovanih metoda, a u cilju unapređivanja efikasnosti i preciznosti entropijski zasnovanog pristupa za potrebe detekcije napada i anomalija. Predloženo rešenje se zasniva na eksperimentalnoj analizi i validaciji dobijenih rezultata.

7.1 Struktura tokova podataka

Za potrebe istraživanja predstavljenog u ovoj disertaciji korišćeni su samo osnovni podaci koji se mogu dobiti primenom NetFlow protokola [34] a koji identifikuju komunikacione tokove (IP izvorišna adresa, IP odredišna adresa, broj izvorišnog porta, broj odredišnog porta, protokol). Ostale informacije se odnose na razmenjenu količinu mrežnog saobraćaja, zadatu u formi ukupnog broja paketa i bajtova.

Tokovi podataka se prilikom prikupljanja čuvaju kao jednosmerni zapisi, međutim, njihovom konverzijom u dvosmerni format dobija se više informacija o komunikacionim profilima. U dvosmernim tokovima, izvor toka podataka se naziva inicijatorom, dok je odredište toka zapravo element mreže koji odgovara na inicijalizaciju i podatke koji mu pristižu sa izvora. U ovoj analizi je primenjena taksonomija koja razlikuje dve vrste nominalnih atributa: (1) identifikacioni atributi i (2) volumetrijski atributi koji se koriste kao metrika voluminoznosti. Primenom algoritama nenadgledanog mašinskog učenja unapređen je entropijski zasnovan pristup detekciji napada i anomalija, koji se zasniva na arhitekturi i taksonomiji izloženim u [39], [177].

Na osnovu tako zadate taksonomije, instance tokova saobraćaja su predstavljene nizom atributa koji mogu biti kategorisani kao identifikacioni i volumetrijski (*volumetric*) atributi (Tabela 7.1). Konkretno, identifikacioni atributi su: izvorišna IP adresa (*S*), odredišna IP adresa (*D*), izvorišni port (*s*), odredišni port (*d*) i protokol (*p*) koji se primenjuje u kontekstu komunikacije. Volumetrijski atributi se određuju na osnovu obima razmenjenog saobraćaja, a tokovi saobraćaja obuhvataju: broj paketa koji su poslati sa izvora (*sP*) i odredišta (*dP*) i broj bajtova poslatih sa izvora (*sB*) i odredišta (*dB*). Volumetrijski atributi su izrazito korisni u slučaju kada se ispituju izražene, intenzivne anomalije i napadi, kao što je slučaj sa DDoS napadima, ali su neefikasni u slučaju potrebe za detekcijom anomalija koje se ne zasnivaju na razmeni velike količine podataka. U tom slučaju, predlog je rešenje koje podrazumeva praćenje strukture saobraćaja kroz tzv. *behaviour* atribute, odnosno atribute ponašanja.

Tabela 7.1 Taksonomija atributa tokova podataka

Naziv atributa	Tip atributa	Oznaka atributa
Izvorišna IP adresa (*Source IP address*)	Identifikacioni	S
Odredišna IP adresa (*Destination IP address*)	Identifikacioni	D
Izvorišni port (*Source Port*)	Identifikacioni	s
Odredišni port (*Destination Port*)	Identifikacioni	d
Protokol (*Protocol*)	Identifikacioni	P
Broj paketa sa izvora (*Source packet counts*)	Volumetrijski	sP
Broj paketa na odredištu (*Destination packet counts*)	Volumetrijski	dP
Broj bajtova sa izvora (Source bytes counts)	Volumetrijski	sB
Broj bajtova na odredištu (*Destination bytes counts*)	Volumetrijski	dB

U cilju primene algoritama nenadgledanog mašinskog učenja, korišćeni su podaci koji su prethodno primenjeni u okviru osnovnog entropijski zasnovanog pristupa detekciji anomalija [39]. Podaci dobijeni na osnovu tog inicijalnog pristupa se dalje smatraju pretprocesiranim instancama tokova mrežnog saobraćaja. U ovom istraživanju se polazi od pretpostavke da je za dobijanje detalja

vezanih za mrežne aktivnosti potrebno primeniti postupak agregacije vrednosti podataka po tokovima u određenim intervalima vremena, a zatim brojanje jedinstvenih pojavljivanja vrednosti ostalih atributa.

U analizi mrežnog saobraćaja entropija se smatra merom varijanse profila mrežnog saobraćaja, tako da varijacije entropije predstavljaju pouzdan pokazatelj prisustva anomalije. Proračunom entropije dobija se mera koja odražava ujednačenost raspodele vrednosti određenog atributa u određenom vremenskom intervalu. Time se prati stanje raspodele vrednosti određenog atributa u okviru instanci podataka u vremenu, tako što se primenjuje postupak agregacije po pojedinim atributima i sumiraju odnosno broje pojavljivanja ostalih atributa u tom vremenskom intervalu. Na taj način se za svaki posmatrani atribut dobija vremenska serija podataka gde svaka vrednost odgovara proračunatoj entropiji u jednoj epohi.

Ovim postupkom se dobijaju vremenske serije različitih atributa, koje se zatim objedinjeno posmatraju i analiziraju. Tokom analize se prate značajna odstupanja od prihvatljivih varijacija, odnosno utvrđenih vrednosti pragova (*threshold*).

Upotreba isključivo entropijskih metoda za detekciju napada u nekim situacijama može da bude izuzetno efikasna, međutim pokazuje se da je nedovoljno precizna. Rešenje predloženo u disertaciji podrazumeva da se entropijski zasnovane metode koriste kao početna instanca rešenja za detekciju napada, čijim bi se unapređivanjem primenom odgovarajućih algoritama mašinskog učenja obezbedio efikasniji, precizniji i skalabilniji sistem detekcije anomalija i napada. Istraživanjem su obuhvaćena dva pristupa.

Prvi pristup se zasniva na analizi rezultata dobijenih na osnovu entropijski zasnovanog pristupa, a zatim primenom EM algoritma klasterovanja. Eksperimentalno dobijeni rezultati i analiza su predstavljeni u [140]. Algoritam EM je opisan u odeljku 4.6, dok su naučno-istraživački doprinosi i ostvareni rezultati predstavljeni u odeljku 7.3.

Istraživanje je zatim značajno unapređeno proračunom novih atributa na nivou svakog komunikacionog toka, a koji se kasnije uzimaju kao opis komunikacionog ponašanja, što se profiliše primenom posebno modifikovanog algoritma hijerarhijskog aglomerativnog klasterovanja, a čiji je detaljan opis dat u odeljku 4.7, dok su ostvareni naučno-istraživački doprinosi i rezultati predstavljeni u odeljku 7.4.

Metode klasterovanja se često kombinuju sa tehnikama izbora atributa, dok se uklanjanjem redudantnih atributa (u smislu da neki atributi imaju jednak uticaj na opšte performanse sistema, te se eliminacijom jednog od njih ne gubi na performansama a dobija se na smanjenju složenosti postupka) povećava efikasnost i tačnost. U slučaju istraživanja predstavljenog u ovoj disertaciji, izbor atributa zavisi od rezultata dobijenih proračunom entropije, svodeći skup atributa na podskupove najreprezentativnijih za primenu u odabranom algoritmu mašinskog učenja.

Osnovne faze istraživanja i razvoja kombinovanih metoda proračuna entropije i mašinskog učenja su bile sledeće:

- Inicijalno utvrđivanje karakteristika skupa podataka određenog za analizu.
- Čišćenje skupa podataka i obeležavanje prethodno neobeleženih anomalija koje su uočljive manuelnim pregledom.
- Fragmentacija dugačkih tokova saobraćaja.

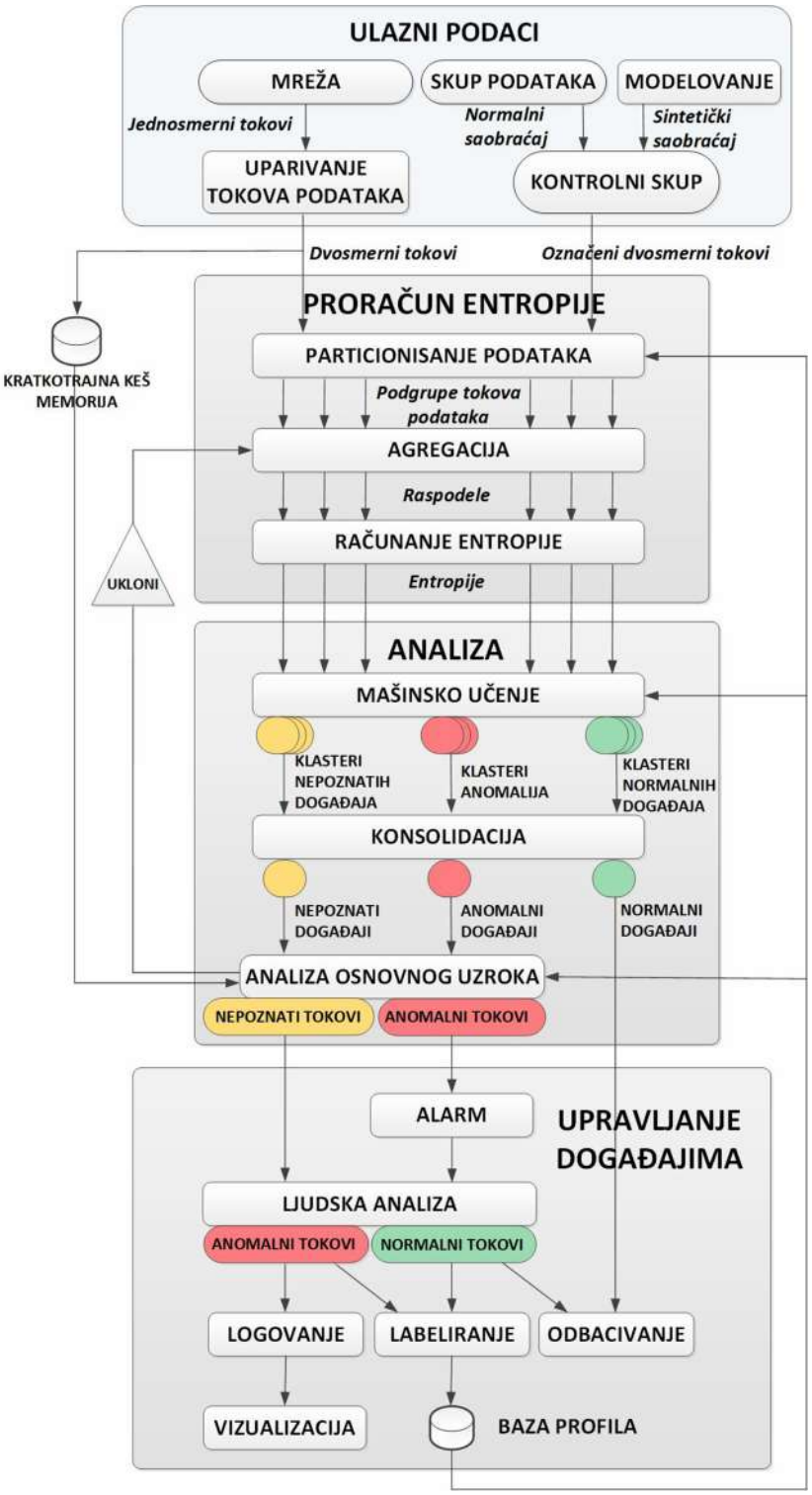
- Proširivanje skupa podataka sintetičkim tokovima mrežnog saobraćaja koji su generisani u skladu sa analiziranim modelom mrežnog saobraćaja.
- Otkrivanje anomalija zasnovano na proračunu vrednosti entropije različitih atributa instanci mrežnog saobraćaja.
- Utvrđivanje zavisnosti ili nezavisnosti primenjene tehnike mašinskog učenja od multiplikativnog parametra *k*.
- Klasterovanje modifikovanog skupa podataka u određeni broj klastera primenom EM metode nenadgledanog mašinskog učenja.
- Klasterovanje modifikovanog skupa podataka u algoritamski zavisan broj klastera primenom hijerarhijskog aglomerativnog algoritma nenadgledanog mašinskog učenja.

Unapređene tehnike mašinskog učenja, koje predstavljaju naučno-istraživački doprinos rešenja predloženog u disertaciji, primenjuju se u okruženju šireg sistema koji funkcionalno obuhvata nekoliko osnovnih modula među kojima je i deo za primenu algoritama mašinskog učenja. Kompletna arhitektura je deo šireg istraživanja, predstavljenog u [39], [177].

Osnovni delovi tako osmišljene arhitekture su: (1) blok za uparivanje tokova podataka; (2) kontrolni skup; (3) blok za particionisanje instanci podataka; (4) blok za agregaciju podataka; (5) blok za proračun entropije; (6) blok za mašinsko učenje; (7) blok za konsolidaciju podataka; (8) blok za *root cause* analizu; (9) blok za ekspertsku (ljudsku) analizu; (10) blok za generisanje baze profila mrežnog saobraćaja i (11) blok kojim se implementira mehanizam za samoobučavanje (slika 7.1).

Podaci koji se koriste u okviru dela koji se odnosi na implementaciju algoritama mašinskog učenja su u formi dvosmernih instanci tokova mrežnog saobraćaja, pružajući dodatne informacije i veću tačnost detekcije u odnosu na jednosmerne tokove. Inicijalni skup podataka je kombinovan sa instancama legitimnog mrežnog saobraćaja i sa sintetički generisanim tokovima podataka kojima se simuliraju određene anomalije različitih intenziteta. Particionisanjem instanci podataka omogućeno je razdvajanje različitih dvosmernih tokova podataka u niz podgrupa koje dele slične karakteristike, kao što su protokol ili usluga, čime se dobija na većoj osetljivosti u procesu detekcije anomalija i napada. Proces agregacije se primenjuje na dvosmerne instance podataka, particionisane u određenim vremenskim intervalima, takozvanim epohama. Kao rezultat, ovaj proces će kreirati distribucije vrednosti atributa sa izbrojanim vrednostima po agregiranom atributu, sortirano naniže.

Modul za izračunavanje entropije, za svaki atribut instanci podataka, za svaku epohu, upravlja izračunavanjem relativnog doprinosa određenog atributa, što rezultira jednim brojem koji predstavlja stopu sličnosti i razlike vrednosti entropije atributa. Rezultati dobijeni kao izlaz iz ovog bloka su u formi vremenske serije entropije za svaki razmatrani atribut i predstavljaju ulazne podatke za dalju obradu primenom algoritama mašinskog učenja.



Slika 7.1 Arhitektura sistema za detekciju anomalija zasnovana na tokovima podataka [177]

Blok mašinskog učenja implementira neki od navedenih algoritama za nenadgledano mašinsko učenje, a u ovom istraživanju to su EM algoritam i hijerarhijski aglomerativni algoritam za

klasterovanje. U mrežama sa realnim saobraćajem, otkrivanje anomalija je proces koje se odvija u realnom vremenu, gde su u opštem slučaju podaci o vrednostima atributa već klasterovani za sve prošle epohe, a dodatno klasterovanje se izvršava samo u trenutnoj epohi. U procesu primene aglomerativnog algoritma klasterovanja arhitektura je modifikovana, a posebnom procedurom se vrši izračunavanje dodatnih atributa čije se vrednosti zatim dodaju tokovima analiziranog saobraćaja. Blok za konsolidaciju obavlja analizu rezultata nakon primenjenog algoritma mašinskog učenja i donosi odluku o tome kako da tretira mrežni saobraćaj u trenutno posmatranoj epohi.

7.2 Taksonomija komunikacionih modela

Većina analiziranih tokova saobraćaja odgovara modelu klijent-server (*client-server*), koji osim legitimnih, koriste i zlonamerni korisnici. U tabeli 7.2 je predstavljena taksonomija komunikacionih modela koja se koristila u okviru istraživanja. Detaljan prikaz i teorijske osnove taksonomije su izloženi u [39], [177]. Navedena taksonomija je deo šireg istraživanja (program EUREKA), a inicijalno je predložena i korišćena za potrebe analize entropijski zasnovanih metoda detekcije napada i anomalija. Komunikacioni modeli su zadati na osnovu vrednosti specifičnih identifikacionih atributa (izvorišna IP adresa - *S*, izvorišni port - *s*, odredišna IP adresa - *D* i odredišni port – *d*), proračunatih u fazi primene entropijskih metoda.

Različiti obrasci ponašanja mrežnog saobraćaja se mogu opisati specifičnim komunikacionim obrascima koji su definisani na osnovu skupa informacionih atributa. Na osnovu broja izvorišnih i odredišnih IP adresa i portova je definisana teorijska taksonomija kojom je opisano 16 različitih modela komunikacije (Tabela 7.2), gde se oznaka „1" odnosi na jedinstvenu vrednost nekog atributa, a oznaka „N" se odnosi na veći broj različitih vrednosti posmatranog atributa [39], [177].

Tabela 7.2 Taksonomija komunikacionog modela

S	s	D	d	Modeli komunikacije
1	1	1	1	Single flow
1	1	1	N	DoS amplification, Port Scan
1	1	N	1	Network Scan
1	1	N	N	ICMP flooding
1	N	1	1	Dictionary attack
1	N	1	N	Port Scan
1	N	N	1	Network Scan
1	N	N	N	Diagonal Scan
N	1	1	1	Amplification DDoS (DNS)
N	1	1	N	Amplification DDoS (NTP)
N	1	N	1	Multiple Network scan
N	1	N	N	Multiple Diagonal scan
N	N	1	1	SYN flooding
N	N	1	N	DDoS
N	N	N	1	Multiple Amplification DDoS
N	N	N	N	Multiple DDoS

Model 1N-N1 označava mrežno skeniranje iz jednog izvora koristeći nasumičan broj izvorišnih portova i komunikaciju sa više odredišnih adresa koristeći jedan specifičan odredišni port.

Ipak, ovako definisani komunikacioni modeli ne karakterišu obavezno neki napad, već se taksonomija modela može uklopiti i za potrebe analize redovnog, normalnog saobraćaja. Na primer, funkcionisanje pružanja usluge jednog veb servera se može okarakterisati modelom NN-11. Rad DNS servera se uklapa u NN-11 model u slučaju kada opslužuje pojedinačne klijente, dok mu u slučaju kada zahteva aktivnost drugih DNS servera odgovara 1N-N1 model. Upravo zbog toga postoji izvestan prostor gde još uvek nisu u dovoljnoj meri rešeni problemi razlikovanja malicioznih od legitimnih korisnika, a razlog je najčešće mali intenzitet, obim i mala dinamika pojedinih oblika zlonamernih aktivnosti.

Tehnike skeniranja se najčešće primenjuju kao uvod u druge, invazivnije, sofisticiranije oblike napada, a obično se primenjuju pre distribuiranih DoS (DDoS) napada. Ove zlonamerne aktivnosti u potrazi za ranjivostima prikupljaju informacije vezane za mrežnu infrastrukturu i konfiguraciju uređaja, čime pripremaju teren za primenu značajno invazivnijih napada.

Vertikalna skeniranja se modeluju 1N-1N i 11-1N modelom, a odnose se na skeniranje portova, gde je fokus na ispitivanju portova i protokola koje koristi određena žrtva (jedna odredišna IP adresa) [111]. Skeniranje portova se obično zasniva na korišćenju TCP i UDP portova, sa namerom dobijanja odgovarajućeg odgovora sa strane aktivnog hosta u mreži koji bi ukazao na otvorene portove, odnosno usluge koje nudi.

Horizontalno ili mrežno skeniranje se modeluje 1N-N1 i 11-N1 modelom, a proteže se na niz odredišnih hostova kako bi se prikupile informacije u vezi sa konfiguracijom, skladištenjem i operativnim sistemom. Prisustvo mrežnog skeniranja se može primetiti tako što se povećava broj uspostavljenih konekcija od jedne ili više izvorišnih IP adresa prema više destinacija, dok je generisani saobraćaj prilično malog obima i intenziteta u poređenju sa saobraćajem legitimnih korisnika.

Cilj **DoS napada** je da se onesposobe određeni servisi ili mrežni resursi, tako što će žrtva biti zatrpana velikim brojem suvišnih zahteva korišćenjem više izvora (DDoS) [105] i slanjem velikog obima mrežnog saobraćaja na jedno odredište. DDoS napad se modeluje N1-11 i N1-1N modelima komunikacije. Uobičajeni oblici DDoS napada se generišu primenom TCP, UDP i ICMP instanci saobraćaja, pri čemu su najpopularniji oblici ovog napada: UDP flood, ICMP Ping flood, SYN flood, NTP i DNS sa pojačanjem [30], [186].

ICMP flood napad se odvija po modelu 11-NN, pri čemu napadač šalje veliki broj ICMP *Echo Request* paketa, na koje bi kao rezultat odredišni uređaj trebalo da odgovori sa velikim brojem *ICMP Echo Reply* paketa. Na taj način se indirektno uzrokuje opterećenje i na kraju zasićenje dostupnog propusnog opsega odredišnog uređaja.

TCP-SYN flooding je oblik napada koji se može modelovati NN-11 modelom iz predstavljene taksonomije, a osnovni cilj ovog napada je zloupotreba ranjivosti mrežnog protokola, odnosno otežano uspostavljanje tokova podataka. Jedan od karakterističnih primera ove vrste napada je beskonačna *three-way* TCP procedura za uspostavljanje konekcije, koja dejstvom ovog napada ostavlja veliki broj konekcija neuspostavljenim, čime se u značajnoj meri troše dostupni resursi [187].

U napadu **DNS amplifikacije** napadač postavlja DNS zahteve na način kojim se značajno povećava obim odgovora, obično zahtevajući sve informacije iz datoteke domenske zone, pritom

koristeći lažnu izvorišnu IP adresu hosta koji je određen da bude žrtva napada. Tako zahtev od 10 bajtova može da generiše 50 puta veći odgovor i pošalje ga žrtvi napada [188].

Napad rečnikom (*Dictionary Attack*) izbegava isprobavanje svih mogućih kombinacija kredencijala, već se oslanja na listu kombinacija lozinki iz određenog rečnika [189]. Slično redovnom saobraćaju, ovaj napad može da se modeluje u skladu sa 1N-11 modelom.

Za potrebe proračuna entropije po atributima tokova podataka mrežnog saobraćaja primenjena je posebno razvijena aplikacija *Entropy Calculator* [136], [177]. Ulazne podatke čine instance tokova podataka, pri čemu se svaka sastoji od identifikacionih i volumetrijskih atributa. Aplikacija će za svaku epohu agregirati po svakom jedinstvenom pojavljivanju identifikacionih podataka, čime se dobija distribucija vrednosti atributa ponašanja, koja za svaki agregacioni ključ sadrži broj različitih elemenata posmatranog atributa. Entropija se zatim izračunava nad ovim skupom vrednosti čime se dobija vrednost entropije za svaki atribut ponašanja. Važno je uočiti promene entropije izazvane anomalijama i razlikovati ih od varijacija entropije izazvanih regularnim saobraćajem. Kada je varijacija regularnog saobraćaja mala, tada je i detekcija anomalija lakša, čak i u slučaju manje intenzivnih anomalija.

U postupku detekcije promene vrednosti vremenskih serija entropija podataka postoje dva osnovna pristupa: (1) metoda kliznih vremenskih prozora, kojima se izračunavaju maksimum i minimum vrednosti u n prethodnih epoha, čime se dobija informacija o varijaciji entropije u vremenu; i (2) procena odstupanja predviđene srednje vrednosti entropije i njene standardne devijacije u vremenu (*baselining*), najčešće primenom metode predikcije eksponencijalnog pomeranja usrednjenih vrednosti (EMA). U oba slučaja margina varijacije entropije proširuje se primenom multiplikativnog faktora k kojim se množi standardna devijacija radi dobijanja optimalnog opsega prihvatljivih vrednosti i daje takozvanu marginu tolerancije (*margin of tolerance*). Osnovni detalji vezani za EMA tehniku se mogu pronaći u [175]. Sve vrednosti koje se nalaze van margine tolerancije (ispod ili iznad) se mogu smatrati anomalijama i izazvaće generisanje alarma. U disertaciji je za proračun entropije korišćena Šenonova metoda, koja je detaljno opisana u odeljku 5.1.

Kako bi se bolje okarakterisala devijacija vrednosti entropije, u istraživanju predstavljenom u disertaciji korišćene su vrednosti entropije (osnovne i normalizovane) u odnosu na granicu tolerancije, čime je omogućena direktnija analiza entropije, bez obzira na njene apsolutne vrednosti. Izloženi pristup i rešenje se mogu primeniti i na parametrizovane oblike entropije.

Jednostavno i brzo izračunavanje entropije u svakoj epohi čini ovaj pristup primenljivim u savremenim mrežama u realnom vremenu, ali nekoliko nedostataka ograničava njegovu upotrebu. Prvo, entropijski zasnovana detekcija je izuzetno osetljiva na podešavanje margine faktorom k, tako da i mala promena margine može da unese velike promene u rezultatima. Potrebno je da se margina tolerancije fino podesi tako da najbolje odgovara profilu mrežnog saobraćaja i njegovim varijacijama. Taj postupak se izvodi podešavanjem faktora množenja k, a eksperimentalni deo istraživanja predstavljen u disertaciji pokazuje da faktor množenja koji ima vrednost jednaku 4 daje najbolje rezultate, precizno hvatajući anomalije i uspešno eliminišući većinu FP alarma. Međutim, dostupna literatura ukazuje na to da su u nekim istraživanjima postignute optimalne performance podešavanjem k na vrednost 2 [190]. Drugi nedostatak se odnosi na isuviše oštar prelaz i automatsko aktiviranje alarma za sve vrednosti entropije koje se nalaze izvan granice tolerancije, bez obzira na njihovu udaljenost i apsolutne vrednosti.

7.3 Primena Expectation-Maximization klasterovanja

U ovom delu istraživanja, za potrebe detekcije napada i anomalija primenom metoda mašinskog učenja primenjen je algoritam *Expectation-Maximization*, kojim se klasteruju vrednosti entropije i izdvajaju odstupanja. Na osnovu tako dobijenih rezultata je izvršeno poređenje sa rezultatima dobijenim primenom klasičnog pristupa detekciji napada i anomalija koji se zasniva na određivanju margine tolerancije putem proračuna EMA entropije i standardne devijacije.

7.3.1 Karakteristike skupa podataka

Za potrebe ovog dela istraživanja korišćen je skup podataka CTU-13. Originalne instance skupa podataka CTU-13 su predstavljene kroz 13 atributa (12 atributa i labela). Glavno ograničenje se odnosi na pozadinski saobraćaj, jer ne postoji dovoljno informacija o topologiji mreže i uslugama, čime je unesena neizvesnost toga da li se radi o normalnom ili anomalnom ponašanju. Glavne modifikacije se mogu opisati na sledeći način.

- Čišćenje skupa podataka od instanci sa nepotpunim ili nedostajućim podacima i čuvanje samo IPv4 podataka sa UDP, TCP i ICMP protokolima.
- Iscrpno uređivanje instanci pozadinskog saobraćaja, sa fokusom na nekategorisane instance saobraćaja, koje nisu označene kao instance malicioznog ili normalnog mrežnog saobraćaja. Neke manje, ali prepoznatljive anomalije su označene pomoću ručne analize.
- U cilju skraćivanja dugačkih tokova podataka, primenjen je proces fragmentacije tokova na epohe u trajanju od 60 sekundi.

Skup podataka korišćen u ovom delu istraživanja sastoji se od 72% UDP, 26% TCP i 2% ICMP tokova saobraćaja, koji uglavnom pripadaju DNS servisu, dok 20% saobraćaja pripada HTTP/HTTPS servisima. Ovaj modifikovani skup podataka ima stabilnu strukturu saobraćaja, bez ikakvih značajnijih odstupanja tokom vremena.

7.3.2 Generisanje tokova saobraćaja

Modifikovani skup podataka je zatim proširen sintetički generisanim tokovima anomalija u zavisnosti od modela (modeli komunikacije definisani u taksonomiji). Simulirane instance sintetički generisanih napada su zatim modifikovane u skladu sa formatom podataka zadatim za potrebe ovog istraživanja.

Modelovanje malicioznog saobraćaja (napada i anomalija) je zasnovano na primeni *Flow Generator* aplikacije, koja je za potrebe ovog istraživanja dodatno izmenjena kako bi se omogućilo prilagođavanje formatu modifikovanog skupa podataka. Uveden je mrežni saobraćaj blagog intenziteta sa 10 tokova po epohi, uz postepeno povećanje intenziteta uvođenjem 25, 50, 100, 200, 500 i 5000 tokova po epohi. Namerno su generisane povremene sitne, nasumične varijacije kako bi se doprinelo realističnijim karakteristikama instanci podataka. Poslednja pojava anomalnog saobraćaja je izuzetno intenzivna, sa namerom da se ukaže na nivo imuniteta na anomalije određenih osobina. Sintetički tokovi anomalija su odvojeno unešeni u skup podataka regularnog saobraćaja, tako da se prvi deo anomalija unosi počev od 60. epohe, sa serijom od 3 epohe, i zatim sa povećanjem intenziteta na svakih 20 epoha.

Eksperimentalna analiza primenom algoritama mašinskog učenja je izvedena u WEKA

okruženju. Važno je naglasiti da boje i pozicije dobijenog klastera (prikaz dobijenih rezultata) nisu uvek uparene, jer WEKA nasumično dodeljuje boje klasterima, tako da to može da ostavlja utisak permutacija. Efikasnost predstavljene metodologije je potvrđena na različitim podskupovima podataka, ciljajući na specifične karakteristike profila ponašanja, a koje dalje služe za bolja podešavanja algoritma mašinskog učenja. Evaluacija ovako postavljenog rešenja podrazumeva procenu pristupa na osnovu nekoliko specifičnih scenarija iz modifikovanih CTU-13 NetFlow podataka:

1. analiza neuobičajenog, malicioznog ponašanja,
2. analiza *botnet* napada,
3. analiza realnog mrežnog saobraćaja.

Važno je da se napomene da u slučaju realnog mrežnog saobraćaja veliki broj napada započinje mnogo ranije u vidu manje intenzivnih napada koji svojim prisustvom ne ometaju uobičajeni rad mreže. Na taj način se prikupljaju informacije o trenutnoj situaciji, karakteristikama ponašanja saobraćaja, konfiguraciji mrežnih resursa i pronalaze ranjivosti mreže i okruženja koje se zatim mogu zloupotrebiti nekim sledećim, značajno intenzivnijim napadima.

Za potrebe evaluacije predloženog IDS rešenja primenjeno je nekoliko oblika ovih komunikacionih profila. Rezultati dobijeni za različite vrednosti faktora k ukazuju na zanemarljivu zavisnost rezultata dobijenih primenom algoritma klasterovanja od vrednosti parametra k, tako da su u disertaciji predstavljeni rezultati za slučaj kada je vrednost k jednaka 4.

Za potrebe istraživanja predstavljenog u ovoj disertaciji, u mnogim razmatranim slučajevima predobrade podataka bilo je potrebe da se porede raspodele entropije podataka i normalizovane raspodele entropije. Vrednosti entropije su skalirane u odnosu na marginu, tako da se margina ($k \cdot \sigma$) skalira u opseg od 0 do 1 (gde je σ standardna devijacija). Takav pristup je obezbedio da svi analizirani atributi podjednako doprinose rezultatu. Normalizacija je tehnika skaliranja zasnovana na principu *Min-Max*, a koja podrazumeva da se opseg vrednosti koje uzima neka promenljiva skaliranjem svodi na opseg između 0 i 1.

U okviru predstavljene analize razmatrane su performanse ostvarive primenom metode klasterovanja i upoređene sa rezultatima ostvarenim primenom proračuna entropije i normalizovane entropije, i to za različite vrednosti faktora k. Eksperimenti su izvedeni za različit broj potencijalnih klastera, pri čemu su prikazani samo relevantni rezultati.

