UDC: 004.85 Info M str. 43-50

DETEKCIJA ARP SPOOFING, SYN I PING FLOOD NAPADA KORIŠĆENJEM MODELA MAŠINSKOG UČENJA
DETECTION OF ARP SPOOFING, SYN AND PING FLOOD ATTACKS USING MACHINE LEARNING MODELS

Aleksandar Rakić,

REZIME: Sigurnost uređaja u okruženjima Interneta stvari (IoT) i koncepta "Donesi svoj uređaj" (BYOD) postaje sve veći izazov kako se bežične mreže šire. Ovaj rad predstavlja sveobuhvatnu studiju koja koristi modele mašinskog učenja za otkrivanje tri uobičajena sajber napada u bežičnim mrežama: ARP Spoofing, SYN i PING Flood. Podaci o mrežnom saobraćaju prikupljeni su korišćenjem alata Wireshark, a evaluirani su različiti modeli mašinskog učenja, uključujući CatBoost, LightGBM, Random Forest, Gradient Boosting, XGBoost, Naivni Bajes, K-najbližih suseda (KNN) i Logističku regresiju. Među njima, CatBoost je pokazao superiorne rezultate u detekciji SYN Flood napada, postigavši tačnost od 96,53% i ROC-AUC vrednost od 0,9961. Za detekciju ARP Spoofing napada, Random Forest se istakao sa tačnošću od 97,00% i ROC-AUC od 0,9945. U poređenju sa ostalima, Naivni Bajes je nadmašio druge modele u detekciji PING Flood napada sa tačnošću od 97,83% i ROC-AUC od 0,9977. Ovi rezultati ukazuju na veliki potencijal modela mašinskog učenja, posebno CatBoost i Naivnog Bajesa, u značajnom unapređenju detekcije različitih sajber pretnji u realnom vremenu. Ovi modeli predstavljaju ključne alate za obezbeđivanje IoT i BYOD ekosistema u praktičnim, stvarnim primenama.

KLJUČNE REĆI: mašinsko učenje, arp spoofing, syn flood, ping flood, bezbednost bežičnih mreža, sajber bezbednost, detekcija anomalija

ABSTRACT: Device security in Internet of Things (IoT) and Bring Your Own Device (BYOD) environments is becoming an increasing challenge as wireless networks proliferate. This paper presents a comprehensive study that uses machine learning models to detect three common cyber attacks in wireless networks: ARP Spoofing, SYN and PING Flood. Network traffic data was collected using the Wireshark tool, and various machine learning models were evaluated, including CatBoost, LightGBM, Random Forest, Gradient Boosting, XGBoost, Naive Bayes, K-Nearest Neighbors (KNN), and Logistic Regression. Among them, CatBoost performed superiorly in detecting SYN Flood attacks, achieving an accuracy of 96.53% and a ROC-AUC value of 0.9961. For the detection of ARP Spoofing attacks, Random Forest excelled with an accuracy of 97.00% and a ROC-AUC of 0.9945. Compared to others, Naive Bayes outperformed the other models in PING Flood attack detection with an accuracy of 97.83% and a ROC-AUC of 0.9977. These results indicate the great potential of machine learning models, especially CatBoost and Naive Bayes, in significantly improving the detection of various cyber threats in real time. These models represent key tools for securing IoT and BYOD ecosystems in practical, real-world applications.

KEY WORDS: change in the concept of the output variable, changes in the distributions of input data, methods and algorithms for detecting a change in the concept of the output variable, sale of cash credits

1 UVOD

Bežični komunikacioni sistemi revolucionisali su komunikaciju, omogućavajući značajnu fleksibilnost i efikasnost. Međutim, sa ekspanzijom Interneta stvari (IoT) **[1]** i uvođenjem politike „Donesi svoj uređaj" (BYOD) u korporativnim okruženjima **[2]**, pojavljuju se ozbiljne bezbednosne ranjivosti **[3]**. Ovi uređaji, često slabo zaštićeni, povećavaju izloženost složenim sajber pretnjama **[4]**. Kako se lični uređaji integrišu u poslovne mreže, rizik od sajber napada se značajno povećava, što predstavlja izazov za tradicionalna rešenja sajber bezbednosti.