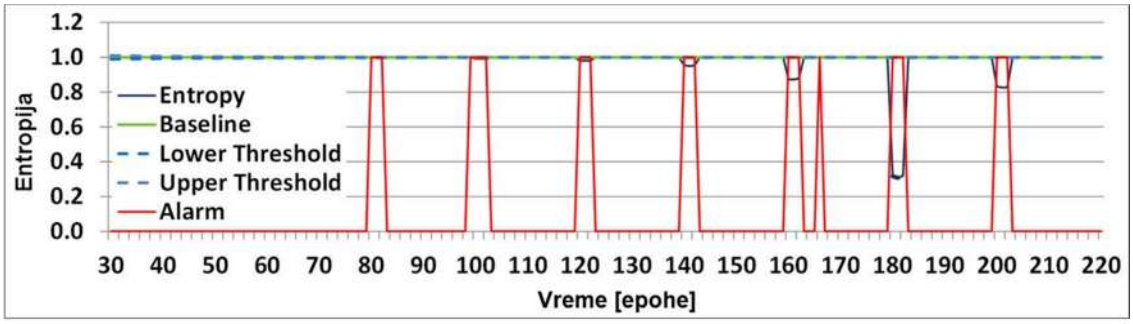
Rezultati su dati u grafičkom obliku, gde je na x osi predstavljeno vreme, zadato u epohama, dok y osa predstavlja vrednost entropije ili normalizovane entropije. Da bi dobijeni rezultati bili što jasniji i čitljiviji u nekim od prikaza rezultata su prilikom grafičkog predstavljanja zanemarene epohe koje nemaju rezultate koji su od važnosti. Klasterovanje je obavljeno nad velikim brojem atributa, međutim samo neki su bili relevantni za dobijanje konkretnijih rezultata i zaključaka. U nastavku poglavlja su predstavljeni rezultati dobijeni primenom algoritma EM nad grupom relevantnih atributa i vrednošću faktora $k = 4$.

7.3.3 Eksperimentalni rezultati analize sintetički generisanog sobraćaja

Jedan od najčešćih tipova mrežnog napada odgovara različitim varijacijama DDoS napada, kojim se sledi model koji podrazumeva da više izvorišnih IP adresa generiše i šalje pakete kojima preplavljuje jednu specifičnu odredišnu IP adresu. Iz definisane taksonomije modela komunikacije, DDoS se može povezati sa modelima N1-11, N1-1N, NN-11 i NN-1N.

Sa druge strane, u slučaju 1N-1N modela, koji odgovara napadima skeniranjem portova sa jedne adrese, napadač uglavnom zasniva svoju aktivnost na kontinuiranom testiranju dostupnosti i odziva odredišnih portova ciljane IP adrese odredišta. Kako bi ostali nevidljivi sistemima detekcije, ovi napadi se oslanjaju na slanje izuzetno malih količina podataka.

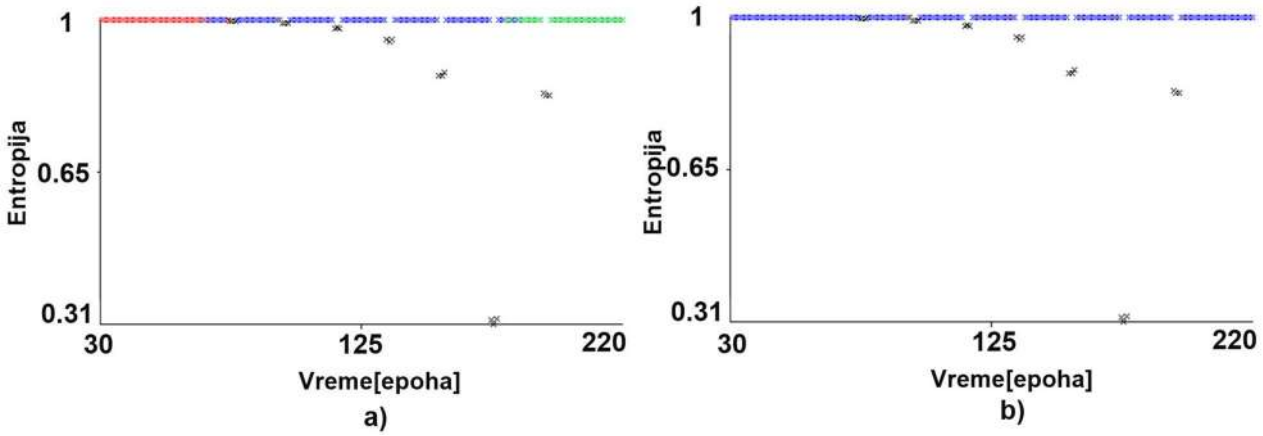
Na slici 7.2 je predstavljena vrednost entropije u slučaju odredišnog porta (atribut koji se razmatra) u slučaju kada je agregacija ostvarena na osnovu kombinovanog ključa sa izvorišnom i odredišnom IP adresom, *d*[*S.D*]. Primećuje se da je algoritam detektovao FP alarm u 166. epohi. Do ove pogrešne detekcije dolazi usled neprilagođenosti margina, odnosno margine standardne devijacije su uske.



Slika 7.2 1N-1N: vrednost entropije, *d*[*S.D*]

Sa druge strane, u slučaju normalizovane vrednosti entropije za ovako definisan atribut, ovaj FP alarm ne bi bio detektovan. Prilikom primene algoritma klasterovanja, za slučaj kada se generiše 4, 3 i 2 klastera, očigledno je da algoritam lako grupiše instance bez generisanja greške detekcijom ovog FP alarma. Na slikama 7.3(a) i (b) su predstavljeni rezultati za 4 i za 2 generisana klastera, respektivno.

U oba slučaja postoji jasna razlika između klastera anomalnog i normalnog saobraćaja, dok za slučaj 4 klastera algoritam dekomponuje i normalan saobraćaj u dva klastera normalnog, ali po karakteristikama međusobno različitog saobraćaja.

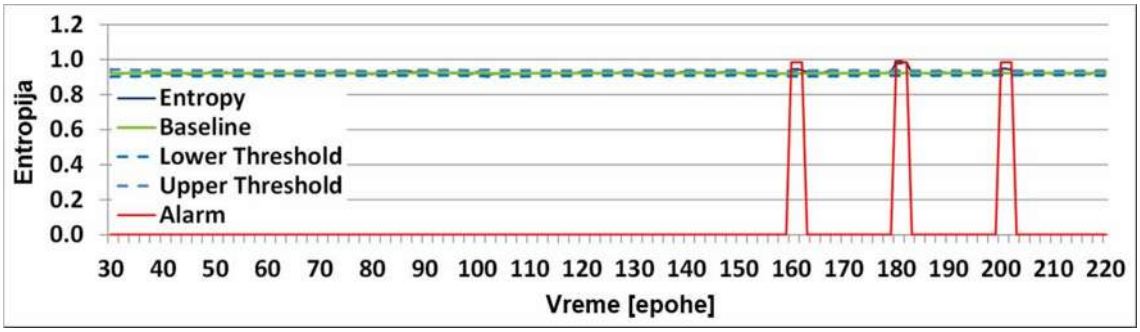


Slika 7.3 1N-1N: rezultati klasterovanja (*d*[*S.D*]), za slučajeve 4 i 2 generisana klastera

Jednostavnim, čisto entropijskim pristupom nije moguće zaobići pojavu FP alarma, međutim

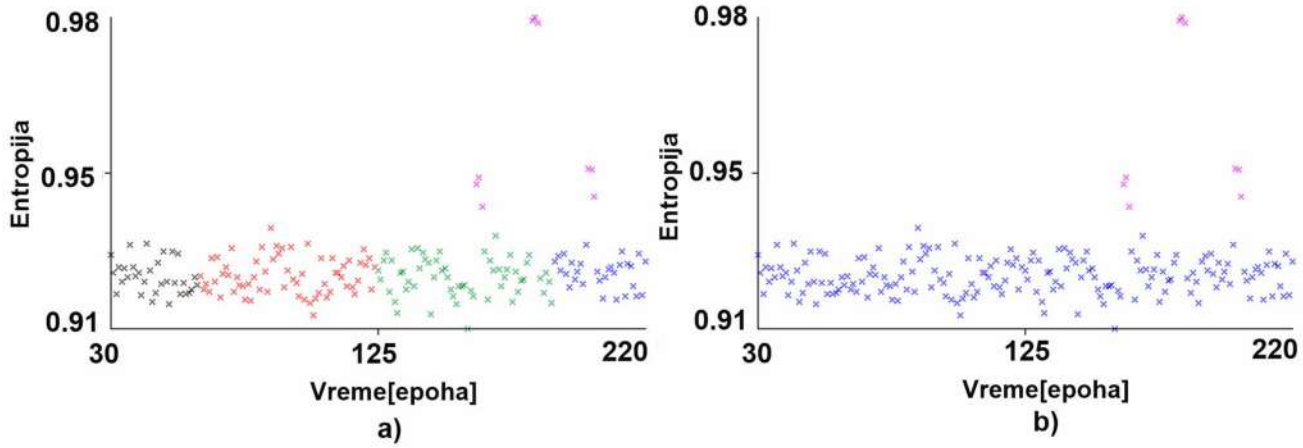
performanse se mogu poboljšati uvođenjem normalizacije entropije. U ovom slučaju, osim ispravne detekcije tačaka, algoritam klasterovanja ima jednake performanse nezavisno od vrednosti *k* parametra.

Daljom analizom rezultati su ukazali na primer detekcije anomalija malog intenziteta, pri čemu su analizirani podaci vezani za IP odredišnu adresu kada je agregirana pomoću kombinacije izvorišne IP adrese i odredišnog porta, *D*[*S.d*].



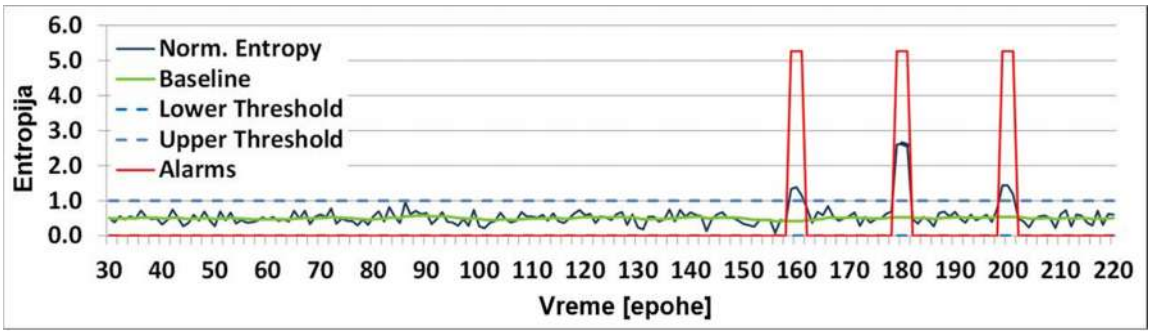
Slika 7.4 1N-1N: vrednost entropije, *D*[*S.d*]

Na slici 7.4 je predstavljena entropija za atribut *D*[*S.d*], a kojom su obuhvaćene tri grupe napada. Primenom dinamičkog klasterovanja podataka dobijenih proračunom vrednosti entropije za ovaj atribut, kao rezultat se dobija 5 klastera koji uspešno izoluju te tri grupe anomalija u jedan poseban klaster (slika 7.5(a)). Iako u nekim slučajevima klasterovanja sa 2 definisana klastera rezultat neće u potpunosti korektno da obavi odvajanje instanci po klasterima, u ovom slučaju algoritam je ispravno uradio klasterovanje i izdvojio instance napada u klaster sa anomalijama (slika 7.5(b)). Ostali deo instanci, koje pripadaju normalnom saobraćaju su uspešno klasterovane u klaster normalnog saobraćaja.



Slika 7.5 1N-1N: rezultati klasterovanja (*D*[*S.d*]), za slučaj generisanja 5 i 2 klastera

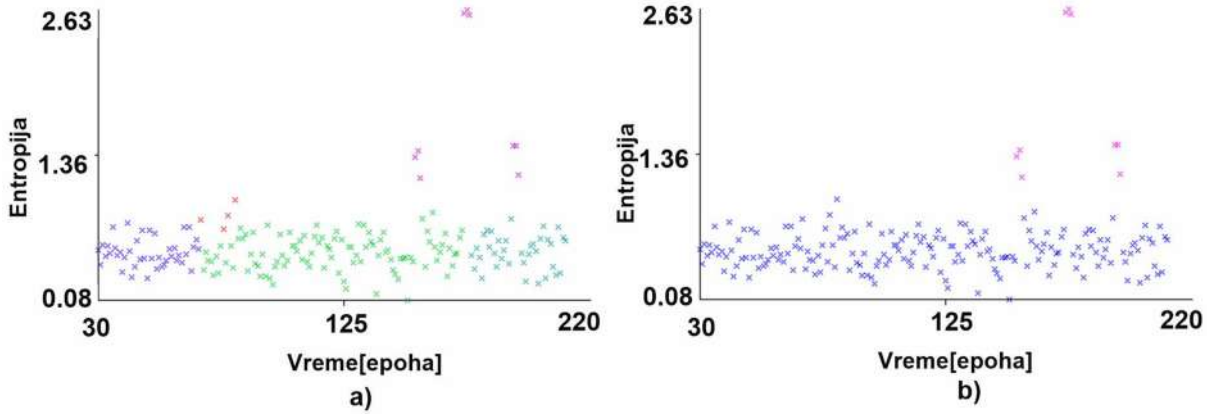
Slika 7.6 daje prikaz normalizovane entropije u slučaju kada je odredišna IP adresa agregirana dvočlanim ključem dobijenim kombinovanjem izvorišne IP adrese i odredišnog porta (1N-1N, D[*S.d*]).



Slika 7.6 1N-1N: normalizovana vrednost entropije, $D[S.d]$

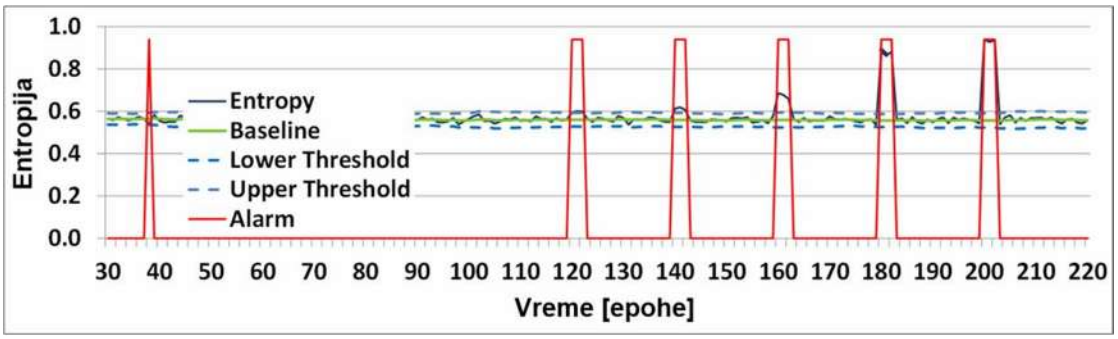
Kada se primenjuje dinamičko grupisanje za tako normalizovanu vrednost entropije, algoritam generiše 5 klastera, odnosno 4 koji obuhvataju instance normalnog saobraćaja (ali sa malo drugačijom preraspodelom u klasterima u odnosu na slučaj entropije) i jedan klaster koji savršeno izoluje anomalije.

Rezultati eksperimenta su pokazali da je obezbeđena potpuna izolacija anomalija u jedan klaster, i to već u slučaju kada se generišu samo 2 klastera. Na slikama 7.7(a) i (b) su prikazani rezultati klasterovanja za 5 i 2 klastera u slučaju podataka predobrađenih normalizacijom vrednosti entropije.

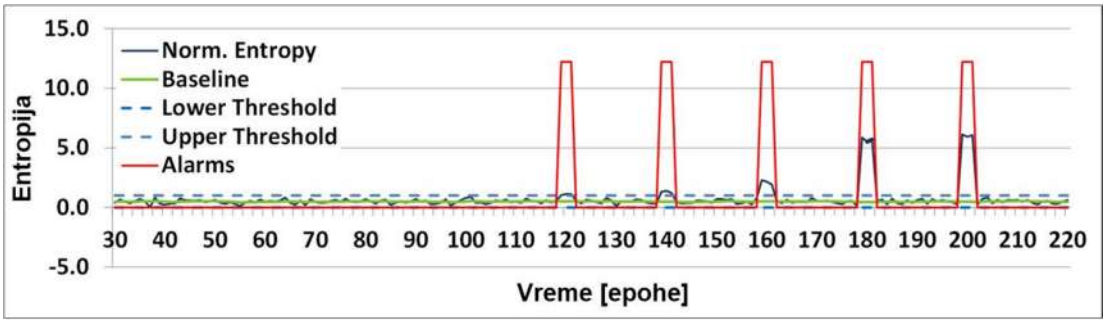


Slika 7.7 1N-1N: rezultati klasterovanja ($D[S.d]$), za 5 i 2 klastera

Analizom je zatim obuhvaćeno ponašanje mrežnog sobraćaja koje je u skladu sa komunikacionim modelom N1-1N, a koji se u okviru podataka manifestuje amplifikacijom DDoS NTP napada. Ovaj napad karakteriše aktivnost jednog karakterističnog izvorišnog porta i jedne odredišne IP adrese. Na osnovu agregacije mrežnog saobraćaja ovako formiranim ključem, omogućeno je efikasno utvrđivanje prisustva zlonamernog saobraćaja. Odredišna IP adresa i broj izvorišnog porta su jedinstveni tokom napada i dobri su kandidati za formiranje agregacionog ključa, čime bi se uhvatio skok u raspodeli. Sa druge strane, izvorišna IP adresa i odredišni port koji se odnose na oznaku 'N' u modelu N1-1N, mogu se koristiti u ključu agregacije za otkrivanje dugačkog „repa" u raspodeli vrednosti posmatranih atributa. Slike 7.8 i 7.9 predstavljaju vrednosti entropije i normalizovane entropije izvorišne IP adrese kada je odredišni port ključ agregacije ($S[d]$).

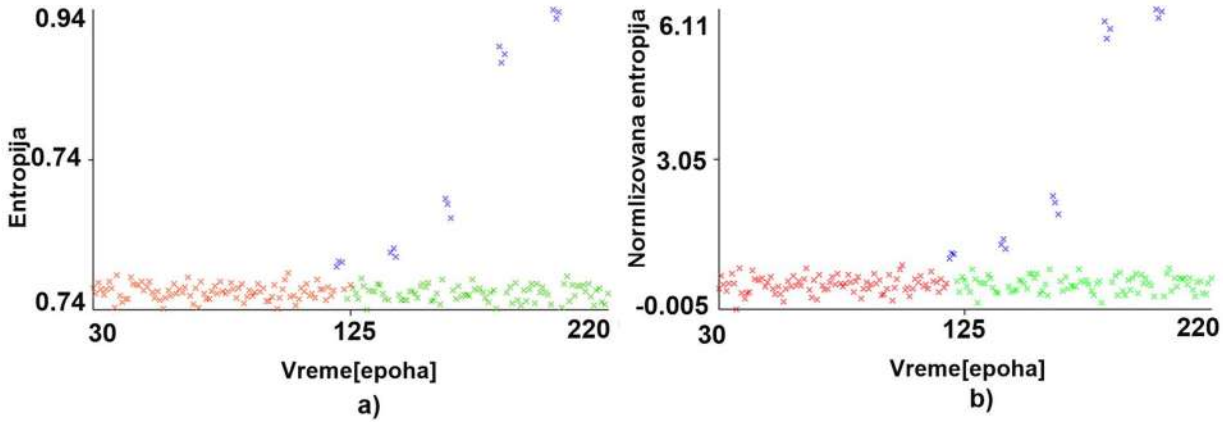


Slika 7.8 N1-1N: vrednost entropije, $S[d]$



Slika 7.9 N1-1N: normalizovana vrednost entropije, $S[d]$

Na slikama 7.10(a) i (b) su predstavljeni rezultati klasterovanja vrednosti entropije i normalizovane entropije izvorišne IP adrese kada je agregirana odredišnim portom kao ključem agregacije ($S[d]$). Rezultat klasterovanja su 3 generisana klastera.



Slika 7.10 N1-1N: rezultati klasterovanja za vrednosti entropije (a) i normalizovane entropije (b), $S[d]$

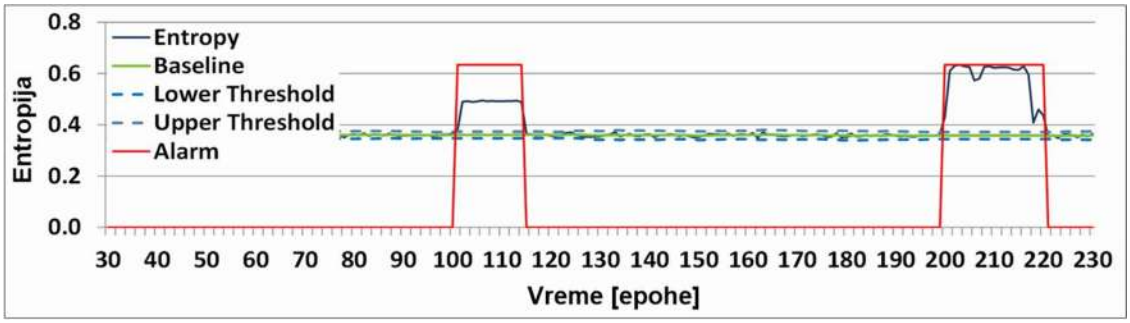
Predstavljeni rezultati potvrđuju uspešnost metode klasterovanja u procesu detekcije i klasterovanja svih anomalija, bez generisanja grešaka niti pogrešnog detektovanja FP događaja na početku opsega epoha čiji podaci su analizirani.

7.3.4 Eksperimentalni rezultati analize botnet saobraćaja

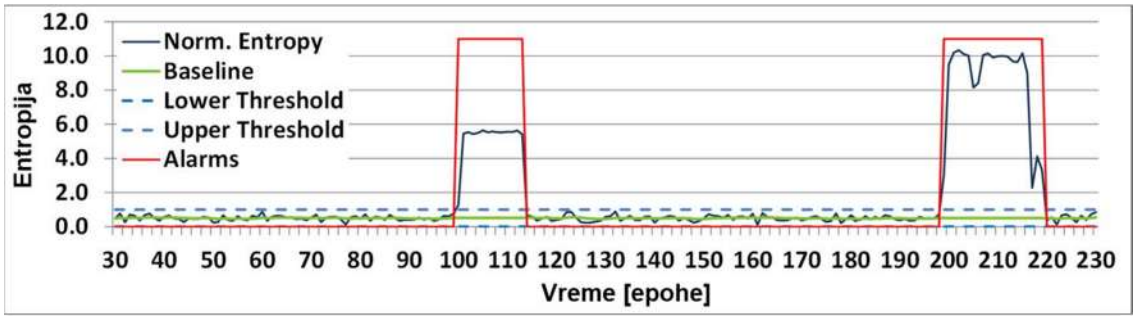
Detekcija i zaštita od *botnet* napada predstavlja jedan od glavnih izazova u obezbeđivanju sigurnosti u modernim poslovnim mrežama. Ovi napadi često podrazumevaju superpoziciju višestrukih malicioznih aktivnosti, koje obično pripadaju različitim oblicima i tipovima napada. Za potrebe ovog istraživanja sprovedena je grupa eksperimenata za procenu pogodnosti primene predloženog rešenja i metodologije u slučaju detekcije *botnet* napada.

Analizirani skup podataka predstavlja emulaciju korišćenog stvarnog mrežnog saobraćaja u uslovima *botnet* napada. Korišćeni skup podataka sa *botnet* saobraćajem obuhvata 238 epoha, od kojih 203 odgovaraju normalnom saobraćaju, a preostalih 35 su epohe u kojima se javlja *botnet* saobraćaj, u dva karakteristična opsega, 101-114 i 200-220.

Polazeći od entropijski pretprocesiranih podataka, pokazalo se da je svega nekoliko atributa relevantno za analizu i za njih je primenjen EM algoritam. Slika 7.11 prikazuje vrednost entropije za broj tokova podataka u slučaju kada je agregiran odredišnim portom kao ključem, $f[d]$. Slika 7.12 daje prikaz normalizovane vrednosti entropije za $f[d]$ atribut.



Slika 7.11 *Botnet*: vrednost entropije, $f[d]$

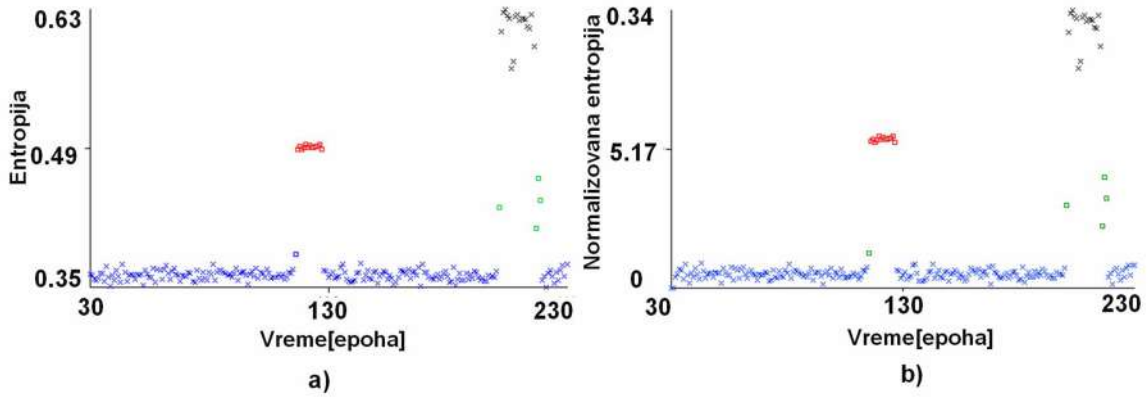


Slika 7.12 *Botnet*: normalizovana vrednost entropije, $f[d]$

Predstavljeni rezultati jasno pokazuju prisustvo dva odvojena bloka *botnet* napada, oba snažna, ali različitog intenziteta. Čak i bez normalizacije, moguće je identifikovati ta dva bloka napada, što je prikazano na slici 7.11. Rezultati zasnovani na analizi raspodele atributa $f[d]$ pokazuju da su anomalije grupisane u dva različita klastera, što je dobro jer su uspešno identifikovana i grupisana dva napada koji se razlikuju po intenzitetu. Ovo ukazuje na mogućnost postojanja dva različita izvora i tipa *botnet* napada.

Slika 7.13 prikazuje razliku koja postoji kada je primenom algoritma klasterovanja generisano 4

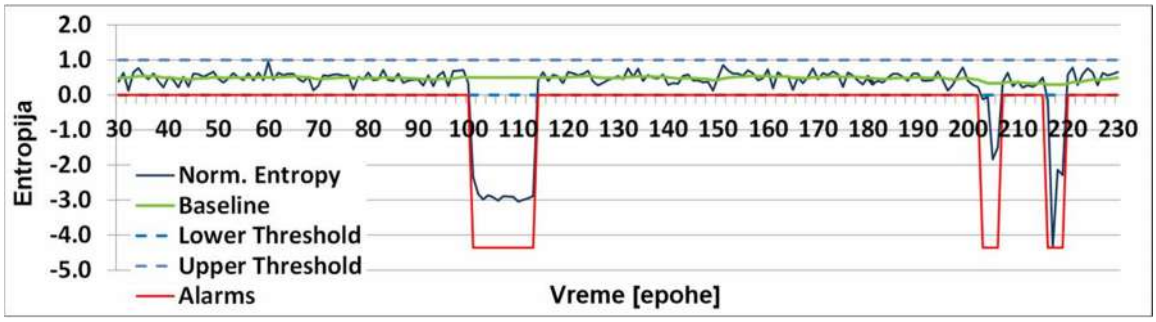
klastera, u slučaju izračunatih vrednosti entropije (a) i normalizovane entropije (b) za atribut *f*[*d*]. Rezultati potvrđuju da se za oba oblika analiziranih vrednosti entropije primenom EM algoritma dobija jasan i pregledan prikaz skoro identičnog klasterovanja instanci anomalija u tri različita klastera. Na taj način se jasno izdvajaju različiti *botnet* napadi u raspodeli.



Slika 7.13 *Botnet*: rezultati klasterovanja vrednosti entropije i normalizovane entropije, *f*[*d*]

U slučaju normalizovane vrednosti entropije detektovane su obe grupe *Botnet* napada, sa manjim brojem FP alarma, što ukazuje na nisku osetljivost algoritma klasterovanja od vrednosti faktora *k*.

Drugi blok *botnet* napada je značajno jačeg intenziteta i kada se analizom rasloži po epohama utvrđuje se varijabilnost strukture i vrednosti koje ostvaruju instance napada. To je jasan pokazatelj mogućnosti postojanja superpozicije nekoliko različitih napada. Primenom veće granularnosti u procesu klasterovanja i poređenjem dobijenih rezultata u slučaju drugih atributa instanci podataka, moguće je doći do mnogo više informacija vezanih za razlike i karakteristično ponašanje pojedinih napada iz superpozicije. Tako se, na primer, pri normalizaciji vrednosti entropije za atribut *s*[*S.D*] obezbeđuje izdvajanje dva različita profila ponašanja u okviru drugog *botnet* bloka (slika 7.14).



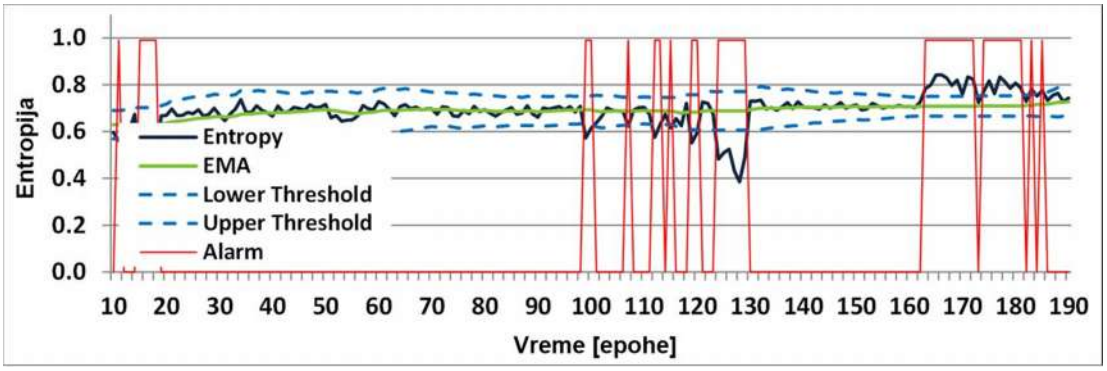
Slika 7.14 *Botnet*: normalizovana vrednost entropije, *s*[*S.D*]

7.3.5 Eksperimentalni rezultati analize realnog mrežnog saobraćaja

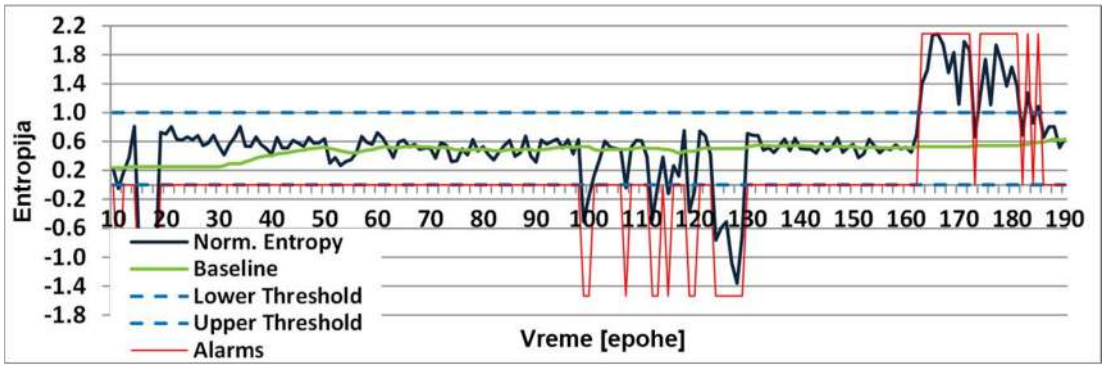
Izuzetna primenljivost i efikasnost metodologije je, pored prethodno predstavljenih rezultata, prikazana i na primerima tokova realnih oblika mrežnog saobraćaja koji su ekstrahovani iz CTU-13 skupa podataka. U okviru originalnog CTU-13 skupa je taj deo instanci obeležen oznakom „43”, a generisan je isključivanjem instanci *botnet* saobraćaja i zadržavanjem instanci normalnog saobraćaja

pomešanih sa velikom količinom instanci pozadinskog saobraćaja i nekoliko manjih oblika anomalija.

U okviru ovog dela istraživanja, prvo su analizirane karakteristike regularnog mrežnog saobraćaja tako što su razmatrani rezultati dobijeni za vrednosti entropije i za normalizovane entropije broja tokova podataka kada je agregiran po izvorišnoj IP adresi, $f[S]$. Na slikama 7.15 i 7.16 su predstavljene vrednosti entropije i normalizovane entropije za analizirani regularni mrežni saobraćaj.



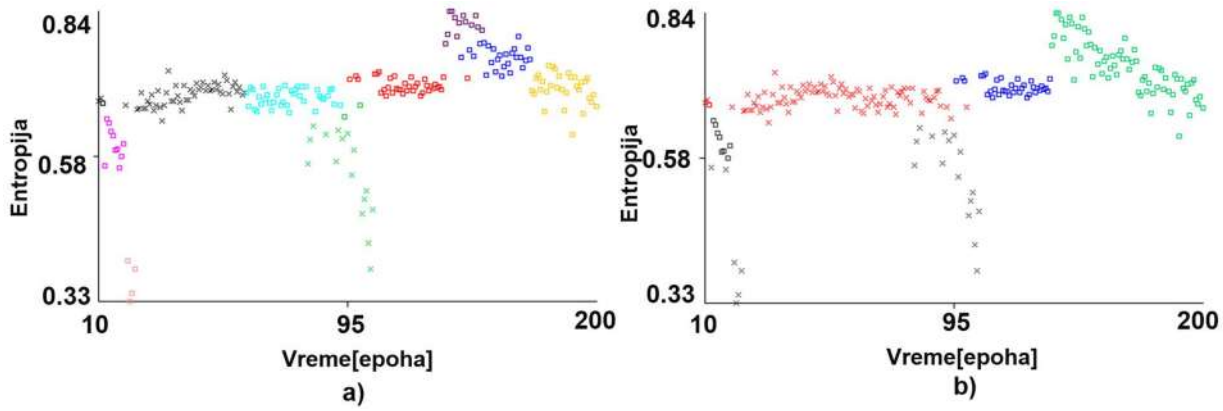
Slika 7.15 „43”: Vrednost entropije, regularni mrežni saobraćaj, $f[S]$



Slika 7.16 „43”: Normalizovana vrednost entropije, regularni mrežni saobraćaj, $f[S]$

Entropija uspeva da uhvati alarme vezane i za jače i za slabije devijacije, dok normalizovana vrednost entropije dodatno pojačava te uhvaćene devijacije.

Na slici 7.17 su predstavljeni rezultati klasterovanja raspodele entropije za slučajeve kada se generiše 9 i 4 klastera. Generisanjem samo 4 klastera se ne obezbeđuje dovoljno precizna detekcija, jer se pokazuje da se u tom slučaju jedan deo devijacije u raspodeli klasterovanjem pridružuje klasteru sa instancama normalnog saobraćaja. Međutim, puštanjem EM algoritma da dinamički odredi optimalan broj klastera u ovom slučaju se kao rezultat dobija 9 klastera koji primenom određenog stepena granulacije izdvajaju različite oblike devijacija i anomalija u 9 grupa.

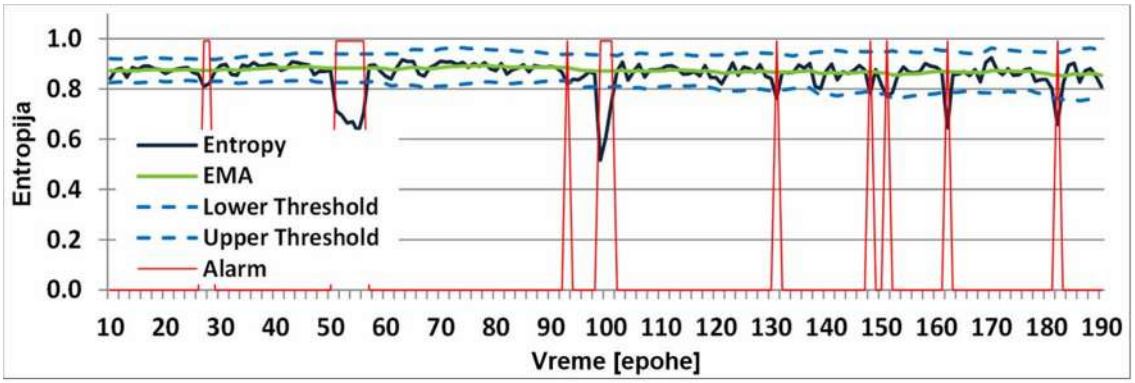


Slika 7.17 Klasterovanje vrednosti entropije u 9 (a) i 4 (b) klastera, $f[S]$

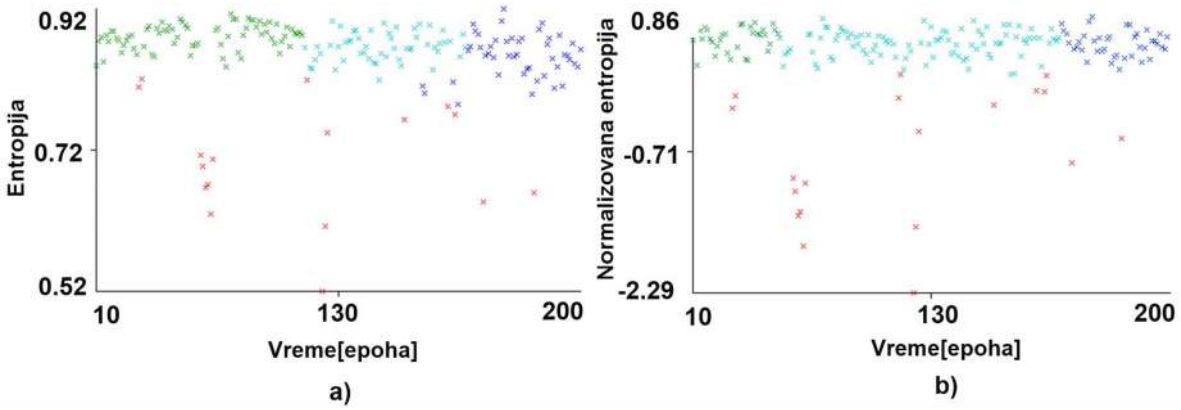
S obzirom na to da algoritam primenom veće granulacije postaje precizniji, a u ovom slučaju je generisao veći broj klastera, jedan od koraka u analizi rezultata jeste određivanje prirode svakog od generisanih klastera. Naime, jasno je da će nekoliko klastera sadržati instance različitih kategorija malicioznog saobraćaja, dok će preostali klasteri sadržati instance normalnog a opet po nekim karakteristika međusobno drugačijeg normalnog saobraćaja, na osnovu kojih se mogu podeliti u više klastera normalnog saobraćaja.

Na osnovu statističkih informacija vezanih za srednje vrednosti i vrednosti standardne devijacije za svaku centralnu tačku klastera, tačka koja je blizu osnovnim (*baseline*) vrednostima entropije može se smatrati da pripada normalnom saobraćaju, dok su udaljene tačke kandidati za to da se smatraju anomalijama. U nekom sledećem koraku stepen granulacije može da se smanji, zatim da se izvrši poređenje klastera, a ako među nekim klasterima postoji sličnost, moguće je izvršiti njihovu konsolidaciju.

Sa druge strane, razmatrana je primena klasterovanja nad proračunatim entropijama i normalizovanim entropijama pri analizi podataka podeljenih na više klasa mrežnog saobraćaja. Precizno diferenciranje instanci mrežnog saobraćaja na osnovu tipa protokola može da doprinese pouzdanijem izdvajanju karakterističnih anomalija. Na primer, na slici 7.18 je predstavljena vrednost entropije za broj tokova podataka pri agregaciji po odredišnoj IP adresi, $f[D]$, dok je na slikama 7.19(a) i (b) dat prikaz rezultata koji su ostvareni pri klasterovanju za taj atribut. U razmatranje je uzet isključivo TCP saobraćaj iz ovog podskupa podataka.



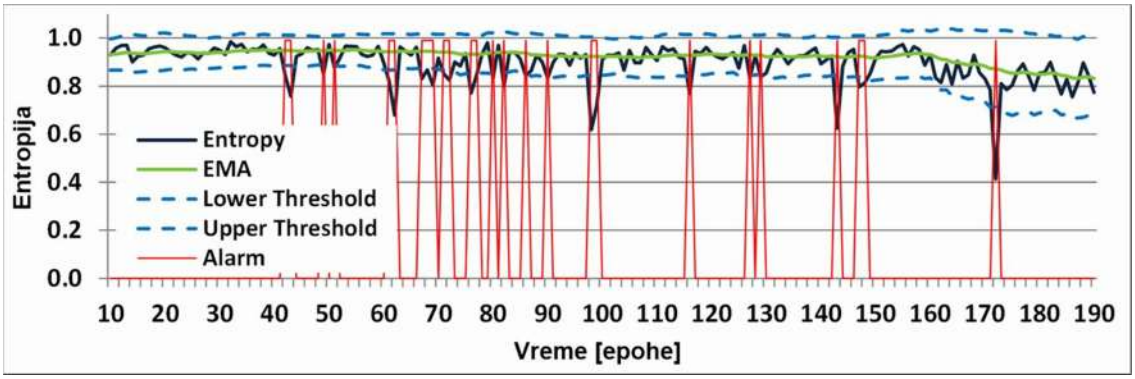
Slika 7.18 TCP mrežni saobraćaj: vrednost entropije, $f[D]$



Slika 7.19 TCP mrežni saobraćaj: rezultati klasterovanja vrednosti entropije (a) i normalizovane entropije (b), $f[D]$

U ovom slučaju, algoritmom klasterovanja je definisano 4 klastera za optimalnu detekciju anomalija i napada. Iako su rezultati dobijeni i primenom samo entropijski zasnovanog pristupa dovoljno dobri, jasno je da se primenom klasterovanja obezbeđuje bolje prepoznavanje i izdvajanje svih instanci anomalija u poseban klaster (na slici obeležen crvenom bojom). Time se dalje dokazuje da u mnogim slučajevima efikasnost algoritma klasterovanja ne zavisi od vrednosti faktora podešavanja margina *k,* dok je vrednost faktora *k* jedan od ključnih elemenata preciznije i uspešnije detekcije kada je u pitanju primena entropijskog pristupa.

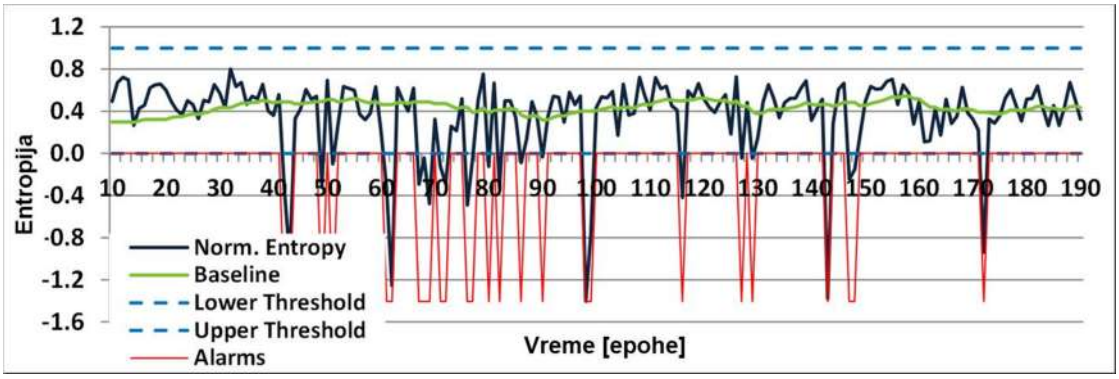
Sledeći ispitivani slučaj se odnosi na analizu čistog ICMP saobraćaja, pri čemu su predstavljeni rezultati dobijeni za analizu vrednosti entropije određenog porta kada se agregira po izvorišnoj IP adresi, $d[S]$ (slika 7.20).



Slika 7.20 ICMP mrežni saobraćaj: vrednost entropije, $d[S]$

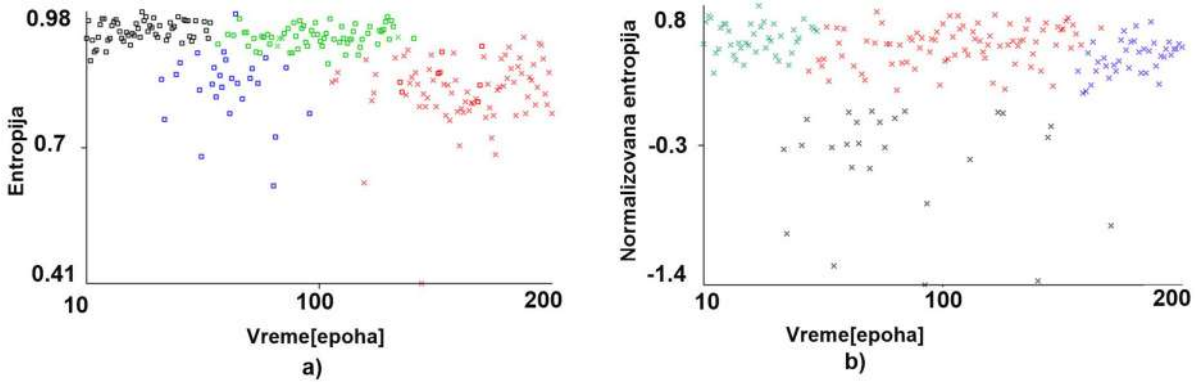
Primenom metode dinamičkog EM klasterovanja nad proračunatom raspodelom entropije podataka generisaće se 4 klastera, ali bez zadovoljavajućeg stepena diferencijabilnosti između specifičnih oblika ponašanja mrežnog saobraćaja obuhvaćenog ovim delom analize. Na slici 7.22(a) se vidi da se dinamičkim klasterovanjem spojilo skoro sve od podataka što se nalazi u drugoj polovini analiziranog intervala, tako da poslednjih nekoliko anomalija nije ispravno obuhvaćeno (pojedine crvene tačke nakon 100. epohe koje bi trebalo da se grupišu u okviru plavog klastera). Plavi klaster na slici 7.22a obuhvata manji broj tačaka nego što isti klaster obuhvata kada se primeni normalizacija, a što je na slici 7.22b (uvedena normalizacija) predstavljeno kao crni klaster. Iako se po boji ne

podudaraju (problem sa WEKA odabirom boja), vizuelno je jasno da je u pitanju isti klaster, samo bolje definisan kada se primeni normalizacija. To znači da postoji potreba za normalizacijom podataka jer je povećanje standardne devijacije u ovom delu intervala izazvalo neosetljivost algoritma na prisustvo anomalije. Rešenje ovog problema je primena algoritma klasterovanja nad normalizovanom vrednošću entropije (slika 7.21), čime se ostvaruju bolji rezultati klasterovanja.



Slika 7.21 ICMP mrežni saobraćaj: normalizovana vrednost entropije, $d[S]$

Ovakvim pristupom je omogućeno dinamičko EM klasterovanje kojim je generisano 4 klastera instanci mrežnog saobraćaja pri čemu je obezbeđena preciznija detekcija i klasterovanje instanci anomalija (WEKA u svom grafičkom okruženju nasumično dodeljuje boje klasterima, tako da su u ovom grafičkom prikazu instance anomalija označene crnom bojom) nego što je slučaj sa rezultatima ostvarenim pri detekciji zasnovanoj na entropijskom pristupu (slika 7.22 (b)).



Slika 7.22 ICMP mrežni saobraćaj: rezultati klasterovanja vrednosti entropije (a) i normalizovane entropije (b), 4 klastera, $d[S]$

Za posmatrane podatke o entropiji, u drugom delu intervala primetno je povećanje vrednosti standardne devijacije, što taj deo podataka čini nepouzdanim za detekciju napada primenom metode klasterovanja. Kada se primeni normalizacija ovaj deo intervala se takođe normalizuje i regularizuje u smislu obezbeđivanja kvalitetnijih podataka za dalju primenu algoritma klasterovanja.

7.3.6 Diskusija dobijenih rezultata analize

Na osnovu analize dobijenih rezultata u ovom delu istraživanja, utvrđeno je da se u odnosu na

entropijski zasnovanu detekciju anomalija primenom EM algoritma klasterovanja ostvaruje blago poboljšanje efikasnosti detekcije, uz precizno izdvajanje izuzetaka (*outlier*) i bez pogrešno uhvaćenih FP alarma, koje su slaba tačka entropijski zasnovanog pristupa. Bolja efikasnost i jednostavnost pristupa primenom algoritma klasterovanja se jednim delom oslanja i na veću otpornost algoritma klasterovanja na varijacije vrednosti multiplikativnog faktora *k*. Time se eliminiše potreba finog podešavanja ovog faktora u cilju obezbeđivanja adekvatne margine, što je inače neophodno za pouzdaniji rad klasičnog pristupa analizi entropije. Dobijeni rezultati ukazuju na poboljšanja koja su uneta primenom metode EM klasterovanja, koji je u najvećem broju slučajeva precizno grupisao instance podataka u različite klastere, uzimajući u obzir strukturu podataka, intenzitete i vreme pojavljivanja određenih napada i anomalija. Ostvarena poboljšanja su dovoljna da se ukaže na izvesne prednosti koje se ostvaruju primenom metoda mašinskog učenja klasterovanjem.

Iako je EM algoratam jednostavan, robustan, lak za implementaciju i pogodan za rad sa višedimenzionalnim podacima, ovaj algoritam zahteva da se *a priori* definiše određeni broj klastera što može da predstavlja problem za primenu u oblasti detekcije napada i anomalija. Ukoliko se predefiniše mali broj klastera, moguće je da neke instance normalnog sobraćaja budu klasterovane kao anomalije, ili obrnuto. Sa druge strane, ukoliko se predefiniše preveliki broj klastera može da se izgubi fokus sa najznačajnijih anomalija njihovim prevelikim rasipanjem u veliki broj klastera. Osim toga, efikasnost EM algoritma opada sa porastom broja analiziranih instanci i sa brojem njihovih atributa, jer je za velike skupove podataka potreban veliki broj iteracija pri obradi podataka i njihovom klasterovanju, a to podrazumeva duže vreme obrade i potrebu za većim procesorskim i memorijskim resursima.

Dalji tok istraživanja i primena unapređenog hijerarhijskog aglomerativnog algoritma su predstavljeni u odeljku 7.4, a rezultati pokazuju da je primena tako unapređenog algoritma dovela do značajno poboljšanih rezultata i bolje detekcije anomalija i napada. Ostvareni rezultati i njihova analiza su detaljno predstavljeni u poglavlju 8 i u radu [174].

7.4 Primena modifikovanog hijerarhijskog aglomerativnog klasterovanja

Ono što pristup predstavljen u ovoj disertaciji izdvaja u odnosu na druge jeste to što na specifičan način kombinuje prednosti entropije i tehnika mašinskog učenja. Ovaj pristup je tokom istraživanja obogaćen različitim tehnikama obrade podataka, te je nakon završene analize rada sa EM algoritmom klasterovanja rešenje dalje razvijano u smeru profilisanja i klasifikacije instanci pojedinačnih tokova, usled čega se dobija veći nivo granularnosti. U tom smislu, daljim istraživačkim radom su obezbeđena dva osnovna doprinosa.

1. Efikasno generisanje i izbor skupa relevantnih atributa ponašanja (*behavior features*) koji se koriste pri primeni entropijskih pristupa, a zatim se dodeljuju svakoj instanci, što dalje omogućava njihovo korišćenje od strane bilo kog algoritma mašinskog učenja.

2. Za tako dobijene nove atribute se vrednosti diskretizuju u kategorije sa vrednostima 0, 1 i 2, a koje označavaju nisku (*low*), srednju (*medium*) i visoku (*high*) vrednost atributa. Ovakva markacija se interpretira kao „potpis" komunikacionih aktivnosti, što se dalje koristi za izdvajanje najčešćih potpisa u okviru realnog saobraćaja kao i potpisa tipičnih anomalija, što se sprovodi primenom modifikovanog hijerarhijskog aglomerativnog klasterovanja uz definisanje funkcije distance.

Na ovaj način se sprovodi profilisanje svake komunikacije uz pridruživanje karakterističnim klasterima koji predstavljaju normalan saobraćaj ili anomalije, što osim profilisanja može da služi i za detekciju i identifikaciju anomalija.

Kako bi se odgovorilo na definisane izazove, bilo je neophodno konkretnije sagledati strukturu podataka o mrežnom saobraćaju, a dalji tok istraživanja je usmeren ka diferencijaciji i izolaciji skrivenih obrazaca mrežnog saobraćaja koji u velikoj meri utiču na atribute drugog stepena.

Kao rezultat, dat je predlog hibridnog rešenja koje se oslanja na primenu modifikovanog hijerarhijskog aglomerativnog grupisanja na NetFlow podatke koji su prethodno obrađeni na sličan način koji se koristi kod detekcije anomalija na bazi entropije. Za potrebe detaljnog ispitivanja karakteristika ponašanja mrežnog saobraćaja, predloženim rešenjem su najpre generisani ključevi agregacije zasnovani na svim parovima atributa, da bi se kasnije sproveo izbor onih agregacionih ključeva i atributa koji nose najviše informacija za efikasno profilisanje i otkrivanje anomalija.

Specifični komunikacioni modeli generisani za potrebe ovog dela istraživanja simuliraju sledeće oblike napada: (1) distribuirani napadi odbijanjem servisa - DDoS kroz NTP i DNS amplifikaciju i plavljenje SYN paketima; (2) napadi skeniranjem portova (*Port Scan*) i mrežnog skeniranja (*Network Scan*); (3) inteligentni softverski agenti - botovi. Kompletna analiza unapređenim hijerarhijskim aglomerativnim algoritmom je realizovana u Python okruženju, pri čemu su generisane sve neophodne skripte vezane za rad sa podacima, proračun rastojanja između klastera, rad sa matricom povezivanja, generisanje dendrograma i generisanje rezultata.

Karakteristike ponašanja (*behavior attributes*) se određuju na osnovu rezultata procesa agregacije tokova saobraćaja. Ovaj proces se odnosi na grupisanje većeg broja tokova podataka uz razmatranje jedne ili više vrednosti karakteristika toka (atributa) mrežnog saobraćaja tokom određenog vremenskog perioda (epohe). Dobijene raspodele atributa su zasnovane na izračunavanju broja pojavljivanja određene vrednosti atributa. Proces agregacije atributa podataka korišćenjem određenog ključa agregacije se sprovodi brojanjem pojavljivanja jedinstvenih vrednosti preostalih atributa za takav slučaj.

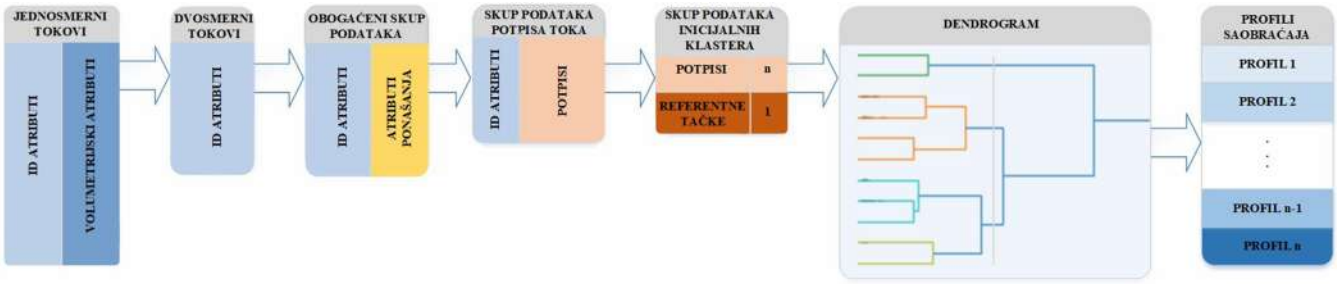
Princip rada predloženog rešenja za profilisanje i klasifikovanje pojedinačnih instanci tokova mrežnog saobraćaja je sledeći:

1. Koriste se samo osnovni atributi dvosmernih tokova: izvorišne i odredišne IP adrese i brojevi portova. Prilikom agregacije po ovim atributima, ukupan broj tokova i broj jedinstvenih vrednosti preostalih atributa se izračunavaju tokom svake epohe čime se dobijaju tzv. karakteristike ponašanja (*behaviour feature*), što zajedno sa osnovnim atributima o toku daje *obogaćeni skup podataka* (*enriched flow dataset*).
2. Vrednosti novogenerisanih atributa (karakteristika ponašanja) su proizvoljne i različite čak i za tokove koji imaju slična ponašanja. U cilju objedinjavanja sličnih ponašanja ove vrednosti se diskretizuju u jednu od tri referentne vrednosti iz skupa {0, 1, 2}, gde „0" odgovara niskim vrednostima atributa, „1" predstavlja vrednosti bliske srednjoj vrednosti, dok „2" označava visoke vrednosti izvedenih atributa. Granica između vrednosti u ovim kategorijama je utvrđena empirijski, a u korišćenim eksperimentima je postavljena na 10 i 100. Ova transformacija se koristi za dobijanje jednostavnijih rezultata za svaki atribut, koji se svi

zajedno interpretiraju kao karakterističan „potpis" komunikacionih aktivnosti na nivou toka podatka. Na ovaj način se dobija *skup podataka potpisa toka* (*flow signature dataset*).

3. U skupu podataka potpisa toka mnogi tokovi sa sličnim komunikacionim karakteristikama imaju iste potpise. Posmatrano tokom dužeg vremenskog intervala (na primer 6 sati ili jedan dan), potpise je moguće agregirati, čime se za svaki potpis dobija i ukupan broj tokova kojima on odgovara. Drugim rečima, svi tokovi sa istim potpisom se inicijalno spajaju u jedan inicijalni klaster, zadržavajući ukupan broj pripadajućih elemenata. Ovaj skup podataka se naziva *skup podataka inicijalnih klastera* (*seed clustering dataset*).
4. Najistaknutije anomalije i napadi u ponašanju mrežnog saobraćaja, kao što su DDoS, skeniranje mreže/portova i različiti napadi grubom silom, modeliraju se pomoću sintetičkih generisanih tokova podataka. Njihovi potpisi se izračunavaju na isti način kao i potpisi ponašanja regularnog saobraćaja, a zatim dodaju skupu podataka koji se koristi za inicijalno klasterovanje. Time se formiraju posebni klasteri koji se tumače kao referentne tačke podataka i koje predstavljaju tipične anomalije.
5. Inicijalni klasteri koji imaju slične potpise se grupišu primenom modifikovanog hijerarhijskog aglomerativnog algoritma koji se zasniva na specifično-definisanoj funkciji proračuna udaljenosti, a koja koristi koordinate potpisa, kao što je *Manhattan*, *Euclidean* rastojanje ili proračunatu vrednost kvadratne greške razdaljine (*Squared Error distance*). Generisani klasteri i njihove udaljenosti se u rezultujućem dendrogramu tumače kao različiti profili tokova mrežnog saobraćaja. Klasteri sa potpisima anomalije (ili u njihovoj neposrednoj blizini) se smatraju anomalijama.
6. Kada se profilisanje obavi nad dužim vremenskim intervalom, sličan postupak se može primeniti u skoro realnom vremenu, obrađujući dolazne tokove mrežnog saobraćaja tokom prethodne epohe. Koristeći istu funkciju udaljenosti, ovi novogenerisani potpisi se pridružuju reprezentativnim regularnim profilima ili profilima anomalija.

Opisani koraci su prikazani na slici 7.23 i detaljnije objašnjeni u nastavku.



Slika 7.23 Proces detekcije anomalija i napada primenom modifikovanog algoritma hijerarhijskog aglomerativnog klasterovanja

Kao najznačajniji naučni doprinos, predloženo rešenje za profilisanje i klasifikaciju pojedinačnih instanci saobraćaja je detaljno opisano u nastavku poglavlja.

7.4.1 Generisanje atributa

U savremenom mrežnom okruženju model komunikacije klijent-server (*client-server*) se smatra najčešćim oblikom komunikacije. Postoje mnoge studije o otkrivanju anomalija koje se oslanjaju na volumetrijske atribute (ukupan broj paketa i bajtova), ali iskustvo ukazuje na njihovu primenljivost samo u slučaju kada je potrebna detekcija jasno uočljivih anomalija, koje zahtevaju saobraćaj velikog intenziteta, kao što je u slučaju DDoS napada. Ove karakteristike su neefikasne za sigurnosne pretnje koje nastaju kao rezultat aktivnosti malih količina mrežnog saobraćaja, dok sa druge strane veliki broj regularnih ponašanja tokova mrežnog saobraćaja, sa velikim obimom podataka, mogu izazvati lažno pozitivne alarme [191–195].

U ovom delu istraživanja je korišćen pristup otkrivanja anomalija [39] koji se zasniva samo na identifikacionim atributima, odnosno na osnovu petorke koja obuhvata izvorišnu IP adresu (*S*), broj izvorišnog porta (*s*), odredišnu IP adresu (*D*), broj odredišnog porta (*d*) i protokol (*p*). Analiziraju se dvosmerni tokovi, što je u skladu sa drugim istraživanjima [190], [196] a takav pristup se koristi u radu sa mnogim postojećim skupovima podataka [56].

Kao što je u odeljku 7.4. objašnjeno, i za ovaj deo istraživanja osnovni atributi toka se koriste za dodatno izvođenje atributa ponašanja, a njihove vrednosti se dobijaju kao rezultat procesa agregacije toka tokom određenog vremenskog intervala, takozvane epohe.

Agregacija se zasniva na tome da se jedan ili više atributa iz kategorije identifikacionih atributa (*S*, *s*, *D*, *d*), koristi kao ključ u procesu agregacije tokom epohe. Peti identifikacioni atribut, protokol, se uglavnom odnosi na nekoliko često korišćenih protokola, kao što su TCP, UDP i ICMP. Zbog toga se više koristi za filtriranje podataka umesto za agregaciju, tako što se na osnovu tog podatka skup podataka može podeliti na nekoliko podskupova kako bi se bolje izdvojili karakteristični klasteri i time efikasnije otkrile anomalije.

Proces agregacije se odnosi na grupisanje različitih vrednosti atributa koji odgovaraju ključu koji se koristi tokom epohe. Ukupan broj elemenata grupisanih po jednoj vrednosti ključnog atributa generiše atribut broj tokova (*flow count*), koji je u tezi označen sa *f*. Atributi ponašanja se izračunavaju kao agregacija drugog stepena drugih identifikacionih atributa koji se ne koriste u ključu agregacije, računajući sve različite pojave ovih atributa po svakoj vrednosti atributa koji je odabran da bude ključ agregacije. Na primer, atribut ponašanja koji predstavlja ukupan broj različitih izvorišnih IP adresa (*S*) pri agregaciji koristeći odredišnu IP adresu (*D*) za ključ, označen je kao *S*[*D*], a njegova visoka vrednost ukazuje na veliki broj komunikacionih tokova koji se ostvaruju iz različitih izvora ka jednom odredišnom hostu, *D*. Autori u [195] ovu osobinu nazvaju „*in-degree*" karakteristika, dok suprotan slučaj, „*out-degree*" karakteristika odgovara broju različitih odredišta po određenom izvorišnom hostu, označenom kao *D*[*S*].

Ovaj koncept agregacije drugog stepena je zatim generalizovan [27], [39] primenom i proračunom nad celim skupom atributa ponašanja, tako što se koriste sve kombinacije identifikacionih atributa. Na primer, korišćenjem složenog ključa za agregaciju koji se sastoji od izvorišne i odredišne IP adrese (označene kao *S.D*), brojanjem ukupnog broja različitih pojavljivanja odredišnih portova dobija se odgovarajući atribut ponašanja označena kao *d*[*S.D*]. Velika vrednost ovog atributa ukazuje na neobičan obrazac komunikacije od jednog izvorišnog hosta do mnogih odredišnih portova na drugom hostu, što je karakteristično za napade skeniranjem portova.

Na osnovu multivarijantne analize primenjene na rezultate proračunatih entropija celog skupa atributa ponašanja [27], [39], može se identifikovati podskup atributa koji zajedno doprinose sa najviše informacija o različitim modelima anomalija. Kao atributi koji najviše doprinose u okvirima ovog istraživanja, posebno se ističu broj tokova podataka i karakteristike ponašanja koje su izvedene pomoću agregacionih ključeva sa samo jednim ili sa dva atributa toka identifikacije, datih sledećim skupom ključeva za agregaciju:

$A=\{S, D, s, d, S.D, S.s, S.d, D.s, D.d, s.d\}$

Uvedenom notacijom je formalizovana identifikacija ključeva. Za svaki agregacioni ključ koji se sastoji od samo jednog atributa potrebno je izračunati četiri dodatna atributa (broj tokova i karakteristike ponašanja za preostala tri atributa), dok se za složeni agregacioni ključ koji je sastavljen od dva atributa dobijaju tri dodatna atributa (broj tokova i dva dodatna atributa ponašanja). Na primer, kada se razmatra agregacioni ključ S, on se koristi za generisanje sledećih novih atributa: $f[S]$, $D[S]$, $s[S]$ i $d[S]$, dok agregacioni ključ $S.D$ daje atribute $f[S.D]$, $s[S.D]$ i $d[S.D]$. Na ovaj način, ukupan broj dobijenih novih atributa je 34.

Dok je proces agregacije isti kao kod pristupa zasnovanih na proračunu entropije, u predloženoj metodi generisane distribucije vrednosti atributa se ne koriste za izračunavanje entropije kao bitne metrike ravnomernosti vrednosti podataka. Umesto toga, izračunate vrednosti se pridružuju pojedinačnim tokovima u posmatranoj epohi. Primenom ovog procesa, svaki tok iz originalnog skupa podataka je obogaćen sa izračunatim vrednostima 34 atributa, na osnovu čega se obezbeđuju značajne dodatne informacije vezane za komunikacione aktivnosti u koje je uključen odgovarajući posmatrani tok podataka tokom epohe.

Važno je napomenuti da neki često korišćeni skupovi podataka takođe imaju neke atribute kojima se ukazuje na ukupan broj pojavljivanja neke druge karakteristike u okviru posmatrane komunikacije na nivou nekog vremenskog intervala, kao što je broj zapisa iste izvorišne IP adrese u poslednjih 100 zapisa [56], [93], [94]. U svim ovim slučajevima, atributi se generišu posebnom obradom sirovih mrežnih paketa.

Koliko je poznato, metod predstavljen u ovoj disertaciji je nov i originalan, u smislu da se veliki broj novih atributa generiše samo na osnovu poznatih osnovnih identifikacionih atributa tokova mrežnog saobraćaja. Ova jedinstvena karakteristika čini predstavljeni metod veoma korisnim ne samo za korišćenje nad postojećim skupovima podataka, već i za analizu stvarnog mrežnog saobraćaja koji je moguće lako prikupiti pomoću NetFlow ili nekog sličnog protokola.

Algoritam za agregaciju podataka i proračun vrednosti atributa predstavlja računarski i memorijski zahtevan proces, koji direktno zavisi od broja instanci mrežnog saobraćaja u epohi. Jednostavan pristup za izračunavanje različitih vrednosti atributa toka uključivao bi poređenje svake instance saobraćaja sa svim drugim instancama u određenoj epohi, što bi dovelo do algoritma kvadratne složenosti. S obzirom na to da je ovaj postupak potrebno primeniti u svakoj epohi, za svaki od 34 novogenerisana atributa, procedura bi bila previše složena i dugotrajna, a samim tim i veoma neefikasna u kontekstu primene u *real-time* aplikacijama.

Zbog toga je predložen efikasniji pristup korišćenjem neuređene asocijativne strukture podataka (*unordered associative array*), takođe poznate kao heš-mapa (*hash map*) u programskom jeziku Java. Primenom ovakve strukture omogućava se efikasna pretraga podataka i primena računskih operacija u

procesu agregacije. U većini slučajeva, vremenska složenost je O(1), dok se u najgorem slučaju kompleksnost O(log n) dobija kada se koriste uravnotežena stabla pretrage (*balanced search trees*), koja se generišu samo za mali broj unosa koji dele isti ključ heš-mape.

Predloženi algoritam je predstavljen u pseudokodu (algoritam 1, slika 7.24). Niz heš-mapa se implementira i indeksira svakim ključem agregacije, sa odgovarajućom strukturom podataka koja sadrži brojač instanci saobraćaja i ugrađeni niz heš-mapa koje su potrebne za agregaciju drugog stepena atributa ponašanja. Ugnežđene heš-mape simuliraju skup podataka kao kolekciju različitih vrednosti, bez potrebe da se računa broj pojavljivanja svakog elementa. Na kraju epohe, broj pojedinačnih elemenata u ugnežđenoj heš-mapi (kardinalnost skupa podataka) predstavlja rezultujuću vrednost odgovarajućeg atributa ponašanja kao ukupan broj različitih vrednosti posmatranog atributa pri agregaciji po drugom atributu.

Na kraju epohe potrebno je uneti izračunate vrednosti kao nove atribute u odgovarajuće instance tokova mrežnog saobraćaja. Međutim, ovaj postupak nije moguće uraditi direktno, s obzirom na to da uvedena struktura podataka agregacije ne zadržava reference na originalne tokove, već je neophodno ponovo proći kroz sve tokove podataka u epohi i koristiti pojedinačne vrednosti atributa toka kao ključeve za pristup izračunatim podacima u strukturi heš-mape. Dobijeni podaci formiraju obogaćeni skup podataka.

Algoritam 1 Algoritam agregacije i računanja vrednosti atributa po epohama

```
# variable declarations
arr[] of {          # array of hash-maps, indexed by the aggregation key types
   map of {         # hash-maps for the aggregation
      f: integer,   # flow count of the aggregated element
      arr[] of {    # array of hash-maps, indexed by the remaining key types
         map        # nested hash-map for the second degree aggregation
   }
}

init()                            # variable initialization

for each flow in epoch {          # iterate flows in the current epoch
   for each K1 in A {             # iterate over aggregation keys
      k1 = getKey(flow, K1)       # get key attribute(s) from the flow
      e1 = arr[K1].map.get(k1)    # get element from the hash-map
      e1.f = e1.f + 1             # increment the flow count
      for each K2 in Φ\{K1} {     # iterate the remaining keys
         k2 = getKey(flow, K2)    # get remaining key attribute
         e1.arr[K2].map.put(k2)   # store the second degree instance
      }
      arr[K1].map.put(k1, e1)     # store the element in the hash-map
   }
}

# update all flows with newly calculated features
for each flow in epoch {          # iterate flows in current epoch
   for each K1 in A {             # iterate over aggregation keys
      k1 = getKey(flow, K1)       # get key attribute(s) from current flow
      e1 = arr[K1].map.get(k1)    # get element from hash-map with key k1
      feature[flow, K1.f] = e1.f  # set the flow count feature
      for each K2 in Φ\{K1} {     # iterate the remaining keys
         feature[flow, K1.K2]     # set the number of distinct elements
            = e1.arr[K2].map.size #
      }
   }
}
```

Slika 7.24 Algoritam agregacije i računanja vrednosti atributa po epohama

S obzirom na visoku efikasnost heš-mape, uz pretpostavku da je složenost pronalaženja elementa blizu $O(1)$, može se smatrati da predstavljeni algoritam ima linearnu složenost koja odgovara broju tokova u epohi (N). Da bi se algoritam ispravno sproveo, potrebno je dva puta proći i analizirati sve tokove podataka u epohi – prvi put za potrebe procesa agregacije i drugi put za unos izračunatih novih atributa, pri čemu je za svaki tok podataka potrebno da se izvrši operacija pretraživanja po svakom atributu (34 puta).

Popularna Python *Pandas* biblioteka integriše strukturu *DataFrame* koja ima ugrađene efikasne mehanizme za grupisanje tabelarno zadatih podataka. Njenom primenom se prethodno opisani algoritam značajno pojednostavljuje, jer već postoje metode za agregaciju po više kolona (*groupby*), tehnike za računanje broja pojavljivanja agregiranih redova (*size*), kao i metoda za pretraživanje broja jedinstvenih različitih elemenata (*unique*). Pored toga, rezultat agregacije automatski čuva listu indeksa odgovarajućih instanci saobraćaja koje su zadate u formi strukture *DataFrame*, čime se pojednostavljuje ažuriranje izračunatih karakteristika i eliminiše potreba za drugim prolazom kroz skup podataka.

Prilikom implementacije na stvarnom saobraćaju u realnom vremenu, proces izračunavanja novih atributa podrazumeva da se svi zapisi toka u jednoj epohi privremeno baferuju tokom trajanja epohe, nakon čega je moguće uneti pojedinačne podatke sa izračunatim vrednostima atributa. Još jedan problem koji se tiče obrade vrednosti atributa u realnom vremenu je izuzetno veliki broj dolaznih instanci saobraćaja, nekada i desetine hiljada u sekundi, a potrebno ih je obraditi u realnom ili blisko realnom vremenu. Rešenje koje bi moglo da se primeni u ovom slučaju je korišćenje tehnike uzorkovanja instance podataka (*flow sampling*), koja omogućava obradu samo statističkog dela toka podataka, dok se ostatak odbacuje. Neke informacije će se u tom slučaju izgubiti, ali se za potrebe ispravnog korišćenja predloženog algoritma i dalje uzima u obzir dovoljna količina podataka (do granice obrade), što rezultira prilično dobrom statističkom aproksimacijom. Sličnu tehniku uzorkovanja podržavaju i mrežni uređaji koji funkcionišu po principu eksportovanja *NetFlow* podataka samo za deo saobraćaja. Drugi pristup bi bio korišćenje više servera, gde svaki server sprovodi obradu po jednoj epohi, koja u tom slučaju može da traje i duže od vremena trajanja definisane epohe.

7.4.2 Generisanje potpisa tokova saobraćaja

Novogenerisani broj tokova i atributi ponašanja koji formiraju deo obogaćenog skupa instanci mrežnog saobraćaja predstavljaju odgovarajuću metriku komunikacione aktivnosti kojom instance mrežnog saobraćaja doprinose u trenutno posmatranoj epohi. Veliki broj tokova odgovara velikom broju sličnih instanci saobraćaja koji su u skladu sa agregacionim atributima, dok visoka vrednost nekog atributa ponašanja ukazuje na veliku raznovrsnost (*high-diversity*) posmatranog atributa drugog stepena. Slično važi i za umerene ili niske vrednosti broja instanci i atributa ponašanja. Samim tim, novogenerisani atributi su se pokazali kao veoma korisni u analizi ponašanja mrežnog saobraćaja, u procesu profilisanja saobraćaja, kao i detekciji anomalija.

Važno je napomenuti da su u nedavno publikovanim rezultatima šireg istraživanja kojoj je pripadala i izrada ove teze [39] obuhvatane sve instance mrežnog saobraćaja u određenoj epohi, pri čemu su korišćene sve moguće karakteristike, broj tokova i atributa ponašanja kako bi se izračunavale entropije kao izuzetno značajne mere ravnomernosti vrednosti posmatranih atributa tokova. Time je omogućeno obezbeđivanje vremenskih serija podataka koje su dalje korišćene za potrebe

multivarijantne analize na nivou pojedinačne epohe. S druge strane, primena ovih novih karakteristika za svaku pojedinačnu instancu mrežnog saobraćaja obezbeđuje više detalja na nivou pojedinačnih instanci podataka (komunikacionih tokova mrežnog saobraćaja), ali i značajno povećava složenost analize podataka.

Imajući u vidu veliku raznolikost rezultujućih vrednosti novogenerisanih atributa, da bi se pojednostavio proces analize, predlaže se da se vrednosti atributa grupišu u tri kategorije: Niska (*Low*), Umerena (*Medium*) i Visoka (*High*), a koje se mogu predstaviti vrednostima 0, 1 i 2, respektivno.

Transformisanje vrednosti atributa u razdvojene kategorije je jednostavan proces, međutim, pravi problem je odrediti vrednosti praga između kategorija. Ove granične vrednosti se ne mogu unapred fiksirati i koristiti u svim situacijama. Prvo, pragovi direktno zavise od trajanja epohe jer se vrednosti atributa akumuliraju tokom epoha. Pragovi takođe zavise od specifičnog mrežnog okruženja i mrežnog saobraćaja koji se prenosi. Na primer, centralni *e-mail* ili DNS server u univerzitetskoj mreži u kontinuitetu generiše visoke protoke podataka i samim tim dovodi do mnogo većih vrednosti atributa u odnosu na situaciju kada su te razmene podataka povremene, sa manjim obimima podataka ili kada pripadaju manjim mrežnim okruženjima. Osim toga, određeni pragovi definisani za jedan atribut najčešće nisu optimalni pragovi za druge atribute. Uprkos svemu tome, da bi se dokazao koncept i potvrdila upotrebljivost predloženog metoda, u ovom delu istraživanja se koriste fiksni pragovi za koje su korišćene vrednosti 10 i 100, za definisanje kategorija u skladu sa skupovima podataka koji se koriste u evaluaciji, a koji su predstavljeni u poglavlju 7.

Vrednosti podeljene u tri nivoa (*buckets*) i dalje predstavljaju prilično dobru indikaciju aktivnosti mrežnog saobraćaja u kontekstu posmatranog atributa. Samim tim se 34 nova atributa mogu tumačiti kao poseban potpis ponašanja mrežnog saobraćaja na nivou instance. Dodatno, iz praktičnih razloga, vrednosti svih 34 atributa su spojene u novo tekstualno polje, koje predstavlja oznaku odgovarajućeg potpisa. Na ovaj način, atributi ponašanja i vrednost broja instanci su spojene odgovarajućim ključem agregacije i odvojene posebnim znakom za razgraničenje, redosledom prikazanim na slici 7.25.

Aggregation key	S				D				s				d				S.D				S.s				S.d				D.s				D.d				s.d			
Features	D	s	d	f	S	s	d	f	S	D	d	f	S	D	s	f	s	d	f		D	d	f		D	s	f		S	d	f		S	s	f		S	D	f	
Example	0	2	2	2	0	2	2	2	0	0	0	0	0	0	1	1	2	2	2		0	0	0		0	1	1		0	0	0		0	1	1		0	0	0	
Label	0222 | 0222 | 0000 | 0011 | 222 | 000 | 011 | 000 | 011 | 000																																							

Slika 7.25 Potpis toka podataka

Skup tokova podataka, obogaćen oznakom potpisa i koordinatama potpisa (kategorisane vrednosti atributa) je označen kao *skup podataka potpisa toka* (*flow signature dataset*).

7.4.3 Inicijalno klasterovanje

Za očekivati je da će tokovi mrežnog saobraćaja koji su u skladu sa istim komunikacionim profilom generisati iste ili vrlo slične potpise u poređenju sa onima koji postoje u bazi potpisa toka podataka. Primenom nekog od nenadgledanih algoritama za mašinsko učenje, kao što je *k-means* ili hijerarhijsko klasterovanje, moguće je grupisati sve instance toka podataka i to na osnovu sličnosti sa nekim od potpisa kojima se predstavljaju različiti profili mrežnog saobraćaja. Međutim, većina ovih

algoritama ima najmanje kvadratnu složenost računanja u zavisnosti od broja tačaka koje obrađuje, što ih čini praktično neupotrebljivim za primenu u realnom vremenu za skupove podataka zasnovane na hiljadama ili čak milionima instanci saobraćaja. Na sreću, postoji veliki broj instanci koje dele isti potpis, što čini ukupan broj različitih potpisa mnogo manjim.

Samim tim, agregacija prema uvedenim potpisima vrši grupisanje svih instanci sa istim potpisom u jedan inicijalni klaster. Ukupan broj agregiranih tokova (instanci) po klasteru, sve zajedno sa oznakom potpisa i 34 koordinate potpisa, daje skup podataka inicijalnih klastera (*seed clustering dataset*). Očigledno, ovaj skup podataka sadrži mnogo manji broj tačaka podataka (inicijalnih klastera) od originalnog skupa instanci tokova podataka, uključujući obogaćeni skup tokova podataka (*enriched flow dataset*) i skup podataka potpisa toka (*flow signature dataset*) (slika 7.23). Iz tog razloga, skup podataka inicijalnih klastera je zatim moguće koristiti u procesu daljeg klasterovanja korišćenjem odgovarajućeg algoritma nenadgledanog mašinskog učenja, čak i u realnom vremenu. Oznaka potpisa u skupu podataka potpisa toka predstavlja referencu svakog toka na odgovarajući klaster u skupu podataka inicijalnih klastera, a koji je identifikovan ovom oznakom potpisa.

7.4.4 Referentni potpisi anomalija

U jednom delu šireg istraživačkog rada, posebna pažnja je usmerena na multivarijantnu analizu entropije atributa ponašanja sa ciljem da se utvrdi jasna taksonomija komunikacionih profila zasnovanih na instancama tokova mrežnog saobraćaja (*flow-based*), a koji često odgovaraju tokovima generisanim u prisustvu anomalija i koji samim tim ukazuju na potencijalne sigurnosne pretnje [39]. Obično je u okolnostima napada intenzitet određenih komunikacionih karakteristika primetno veći nego u slučaju redovnog mrežnog saobraćaja, dok se razlike uglavnom posmatraju kroz opseg vrednosti atributa ponašanja.

Tabela 7.3 Taksonomija potpisa tokova

Ss-Dd	Primer	Labela potpisa
11-11	Single flow	0002|0002|0002|0002|002|002|002|002|002|002
11-1N	Port Scan	0022|0022|0022|0000|022|022|000|022|000|000
11-N1	Network Scan	2002|0000|0202|0202|000|202|202|000|000|022
11-NN	ICMP flooding	2022|0000|0222|0000|000|222|000|000|000|000
1N-11	Dictionary attack	0202|0202|0000|0022|202|000|022|000|022|000
1N-1N	Port Scan	0222|0222|0000|0000|222|000|000|000|000|000
1N-N1	Network Scan	2202|0000|0000|0222|000|000|222|000|000|000
1N-NN	Diagonal Scan	2222|0000|0000|0000|000|000|000|000|000|000
N1-11	Amplification DDoS (DNS)	0000|2002|2002|2002|000|000|000|202|202|202
N1-1N	Amplification DDoS (NTP)	0000|2022|2022|0000|000|000|000|222|000|000
N1-N1	Multiple Network scan	0000|0000|2202|2202|000|000|000|000|000|222
N1-NN	Multiple Diagonal scan	0000|0000|2222|0000|000|000|000|000|000|000
NN-11	SYN flooding	0000|2202|0000|2022|000|000|000|000|222|000
NN-1N	DDoS	0000|2222|0000|0000|000|000|000|000|000|000
NN-N1	Multiple Amplification DDoS	0000|0000|0000|2222|000|000|000|000|000|000
NN-NN	Multiple DDoS	0000|0000|0000|0000|000|000|000|000|000|000

Karakteristični primer je DNS DDoS napad koji se zasniva na formi „otvorenog servera", gde napadač generiše i šalje serveru ogroman broj mikro zahteva, koristeći lažnu izvorišnu IP adresu ciljnog hosta. Kao rezultat, svi serveri će poslati odgovor koristeći fiksni izvorišni port (53 za DNS ili 123 za NTP) ciljanom hostu i fiksni ili nasumični odabrani broj odredišnog porta [196]. Na osnovu taksonomije komunikacionih modela (detaljno opisana u odeljku 7.3), ovaj DDoS napad se može opisati oznakom N1-11 u slučaju fiksnog odredišnog porta (karakteristično za DNS pojačanja) ili sa N1-1N za nasumično generisani odredišni port (karakteristično za NTP pojačanja). Tako su za svaki profil, simulirajući određeni model anomalije, generisane sintetičke instance tokova mrežnog saobraćaja i kombinovane sa tokovima redovnog mrežnog saobraćaja. Dobijeni skup podataka svakog modela anomalije je dodatno obogaćen brojem instanci tokova po epohi i atributima ponašanja, a koji se transformišu u potpise primenom prethodno opisane procedure. Veliki broj instanci različitih anomalija deli karateristike sa nekim od potpisa tokova mrežnog saobraćaja koji je ekstrahovan kao karakteristični otisak odgovarajućeg modela anomalije.

Kako bi se omogućila detekcija i klasifikacija anomalija u ponašanju mrežnog saobraćaja, rezultujuća oznaka potpisa i koordinate potpisa svakog modela anomalije se dodaju skupu podataka inicijalnih klastera (*seed clustering dataset*). Pošto se ove nove tačke podataka tumače kao posebni klasteri koji predstavljaju 16 referentnih modela anomalija, ukupan broj njegovih elemenata je postavljen na vrednost 1. Ove referentne tačke se u algoritmu klasterovanja posebno tretiraju u odnosu na ostale podatke iz skupa podataka.

7.4.5 Algoritam klasterovanja

Agregacijom svih instanci mrežnog saobraćaja sa istim potpisom se dobija skup podataka inicijalnih klastera, što predstavlja efikasan način generisanja početnih klastera i što je prvi korak u procesu klasterovanja. Što je još važnije, ukupan broj inicijalnih klastera je mnogo manji od početnog broja instanci koje se posmatraju, što omogućava znatno efikasniji rad algoritma klasterovanja. U ovom delu istraživanja je predložena upotreba hijerarhijskog aglomerativnog klasterovanja nad svim koordinatama potpisa.

Hijerarhijski aglomerativni algoritam (odeljak 4.7) u svakom koraku spaja dva najsličnija klastera u novi klaster, sve dok se svi klasteri ne kombinuju u jedan klaster. Tokom ovog iterativnog procesa održavaju se dve strukture podataka: matrica povezivanja (*linkage matrix*) koja pruža informacije o klasterima i njihovom odnosu, i matrica udaljenosti (*distance matrix*) u kojoj se smeštaju podaci o rastojanjima između klastera i daje mera njihovih različitosti. Počevši od N početnih tačaka podataka kao singlton klastera, novoformirani klaster se dodaje u matricu povezivanja u svakom koraku, zadržavajući reference na spojene klastere i njihovu udaljenost. Istovremeno, dva spojena klastera se uklanjaju iz matrice udaljenosti, dok se novoformirani klaster dodaje, ažurirajući njegove udaljenosti u matrici udaljenosti ka svim preostalim klasterima. Tačnije, zbog simetrije, potrebno je da se ažurira samo polovina matrice udaljenosti. Na kraju, u matricu povezivanja se dodaje ukupno $N-1$ novih klastera, dok se matrica udaljenosti kolabira u jedan zapis koji odgovara konačnom „superklasteru". Dobijena matrica povezivanja se zatim grafički predstavlja u formi dendrograma, strukture podataka zasnovane na generisanju stabla, gde svaki čvor predstavlja klaster na nivou koji odgovara udaljenosti spojenih podklastera, predstavljenih granama do sledećeg čvora koji se nalazi u nižem sloju u generisanoj hijerarhiji ili do tačke gde se nalaze singletoni početnih podataka. Presekom dendrograma na određenom nivou udaljenosti se odvaja određeni broj klastera, od kojih je svaki

dovoljno različit da predstavlja specifične karakteristike svih pripadajućih podklastera i početnih instanci podataka koje obuhvata.

Najvažniji preduslovi za sprovođenje algoritma hijerarhijskog aglomerativnog klasterovanja su određivanje specifične funkcije udaljenosti i metode klasterovanja. Funkcija udaljenosti se primenjuje na koordinate potpisa, gde više sličnih potpisa ima manje međusobno rastojanje, što predstavlja meru različitosti. Primenom proračuna funkcija udaljenosti i metrika udaljenosti klastera predstavljenih u odeljku 4.5 računaju se rastojanja koja su neophodna za primenu u ovom delu rada algoritma hijerarhijskog aglomerativnog klasterovanja. Tako funkcija *Manhattan Distance* sumira rastojanja (razlike) koordinata u svakoj dimenziji posebno, i za svaki par tačaka x i y u n-dimenzionalnom prostoru, *Manhattan Distance* se proračunava na sledeći način (relacija 7.1):

$$d_M(x,y) = \sum_{i=1}^{n} |x_i - y_i| \tag{7.1}$$

gde x_i i y_i predstavljaju koordinate tačaka x i y respektivno u dimenziji i.

U ovom slučaju, tačke predstavljaju klastere, a njihove koordinate predstavljaju atribute potpisa. S obzirom na to da koordinate potpisa mogu imati vrednosti 0, 1 ili 2, razlike u vrednosti 1 u dve dimenzije podjednako doprinose kao i razlika koja ima vrednost 2 u jednoj dimenziji. Na primer, sa istom razdaljinom od 2, delovi potpisa „0110” i „0220” su podjednako slični kao i „0000” i „0200”. Međutim, prirodno tumačenje je da sličnost između potpisa „0110” i „0220” manja nego sličnost između potpisa „0000” i „0200”, posebno imajući u vidu način na koji su originalne vrednosti potpisa podeljene u kategorije *Low*, *Medium* i *High*.

Da bi se dala veća težina razlici između kategorija *Low* i *High*, nego između *Low* i *Medium*, kao i između *Medium* i *High* kategorija, predlaže se upotreba kvadratne funkcije udaljenosti kao zbira kvadrata razlika u svakoj dimenziji, a koja je definisana jednačinom (7.2):

$$d_{sd}(x,y) = \sum_{i=1}^{n} |x_i - y_i|^2 \tag{7.2}$$

Ovakvim pristupom, rastojanje između „0110” i „0220” je 2, dok rastojanje između „0000” i „0200” ima vrednost 4, što drugi slučaj čini drugačijim od prvog.

Slično ovome, takođe može da se koristi Euklidova funkcija udaljenosti kao kvadratni koren kvadratnog rastojanja (*square root of the squared distance*), ali bi razlika između dva sasvim različita klastera mogla biti manje očigledna, posebno u daljoj vizuelnoj analizi odgovarajućeg dendrograma.

Dok funkcija rastojanja definiše rastojanje između dve instance podataka, metode klasterovanja definišu kako se izračunava rastojanje između dva klastera koji sadrže proizvoljan broj instanci podataka. Udaljenost između klastera je važna metrika jer hijerarhijski aglomerativni algoritam klasterovanja u svakom koraku spaja dva najbliža klastera, te je potrebno da ponovo izračuna rastojanje novoformiranih klastera do svih ostalih, preostalih klastera.

Postoji veliki broj različitih metoda za izračunavanje rastojanja između klastera, među kojima su *single-link*, *complete-link*, *average-link*, *Ward's* metoda, metoda centroida i druge, a sve su opisane u odeljku 4.5.

Da bi se omogućio pravilan izbor metode klasterovanja, neophodno je u obzir uzeti sve instance podataka u klasterima, jer njihovi potpisi doprinose karakteristikama odgovarajućeg klastera. U skupu podataka inicijalnih klastera, početna težina potpisa koji predstavlja ovaj pojedinačni klaster je zadata ukupnim brojem agregiranih instanci saobraćaja. Spajanjem dva klastera u novi klaster, njihovi potpisi se moraju uzeti u obzir u skladu sa njihovim relativnim doprinosom u novom klasteru (jednačine 7.3 – 7.8). Ako je klaster C_1, sa ukupno n_1 instanci podataka koje imaju potpis S_1, spojen sa klasterom C_2, koji ima n_2 instanci podataka sa potpisom S_2, onda je ekvivalentni potpis S_{12} novog klastera $C_{1\cup2}$ predstavljen sledećom relacijom (7.3):

$$S_{12,i} = \frac{n_1 S_{1,i} + n_2 S_{2,i}}{n_1 + n_2}, i = 1..n \tag{7.3}$$

gde $S_{x,i}$ predstavlja i-tu koordinatu potpisa S_x.

Umesto diskretnih celih brojeva u originalnim potpisima toka podataka (0, 1 i 2), vrednosti koordinata centroida u novom potpisu mogu biti bilo koji racionalni brojevi između 0 i 2, ali to ne utiče na uvedenu funkciju rastojanja. Ako je rastojanje između dva klastera definisano rastojanjem između njihovih centara, metoda klasterovanja se naziva *Centroid Clustering*. Pošto je originalni potpis svakog originalnog toka jednako ponderisan u izračunavanju prosečnih koordinata centroida, ovaj metod je poznat i kao neponderisano klasterovanje centroida (*Unweighted Centroid Clustering*) ili metoda neponderisane grupe sa usrednjavanjem centroida (*Unweighted Pair-Group Method with Centroid Averaging, UPGMC*). Ovo se ne sme mešati sa početnim težinama potpisa u inicijalnim klasterima, koji predstavljaju broj agregiranih instanci podataka jednake težine.

Čuvajući podatak o ukupnom broj instanci podataka u svakom klasteru i koristeći reprezentativni centroid za izračunavanje udaljenosti između bilo koja dva klastera, relacija 7.3 se može primeniti u bilo kojem od sledećih koraka, kao što je ponovno izračunavanje matrice rastojanja za novoformirani klaster. Prirodno je očekivati da se spajanjem dva najbliža klastera C_1 i C_2 u novi klaster $C_{1\cup2}$ povećava rastojanje između klastera $C_{1\cup2}$ i bilo kog drugog klastera C_x. Međutim, ovo se odnosi samo na tzv. ultrametrički prostor, gde je za svake tri tačke, *x*, *y* i *z*, zadovoljen uslov zadat relacijom 7.4:

$$d(x,y) \leq max\{d(x,y), d(y,z)\} \tag{7.4}$$

Međutim, klasterovanje zasnovano na proračunu centroida narušava ultrametričko svojstvo, što ponekad može da dovede do niže vrednosti ažurirane udaljenosti od neke tačke do novoformiranog klastera u odnosu na prethodno izračunatu minimalnu udaljenost između klastera koji su spojeni u prethodnom koraku (relacija 7.5), odnosno:

$$d(C_{1\cup2}, C_x) < d(C_1, C_2) \tag{7.5}$$

U odgovarajućem dendrogramu, ovo je predstavljeno skraćivanjem dužine spojenog čvora, a ovakva pojava se naziva preokret (*reversal*). Iako ovo u principu nije greška, pojava ovakvih situacija može u značajnoj meri da zakomplikuje proces tumačenja karakteristika dendrograma.

Iz tog razloga, umesto klasterovanja zasnovanog na proračunu centroida, predlaže se metod *Average Clustering* (klasterovanje na osnovu proračuna proseka), poznat kao metod neponderisane grupe parova sa aritmetičkom sredinom (*Unweighted Pair Group Method with Arithmetic Mean*,

UPGMA), koji zadovoljava ultrametričko svojstvo [198], [199]. Ovom metodom rastojanje između dva klastera C_1 i C_2, pri čemu svaki ima n_1 odnosno n_2 instanci, definisano je aritmetičkom sredinom rastojanja $d(x, y)$ između svakog para tačaka podataka, pri čemu je tačka x u C_1 klasteru, a tačka y u C_2 klasteru (relacija 7.6):

$$d(C_1, C_2) = \frac{1}{n_1 \cdot n_2} \sum_{x \in C_1} \sum_{y \in C_2} d(x, y) \tag{7.6}$$

Zapravo, u svakom koraku u procesu klasterovanja vrši se ažuriranje udaljenosti između spojenih klastera C_1 i C_2, dok je novi klaster nastao njihovim spajanjem $C_{1\cup2}$ zadat proporcionalnim usrednjavanjem rastojanja $d_{C_1,C_{1\cup2}}$ i $d_{C_2,C_{1\cup2}}$ (relacija 7.7):

$$d_{C_{1\cup2}} = \frac{n_1 \cdot d_{C_1,C_{1\cup2}} + n_2 \cdot d_{C_2,C_{1\cup2}}}{n_1 + n_2} \tag{7.7}$$

Primenom *Average Clustering* metode, direktno ažuriranje matrice rastojanja izračunavanjem rastojanja između svakog para instanci podataka, u svakom klasteru, bi bilo previše složen i veoma neefikasan postupak. Međutim, pokazalo se da je primenom *Lance-Williams* rekurentne formule ovaj postupak efikasniji, a ovom metodom se ažurira matrica udaljenosti na osnovu udaljenosti izračunatih u prethodnom koraku [174] (odeljak 4.5). U prethodnom koraku, u matrici rastojanja (*distance matrix*) su već bile upisane vrednosti rastojanja između svakog od parova klastera u ovom koraku, uključujući i rastojanja do klastera C_1 i do C_2, na primer $d(C_1, C_x)$ i $d(C_2, C_x)$ za bilo koji od preostalih klastera C_x.

U svrhu profilisanja mrežnog saobraćaja predstavljenog potpisom u *agregiranom skupu podataka inicijalnih klastera* i kombinovanja sa referentnim potpisima modela anomalija, originalni hijerarhijski algoritam aglomerativnog klasterovanja je za potrebe ovog istraživanja modifikovan na sledeći način:

1. Polazna tačka nisu singlton klasteri sa samo jednim elementom, već su to već agregirani inicijalni klasteri sa ukupnim brojem originalnih instanci tokova koji imaju isti potpis.
2. Svaki novoformirani klaster čuva podatke o najvećem pripadajućem inicijalnom klasteru, tzv. dominantnom inicijalnom klasteru i njegovim početnim elementima.
3. Oznaka sa potpisom dominantnog inicijalnog klastera predstavlja odgovarajući superklaster na svakom nivou hierarhije.
4. Relativni doprinos dominantnog inicijalnog klastera u superklasteru je dat odnosom ukupnog broja elemenata u dominantnom inicijalnom klasteru i ukupnog broja svih elemenata u superklasteru.
5. Prvi referentni model anomalije spojen u neki klaster se čuva i prenosi na sve dalje superklastere, predstavljajući najsličniju anomaliju.

8. VALIDACIJA PREDLOŽENOG REŠENJA

Na osnovu modifikovanog hijerarhijskog aglomerativnog algoritma klasterovanja izveden je niz eksperimenata za validaciju predloženog kombinovanog rešenja za detekciju anomalija i napada.

8.1 Istraživanje primenom hijerarhijskog aglomerativnog algoritma

8.1.1 Karakteristike korišćenih skupova podataka

Za potrebe validacije predloženog rešenja korišćena su dva moderna, obeležena, slobodno dostupna skupa podataka, CICIDS2017 i CTU-13, pri čemu je za detaljnu analizu i validaciju rešenja odabrano 4 reprezentativnih, različitih delova ovih skupova:

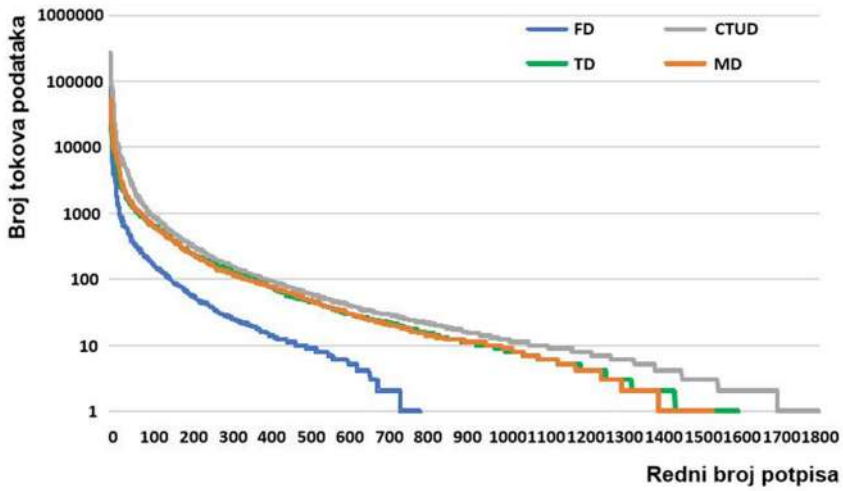
- CICIDS2017, podskup pod oznakom „Monday" (MD), koji obuhvata instance normalnog saobraćaja, bez ijedne instance napada.
- CICIDS2017, podskup pod oznakom „Friday-Afternoon" (FD), koji obuhvata instance mrežnog saobraćaja koje odgovaraju *Port Scan* napadima.
- CICIDS2017, podskup instanci mrežnog saobraćaja označen kao „Tuesday" (TD), a koji obuhvata instance mrežnog saobraćaja koje odgovaraju *FTP-Patator* i *SSH-Patator* napadima.
- CTU-13 skup podataka, scenario 10 (CTUD), koji je zasnovan na podskupu podataka „CTU-Malware-Capture-*Botnet*-51".

Ovi skupovi podataka su detaljno opisani u okviru poglavlja 6. Sve modifikacije nad podacima iz CTU-13 skupa podataka (koje su navedene u okviru odeljka 7.3) se primenjuju i u okviru podataka podskupova koji su korišćeni u okviru ovog dela istraživanja. Dodatne modifikacije, opisane u okviru odeljka 7.4, su takođe primenjene nad skupovima i podskupovima podataka korišćenim u ovom delu istraživanja.

8.1.2 Eksperimentalni rezultati i analiza

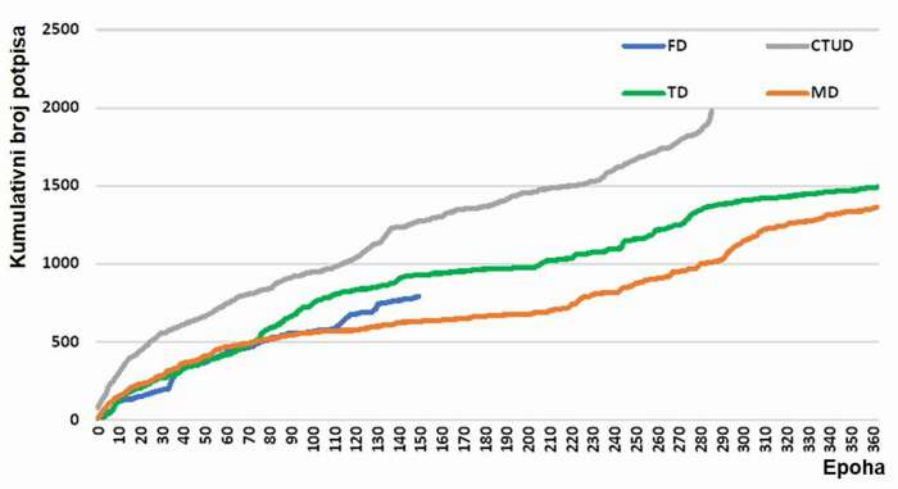
Zadržavajući samo osnovne karakteristike identifikacije toka i koristeći trajanje epohe od 60 sekundi, skupovi podataka se prethodno obrađuju primenom metode koja je predstavljena u odeljku 7.4. Ukupno je generisano 34 novih karakteristika koje su diskretizovane i kombinovane u potpis koji se agregira kako bi se dobili skupovi podataka inicijalnih klastera.

Kada se analiziraju dobijeni skupovi podataka inicijalnih klastera, primetno je da je raspodela pojavljivanja potpisa veoma neujednačena, pri čemu su neki potpisi veoma česti, dok se mnogi drugi pojavljuju samo sporadično. Slika 8.1 prikazuje sortiranu raspodelu broja tokova (y osa) koji odgovaraju različitim potpisima (x osa) za svaki razmatrani skup podataka (vrednosti po x osi predstavljaju internu poziciju potpisa u raspodeli). Čak i u logaritamskoj skali, za svaki od skupova postoji izrazit eksponencijalni pad na početku raspodele.



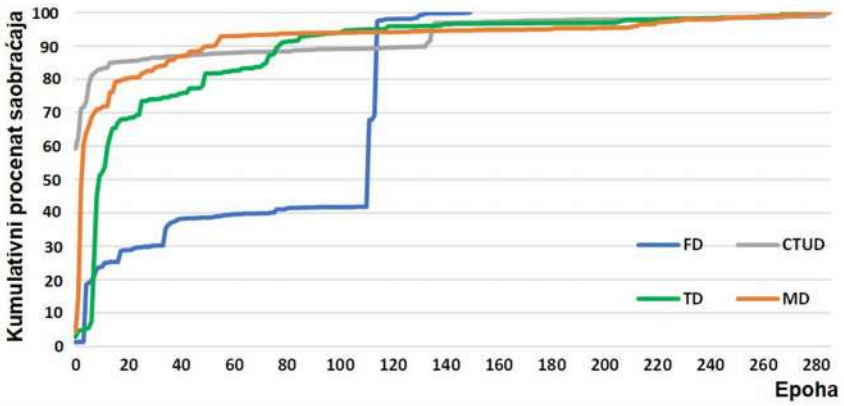
Slika 8.1 Sortirana raspodela broja tokova u zavisnosti od rednog broja potpisa

Na slici 8.2 je prikazana kumulativna suma broja potpisa koji su otkriveni u vremenu (po epohama). S obzirom na to da je skup podataka u vremenu podeljen po epohama, najčešći potpisi će se pojaviti vrlo brzo, već u ranim epohama. Međutim, zbog varijacije saobraćaja, neki potpisi, obično oni koji se ređe pojavljuju, će se javiti i u kasnijim epohama.



Slika 8.2 Kumulativna suma potpisa

Iako se broj potpisa ne zasićuje novim epohama, već postepeno nastavlja da raste u posmatranim periodima od po nekoliko sati, očekuje se da najčešći potpisi praktično obuhvate najveći procenat saobraćaja. Shodno tome, fokusiranjem na potpise koji se otkrivaju tokom epoha i praćenjem kumulativnog procenta ukupnog saobraćaja obuhvaćenog tim potpisima, može se uočiti da se potpisi koji se odnose na većinu podataka pojavljuju veoma brzo (slika 8.3).



Slika 8.3 Kumulativni procenat ukupnog mrežnog saobraćaja pokriven potpisima

Manja povećanja tog broja koja se javljaju u kasnijim epohama su posledica novonastalih komunikacija (pojava novih potpisa) koje su dovoljno intenzivne da budu uočljive. Veći skokovi, kao što je u slučaju skupa podataka FD, rezultat su anomalija ili napada koji generišu veliki broj tokova sa novim šablonom potpisa.

Prethodna analiza dovodi do zaključka da se najčešći potpisi mogu smatrati najrelevantnijim jer odgovaraju najvećem delu saobraćaja. Shodno tome, ređi potpisi se pojavljuju kod manjeg broja komunikacionih tokova, pa se može smatrati da su povezani sa sporadičnim saobraćajem i mogu se tretirati kao vanredni, odnosno irelevantni za dalje profilisanje i analizu.

Zbog toga se uvodi pravilo odsecanja na osnovu percentila (*percentile cutting off rule*), kojim bi se u analizi zadržavali potpisi koji su u skladu sa granicom procenta postavljenom na 95% ili više. Na ovaj način, kao najrelevantniji potpisi biće odabrani oni koji pokrivaju 95% ukupnog saobraćaja, iako predstavljaju manji procenat svih identifikovanih potpisa, što je prikazano u tabeli 8.1.

Tabela 8.1 Raspodela obuhvaćenih potpisa

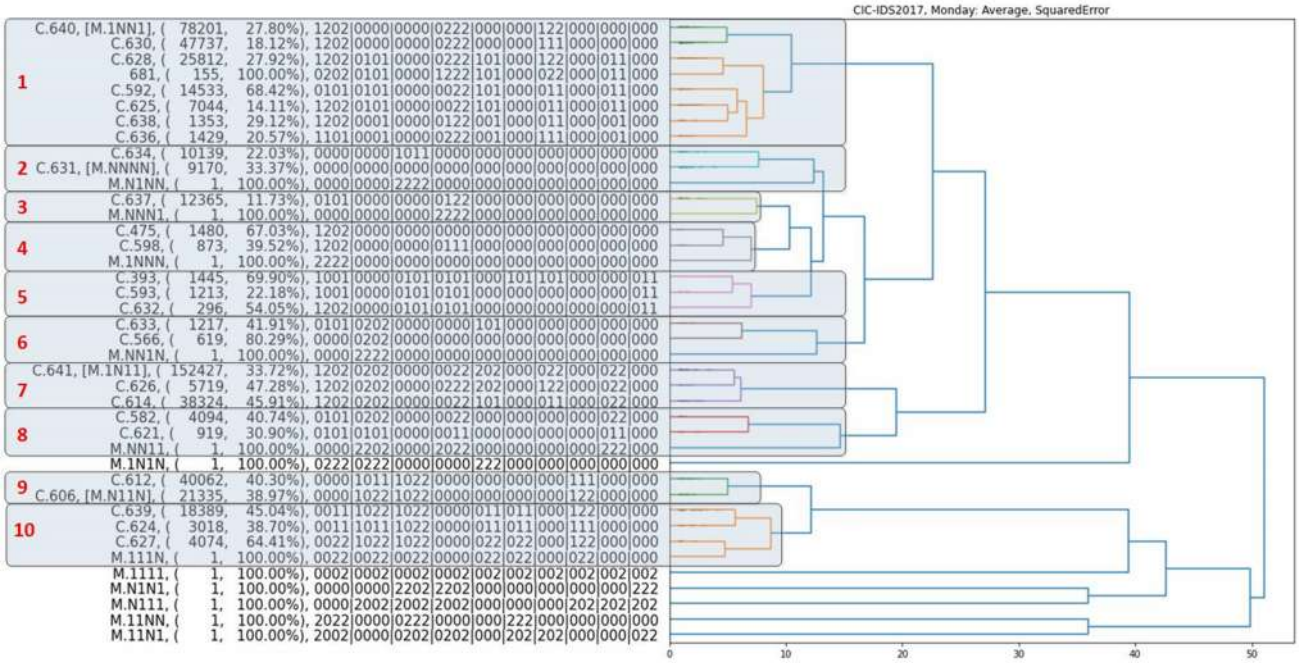
	MD	FD	CTUD	TD	TD(filtriran)
Ukupan broj potpisa	1542	792	1980	1608	153
Potpisi u 95. percentilu	325	138	197	366	71
Potpisi u 95. percentilu (%)	**21.1%**	**17.4%**	**9.9%**	**22.8%**	**46.4%**

Na primer, u slučaju skupa podataka CTU-51, sa ukupno 1980 različitih potpisa, manje od 10% njih (197 potpisa) pokriva više od 95% ukupnog saobraćaja.

Ova procedura na veoma elegantan način postiže dve prednosti. Prvo, broj potpisa je značajno smanjen, što čini hijerarhijsko aglomerativno klasterovanje efikasnijim. Drugo, eliminišu se iz dalje analize irelevantni potpisi izuzetaka (*outlier*), koji se mogu pojaviti kao odvojeni klasteri (tačke) u rezultujućem dendrogramu.

8.1.3 Eksperimentalni rezultati i analiza - CICIDS2017 MONDAY DATASET

Predloženi metod za profilisanje mrežnog saobraćaja je prvobitno primenjen na skupu „Monday" koji predstavlja podskup CICIDS2017 skupa podataka (obeležen na slikama kao MD) i koji obuhvata samo normalan saobraćaj bez napada. Primenom predloženog metoda i modifikovanog algoritma klasterovanja na ovaj skup podataka dobijeni su rezultati u obliku dendrograma sa 40 najviših klastera u hijerarhiji (slika 8.4). Svaki od ovih klastera je označen potpisom dominantnog podklastera, u kombinaciji sa informacijom o ukupnom broju pripadajućih tačaka podataka (tokova) i procentu ovih tokova koji pripadaju dominantnom podklasteru. Vodeća oznaka predstavlja internu identifikaciju klastera, a koja se koristi za dublji uvid u sva prethodna spajanja i podklastere koji se evidentiraju u posebnom fajlu. Ako referentni profil pripada klasteru, njegova oznaka je prikazana u uglastim zagradama, što ukazuje na povezano ponašanje komunikacije (zadržava se samo prvi zajednički referentni profil). Klasteri sa singlton referentnim profilom su označeni imenom referentnog profila.



Slika 8.4 Rezultati klasterovanja za MD skup podataka

Već prvi pogled na predstavljeni dendrogram (slika 8.4) jasno potvrđuje da su najviši klasteri grupisani po sličnosti svojih dominantnih potpisa. Sečenjem grane na rastojanju između 10 i 15 karakteristični klasteri se izdvajaju i grupišu u različite segmente (obeleženo transparentnim pravougaonicima na slici 8.4). Podklasteri koji nisu prikazani na dendrogramu su spojeni u prethodnim koracima sa manjim rastojanjem. Shodno tome, njihovi potpisi su još sličniji, kao što je u slučaju klastera C.640 prikazano na slici 8.5, gde poslednja kolona predstavlja broj tokova svakog potpisa, dok su dominantni potpis i referentna tačka podataka anomalije (1N-N1) podebljani.

Komunikacioni obrazac klastera ekstrahovan u dendrogramu se može analizirati u kontekstu pripadajućeg referentnog profila (ako postoji) i aktiviranih karakteristika u potpisu („1" ili „2"). Međutim, detaljnom analizom zapisa tokova moguće je utvrditi osnovni uzrok (*root analysis*) na

osnovu kojeg se može objasniti ponašanje mrežnog saobraćaja koje se definiše uočenim potpisom. U slučaju skupa podataka MD - CICIDS2017, analizom je moguće izdvojiti sledeće grupe klastera:

1. Referentni profil 1N-N1 iz prve grupe ukazuje na obrazac komunikacije sa malim brojem izvorišnih hostova sa različitim izvorišnim portovima, a koji komuniciraju sa velikim brojem odredišnih hostova i samo nekoliko odredišnih portova. Analizom sirovih podataka jasno je da se dominantni potpis odnosi na komunikaciju koja se ostvaruje između 11 lokalnih hostova sa ukupno oko 3500 Web servera. Zapravo, svaki od ovih 11 hostova radi samostalno, generišući sporadično mrežni saobraćaj u različitim epohama i sa različitim obimima saobraćaja, sve vreme prateći 1N-N1 komunikacioni model.

ID	Model	child Label	Count
C.640	M.1NN1	1202|0000|0000|0222|000|000|122|000|000|000	78201
1416	Data	2202|0000|0000|0222|000|000|122|000|000|000	6586
1412	Data	2202|0000|0000|0122|000|000|122|000|000|000	4339
1417	Data	2202|0000|0000|0222|000|000|222|000|000|000	14576
M.1NN1	Model	**2202|0000|0000|0222|000|000|222|000|000|000**	1
1420	Data	2202|0000|0000|1222|000|000|222|000|000|000	952
1419	Data	2202|0000|0000|1222|000|000|122|000|000|000	348
1111	Data	1202|0000|0000|1222|000|000|122|000|000|000	638
1104	Data	**1202|0000|0000|0222|000|000|122|000|000|000**	21743
1096	Data	1202|0000|0000|0122|000|000|122|000|000|000	12470
1103	Data	1202|0000|0000|0222|000|000|112|000|000|000	4418
1095	Data	1202|0000|0000|0122|000|000|112|000|000|000	3104
1415	Data	2202|0000|0000|0222|000|000|112|000|000|000	493
1411	Data	2202|0000|0000|0122|000|000|112|000|000|000	267
1451	Data	2202|0001|0000|0222|001|000|222|000|001|000	1311
1449	Data	2202|0001|0000|0222|001|000|122|000|001|000	525
1152	Data	1202|0001|0000|0122|001|000|112|000|001|000	581
1150	Data	1202|0001|0000|0122|001|000|111|000|001|000	425
1168	Data	1202|0001|0000|0222|001|000|111|000|001|000	409
1170	Data	1202|0001|0000|0222|001|000|112|000|001|000	394
1438	Data	2202|0001|0000|0122|001|000|122|000|001|000	327
1179	Data	1202|0001|0000|1222|001|000|122|000|001|000	122
1163	Data	1202|0001|0000|0222|000|000|122|000|001|000	207
1172	Data	1202|0001|0000|0222|001|000|122|000|001|000	2205
1154	Data	1202|0001|0000|0122|001|000|122|000|001|000	1760

Slika 8.5 Rezultati klasterovanja za C.640 klaster skupa MD

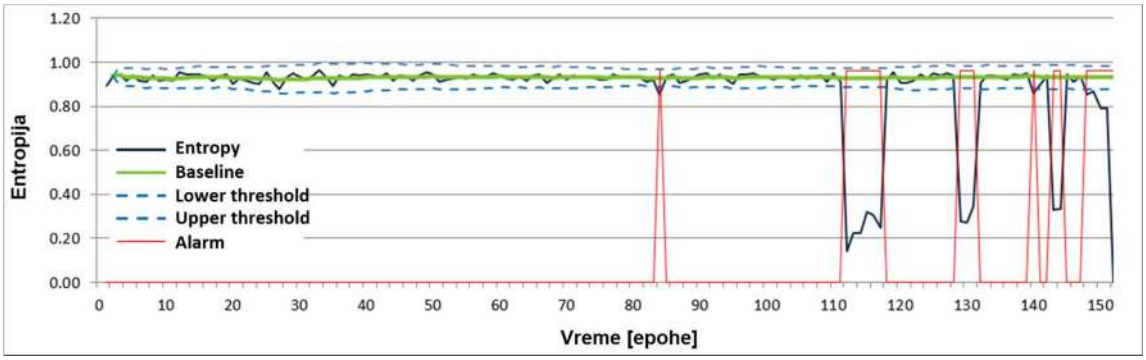
2. Grupa 2 ukazuje na aktivnost koja liči na slanje odgovora sa nekoliko Web servera (897 izvorišnih adresa) ka nekoliko (12) odredišnih adresa, koristeći specifične portove Web servisa kao izvorišne portove (80 i 433) i 2096 različitih odredišnih portova. Jasno je da ovo ponašanje odgovara modelu N1-NN. Ovo ponašanje je suprotno ponašanju identifikovanom u grupi 1 i praktično je isto samo sa obrnutim izvorišnim i odredišnim parametrima, gde su adrese i portovi prethodno detektovani kao izvorišni u ovom slučaju odredišne adrese i portovi. Samim tim, može se zaključiti da se komunikaciono ponašanje uočeno u okviru ove grupe može objasniti eventualnim greškama u procesu dvosmernog uparivanja, gde jednosmerni tokovi nisu bili ispravno upareni. Klaster sa NN-NN modelom i dominantnim potpisom sa svim nulama je u osnovi povezan sa sporadičnim komunikacijama sa samo nekoliko atributa čije su vrednosti *Medium* intenziteta.
3. Grupa 3 prikuplja zahteve nekoliko izvorišnih adresa prema Web serverima (odredišni port 80 i 433), što je isti komunikacioni saobraćaj kao i saobraćaj u grupi 1, ali su u ovom slučaju izvorišni hostovi manje aktivni. Zbog toga su aktivne samo karakteristike agregirane prema odredišnom portu („0122" - četvrti deo u potpisu), što odgovara modelu NN-N1.

4. Grupa 4 se oslanja na mali broj izvorišnih adresa (pojedinačnih izvora koji komuniciraju u različitim vremenima, epohama i različitih su intenziteta), koje imaju komunikaciju sa velikim brojem različitih odredišnih adresa i portova, a komunikacija je opisana 1N-NN modelom.
5. Grupa 5 pokriva periodičnu komunikaciju NTP servera, koja najčešće uključuje 3 različita izvorišna hosta koji s vremena na vreme komuniciraju sa 74 različita odredišna hosta, koristeći i izvorišni i odredišni NTP port broj 123. Shodno tome, odgovarajuće karakteristike u potpisu su sa vrednostima na *Medium* nivou u svim slučajevima kada se odredišna adresa ne koristi u ključu agregacije.
6. Grupa 6 predstavlja tokove mrežnog saobraćaja koji potiču od specifičnih izvorišnih hostova (identifikovano je 13 hostova) prema jednom određenom odredišnom hostu, koristeći veliki broj izvorišnih portova (350 portova) i nekoliko odredišnih portova (do 10). Povezane karakteristike agregirane od strane odredišne adrese imaju vrednosti u *High* opsegu (druga grupa agregacije sa vrednošću „0202"), što odgovara komunikacionom modelu NN-1N.
7. Grupa 7 predstavlja komunikaciju koju ostvaruje 10 različitih izvorišnih hostova koji šalju zahteve ka jednom odredišnom serveru preko DNS odredišnog porta 53. S obzirom na to da je komunikacija intenzivna, komunikacija svakog od ovih izvorišnih hostova pojedinačno spada u 1N-11 model.
8. Slično grupi 7, grupa 8 obuhvata DNS zahteve sa istim izvorišnim adresama i određenim odredišnim hostom. Međutim, broj tokova u odgovarajućim epohama je mnogo manji, a korišćenje izvorišne adrese u ključu agregacije proizvodi odgovarajuće karakteristike čije su vrednosti ispod praga („000" u potpisima), što ovakvu komunikaciju čini sličnom modelu NN-11.
9. Grupa 9 pokriva odgovore velikog broja Web servera (koji deluju kao izvorišni hostovi), uparenih sa izvorišnim brojevima porta 443 ili 80, a koji komuniciraju sa jednim (ili 6, maksimalno u ovom slučaju) odredišnih hostova koji poruke upućuju ka slučajnom, ali velikom broju odredišnih portova (ukupno se koristi 6045 različitih brojeva portova). Ovakav model komunikacije odgovara modelu N1-1N.
10. Grupa 10 pokriva odgovore malog broja Web servera (7 jedinstvenih izvorišnih adresa) sa izvorišnim portom broj 443, ka malom broju odredišnih hostova (2 hosta) koristeći veliki broj nasumično odabranih odredišnih portova (2372 jedinstvenih brojeva portova). Samim tim može da se zaključi da se komunikacija zasniva na modelu 11-1N.

Analiza sirovih podataka pokazuje da ovim skupom podataka dominira Web i DNS saobraćaj koji uglavnom generišu klijenti iz privatne mreže 192.168.10.0/26. Takođe, identifikovan je značajan deo tokova koji za izvorišne brojeve portova koriste 80 i 443, umesto da ih koriste kao odredišne. Zaključak koji bi iz takve situacije mogao da se izvede je da su ti tokovi i komunikacija ostali u skupu podataka kao posledica loše sprovedenog dvosmernog uparivanja prilikom generisanja skupa podataka. Osim toga, brojevi portova za Web servis (80, 443) se kao izvorišni pojavljuju u dve grupe, označene kao 2 i 9, koje su i dalje međusobno veoma „daleke" u okviru generisanog dendrograma. Obe grupe imaju aktivne karakteristike agregirane izvorišnim portom kao ključem (vrednosti „1022" naspram „1122"). U slučaju grupe 9, koriste se samo jedna ili dve odredišne adrese, prateći model N1-1N i aktivirajući funkcije u agregacijama na osnovu odredišnih adresa. S druge strane, komunikacije iz grupe 2 su raspoređene na nekoliko destinacija (N1-NN model) i nijedna od njih nije dovoljno intenzivna da aktivira ostale atribute.

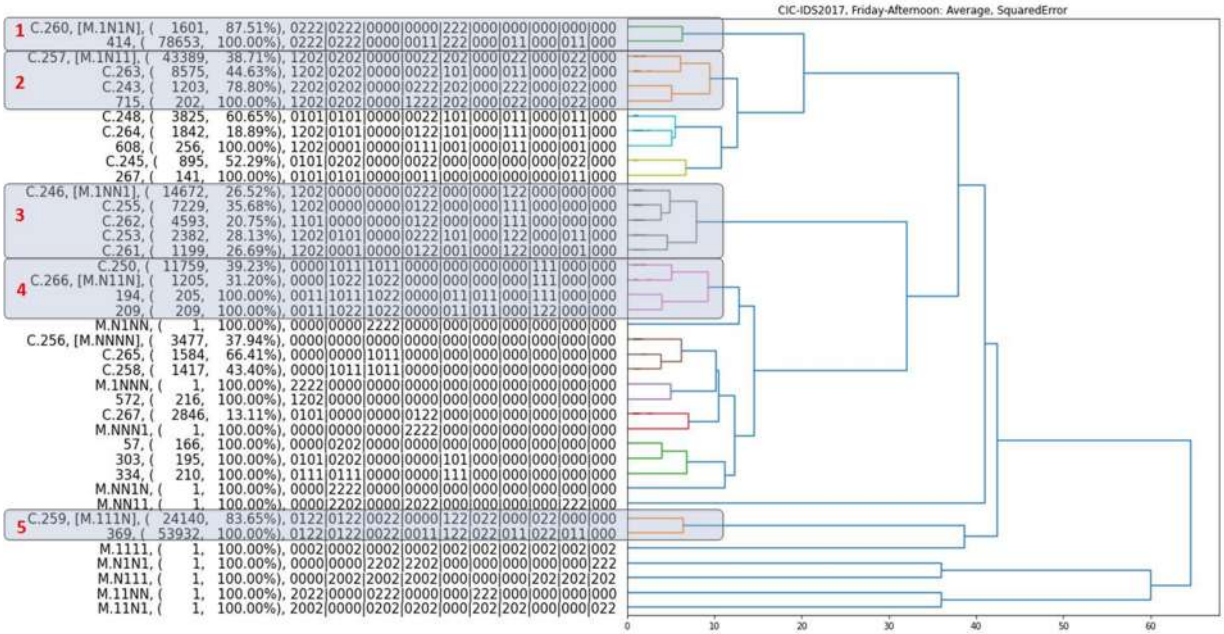
8.1.4 Eksperimentalni rezultati i analiza - CICIDS2017 FRIDAY DATASET

Ovaj skup podataka (FD) sadrži tri serije napada izvedenih skeniranjem portova, što se može primetiti po promenama vrednosti entropije nekih karakteristika ponašanja tokom epoha. Takav je slučaj kada je odredišni port agregiran prema izvorišnoj adresi ($d[S]$), što je prikazano na slici 8.6. Vidi se da je napad započeo u epohi 112, što je u korelaciji sa značajnim skokom na grafiku sa slike 8.6. Tačnije, napad je označen novim potpisom koji pokriva veliku particiju tokova podataka.



Slika 8.6 Entropija odredišnog porta agregiranog izvorišnom adresom, $d[S]$, za FD skup podataka

Primenom predloženog metoda generisano je ukupno 792 potpisa, od kojih se 138 koriste kao najrelevantniji za hijerarhijsko grupisanje, pokrivajući definisanu marginu od 95% celokupnog saobraćaja. Analizirajući dendrogram prikazan na slici 8.7, od interesa su posebno klasteri koji obuhvataju napad skeniranja portova koji se pojavljuje u originalnom skupu podataka.



Slika 8.7 Rezultati klasterovanja za FD skup podataka

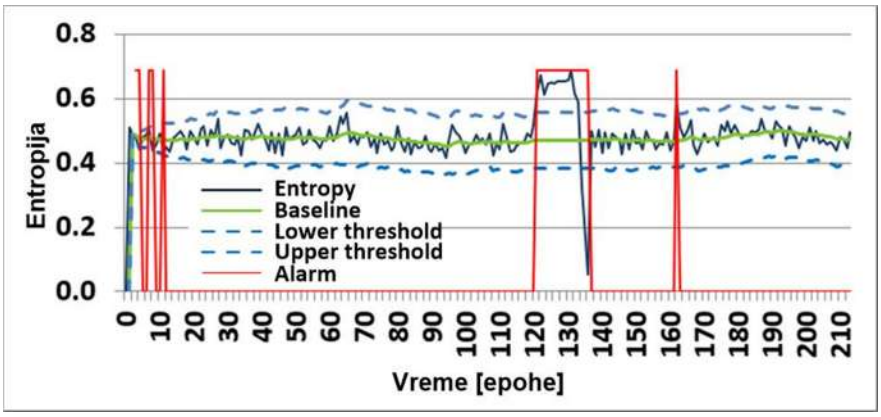
Analizom karakterističnih grupa istaknutih na slici 9.7, može da se primeti sledeće:

1. Grupa 1 je predstavljena komunikacionim modelom 1N-1N, a koji opisuje aktivnost skeniranja portova korišćenjem porta sa slučajnim izvorišnim portom. U okviru detekcije je identifikovana aktivnost dva hosta (sa IP adresama 172.16.0.1 i 192.168.10.50) koji su generisali mrežni saobraćaj koristeći nasumične izvorišne i odredišne portove (1287 izvorišnih i 1391 odredišnih portova), dok je komunikacija sve vreme bila zasnovana na TCP protokolu.
2. Grupa 2 pokriva DNS saobraćaj koji potiče od 9 različitih servera koji komuniciraju sa jednim serverom, koristeći broj odredišnog porta 53. Komunikacija svakog od izvorišnih servera je individualna i ostvaruje se u različitim epohama, tako da ova grupa komunikacionih tokova odgovara modelu komunikacije 1N-11.
3. Grupa 3 obuhvata tokove Web saobraćaja koji potiče od 10 jedinstvenih hostova, koji su aktivni u okviru iste mreže (192.168.10.0/24), a generisani saobraćaj se prosleđuje velikom broju Web servera koristeći odredišni port broj 443. Komunikacija svakog od izvorišnih uređaja se ostvaruje u različitim epohama, tako da prema taksonomiji komunikacionih modela ovaj obrazac ponašanja odgovara referentnom profilu 1N-N1.
4. Grupa 4 predstavlja tokove mrežnog Web saobraćaja koji se zasniva na aktivnosti velikog broja izvorišnih hostova koji koriste izvorišne portove 80 i 443, generišući i prosleđujući saobraćaj ka nekoliko servera (svaki deluje kao posebna odredišna adresa sa tokovima u različitim vremenima i epohama). Za takvu komunikaciju se uređaji služe slučajnim brojem odredišnog porta iz velikog broja odredišnih portova koji se koriste (u ovom slučaju se koristi 4078 odredišnih portova). Ova grupa je najbliža N1-1N referentnom modelu.
5. Grupa 5, slično grupi 1, odgovara napadu skeniranja portova sa istim hostovima ali uglavnom sa fiksnim izvorišnim portom. Referentni komunikacioni profil je 11-1N.

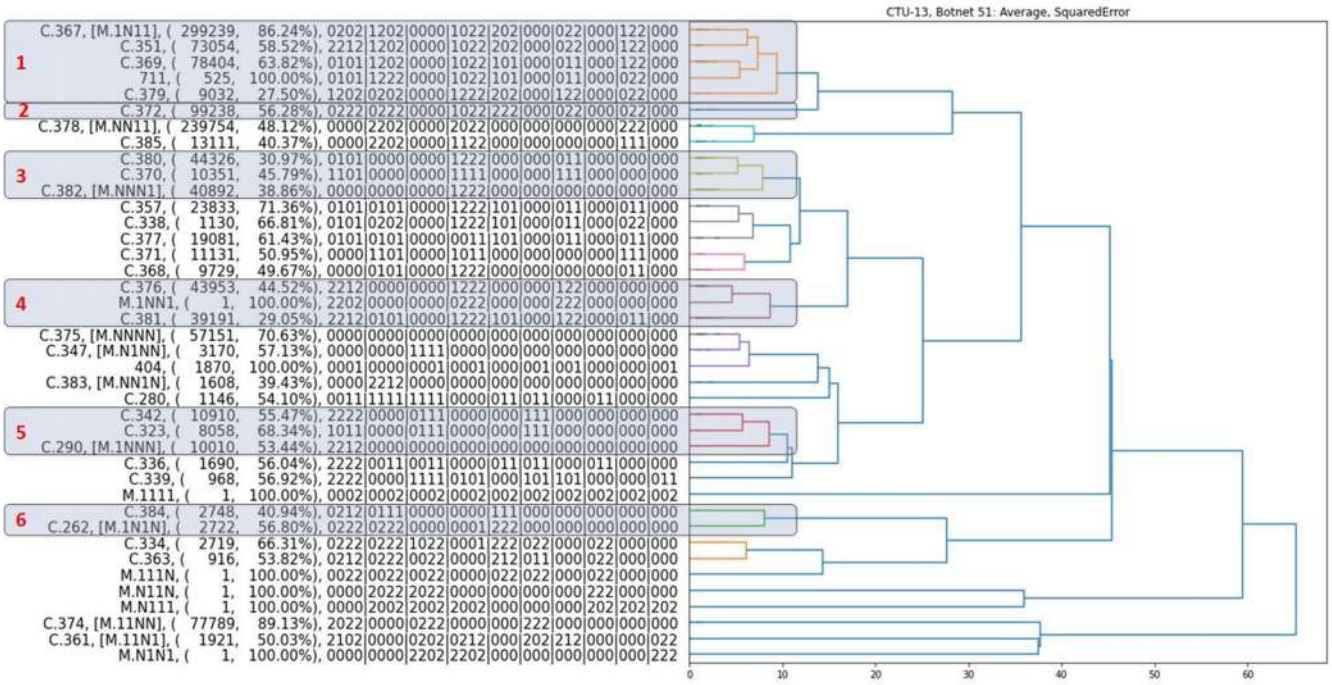
Važno je primetiti da uprkos tome što grupe 1 i 5 odgovaraju napadu skeniranja portova, njihovi potpisi su veoma udaljeni u hijerarhiji dendrograma. Zapravo, jednostavnim poređenjem njihovih potpisa, može se videti da je u grupi 5 više karakteristika čije vrednosti su u *High* nivou („2”), posebno onih koje koriste izvorišni port u ključu agregacije (3., 6. i 8. deo, vezano za *s*, *S.s* i *D.s* agregacione ključeve). Razlika u načinu na koji se koristi izvorišni port (fiksan ili nasumičan) utiče na to da nekoliko atributa kumulativno doprinose unošenju razlika između ovih potpisa, čineći ih udaljenim u dendrogramu.

8.1.5 Eksperimentalni rezultati i analiza – CTU-51 DATASET

Ovaj skup podataka (CTUD) sadrži ICMP *botnet* saobraćaj visokog intenziteta koji se pojavljuje u određenim epohama. Na slici 8.8 je prikazana raspodela entropije za slučaj kada se izvorišni port agregira po odredišnoj adresi. Primećuje se povećanje vrednosti entropije za *s*[*D*] (različiti broj izvorišnog porta po odredišnoj adresi), što je zatim praćeno naglim padom vrednosti. U tim epohama je *botnet* trajao praktično sve vreme i potiskivao regularan mrežni saobraćaj, što je za posledicu imalo poremećaj vrednosti u raspodeli entropije.



Slika 8.8 Entropija izvorišnog porta agregiranog odredišnom adresom, $s[D]$, za CTUD skup podataka



Slika 8.9 Rezultati klasterovanja za CTUD skup podataka

Dendrogram na slici 8.9 ukazuje na 6 specifičnih grupa najsličnijih klastera:

1. Grupa 1 se sastoji od većeg broja instanci DNS zahteva, koji potiču sa 20 servera ka jednom DNS serveru, koristeći nasumične izvorišne brojeve portova (ukupno 3128 portova). Ovo je intenzivna ali istovremeno i regularna DNS komunikacija koja je tačno prepoznata kao komunikacija po modelu 1N-11.
2. Grupa 2 odgovara *botnet* saobraćaju gde se velika količina ICMP paketa šalje sa više izvorišnih adresa na jednu odredišnu adresu (147.32.96.69), koristeći nasumičan broj izvorišnih portova (ukupno 38386) i samo jedan odredišni port, što je u ovom slučaju ICMP kod 0x0000.

3. Grupa 3 obuhvata Web saobraćaj koji potiče iz velikog broja izvora i prosleđuje se ka velikom broju odredišnih hostova, prateći NN-N1 model komunikacije.
4. Grupa 4 se oslanja na jednu specifičnu izvorišnu IP adresu (147.32.84.59), koja koristi nasumični izvorišni port za razmenu Web saobraćaja sa velikim brojem servera (1648 odredišnih adresa), pomoću odredišnog porta broj 80. U skladu sa tim, grupa se može poistovetiti sa referentnim modelom 1N-N1.
5. Grupa 5 odgovara komunikaciji koju ostvaruje jedan veoma aktivan izvorišni host (sa izvorišnom IP adresom 147.32.84.59) sa velikim brojem odredišnih adresa, koristeći različite brojeve portova. Atributi koji se zasnivaju na izvorišnoj adresi kao ključu agregacije su izuzetno visokih vrednosti sa komunikacionim ponašanjem koje je isto ili vrlo slično potpisu 1N-NN komunikacionog modela.
6. Grupa 6 izdvaja ICMP saobraćaj koji se generiše i šalje ka velikom broju odredišnih portova, prateći komunikacioni model 1N-1N. Uključeni su isti hostovi kao u grupi 2, ali ovog puta su aktivni u suprotnom smeru – od jedinstvenog izvorišnog hosta (sa IP adresom 147.32.96.69) ka nekoliko odredišnih adresa. Činjenica da ovi tokovi generišu podatke (bajtove i pakete) samo u pravcu od odredišta do izvora navodi na zaključak da je najverovatnije načinjena greška u procesu transformisanja jednosmernih tokova u dvosmerne.

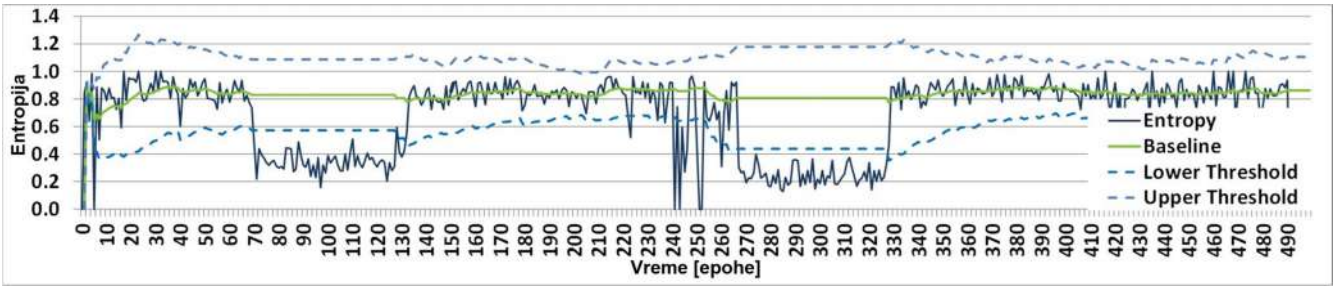
U ovom skupu podataka ICMP *botnet* napad je izolovan u poseban klaster, ali još uvek nije precizno spojen ni sa jednim od referentnih profila. Najsličniji je komunikacionom modelu 1N-11, koji je zajednički grupi 1 sa redovnim saobraćajem. Razlika njihovih potpisa je u karakteristikama koje se odnose na odredišni port u 1., 2. i 5. delu potpisa, koji odgovara agregacionim ključevima *S*, *D* i *S.D*. Ovakva situacija se dešava zbog dela *botnet* saobraćaja koji koristi slučajni broj odredišnog porta, priključujući 1N-1N model dominantnom 1N-11 profilu.

8.1.6 Eksperimentalni rezultati i analiza - CICIDS2017 TUESDAY DATASET

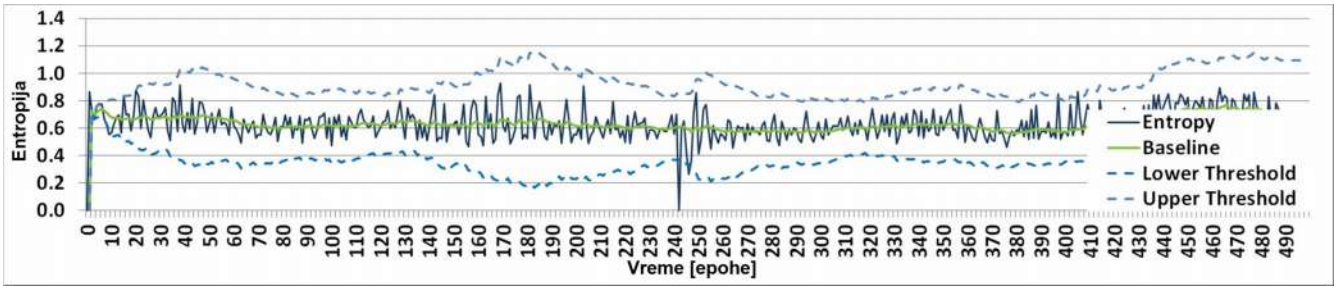
Prethodno predstavljeni rezultati su već pokazali da potpisi generisani predloženom metodom predstavljaju relevantan izvor informacija za proveru sličnosti mrežnog saobraćaja koji se koristi u procesu grupisanja. Pošto su karakteristike koje se koriste u potpisu izvedene iz identifikacionih atributa tokova podataka i njihovog pojavljivanja tokom epoha, očigledno je da se one aktiviraju samo ako je mrežna aktivnost dovoljno intenzivna da se time pređu definisani pragovi. Međutim, u nekim slučajevima to nije dovoljno za otkrivanje i identifikaciju anomalija, posebno onih čiji je komunikacioni profil sličan profilu redovnog mrežnog saobraćaja. Obično se odnosi na komunikaciju klijent-server koja je zadata u skladu sa modelom 1N-11. Tipičan slučaj su DNS i Web usluge, koje predstavljaju ogromnu većinu realnog mrežnog saobraćaja i veliki deo tokova mrežnog saobraćaja sadržanog u analiziranim skupovima podataka. Samim tim, intenzivni mrežni napadi i druge anomalije mogu biti zamaskirani aktivnostima koje odgovaraju redovnim mrežnim aktivnostima i mogu ostati sakriveni u velikom zajedničkom klasteru.

Poznavanje strukture mrežnog saobraćaja daje mogućnost isključivanja uobičajenog saobraćaja koji se odvija kao komunikacija sa pouzdanim hostovima, pod pretpostavkom da je u pitanju regularan mrežni saobraćaj. Ovo ostavlja dovoljno prostora za rad na otkrivanju i izolaciji sumnjivog neregularnog saobraćaja za šta je potrebna posebna analiza. Ovakav pristup, zasnovan na filtriranju saobraćaja je već dokazan primenom metoda zasnovanih na proračunu entropije, a koje se oslanjaju na isti skup karakteristika ponašanja izvedenih iz osnovnih atributa toka [39].

„Tuesday" CICIDS2017 skup podataka (TD) obuhvata napad grubom silom primenom SSH i FTP koristeći se višenamenskim generatorom *brute-force* napada, *Patator*. Kako napad prati model 1N-11, kao i veliki deo tokova saobraćaja koji se odnose na DNS i Web usluge, vrednosti entropije relevantnih atributa karakteristika imaju samo statističku varijaciju, bez značajnih promena koje bi mogle da ukažu na napade (slika 8.10a). Sa druge strane, kada su DNS i Web saobraćaj isključeni, očigledne su promene vrednosti entropije tokom napada (slika 8.10b).



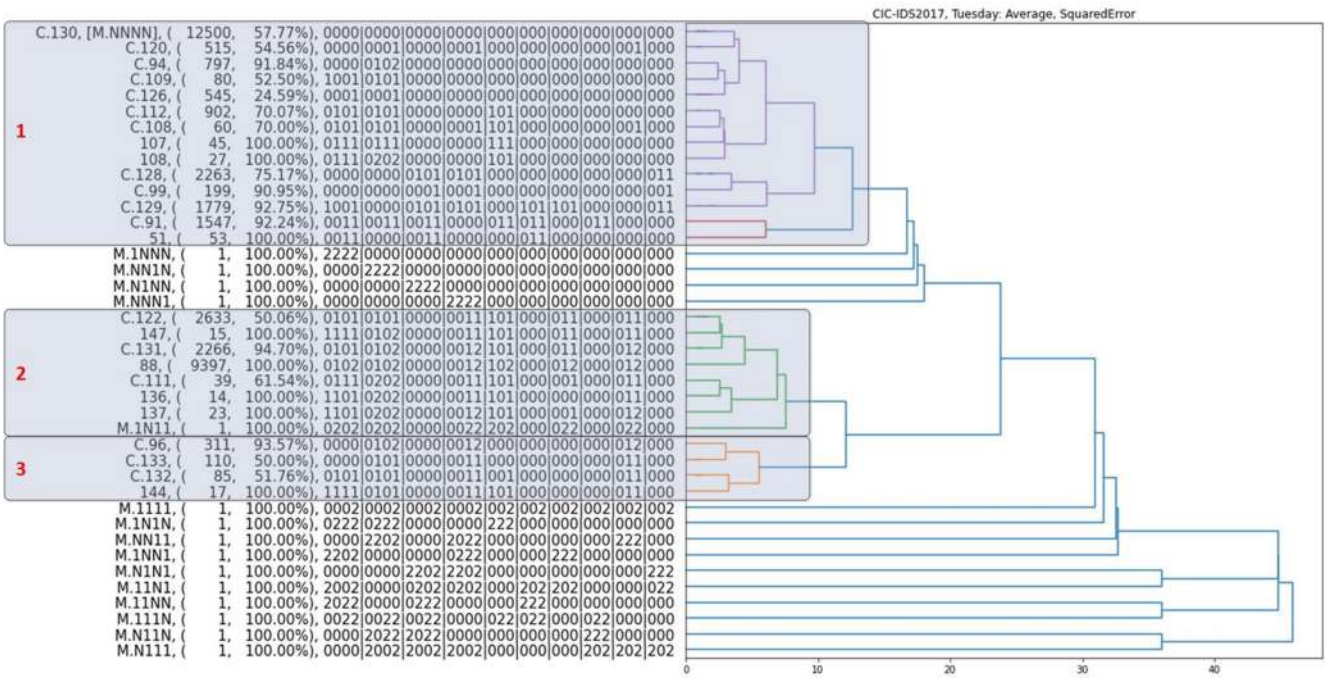
Slika 8.10a Entropija izvorišnog porta agregiranog odredišnom adresom, $s[D]$, za originalni TD skup podataka



Slika 8.10b Entropija izvorišnog porta agregiranog odredišnom adresom, $s[D]$, za redukovani TD skup podataka, bez DNS i Web saobraćaja

Iz istog razloga, radi boljeg profilisanja i analize neregularnog saobraćaja, uključujući *brute-force* napade predstavljene u ovom skupu podataka, uvedeno je filtriranje DNS i SSH saobraćaja, čime se u značajnoj meri smanjila veličina skupa podataka, za više od 90%. U skladu sa tim, ukupan broj potpisa se takođe smanjuje u sličnoj meri, sa 1603 na 153.

Da bi se isključile granične vrednosti, ali i dalje zadržao reprezentativni skup potpisa, u ovom slučaju je primenjen prag od 99 procenta, koji izdvaja ukupno 71 potpis kao skup najrelevantnijih potpisa. Nakon primene algoritma klasterovanja, generisan je dendrogram prikazan na slici 8.11, a u okviru kojeg su izdvojene tri karakteristične grupe klastera.



Slika 8.11 Rezultati klasterovanja za TD skup podataka

1. Grupa 1 obuhvata različit saobraćaj slabijeg intenziteta, većinom bez aktiviranih vrednosti pojedinih atributa (svi atributi u potpisima imaju vrednost 0).
2. Grupa 2 izoluje intenzivan komunikacioni saobraćaj koji se odvija u skladu sa 1N-11 modelom, gde klasteri sa najvećim brojem tokova gotovo bez izuzetka uključuju napad grubom silom na SSH i FTP servere. Jedino klasteri sa malim brojem tokova podataka (ID klastera 111, 136, 137 i 147) obuhvataju normalan saobraćaj generisan primenom Kerberos i LDAP usluga (odredišni port 88 i 389, respektivno), a koji takođe prate komunikacioni model 1N-11.
3. U treću grupu spadaju varijacije različitog redovnog saobraćaja. Obuhvaćeni hostovi su aktivni u drugim komunikacijama što je aktiviralo određene atribute u potpisima, čineći ih sličnim modelu 1N-11.

U ovom slučaju, mnogi referentni profili nisu zajednički sa drugim klasterima podataka zbog odsustva odgovarajućeg saobraćaja u ovom filtriranom skupu podataka sa relativno malim brojem tokova.

8.2 Diskusija dobijenih rezultata analize

Kao što se i očekivalo, predstavljeni dendrogrami prilično smisleno izražavaju sličnost generisanih potpisa, izolujući najsličnije klastere. Sprovedena analiza neobrađenih podataka potvrđuje da izolovani klasteri pouzdano predstavljaju određeni profil ponašanja mrežnog saobraćaja, odnosno obuhvataju tokove mrežnog saobraćaja koji dele isti komunikacioni obrazac.

S obzirom na to da je komunikacijsko ponašanje izraženo potpisima, tačnost ove metode direktno zavisi od toga kako se potpisi generišu i koriste. U predstavljenom istraživanju korišćena je

jednostavna metoda sa fiksnim pragovima za diskretizaciju vrednosti atributa i jednako ponderisanim atributima u funkciji kvadratne greške udaljenosti, ali bez obzira na to, rezultati potvrđuju relevantnost predložene metode za profilisanje saobraćaja.

Prema prikazanim rezultatima i analizi, ističu se sledeći detalji i zaključci:

- Atributi „aktivirani" u potpisu ne zavise samo od odgovarajućeg toka podataka već i od ukupne aktivnosti uključenih hostova i brojeva portova koji su aktivni tokom epoha. Samim tim, potpisi tokova podataka sa sličnim komunikacionim profilima, a koji dele iste atribute u potpisu, i dalje mogu značajno da se razlikuju po vrednostima u nekim drugim atributima.

- Slično tome, neke komunikacijske aktivnosti mogu da se međusobno mešaju tokom epohe, a da rezultujući potpisi budu superpozicija svakog pojedinačnog potpisa tokova koji su bili aktivni. Takav je slučaj sa potpisom ICMP *botnet* saobraćaja, koji je kombinovao 1N-11 i 1N-1N modele.

- Ubačene kontrolne referentne tačke, koje predstavljaju karakteristične modele komunikacija uključujući i anomalije, predstavljaju koristan metod za prepoznavanje osnovnih komunikacionih profila i time u značajnoj meri olakšavaju sveukupnu analizu. Ovo se posebno odnosi na neuobičajene komunikacione tokove mrežnog saobraćaja, a koji često predstavljaju aktivnosti različitih sajber napada i drugih sumnjivih aktivnosti, kao što su skeniranje portova (1N-1N), skeniranje mreže (1N-N1) ili DDoS napadi pojačanjem (N1-11, N1-1N).

- Napadi koji prate uobičajenu komunikaciju klijent-server, opisanu profilom 1N-11, često su maskirani regularnim saobraćajem, koji dominira mrežom. Da bi se otkrile takve aktivnosti predlaže se filtriranje saobraćaja koji potiče sa pouzdanih hostova (hostovi za koje se pouzdano zna da nisu uključeni u bilo kakvu formu napada) i njihovo isključivanje iz daljeg profilisanja.

- Potpisi referentnih profila su generisani sintetičkim saobraćajem visokog intenziteta, na osnovu odgovarajućih komunikacionih modela. Shodno tome, vrednosti atributa u njihovim potpisima su postavljene na visok nivo („2"), dok su vrednosti ostalih atributa na niskom nivou („0"). Neki realan saobraćaj može imati potpis sa istim profilom, ali sa vrednostima atributa na srednjem nivou („1"). Pošto su isti atributi iz različitih agregacionih grupa u korelaciji, njihove diskretne vrednosti se mogu ponoviti. Uprkos sličnom obrascu u potpisima, kumulativna udaljenost je u ovom slučaju veća, što dovodi do neoptimalnog klasterovanja.

- Klasteri sa potpisima anomalije (ili u njihovoj neposrednoj blizini) se primenom ove procedure dalje smatraju anomalijama (odnosno, velika je verovatnoća da je u pitanju napad ili anomalija)

- Osim toga, primenom predloženog rešenja obezbeđena je dodatna efikasnost zasnovana na značajnoj uštedi procesorskih i memorijskih resursa, a koja se zasniva na uvedenom pravilu odsecanja percentila koje ne utiče na visoku pouzdanost i tačnost dobijenih rezultata. Uvođenjem ovakvog pravila u okviru dalje analize i primene modifikovanog hijerarhijskog aglomerativnog algoritma klasterovanja se u analizi zadržavaju samo potpisi koji ispunjavaju uslov postavljen granicom od 95. percentila, odnosno ti se potpisi smatraju relevantnim, iako predstavljaju manji procenat svih identifikovanih potpisa. Tako odabranim potpisima se pokriva značajno manji obim razmatranog mrežnog saobraćaja, dok se analiza čini bržom, efikasnom i primenljivijom za rad u realnom vremenu u realnim mrežnim okruženjima.

9. ZAKLJUČAK

U ovoj disertaciji je na sveobuhvatan način sagledana problematika obezbeđivanja sigurnosti u savremenim mrežnim okruženjima, pri čemu je fokus istraživačkog rada bio na proučavanju problema detekcije napada i anomalija na osnovu tokova mrežnog saobraćaja. Rezultat predstavljenog istraživanja predstavlja predlog nove metode za profilisanje mrežnog saobraćaja zasnovane na obogaćivanju osnovnih podataka o mrežnim tokovima nad kojima se primenjuje unapređeni algoritam nenadgledanog mašinskog učenja, hijerarhijski aglomerativni algoritam klasterovanja.

Kroz različita poglavlja su metodički predstavljeni osnovni teorijski principi na kojima se zasniva predloženo rešenje. Definisane su anomalije i napadi u mrežnom okruženju, pri čemu je dat širi opis karakteristika kategorija napada koje su bile obuhvaćene predstavljenim istraživanjem. U delu koji je posvećen oblasti mašinskog učenja dat je osvrt na najvažnije aspekte razvoja u ovoj oblasti, sa kratkim opisom karakteristika različitih kategorija algoritama, a koje su zadate u skladu sa opštom podelom tehnika mašinskog učenja. Pri tome je posebna pažnja posvećena algoritmima nenadgledanog hijerarhijskog klasterovanja, Expectation-Maximization algoritmu i hijerarhijskom aglomerativnom algoritmu klasterovanja, koji predstavljaju osnov predloženog rešenja sistema detekcije napada i anomalija. Osim toga, u tom delu disertacije je izložen teorijski okvir proračuna karakterističnih funkcija udaljenosti instanci podataka i mera za proračun udaljenosti između klastera.

Zatim su u kratkim crtama predstavljene osnovne karakteristike entropijski zasnovanih metoda, date su osnovne teorijske postavke i ukazano je na njihove prednosti i mane u kontekstu primene u procesu detekcije anomalija i napada.

Posebno poglavlje je posvećeno sistemima detekcije napada i anomalija, obuhvatajući opis njihovih osnovnih karakteristika, namena i kratak opis karakterističnih grupa rešenja. Posebna pažnja je posvećena sistemima zasnovanim na detekciji anomalija (*anomaly-based*), a u specijalnim odeljcima je dat matematički okvir proračuna različitih metrika detekcije anomalija i napada, predstavljene su metode za izbor atributa, kao i metode koje se primenjuju za potrebe skaliranja podataka.

U različitim fazama istraživanja predstavljenog u disertaciji primenjivani su različiti softverski alati i okruženja, a njihov opis, kao i opis osnovnih karakteristika korišćenih skupova podataka, su predstavljeni u posebnom poglavlju. Najvažniji deo disertacije predstavlja predloženo rešenje novog pristupa detekciji napada i anomalija, i to u dve varijante koje su detaljno izložene u posebnom poglavlju. Poseban deo disertacije je posvećen detaljnoj validaciji predloženog rešenja kroz skup različitih eksperimenata.

Eksperimentalna analiza je obuhvatila oba pristupa unapređivanju efikasnosti detekcije anomalija i napada, a koji su se zasnivali na razvoju, primeni i validaciji dve metode nenadgledanog mašinskog učenja: *Expectation–Maximization* algoritma i unapređenog algoritma hijerarhijskog aglomerativnog klasterovanja.

Prvi naučni doprinosi istraživanja su rezultati dobijeni primenom *Expectation-Maximization* algoritma klasterovanja. Rezultati su dobijeni na osnovu primene unapređenog procesa analize i detekcije anomalija primenom nekoliko algoritama klasterovanja i sa posebnim fokusom na EM algoritam. Rezultati su pokazali da se primenom EM algoritma može obezbediti ista ili bolja efikasnost u odnosu na entropijski zasnovane metode, sa smanjenim brojem FP alarma, koji su i dalje slaba tačka entropijskih metoda. Takođe je utvrđeno da je veća efikasnost i jednostavnost rešenja primenom

algoritma klasterovanja zasnovana na njihovoj većoj otpornosti na varijacije vrednosti multiplikativnog faktora *k*, te eliminisanju potrebe da se vrše njegova fina podešavanja, koja su inače neophodna za pravilnu detekciju u okviru entropijski zasnovanih metoda.

Kao jedan od doprinosa ovog dela istraživanja, formiran je i generalizovan koncept agregacije i predložen algoritam koji generiše izvedene karakteristike ponašanja, kako bi se preciznije predstavila struktura mrežnog saobraćaja kada se koriste samo osnovni atributi instanci tokova mrežnog saobraćaja. Na osnovu ovih karakteristika, korišćeno je 16 modela napada, a koji se povezuju sa velikim brojem različitih napada. Definisane karakteristike ponašanja dodeljuju se svakoj instanci podataka, što dalje omogućava njihovu upotrebu od strane bilo kog algoritma nenadgledanog mašinskog učenja. Predstavljeni koncept se primenjuju u okruženju šireg sistema koji funkcionalno obuhvata nekoliko osnovnih modula, među kojima je i deo za primenu algoritama mašinskog učenja.

Rezultati nesumnjivo odražavaju uneta poboljšanja, jer je u mnogim slučajevima algoritam klasterovanja tačno grupisao instance podataka u različiti broj klastera, pri čemu su precizno uzeti u obzir intenzitet i vreme pojavljivanja napada. U opštem slučaju, pretpostavljeno je dinamičko grupisanje entropijski obrađenih podataka, čime je obezbeđeno generisanje različitog broja klastera kojima se preciznije detektuju različite i nepredvidive vrednosti entropije. Time se obezbeđuje pouzdanije izdvajanje specifičnih grupa različitih anomalija, pa i više klastera normalnog ponašanja ukoliko postoje instance koje pripadaju različitim oblicima normalnog ponašanja. Posebna pogodnost ove metode je mogućnost naknadne analize generisanih klastera, unošenje većeg ili manjeg stepena granulacije, kao i naknadne konsolidacije klastera u posebne normalne i abnomalne grupe.

Najvažnije deo predstavljenog istraživanja odnosi se na razvoj originalnog pristupa profilisanja, klasifikacije i detekcije anomalija na nivou pojedinačnih instanci tokova mrežnog saobraćaja primenom unapređenog algoritma hijerarhijskog aglomerativnog klasterovanja. Ovaj algoritam je unapređen primenom posebnih metoda razvijenih i testiranih u Python okruženju, pružajući veću efikasnost, brzinu i preciznost izvršavanja procedure detekcije.

Originalnost predstavljenog pristupa zasniva se na sledećem:

- Predloženo rešenje omogućava da se na osnovu samo osnovnih identifikacionih atributa tokova mrežnog saobraćaja (IP izvorišne i odredišne adrese i izvorišni i odredišni brojevi portova) generišu atributi koji se uobičajeno obezbeđuju primenom entropijski zasnovanih metoda.

- Generisani atributi se zatim diskretizuju kako bi se pojednostavio proces grupisanja. Diskretizovane vrednosti svih atributa se koriste kao poseban „potpis" koji karakteriše strukturu mrežnog saobraćaja i izražava komunikacione aktivnosti toka mrežnih podataka, dok se profilišu najčešći tipovi normalnog mrežnog saobraćaja zajedno sa potpisima tipičnih napada/anomalija.

- Primenom modifikovanog hijerarhijskog aglomerativnog algoritma klasterovanja, koji se zasniva na posebno definisanoj funkciji udaljenosti, grupišu se potpisi zajedno sa unešenim potpisima karakterističnih komunikacionih profila ponašanja mrežnog saobraćaja, uključujući i anomalije prouzrokovane tipičnim sigurnosnim pretnjama, a koji se koriste kao referentni profili. Slični klasteri, sa pripadajućim referentnim profilima se u zavisnosti od definisane

vrednosti praga udaljenosti tumače kao specifični komunikacioni profili za odgovarajuće tokove podataka. Ostvareni rezultati ukazuju na visoku efikasnost predložene metodologije.

- Predloženo rešenje doprinosi optimizaciji parametara i demonstriranjem efikasnosti sprovođenjem niza eksperimenata nad grupom nekoliko različitih savremenih skupova podataka zasnovanih na instancama tokova mrežnog saobraćaja. Rezultati su pokazali da je primenom predloženog rešenja moguće efikasno poređenje tokova mrežnog saobraćaja sa utvrđenim profilima, a zatim da se na osnovu generisanih potpisa pojedinačnih profila, uporednim procesom, vrši izdvajanje novih, prethodno nepoznatih profila u slučajevima kada se pojave nepoznati obrasci ponašanja. Ovakvi profili ukazuju na pojavu neuobičajenih komunikacionih modela koji ukazuju na anomaliju i napad, a koje je predloženo rešenje uspešno detektovalo.

- Predloženo rešenje je generalno i nezavisno od veličine i karakteristika infrastrukture mreže, od obima saobraćaja, tipova anomalija i njihovog intenziteta.

- Predloženo rešenja ima mogućnost praktične implementacije u realnim mrežnim okruženjima i može da obezbedi skalabilnost, proširivost, efikasnost i otpornost na napade.

- U akademskoj literaturi i industrijskoj praksi nije utvrđen sličan pristup. Samim tim, jedan od glavnih doprinosa teze je predstavljanje prvog rešenja koje se oslanja na posebnu proceduru za diskretizaciju vrednosti atributa u okviru instanci podataka, a u cilju dobijanja potpisa specifičnih komunikacionih aktivnosti, koji se koriste u profilisanju i detekciji anomalija.

- Predstavljeni pristup je jedan od retkih koji uspešno kombinuje prednosti entropije i tehnika nenadgledanog mašinskog učenja, dok istovremeno doprinosi razvoju novih pristupa rešavanju problema analize različitih struktura mrežnog saobraćaja. Na ovaj način se profilisanje svakog oblika komunikacije vrši njenim spajanjem u klastere normalnog saobraćaja ili u klastere anomalija, koji se osim profilisanja mogu koristiti i za otkrivanje i klasifikaciju anomalija.

Na osnovu predstavljenih rezultata istraživanja se pokazuje da se primenom metode profilisanja mrežnog saobraćaja omogućava efikasno i precizno detektovanje i razumevanje ponašanja tokova mrežnog saobraćaja tokom određenog perioda. Imajući saznanja o identifikovanim profilima ponašanja moguće je iz daljeg profilisanja da se izdvajaju tokovi saobraćaja koji odgovaraju redovnom mrežnom saobraćaju i koji potiču sa pouzdanih hostova. Time bi se omogućilo rasterećivanje predloženog rešenja u cilju efikasnijeg otkrivanja neobičnih i sumnjivih aktivnosti mrežnog saobraćaja.

Predloženo rešenje omogućava kontinuirano profilisanje mrežnog saobraćaja u skoro realnom vremenu, tokom svake epohe, uparujući novi saobraćaj sa osnovnim profilima ili izdvajajući nove, prethodno nepoznate profile. Pri tome, referentni profili za instance koje odgovaraju neuobičajenim komunikacionim modelima ukazuju na prisustvo anomalije i mogućeg napada. Predloženi metod je izuzetno atraktivan za praktičnu implementaciju u mrežnim okruženjima iz stvarnog života, s obzirom na to da se predložena metoda oslanja samo na analizu osnovnih atributa tokova podataka, a koji se lako obezbeđuju primenom *NetFlow* ili nekog sličnog protokola.

Svi prethodno sprovedeni eksperimenti i prezentovani rezultati potvrđuju ispravnost koncepta (*proof-of-concept*) i ukazuju na izuzetnu primenljivost predložene metode, ostavljajući izvestan prostor za dalja istraživanja i unapređenja rešenja. Neki od potencijalnih pravaca daljeg rada su sledeći:

- Dinamičko postavljanje optimalnih pragova za *Medium* i *High* vrednosti, na nivou svakog posebnog atributa, u zavisnosti od intenziteta saobraćaja.
- Pronalaženje optimalne kombinacije atributa koje bi se koristile u potpisu. U tom smislu, moguće je dodatno istražiti volumetrijski zasnovane atribute (bajtovi i paketi) kako bi se omogućila efikasnija detekcija u slučaju komunikacionih profila zasnovanih na velikim obimima saobraćaja, kao što su DDoS napadi.
- Pronalaženje optimalne funkcije udaljenosti, uzimajući u obzir korelaciju atributa i njenu težinu.
- Proširivanje skupa referentnih profila radi boljeg izdvajanja karakterističnih saobraćajnih profila.

10. LITERATURA

[1] Internet of things forecast, mobility-report 2021, Ericsson Mobility Report, November 2021. Online: https://www.ericsson.com/en/mobility-report/internet-of-things-forecast

[2] European Union Agency for Cybersecurity, *ENISA threat landscape 2021: April 2020 to mid-July 2021,* European Network and Information Security Agency, 2021. Online: https://data.europa.eu/doi/10.2824/324797

[3] *DDoS threat report FHY 2021,* NexusGuard, 2021. Online: https://blog.nexusguard.com/threat-report/ddos-threat-report-fhy-2021

[4] D. E. Denning, „An intrusion-detection model“, *IEEE Trans. on Software Engineering*, vol. SE-13, no. 2, pp. 222-232, 1987. doi: 10.1109/TSE.1987.232894

[5] D. Widhalm, K. M. Goeschka, W. Kastner, „SoK: a taxonomy for anomaly detection in wireless sensor networks focused on node-level techniques“, in *15th Int. Conf. on Availability, Reliability and Security ARES 2020*, 2020. doi: 10.1145/3407023.3407027

[6] H. Debar, „Towards a taxonomy of intrusion detection systems“, *Computer Networks*, vol. 31, no. 8, pp. 805-822, 1999. doi:10.1016/S1389-1286(98)00017-6.

[7] J. McHugh, „Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory“, *ACM Tran. on Information and Syst. Security*, vol. 3, no.4, 2000, pp. 262–294. doi: https://doi.org/10.1145/382912.382923

[8] A. Lazarevich et al., „A comparative study of anomaly detection schemes in network intrusion detection“, in *SIAM Conf. on Data Mining*, 2003. doi: 0.1137/1.9781611972733.3

[9] E. J. Cho, J. H. Kim, C. S. Hong, „Attack model and detection scheme for Botnet on 6LoWPAN“, *APNOMS2009, Lecture Notes in Computer Science*, Springer, Berlin Heidelberg, Germany, 2009, vol. 5787, pp. 515–518. doi: 10.1007/978-3-642-04492-2_66

[10] N. Stakhanova, S. Basu, and J. Wong, „On the symbiosis of specification-based and anomaly-based detection“, *Computers and Security*, vol. 29, no. 2, 2010, pp. 253-268. doi: 10.1016/j.cose.2009.08.007

[11] B. Agarwal, N. Mittal, „Hybrid approach for detection of anomaly network traffic using data mining techniques“, *Procedia Technology*, vol. 6, pp. 996-1003, 2012. doi:10.1016/j.protcy.2012.10.121

[12] M.H. Bhuyan, D.K. Bhattacharyya, J.K. Kalita, „Network anomaly detection: methods, systems and tools“, *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, 2014, pp. 303-336. doi: 10.1109/SURV.2013.052213.00046

[13] A. A. Diro, N. Chilamkurti, „Distributed attack detection scheme using deep learning approach for Internet of Things“, *Future Generation Computer Syst.*, vol. 82, pp. 761–768, 2018. doi: https://doi.org/10.1016/j.future.2017.08.043

[14] A. Khraisat et al., „A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks“, *Electronics*, vol. 8, no. 11, p. 1210, 2019. doi: 10.3390/electronics8111210

[15] E. M. Knorr, R. T. Ng and V. Tucakov, „Distance-based outliers: algorithms and applications“, *The VLDB J.*, vol. 8, no. 3, pp. 237-253, 2000. doi: https://doi.org/10.1007/s007780050006

[16] A. Valdes and K. Skinner, „Adaptive, model-based monitoring for cyber attack detection“, *Int. Workshop on Recent Advances in Intrusion Detection*. Springer, Berlin, Heidelberg, 2000. doi: https://doi.org/10.1007/3-540-39945-3_6

[17] I. Ben-Gal, „Outlier detection“, in *Data Mining And Knowledge Discovery Handbook*, pp. 131-146, 2005. Springer, Boston, MA. doi: https://doi.org/10.1007/0-387-25465-X_7

[18] D. Georgiadis et al., „Continuous outlier detection in data streams: an extensible framework and state-of-the-art algorithms“, in *ACM SIGMOD Int. Conf. on Management of Data*, pp. 1061-1064, 2013. doi: https://doi.org/10.1145/2463676.2463691

[19] M. Gupta et al., „Outlier detection for temporal data: A survey“, *IEEE Trans. on Knowledge and Data Engineering*, vol. 26, no. 9, pp. 2250-2267, 2013. doi: 10.1109/TKDE.2013.184

[20] S. E Benkabou, B. Khalid, and B. Canitia, „Unsupervised outlier detection for time series by entropy and dynamic time warping“, *Knowledge and Information Syst.*, vol. 54, no. 2, pp. 463-486, 2018. doi:10.1007/s10115-017-1067-8

[21] A. Smiti, „A critical overview of outlier detection methods“, *Computer Science Review*, vol. 38, pp. 100306, 2020. doi: https://doi.org/10.1016/j.cosrev.2020.100306

[22] K. Xu, Kuai, Z.-L. Zhang, and S. Bhattacharyya, „Internet traffic behavior profiling for network security monitoring,” *IEEE/ACM Trans. on Netw.*, vol. 16, no. 6, pp. 1241-1252, 2008. doi: 10.1109/TNET.2007.911438

[23] S. Manganaris et al., „A data mining analysis of RTID alarms“, *Computer Networks*, vol. 34, no. 4, pp. 571/577, 2000. doi: https://doi.org/10.1016/S1389-1286(00)00138-9

[24] A. Sperotto et al., „An overview of IP flow-based intrusion detection“, *IEEE Commun. Surveys and Tutorials*, vol. 12, no. 3, pp. 343 – 356, 2010. doi: 10.1109/SURV.2010.032210.00054

[25] B. Li et al., „A survey of network flow applications“, *J. of Netw. and Computer Appl.*, vol. 36, no. 2, pp. 567–581, 2013. doi: 10.1016/j.jnca.2012.12.020

[26] I. Özçelik, and R. R. Brooks, “Deceiving entropy based DoS detection“, *Computers and Security,* vol. 48, pp. 234-245, 2015. doi: 10.1016/j.cose.2014.10.013

[27] S. Gajin and V. Timcenko, „Comparison of entropy-based and machine learning approaches in intrusion detection“, in *11th Int. Conf. Information Society and Technology-ICIST2021*, pp.113-118, 2021. Online: https://www.eventiotic.com/eventiotic/library/paper/651

[28] P. N. Tan et al., *Introduction to Data Mining*, 2nd edition. Pearson Education India, 2019. Online: https://books.google.rs/books?id=_ZQ4MQEACAAJ

[29] M. Ring et al., „A toolset for intrusion and insider threat detection“, *Data analytics and decision support for cybersecurity: trends, methodologies and applications*, Springer, pp. 3-31, 2017. doi:10.1007/978-3-319-59439-2_1

[30] C. Douligeris, A. Mitrokotsa, „DDoS attacks and defense mechanisms: classification and state-of-the-art“, *Computer Networks*, vol. 44, no. 5, pp. 643-666, 2004. doi:10.1016/j.comnet.2003.10.003

[31] J. Wang, I. C. Paschalidis, „Botnet detection based on anomaly and community detection“, *IEEE Trans. on Control of Netw. Syst.*, vol. 4, no. 2, pp. 392-404, 2016. doi: 10.1109/TCNS.2016.2532804

[32] M. Ring, D. Landes, A. Hotho, „Detection of slow port scans in flow-based network traffic“, *PloS one*, vol. 13, no. 9, e0204507, pp. 1–18, 2018. doi:10.1371/journal.pone.0204507.

[33] A. Sperotto et al., „Hidden Markov model modeling of SSH brute-force attacks“, *Int. Workshop on Distributed Syst.: Operations and Management, Springer*, 2009, pp. 164–176. doi:10.1007/978-3-642-04989-7_13.

[34] B. Claise, „Cisco systems netflow services export version 9“, No. RFC 3954. 2004. https://www.hjp.at/doc/rfc/rfc3954.html

[35] M. Ring et al., „A survey of network-based intrusion detection data sets“, *Computers and Security*, vol. 86, pp. 147-167, 2019. doi:10.1016/j.cose.2019.06.005.

[36] H. Liu, M. Cocea, „Granular computing-based approach for classification towards reduction of bias in ensemble learning“, *Granular Computing*, vol. 2, pp. 131-139, 2017. doi 10.1007/s41066-016-0034-1.

[37] M. Antonelli et al., „Multi-objective evolutionary design of granular rule-based classifiers“, *Granular Computing*, vol. 1, no. 1, pp. 37-58, 2016. doi: https://doi.org/10.1007/s41066-015-0004-z

[38] M. A. Wani et al., Advances in deep learning. Studies in Big Data. Vol. 57. Springer, 2020. doi: https://doi.org/10.1007/978-981-13-6794-6

[39] I. Juma, and S. Gajin, „Entropy-based network traffic anomaly classification method resilient to deception“, *Computer Science and Information Syst.*, vol. 19, no.1, pp. 87-116, 2022. doi:10.2298/CSIS201229045I

[40] N. Moustafa, J. Hu, and J. Slay, „A holistic review of network anomaly detection systems: a comprehensive survey“, *J. of Network and Computer Appl.*, vol. 128, pp. 33-55, 2019. doi: 10.1016/j.jnca.2018.12.006

[41] A. Shiravi et al., „Toward developing a systematic approach to generate benchmark datasets for intrusion detection“, *Computers and Security*, vol. 31, no. 3, 2012, pp. 357-374. doi: https://doi.org/10.1016/j.cose.2011.12.012

[42] W. Liu et al., „Future frame prediction for anomaly detection–a new baseline“, in *2018 IEEE/CVF Conf. Computer Vision and Pattern Recognition (CVPR),* pp. 6536-6545, 2018. doi: 10.1109/CVPR.2018.00684

[43] A. Wani, and S. Revathi, „DDoS detection and alleviation in IoT using SDN (SDIoT-DDoS-DA) “, *J. of The Institution of Engineers (India): Series B*, vol. 101, no. 2, pp. 117-128, 2020. doi: https://doi.org/10.1007/s40031-020-00442-z

[44] N. Shone et al., „A deep learning approach to network intrusion detection“, *IEEE Trans. on Emerging Topics in Computational Intell.*, vol. 2, no. 1, pp. 41-50, 2018. doi:10.1109/TETCI.2017.2772792

[45] A. L. H. Muna, N. Moustafa, and E. Sitnikova, „Identification of malicious activities in industrial internet of things based on deep learning models“, *J. of Information Security and Applic.*, vol. 41, 2018, pp. 1-11. doi: 10.1016/j.jisa.2018.05.002

[46] R. B. Basnet et al., „Towards detecting and classifying network intrusion traffic using deep learning frameworks“, *J. of Internet Services and Information Security (JISIS)*, vol. 9, no. 4, 2019, pp. 1-17. doi: 10.22667/JISIS.2019.11.30.001.

[47] H. Hindy et al., „Towards an effective zero-day attack detection using outlier-based deep learning techniques“, *CoRR*, vol. abs/2006.15344, 2020. https://arxiv.org/abs/2006.15344.

[48] B. Tellenbach et al., „Accurate network anomaly classification with generalized entropy metrics“, *Computer Networks*, vol. 55, no. 1, 2011, pp. 3485-3502, 2011. doi: 10.1016/j.comnet.2011.07.008

[49] V. Timcenko, S. Gajin, „Time-series entropy data clustering for effective anomaly detection“, in *10th Int. Conf. Information Society and Technology – ICIST2020*, pp. 170-175, 2020. Online: https://www.eventiotic.com/eventiotic/library/paper/608

[50] P. Berezinski, B. Jasiul, M. Szpyrka, „An entropy-based network anomaly detection method“, *Entropy*, vol. 17, no. 4, pp. 2367–2408, 2015. doi: doi.org/10.3390/e17042367

[51] A. Rényi, „On measures of entropy and information“, in *4th Berkeley Symp. Math. Statistics and Probability*, *Volume 1: Contributions to the Theory of Statistics,* vol. 1, pp. 547–561, 1961.

[52] C. Tsallis, „Possible generalization of Boltzmann–Gibbs statistics“, *J. of Statistical Physics*, vol. 52, no. 1-2, pp. 479–487, 1988. doi: 10.1007/BF01016429

[53] M. Ring et al., „Creation of flow-based data sets for intrusion detection“, *J. of Information Warfare (JIW)*, vol. 16, Issue 4, pp. 40-53, 2017. Online: https://www.jstor.org/stable/26504117.

[54] A. Sperotto et al., „A labeled data set for flow-based intrusion detection“, *9th IEEE Int. Workshop IP Operations and Management, IPOM 2009*, Springer, vol. 5843, pp. 39-50, 2009. doi:10.1007/978-3-642-04968-2_4.

[55] P. Winter, E. Hermann, M. Zeilinger, „Inductive intrusion detection in flow-based network data using one-class support vector machines“, in *4th IFIP Int. Conf. on New Technologies, Mobility and Security*, pp. 1-5, 2011. doi:10.1109/NTMS.2011.5720582

[56] N. Moustafa, and J. Slay, „The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set“, *Information Security J.: A Global Perspective*, vol. 25, no. 1-3, pp. 18-31, 2016. doi: https://doi.org/10.1080/19393555.2015.1125974

[57] S. García, *Malware capture facility project*, CVUT University. Dataset CTU-Malware-Capture-Botnet-1, 2013. Online: https://mcfp.weebly.com/mcfp-dataset.html

[58] S. García et al., „An empirical comparison of botnet detection methods“, *Computers and Security J.*, vol. 45, pp. 100-123, 2014. doi: 10.1016/j.cose.2014.05.011

[59] O. Yavanoglu, and M. Aydos, „A review on cyber security datasets for machine learning algorithms“, in *IEEE Int. Conf. Big Data (Big Data)*, 2017, pp. 2186-2193. doi:10.1109/BigData.2017.8258167

[60] S. Panwar, Y.P. Raiwani, and L.S. Panwar, „Evaluation of network intrusion detection with features selection and machine learning algorithms on CICIDS-2017 dataset“, in *Int. Conf. Advances in Engineering Science Management & Technology (ICAESMT), 2019*. doi: http://dx.doi.org/10.2139/ssrn.3394103

[61] Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, „Toward generating a new intrusion detection dataset and intrusion traffic characterization“, in *4th Int. Conf. Information Syst. Security and Privacy (ICISSP)*, vol.1, pp. 108-116, 2018. doi: 10.5220/0006639801080116

[62] A. Yulianto, P. Sukarno, and N. A. Suwastika, „Improving adaboost-based intrusion detection system (IDS) performance on CIC IDS 2017 dataset“, in *J. of Physics: Conf. Series*, IOP Publishing, vol. 1192, no. 1, p. 012018, 2019. doi: 10.1088/1742-6596/1192/1/012018

[63] M. Antonakakis, et al., „Understanding the Mirai Botnet This paper is included in the Proceedings of the Understanding the Mirai Botnet“, in 26th USENIX security symposium (USENIX Security 17), pp. 1093–1110, 2017. Online: https://ericberthomier.fr/IMG/pdf/sec17-antonakakis.pdf

[64] H. Bostani, S. Sheikhan, „Hybrid of anomaly-based and specification-based IDS for internet of things using unsupervised OPF based on MapReduce approach“, *Computer Commun.*, vol. 98, pp. 52-71, 2017. doi:10.1016/j.comcom.2016.12.001

[65] A. Rehman, S. Tanzila, „Evaluation of artificial intelligent techniques to secure information in enterprises," *Artif. Intell. Review*, vol. 42, no. 4, pp. 1029-1044, 2014. doi:10.1007/s10462-012-9372-9.

[66] G. Peters, R.Weber, „DCC: A framework for dynamic granular clustering", *Granular Computing*, vol. 1, no. 1, pp. 1-11, 2016. doi:10.1007/s41066-015-0012-z

[67] A. Lakhina, M. Crovella, and C. Diot, „Mining anomalies using traffic feature distributions", *ACM SIGCOMM Computer Commun. Review*, vol. 35, no. 4, pp. 217-228, 2005. doi/pdf/10.1145/1080091.1080118

[68] A. Fahad et al., „A survey of clustering algorithms for big data: taxonomy and empirical analysis," *Trans. Emerging Topics in Computing*, vol. 2, pp. 267-279, 2014. doi: 10.1109/TETC.2014.2330519

[69] M.R. Ackermann et al., „Streamkm++: a clustering algorithm for data streams", *J. of Experimental Algorithmics*, vol. 17, no. 1, pp. 2–4, 2012. doi: https://doi.org/10.1145/2133803.2184450

[70] T. Zhang, R. Ramakrishnan, and M. Linvy, „BIRCH: an efficient method for very large databases", in *ACM SIGMOD Int. Conf. on Management of Data*, ACM, vol. 25, no. 2, pp. 103-114, 1996. doi: https://doi.org/10.1145/235968.233324

[71] S. Guha, R. Rastogi, and K. Shim, „CURE: an efficient clustering algorithm for large databases", *Information Syst.*, vol. 26, no. 1, pp. 35-58, 2001, doi: https://doi.org/10.1016/S0306-4379(01)00008-4

[72] R. Cai et al., „A general framework of hierarchical clustering and its applications", *Information Sciences*, vol. 272, pp. 29-48, 2014. doi: https://doi.org/10.1016/j.ins.2014.02.062

[73] D. Steinley, „K-means clustering: a half-century synthesis", *British J. of Math. and Statistical Psychology*, vol. 59, no. 1, pp.1-34, 2006. doi:10.1348/000711005X48266

[74] D. Beeferman, and A. Berger, „Agglomerative clustering of a search engine query log", in *6th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data mining*, pp. 407-416, 2000. doi: https://doi.org/10.1145/347090.347176.

[75] W. Zhang, D. Zhao, and X. Wang, „Agglomerative clustering via maximum incremental path integral", *Pattern Recognition*, vol. 46, pp. 3056-3065, 2013. doi: https://doi.org/10.1016/j.patcog.2013.04.013

[76] A. Saxena et al., „A review of clustering techniques and developments", *Neurocomputing*, vol. 267, pp.664-681, 2017. doi: https://doi.org/10.1016/j.neucom.2017.06.053

[77] X. Peng et al., „Constructing the l2-graph for robust subspace learning and subspace clustering", *IEEE Trans. on Cybernetics*, vol. 47, no. 4, pp. 1053-1066, 2017. doi: 10.1109/TCYB.2016.2536752

[78] K.C. Gowda, and G. Krishna, „Agglomerative clustering using the concept of mutual nearest neighbourhood", *Pattern Recognition*, vol. 10, no. 2, pp. 105-112, 1978. doi: https://doi.org/10.1016/0031-3203(78)90018-3

[79] I. Davidson, and S. S. Ravi, „Agglomerative hierarchical clustering with constraints: Theoretical and empirical results", in *9th European Conf. on Principles and Practice of Knowledge Discovery in Databases*, 2005, Springer, Berlin, Heidelberg, pp. 59-70, 2005. Online: https://link.springer.com/chapter/10.1007/11564126_11

[80] D. Müllner, „Modern hierarchical, agglomerative clustering algorithms", *Statistics, Machine Learning*, Cornell university, 2011. arXiv preprint arXiv:1109.2378.

[81] A. Bouguettaya et al., „Efficient agglomerative hierarchical clustering“, *Expert Syst. with Appl.*, vol. 42, no.5, pp. 2785-2797, 2015. doi: https://doi.org/10.1016/j.eswa.2014.09.054

[82] W. Kim, A. Kanezaki, and M. Tanaka, „Unsupervised learning of image segmentation based on differentiable feature clustering“, *IEEE Trans. on Image Process.*, vol. 29, pp. 8055-8068, 2020. Doi: https://doi.org/10.1109/TIP.2020.3011269

[83] P. Yildirim, and D. Birant, „K-linkage: A new agglomerative approach for hierarchical clustering“, *Advances in Electrical and Computer Engineering*, vol. 17, no. 4, pp. 77-88, 2017. doi:10.4316/AECE.2017.04010

[84] L. R. Emmendorfer, „An empirical evaluation of two novel linkage criteria for hierarchical agglomerative clustering“, in *8th IEEE Brazilian Conf. on Intelligent Syst. (BRACIS)*, pp. 622-626, 2019. doi: 10.1109/BRACIS.2019.00114

[85] J.Z. Lai, and T. Huang, „An agglomerative clustering algorithm using a dynamic k-nearest-neighbor list“, *Information Sciences*, vol. 181, no. 9, pp. 1722–1734, 2011. doi: https://doi.org/10.1016/j.ins.2011.01.011

[86] F. Murtagh, P. Legendre, „Ward's hierarchical agglomerative clustering method: which algorithms implement ward's criterion?“, *J. of Classification*, vol. 31, pp. 274–295, 2014. doi: https://doi.org/10.1007/s00357-014-9161-z

[87] Z. Cai et al., „A new similarity combining reconstruction coefficient with pairwise distance for agglomerative clustering“, *Information Sciences*, vol. 508, pp. 173-182, 2020. doi: https://doi.org/10.1016/j.ins.2019.08.048

[88] S. Kwon and C. Han, „Hybrid clustering method for DNA microarray data analysis“, *Genome Informatics*, vol. 13, pp. 258-259, 2002, doi: https://doi.org/10.11234/gi1990.13.258

[89] E. Y. Cheu, C. Keongg, and Z. Zhou, „On the two-level hybrid clustering algorithm“, in *AISAT Int. Conf. on Artif. Intell. in Science And Technology*, pp. 138–142, 2004.

[90] G. Cabanes and Y. Bennani, „A simultaneous two-level clustering algorithm for automatic model selection“, *6th Int. Conf. on Machine Learning and Appl.*, 2007, pp. 316-321, doi: 10.1109/ICMLA.2007.71.

[91] G. Thatte, U. Mitra, and J. Heidemann, „Parametric methods for anomaly detection in aggregate traffic“, *IEEE/ACM Trans. Netw.*, vol. 19, no. 2, pp. 512-525, 2010. doi: 10.1109/TNET.2010.2070845

[92] H. Hindy et al., „Utilising deep learning techniques for effective zero-day attack detection“, *Electronics*, vol. 9, no. 10, pp.1684, 2020. doi: 10.3390/electronics9101684

[93] J. Song et al., „Statistical analysis of honeypot data and building of Kyoto 2006+ dataset for NIDS evaluation“, in *ACM 1st Workshop On Building Analysis Datasets and Gathering Experience Returns for Security*, pp. 29-36, 2006. doi: https://doi.org/10.1145/1978672.1978676

[94] M. Tavallaee et al., „A detailed analysis of the KDD CUP 99 data set,” *2009 IEEE Symp. Computational Intell. for Security and Defense Appl.*, pp. 1-6, 2009. doi:10.1109/CISDA.2009.5356528

[95] N. Moustafa, J. Slay, „UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) “, in *2015 Military Commun. and Information Syst. Conf. (MilCIS)*, pp. 1-6, 2015. doi: 10.1109/MilCIS.2015.7348942

[96] N. Moustafa, and J. Slay, „The significant features of the UNSW-NB15 and the KDD99 data sets for network intrusion detection systems“, in *IEEE 4th Int. Workshop On Building Analysis Datasets And Gathering Experience Returns For Security (BADGERS)*, pp. 25-31, 2015. doi: 10.1109/BADGERS.2015.014

[97] M. K. Marhas, A. Bhange, and P. Ajankar, „Anomaly detection in network traffic: A statistical approach“, *Int. J. of IT, Engineering and Applied Sciences Research (IJIEASR)*, vol. 1, no. 3, 2012, pp. 16-20.

[98] M. Ahmed, A.N. Mahmood, J. Hu, „A survey of network anomaly detection techniques“, *J. of Netw. and Computer Applic.*, vol. 60, 2016, pp. 19-31. doi: https://doi.org/10.1016/j.jnca.2015.11.016

[99] D. M. Hawkins, *Identification of outliers*, in series *Monographs on Applied Probability and Statistics*, vol. 11, London, Chapman and Hall, 1980. doi: https://doi.org/10.1007/978-94-015-3994-4

[100] K. Scarfone and P. Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-94, Gaithersburg, MD 20899-8930, 2007. Online: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50951

[101] S. Boštjančič Rakas et al., „Detekcija sajber napada u inteligentnim elektroenergetkim sistemima“, Zbornik radova 35. Savetovanja CIGRÉ Srbija, pp. R D2 13 (1-8), 2021.

[102] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, and Q. Wu, “AVOIDIT: A cyber attack taxonomy“, in *9th Annual Symp. Information Assurance*, pp. 2-12, 2014

[103] M. Rabbani et al., „Review on machine learning approaches for network malicious behavior detection in emerging technologies“, *Entropy*, 2021, vol. 23, no. 5, p.529. doi: https://doi.org/10.3390/e23050529

[104] S. Bellovin, „Security problems in the TCP/IP protocol suite“, *Computer Commun. Review*, vol. 19, no. 2, pp. 32–48, 1989. doi: https://doi.org/10.1145/378444.378449

[105] J. Mirkovic, P. Reiher, „A taxonomy of DDoS attack and DDoS defense mechanisms“, *ACM SIGCOMM Computer Commun. Review*, vol. 34, no. 2, pp. 39-53, 2004. doi: 10.1145/997150.997156.

[106] S. M. Specht and R. B. Lee, „Distributed denial of service: taxonomies of attacks, tools, and countermeasures“, in *17th Int. Conf. on Parallel and Distributed Computing Syst., 2004 Int. Workshop on Security in Parallel and Distributed Syst.*, pp. 543-550, 2004.

[107] M. de Vivo, E. Carrasco, G. Isern, G. O. de Vivo, „A review of port scanning techniques“, *ACM SIGCOMM Computer Commun. Review*, vol. 29. no. 2, pp. 41-48, 1999. doi: https://doi.org/10.1145/505733.505737

[108] C. Leckie, R. Kotagiri, „A probabilistic approach to detecting network scans“, in *NOMS 2002. IEEE/IFIP Netw. Operations and Management Symp.*, *Management Solutions for the New Commun. World,* Cat. No. 02CH37327, pp. 359-372, 2002. doi: 10.1109/NOMS.2002.1015594

[109] S. Jajodia, S. Noel, B. O’Berry, „Topological analysis of network attack vulnerability“, in *Managing Cyber Threats. Massive Computing*, vol 5, 2005. Springer, Boston, MA. https://doi.org/10.1007/0-387-24230-9_9

[110] M. H. Bhuyan, D. K. Bhattacharyya, J. K. Kalita, „Surveying port scans and their detection methodologies“, *The Computer J.*, vol. 54, no. 10, pp. 1565-1581, 2011. doi: https://doi.org/10.1093/comjnl/bxr035

[111] A. Webster et al., „An improved method for anomaly-based network scan detection“, *Security and Privacy in Commun. Syst.*, Springer, Cham, vol. 164, pp. 385-400, 2015. doi:10.1007/978-3-319-28865-9_21.

[112] D. Stiawan, „Investigating Brute Force Attack Patterns in IoT Network,” *Hindawi J. Electrical and Computer Engineerin*g, vol. 2019, Art.ID 4568368, 2019. doi.org/10.1155/2019/4568368

[113] T. M. Mitchell, „Machine Learning“, McGraw-Hill Science/Engineering/Math, March 1997, ISBN: 0070428077
[114] T. M. Mitchell, „Machine learning and data mining“, Communications of the ACM 42.11 (1999): 30-36. doi: https://doi.org/10.1145/319382.319388
[115] S. B. Kotsiantis, I. Zaharakis, P. Pintelas, „Machine learning: a review of classification and combining techniques“, *Artif. Intell. Review*, vol. 26, no. 1, pp. 159-190. Springer, 2006. doi: https://doi.org/10.1007/s10462-007-9052-3.
[116] L. Zhou et al., „Machine learning on big data: Opportunities and challenges“, *Neurocomputing*, vol. 237, pp. 350-361, 2017. doi: https://doi.org/10.1016/j.neucom.2017.01.026
[117] D. P. Kumar, T. Amgoth, and C. S. R. Annavarapu, „Machine learning algorithms for wireless sensor networks: A survey,” *Information Fusion*, vol. 49, pp. 1-25, 2019.
[118] M. Usama et al., „Unsupervised machine learning for networking: Techniques, applications and research challenges“, *IEEE Access*, vol. 7, 2019, pp. 65579-65615. doi: 10.1109/ACCESS.2019.2916648
[119] U. A. Butt et al., „A review of machine learning algorithms for cloud computing security“, *Electronics*, vol. 9, no. 9, pp. 1379, 2020. doi: https://doi.org/10.3390/electronics9091379
[120] J.E. van Engelen, and H. H. Holger, „A survey on semi-supervised learning“, *Machine Learning*, vol. 109, no.2, 2020, pp. 373-440. doi: https://doi.org/10.1007/s10994-019-05855-6.
[121] L. P. Kaelbling, M. L. Littman, and A. W. Moore, „Reinforcement learning: A survey“, *J. of Artificial Intelligence Researc*h, vol. 4, no. 1, 1996, pp. 237-285. doi: 10.1613/jair.301.
[122] Z. H. Zhou, „Ensemble Learning“, *Machine Learning*, Springer, Singapore, pp. 181-210, 2021. doi: https://doi.org/10.1007/978-981-15-1967-3_8
[123] V. Timčenko, S. Gajin, „Ensemble classifiers for supervised anomaly based network intrusion detection“, in *IEEE Int. Conf. Intelligent Computer Commun. and Process. ICCP2017*, 2017, doi: 10.1109/ICCP.2017.8116977
[124] J. Mallick et al., „A novel classifier for improving wetland mapping by integrating image fusion techniques and ensemble machine learning classifiers“, *Ecological Informatics*, vol. 65, 2021, pp. 101426. doi: https://doi.org/10.1016/j.ecoinf.2021.101426
[125] V. Timčenko, S. Gajin, „Machine learning based network anomaly detection for IoT environments“, in *8th Int. Conf.Information Society and Technology – ICIST2018*, pp. 196 – 201, 2018. Online: https://www.eventiotic.com/eventiotic/library/paper/410
[126] Y. Dodge, The Concise Encyclopedia of Statistics, Springer, 2008
[127] D. C. Montgomery, E. A. Peck i G. G. Vining, Introduction to linear regression, analysis, 5th edition, John Wiley & Sons, 2012.
[128] L. Rokach, M. Oded, „Decision trees“, *Data Mining and Knowledge Discovery Handbook*, Springer, Boston, MA, 2005, pp. 165-192. doi: https://doi.org/10.1007/b107408
[129] C. M. Bishop, „Neural networks for pattern recognition“, *Oxford university press*, 1995.
[130] O. I. Abiodun et al., „State-of-the-art in artificial neural network applications: A survey“, *Heliyon*, vol. 4, no. 11, e00938, 2018. doi: https://doi.org/10.1016/j.heliyon.2018.e00938
[131] T. S. Pooja, and S. Purohit, „Evaluating neural networks using bi-directional LSTM for network IDS (Intrusion Detection Systems) in cyber security“, *Global Transitions Proc.*, vol. 2, no. 2, pp. 448-454, 2021. doi: https://doi.org/10.1016/j.gltp.2021.08.017
[132] S. Barzut et al., „A novel fingerprint biometric cryptosystem based on convolutional neural networks“, *Mathematics*, vol. 9, no. 7, pp. 730, 2021. doi: https://doi.org/10.3390/math9070730.

[133] M. Belgiu, L. Drăguţ, „Random forest in remote sensing: A review of applications and future directions“, *ISPRS J. of Photogrammetry And Remote Sensing*, vol. 114, pp. 24-31, 2016. doi: https://doi.org/10.1016/j.isprsjprs.2016.01.011

[134] G. Biau, E. Scornet, „A random forest guided tour“, *Test*, vol. 25, no. 2, pp. 197-227, 2016. doi: https://doi.org/10.1007/s11749-016-0481-7

[135] A. Darwiche, „Bayesian Networks“, *Handbook of Knowledge Representation, Foundations of Artificial Intelligence*, Frank Van Harmelen, Vladimir Lifschitz and Bruce Porter (Eds.), Elsevier, Amsterdam, vol. 3, pp. 467-499, 2008. doi: https://doi.org/10.1016/S1574-6526(07)03011-8.

[136] O. Kramer, „K-nearest neighbors“, in *Dimensionality Reduction With Unsupervised Nearest Neighbors*, pp. 13-23, 2013. Springer, Berlin, Heidelberg. doi: https://doi.org/10.1007/978-3-642-38652-7

[137] V. Timčenko, I. Juma, and S. Gajin, „The hybrid machine learning support for entropy based network traffic anomaly detection“, in *9th Int. Conf. Information Society and Technology – ICIST2019*, pp. 144-149, 2019. Online: https://www.eventiotic.com/eventiotic/library/paper/467

[138] A. K. Jain, M. N. Murty, and P. J. Flynn, „Data clustering: a review“, *ACM Computing Surveys (CSUR)*, vol. 31, no. 3, 1999, pp. 264-323. doi: https://doi.org/10.1145/331499.331504.

[139] L. Rokach, and M. O. Maimon, „Clustering methods“, *Data Mining And Knowledge Discovery Handbook*, Springer, Boston, MA, 2005, pp. 321-352. doi: https://doi.org/10.1007/0-387-25465-X_15.

[140] V. Timcenko, S. Gajin, „Machine learning enhanced entropy-based network anomaly detection“, *Advances in Electrical and Computer Engineering*, vol. 21, no. 4, pp. 51-60, 2021. doi:10.4316/AECE.2021.04006

[141] J. C. Bezdek, R. Ehrlich, W. Full, „FCM: The fuzzy c-means clustering algorithm“, *Computers and Geosciences*, vol. 10, no. 2-3, pp. 191-203, 1984. doi: https://doi.org/10.1016/0098-3004(84)90020-7.

[142] R. T. Ng, and J. Han, „CLARANS: A method for clustering objects for spatial data mining“, *IEEE Trans. on Knowledge And Data Engineering*, vol. 14, no. 5, pp. 1003-1016, 2002. doi: 10.1109/TKDE.2002.1033770

[143] A. Likas, N. Vlassis, and J. J. Verbeek, „The global k-means clustering algorithm“, *Pattern Recognition*, vol. 36, no. 2, pp. 451-461, 2003. doi: https://doi.org/10.1016/S0031-3203(02)00060-2

[144] T. K. Moon, „The expectation-maximization algorithm“, *IEEE Signal Process. Magazine*, vol. 13, no. 6, pp. 47-60, 1996. doi: 10.1109/79.543975

[145] C. B. Do, and S. Batzoglou, „What is the expectation maximization algorithm?“, *Nature Biotechnology*, vol. 26, no. 8, 2008, pp. 897-899. doi: 10.1038/nbt1406

[146] P. C. Cheeseman, J. C. Stutz, “Bayesian classification (AutoClass): theory and results“, *Advances in Knowledge Discovery And Data Mining*, vol. 180, pp. 153-180, 1996.

[147] T. L. Huntsberger, P. Ajjimarangsee, „Parallel self-organizing feature maps for unsupervised pattern recognition“, *Int. J. of General Sys.*, vol. 16, no. 4, pp. 357-372, 2007. doi: https://doi.org/10.1080/03081079008935088

[148] D. H. Fisher, „Knowledge acquisition via incremental conceptual clustering“, *Machine learning*, vol. 2, no. 2, pp. 139-172, 1987.

[149] J. H. Gennari, P. Langley, and D. Fisher, „Models of incremental concept formation,” *Artif. Intell.*, vol. 40, no.1-3, pp. 11-61, 1989. doi: https://doi.org/10.1016/0004-3702(89)90046-5

[150] M. Ankerst et al., „OPTICS: Ordering points to identify the clustering structure“, *ACM Sigmod Record*, vol. 28, no. 2, pp. 49-60, 1999. doi: https://doi.org/10.1145/304181.304187

[151] D. Birant, and A. Kut, „ST-DBSCAN: An algorithm for clustering spatial–temporal data“, *Data & Knowledge Engineering*, vol. 60, no. 1, pp. 208-221, 2007. doi: https://doi.org/10.1016/j.datak.2006.01.013

[152] A. Hinneburg and H. H. Gabriel, „Denclue 2.0: Fast clustering based on kernel density estimation“, *Int. Symp. Intelligent Data Analysis*, *Lecture Notes in Computer Science*, vol. 4723, Springer, Berlin, Heidelberg, 2007. doi: https://doi.org/10.1007/978-3-540-74825-0_7

[153] W. Wang, J. Yang, and R. Muntz, „STING: A statistical information grid approach to spatial data mining“, in *Very Large Data Bases (VLDB)*, vol. 97, pp. 186-195, 1997.

[154] G. Sheikholeslami, S. Chatterjee, A. Zhang, „Wavecluster: A multi-resolution clustering approach for very large spatial databases“, in *Very Large Data Bases (VLDB)*, vol. 98, pp. 428-439, 1998.

[155] T. van Craenendonck, H. Blockeel, „Constraint-based clustering selection“, *Machine Learning*, vol. 106, no. 9, pp. 1497-1521, 2017. doi: https://doi.org/10.1007/s10994-017-5643-7

[156] D. Fogaras, and R. Balázs, „Scaling link-based similarity search“, in *14th Int. Conf. on World Wide Web*, pp. 641-650, 2005. doi: https://doi.org/10.1145/1060745.1060839

[157] X. Yin, J. Han, and P. S. Yu, „LinkClus: efficient clustering via heterogeneous semantic links“, in *32nd Int. Cnf. on Very Large Data Bases*, pp. 427-438, 2006.

[158] H. Wang et al., „A fast algorithm for subspace clustering by pattern similarity“, in *16th Int. Conf. on Scientific and Statistical Database Management*, pp. 51-60, 2004. doi: 10.1109/SSDM.2004.1311193.

[159] M. M. Breunig et al., „LOF: identifying density-based local outliers“, in *ACM SIGMOD Int. Conf. on Management of data*, pp. 93-104, 2000. doi: https://doi.org/10.1145/342009.335388

[160] S. C. Johnson, „Hierarchical clustering scheme“, *Psychometrika*, vol. 32, no.3, pp. 241-254, 1967. doi: https://doi.org/10.1007/BF02289588

[161] A. P. Reynolds et al., „Clustering rules: a comparison of partitioning and hierarchical clustering algorithms“, *J. of Math. Modelling and Algorithms*, vol. 5, no. 4, pp. 475-504, 2006. doi: https://doi.org/10.1007/s10852-005-9022-1

[162] G. Karypis, E-H. Han, and V. Kumar, „Chameleon: Hierarchical clustering using dynamic modeling“, *Computer*, vol. 32, no. 8, pp. 68-75, 1999. doi: 10.1109/2.781637

[163] A. K. Patnaik, P. K. Bhuyan, K. K. Rao, „Divisive analysis (DIANA) of hierarchical clustering and GPS data for level of service criteria of urban streets“, *Alexandria Engineering J.*, vol. 55, no. 1, pp. 407-418, 2016. doi: https://doi.org/10.1016/j.aej.2015.11.003

[164] I. Dokmanic et al., „Euclidean distance matrices: essential theory, algorithms, and applications“, *IEEE Signal Process. Magazine*, vol. 32, no. 6, 2015, pp. 12-30. doi: 10.1109/MSP.2015.2398954.

[165] X. Qian, Z. Xianyuan, and S. V. Ukkusuri, „Characterizing urban dynamics using large scale taxicab data“, *Engineering and Applied Sciences Optimization*, Springer, 2015, pp. 17-32. doi: 10.1007/978-3-319-18320-6_2

[166] R. C. de Amorim, and B. Mirkin, „Minkowski metric, feature weighting and anomalous cluster initializing in K-Means clustering“, *Pattern Recognition*, vol. 45, no. 3, 2012, pp. 1061-1075. doi: https://doi.org/10.1016/j.patcog.2011.08.012.

[167] P. Jaccard, „The distribution of the flora in the Alpine zone“, *The New Phytologist*, 1912, vol. 11, no. 2, pp. 37-50. doi: https://doi.org/10.1111/j.1469-8137.1912.tb05611.x

[168] V. Lavrenko, *Lectures on Hierarchical Clustering*, 2013. Online: https://www.youtube.com/c/VictorLavrenko/featured
[169] G.N. Lance, W. T. Williams, „A general theory of classificatory sorting strategies. 1. Hierarchical systems“, *Computer J.*, vol. 9, no. 4, pp. 373–380, 1967. doi: https://doi.org/10.1093/comjnl/9.4.373
[170] Y. Wang et al., „Internet traffic classification using constrained clustering“, *IEEE Trans. On Parallel And Distributed Syst.*, vol. 25, no. 11, pp. 2932-2943, 2013. doi: 10.1109/TPDS.2013.307.
[171] C. Ding, and X. He, „Cluster merging and splitting in hierarchical clustering algorithms“, *IEEE Int. Conf. on Data Mining*, pp. 139-146, 2002. doi: 10.1109/ICDM.2002.1183896
[172] C. H. Ding et al., „A Min-Max Cut algorithm for graph partitioning and data clustering“, in *IEEE Int. Conf. on Data Mining*, pp. 107-11, 2001. doi: 10.1109/ICDM.2001.989507
[173] C. E. Shannon, „A mathematical theory of communication“, *Bell Syst. Technical J.*, vol. 27, no. 3, pp. 379-423, 1948. doi: https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.
[174] V. Timcenko, S. Gajin, „Network traffic profiling and anomaly detection“. (biće podneto za potencijalno objavljivanje u *IEEE Access*)
[175] A. J. Lawrance, P.A.W. Lewis, „An exponential moving-average sequence and point process (EMA1) “, *J. of Applied Probability*, vol. 14, no. 1, pp. 98-113, 1977. doi:10.2307/3213263
[176] MATLAB and Statistics Toolbox Rel. R2019a, The MathWorks, Inc., Natick, Massachusetts, United States.
[177] I. Juma, V. Timčenko, and S. Gajin, „A comprehensive flow-based anomaly detection architecture using entropy calculation and machine learning classification“, in *9th Int. Conf. Information Society and Technology – ICIST2019*, pp. 138-143, 2019. Online: https://www.eventiotic.com/eventiotic/library/paper/466
[178] I. H. Witten, E. Frank, Data Mining Practical Machine Learning Tools and Techniques,2nd edition, The Morgan Kaufmann Series in Data Management Systems. Microsoft Research, 2005. doi: https://doi.org/10.1145/507338.507355
[179] M. Hall et al., „The WEKA data mining software: an update“, *ACM SIGKDD Explorations Newsletter*, vol. 11, no. 1, pp.10–18, 2009. doi: https://doi.org/10.1145/1656274.1656278
[180] R. R. Bouckaert et al., *WEKA Manual for Version 3-8-1*, Univ. of Waikato, Hamilton, New Zealand, 2016.
[181] Python Documentation by Version. https://www.python.org/doc/versions/.
[182] A. C. Müller, and S. Guido. Introduction to machine learning with Python: a guide for data scientists. O'Reilly Media, Inc., 2016.
[183] Scikit-learn: Machine Learning in Python. http://scikit-learn.org/stable/index.html.
[184] D. Pantić, Softver za analizu efikasnosti računanja entropije mrežnog saobraćaja, Master rad, Elektrotehni;ki fakultetu u Beogradu, 2018
[185] L. Dhanabal, S. P. Shantharajah, „A study on NSL-KDD dataset for intrusion detection system based on classification algorithms“, *Int. J. of Adv. Research in Computer and Commun. Engineering*, vol. 4, no. 6, pp. 446-452, 2015. doi:10.17148/IJARCCE.2015.4696
[186] J. Nazario, „DDoS attack evolution“, *Network Security*, Elsevier, vol. 7, pp. 7-10, 2008. doi:10.1016/S1353-4858(08)70086-2
[187] H. Wang, D. Zhang, K. G. Shin, „Detecting SYN flooding attacks“, in *21st Joint Conference IEEE Computer and Commun. Societies*, vol. 3, pp. 1530-1539, 2002. doi:10.1109/INFCOM.2002.1019404

[188] G. Kambourakis et al., „Detecting DNS amplification attacks“, *Int. Workshop On Critical Inf. Infrastructures Security*, Springer, Berlin, Heidelberg, vol. 5141, pp. 185-196, 2008. doi:10.1007/978-3-540-89173-4_16

[189] J. Vykopal, T. Plesnik, P. Minarik, „Network-based dictionary attack detection“, *Int. IEEE Conf. on Future Networks*, pp. 23-27, 2009. doi:10.1109/ICFN.2009.36

[190] P. Berezinski et al., „Network anomaly detection using parameterized entropy“, *Computer Information Syst. and Industrial Management*, Springer, vol. 8838, pp. 465-478, 2014. doi:10.1007/978-3-662-45237-0_43

[191] P. Barford et al., „A signal analysis of network traffic anomalies“, in *2nd ACM SIGCOMM Workshop on Internet measurement*, Marseille, France, 2002, pp. 71-82. doi: 10.1145/637201.637210

[192] H.A. Nguyen et al., „Network traffic anomalies detection and identification with flow monitoring“, *5th IEEE IFIP Int. Conf. Wireless and Optical Commun. Networks (WOCN '08)*, pp. 1-5, 2008. doi: 10.1109/WOCN.2008.4542524

[193] D. Roosi, an S. Valenti, „Fine-grained traffic classification with netflow data“, in *6th Int. Wireless Commun. and Mobile Computing Con.*, pp. 479-483, 2010. ACM NY, USA. doi: 10.1145/1815396.1815507

[194] O. Joldzic, Z. Djuric, and P. Vuletic, „A transparent and scalable anomaly-based DoS detection method“, *Computer Networks*, vol. 104, pp. 27-42, 2016. doi: 10.1016/j.comnet.2016.05.004

[195] P.D. Bojovic et al., „A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method“, *Computers and Electrical Engineering*, vol. 73, pp. 84-96, 2018. doi: 10.1016/j.compeleceng.2018.11.004. ISSN: 0045-7906

[196] G. Nychis et al., „An empirical evaluation of entropy-based traffic anomaly detection“, in *8th ACM SIGCOMM Conf. Internet Measurement (IMC08)*, pp. 151–156, 2008. ACM NY, USA. doi: 10.1145/1452520.1452539

[197] C. Fachkha, E. Bou-Harb, and M. Debbabi, „Fingerprinting Internet DNS amplification DDoS activities“, in *6th Int. Conf. on New Technologies, Mobility and Security (NTMS)*, pp. 1–5, 2014. doi: 10.1109/NTMS.2014.6814019

[198] R. R. Sokal, C. D. Michener, „A statistical method for evaluating systematic relationships“, Univ. Kansas, *Science Bulletin*, vol. 38, part.2, pp. 1409-1438, 1958.

[199] I. Gronau, and M. Shlomo, „Optimal implementations of UPGMA and other common clustering algorithms“, *Information Process. Letters*, vol. 104, no. 6, pp. 205-210, 2007. doi: 10.1016/j.ipl.2007.07.002

BIOGRAFIJA

Valentina Timčenko je rođena 1978. godine u Beogradu, gde je završila osnovnu školu i gimnaziju. Studije na Elektrotehničkom fakultetu u Beogradu započela je 1997. godine, gde je diplomirala 2004. godine na Odseku za telekomunikacije sa temom „Optičke WDM mreže", pod mentorstvom prof. dr Petra Matavulja sa ocenom diplomskog rada 10. Prosečna ocena u toku studija bila je 8,00. Postdiplomske studije je upisala 2004. godine na Elektrotehničkom fakultetu Univerziteta u Beogradu, smer Telekomunikacije, i položila sve predmete predviđene nastavnim planom, sa prosečnom ocenom 10.00. Magistrirala je 9.3.2010. godine sa temom „Principi simulacije mobilnih ad hoc mreža" (Komisija: dr Mirjana Stojanović, mentor, prof. dr Miroslav Dukić, prof. dr Vladanka Aćimović-Raspopović, doc. dr Miljko Erić). Iste godine je izabrana u zvanje istraživač-saradnik Instituta „Mihajlo Pupin".

Tokom magistarskih studija, a zatim i nakon odbrane magistarske teze, kandidatkinja je nastavila svoj istraživački rad na problemima bezbednosti modernih mrežnih okruženja obuhvatajući nove tehnologije, konceptualne trendove i informaciono-komunikacione infrastrukture (računarstvo u oblaku, Internet stvari). Rezultate svog rada objavila je kao autor i koautor u nekoliko radova u časopisima sa SCI liste.

Doktorske akademske studije je upisala 2016. godine na Elektrotehničkom fakultetu, Univerziteta u Beogradu, na modulu Računarska tehnika i informatika. Tom prilikom je, u skladu sa Pravilnikom za doktorske studije Elektrotehnikog fakulteta i Univerziteta u Beogradu, na osnovu magistrature po starom programu stekla uslov da upiše treću godinu doktorskih studija po novom programu. S obzirom na to da je tom prilikom promenila smer, definisani su ispiti razlike koje je bilo potrebno da položi. Definisana su dva ispita razlike: Organizacija sistema diskova i TCP/IP arhitektura. Ispite razlike je kandidatkinja uspešno položila. Rezultati koji su ostvarivani istraživačkim radom kandidatkinje predstavljeni su u šest radova na međunarodnim konferencijama i jednom radu objavljenom u časopisu sa SCI liste. Još jedan rad je u pripremi za slanje u časopis sa SCI liste. Javna usmena odbrana predložene teme doktorske disertacije je sprovedena 9.10.2019. godine na Elektrotehničkom fakultet Univerziteta u Beogradu.

Zaposlena je u Institutu „Mihajlo Pupin" u Beogradu od 2004. godine, na poslovima istraživanja, razvoja i projektovanja telekomunikacionih mreža i sistema. Do sada je učestvovala u nekoliko naučno-istraživačkih projekata finansiranih od strane Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije. Učestvuje na međunarodnoj COST akciji CA20120 INTERACT (Intelligence-Enabling Radio Communications for Seamless Inclusive Interactions), a bila je učesnik međunarodne COST akcije CA15104 IRACON (Inclusive Radio Communication Networks for 5G and beyond), učestvovala je na projektu finansiranom od strane Evropske komisije SEE TV-WEB (South-East Europe Transnational Cooperation Programme), a takođe je učestvovala u projektima i studijama telekomunikacionih sistema Elektroprivrede Srbije i Agencije za kontrolu letenja.

Tokom magistarskih studija intenzivno se bavila radom u oblasti primene znanja iz oblasti telekomunikacionih mreža, pri čemu je pohađala Cisco Akademiju Računskog centra Elektrotehničkog fakulteta u Beogradu i sertifikovala se za nekoliko sertifikata, od kojih trenutno poseduje: CCNA, CCS-EAII (obuhvatajući CCNP Routing and Switching TSHOOT i ENARSI).

Valentina Timčenko je višegodišnji član IEEE organizacije. Bila je recenzent većeg broja međunarodnih konferencija, među kojima su ICACCI-2015, IEEE WCNC 2015, ATC'14, a nekoliko

godina unazad je stalni recenzent radova na međunarodnim konferencijama TELFOR, MIC, ISDOC/OSDOC, INFOTEH. Za konferencije ISDOC/OSDOC je više puta bila član programskog odbora.

Bila je ko-mentor na više master radova odbranjenih na Elektrotehničkom fakultetu u Beogradu i na Akademiji tehničko-umetničkih strukovnih studija Beograd, odsek Visoka škola elektrotehnike i računarstva strukovnih studija – VISER.

Autor je i koautor 116 naučnih i stručnih radova iz oblasti telekomunikacija i računarskih sistema, pri čemu je 33 na domaćim konferencijama, 69 na međunarodnim konferencijama, 7 radova u međunarodnim časopisima, 1 rad u domaćem časopisu, 4 u monografijama međunarodnog značaja. Koautor je većeg broja tehničkih rešenja.

PRILOG: SPISAK RADOVA VEZANIH ZA ISTRAŽIVANJE

Rezultati istraživanja koji su predstavljeni u okviru doktorske disertacije se objavljeni kroz sledeće radove:

Radovi u međunarodnim časopisima, M23

[1] V. Timcenko, S. Gajin, „Machine learning enhanced entropy-based network anomaly detection“, *Advances in Electrical and Computer Engineering*, vol. 21, no. 4, pp. 51-60, 2021. **doi:10.4316/AECE.2021.04006**

Rad u međunarodnom časopisu (M2x)

[1] V. Timcenko, S. Gajin, „Network Traffic Profiling and Anomaly Detection“. (biće podneto za potencijalno objavljivanje u *IEEE Access*)

Radovi na međunarodnim konferencijama, štampani u celini, M33

[1] S. Gajin and V. Timcenko, „Comparison of entropy-based and machine learning approaches in intrusion detection,“ in *11th Int. Conf. Information Society and Technology-ICIST2021*, pp.113-118, 2021. Online: https://www.eventiotic.com/eventiotic/library/paper/651

[2] V. Timcenko, S. Gajin, „Time-series entropy data clustering for effective anomaly detection,“ *in 10th Int. Conf. Information Society and Technology – ICIST2020*, pp. 170-175, 2020. Online: https://www.eventiotic.com/eventiotic/library/paper/608

[3] V. Timčenko, J. Ibrahim, and S. Gajin, „The hybrid machine learning support for entropy based network traffic anomaly detection“, in *9th Int. Conf. Information Society and Technology – ICIST2019*, pp. 144-149, 2019. Online: https://www.eventiotic.com/eventiotic/library/paper/467

[4] J. Ibrahim, V. Timčenko, and S. Gajin, „A comprehensive flow-based anomaly detection architecture using entropy calculation and machine learning classification “, in *9th Int. Conf. Information Society and Technology – ICIST2019*, pp. 138-143, 2019. Online: https://www.eventiotic.com/eventiotic/library/paper/466

[5] V. Timčenko, S. Gajin, „Machine learning based network anomaly detection for IoT environments“, in *8th Int. Conf.Information Society and Technology – ICIST2018*, pp. 196 – 201, 2018. Online: https://www.eventiotic.com/eventiotic/library/paper/410

[6] V. Timčenko, S. Gajin, „Ensemble classifiers for supervised anomaly based network intrusion detection“, in *IEEE Int. Conf. Intelligent Computer Commun. and Process. ICCP2017*, 2017, doi: 10.1109/ICCP.2017.8116977

Radovi su publikovani u okviru nekoliko domaćih i međunarodnih projekata:

2011-2020: „Razvoj novih metoda i alata za unapređenje performansi, mrežne i ekonomske efikasnosti telekomunikacionih mreža naredne generacije“, projekat tehnološkog razvoja TR32025, Ministarstvo za nauku i tehnološki razvoj Republike Srbije, učesnik na projektu.

2011-2020:„Istraživanje i razvoj robusnih sistema za prenos podataka i njihova primena u korporativnim mrežama“, projekat tehnološkog razvoja TR32037, Ministarstvo za nauku i tehnološki razvoj Republike Srbije, učesnik na projektu.

2016-2020: International COST action CA15104, IRACON („Inclusive Radio Communication Networks for 5G and beyond“) http://www.iracon.org/. (supported by Horizon 2020).

2021-2025: International COST action CA20120, INTERACT („Intelligence-Enabling Radio Communications for Seamless Inclusive Interactions“) https://e-services.cost.eu/action/CA20120.

Eksperimentalni deo doktorske disertacije i odgovarajuća istraživanja su sprovedena u Institutu „Mihajlo Pupin“ u Beogradu i na Elektrotehničkom fakultetu Univerziteta u Beogradu u okviru RCUB, Računarskog centra Univerziteta u Beogradu.

образац изјаве о ауторству

Изјава о ауторству

Име и презиме аутора ВАЛЕНТИНА ТИМЧЕНКО

Број индекса 5046/2016

Изјављујем

да је докторска дисертација под насловом

ДЕТЕКЦИЈА НАПАДА У РАЧУНАРСКИМ МРЕЖАМА ЗАСНОВАНА НА АНАЛИЗИ СТРУКТУРЕ САОБРАЋАЈА ПРИМЕНОМ КОМБИНОВАНИХ АЛГОРИТАМА МАШИНСКОГ УЧЕЊА

- резултат сопственог истраживачког рада;
- да дисертација у целини ни у деловима није била предложена за стицање друге дипломе према студијским програмима других високошколских установа;
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио/ла интелектуалну својину других лица.

Потпис аутора

У Београду, 28.02.2022.

образац изјаве о истоветности штампане и електронске верзије докторског рада

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора ВАЛЕНТИНА ТИМЧЕНКО

Број индекса 5046/2016

Студијски програм ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Наслов рада ~~ДЕТЕКЦИЈА НАПАДА У РАЧУНАРСКИМ МРЕЖАМА ЗАСНОВАНА НА АНАЛИЗИ СТРУКТУРЕ САОБРАЋАЈА ПРИМЕНОМ КОМБИНОВАНИХ АЛГОРИТАМА МАШИНСКОГ УЧЕЊА~~

Ментор ДР СЛАВКО ГАЈИН, ВАНРЕДНИ ПРОФЕСОР, УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла ради похрањивања у **Дигиталном репозиторијуму Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског назива доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис аутора

У Београду, 28.2.2022.

образац изјаве о коришћењу

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

ДЕТЕКЦИЈА НАПАДА У РАЧУНАРСКИМ МРЕЖАМА ЗАСНОВАНА НА АНАЛИЗИ СТРУКТУРЕ САОБРАЋАЈА ПРИМЕНОМ КОМБИНОВАНИХ АЛГОРИТАМА МАШИНСКОГ УЧЕЊА

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигиталном репозиторијуму Универзитета у Београду и доступну у отвореном приступу могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство (CC BY)

2. Ауторство – некомерцијално (CC BY-NC)

3. Ауторство – некомерцијално – без прерада (CC BY-NC-ND)

4. Ауторство – некомерцијално – делити под истим условима (CC BY-NC-SA)

5. Ауторство – без прерада (CC BY-ND)

6. Ауторство – делити под истим условима (CC BY-SA)

(Молимо да заокружите само једну од шест понуђених лиценци.
Кратак опис лиценци је саставни део ове изјаве).

Потпис аутора

У Београду, 28.02.2022

1. **Ауторство**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.

2. **Ауторство – некомерцијално**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела.

3. **Ауторство – некомерцијално – без прерада**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дела.

4. **Ауторство – некомерцијално – делити под истим условима**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дела и прерада.

5. **Ауторство – без прерада**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дела.

6. **Ауторство – делити под истим условима**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.