Mašinsko učenje je postalo moćan alat za poboljšanje sajber bezbednosti, omogućavajući detekciju pretnji u realnom vremenu i adaptivno reagovanje **[5]**. Posebno je efikasan u analizi mrežnog saobraćaja, identifikovanju anomalija i odgovoru na promene u šablonima napada **[6]**. Ova studija se bavi detekcijom i mitigacijom tri uobičajena sajber napada na bežične mreže: ARP Spoofing, SYN i PING Flood, koji koriste ranjivosti mrežnih protokola, izazivajući neovlašćen pristup, uskraćivanje usluge i curenje podataka.

Doprinos ovog rada ogleda se u sveobuhvatnom pristupu korišćenjem različitih modela mašinskog učenja—CatBoost, LightGBM, Random Forest i XGBoost—kako bi se razvila skalabilna i robusna rešenja za razlikovanje normalnog i zlonamernog mrežnog saobraćaja. Simulacije napada u realnim mrežnim uslovima pružaju uvide u performanse različitih modela. Za razliku od prethodnih studija koje se često fokusiraju na jedan tip napada ili manji broj modela, ovo istraživanje uključuje širi spektar napada i algoritama, pružajući dublje razumevanje njihovih snaga i slabosti u kontekstu bezbednosti bežičnih mreža.

Aktuelna istraživanja i dalje se suočavaju sa izazovima u upravljanju mrežama sa visokim protokom podataka i u identifikaciji napada koji koriste napredne tehnike izbegavanja detekcije **[7]**. Ova studija predlaže rešenja za poboljšanje analize velikih podataka i primenu naprednih metoda prepoznavanja obrazaca, čime se povećava otpornost mreža na složene i adaptivne pretnje. Pored toga, identifikovane su oblasti za dalja istraživanja, sa fokusom na razvoj efikasnijih tehnika za detekciju napada u realnom vremenu.

Glavni cilj ovog istraživanja je procena performansi različitih modela mašinskog učenja u detekciji napada ARP Spoofing, SYN i PING Flood. Rezultati pokazuju da modeli po-

put CatBoost i Naivnog Bajesa ostvaruju superiorne rezultate u tačnosti i skalabilnosti. Ovi modeli predstavljaju praktična rešenja za zaštitu modernih bežičnih mreža, posebno u IoT i BYOD okruženjima, pružajući stručnjacima za sajber bezbednost alate i znanje za implementaciju robusnih sigurnosnih mera protiv širokog spektra pretnji.

2 PREGLED LITERATURE

U poslednjih nekoliko godina, postignut je značajan napredak u poboljšanju sigurnosti bežičnih mreža, vođen potrebom za suzbijanjem sajber napada poput napada čoveka u sredini (MITM), ARP Spoofing-a i drugih mrežnih upada. Tehnike mašinskog učenja (ML) su se pojavile kao ključni alati za poboljšanje detekcije i ublažavanja ovih sofisticiranih napada, što je dovelo do razvoja naprednijih i agilnijih okvira za sajber bezbednost.

Al-Juboori i saradnici **[8]** istražili su upotrebu metoda ansambl učenja, posebno Random Forest-a i stabla odlučivanja, za detekciju MITM i DoS napada u realnom vremenu. Njihovo istraživanje je pokazalo da ansambl metode značajno poboljšavaju tačnost u poređenju sa pojedinačnim modelima, postižući tačnost veću od 99%. Takođe su istraživali efikasnost Long Short-Term Memory (LSTM) mreža u detekciji evolutivnih mrežnih pretnji. Studija je zaključila da su moderni modeli mašinskog učenja, posebno tehnike ansambla i dubokog učenja, neophodni za osiguranje dinamičnih bežičnih okruženja. Međutim, njihov fokus na ansambl učenje za MITM i DoS napade ostavlja prostor za dalje istraživanje u detekciji šireg spektra napada, kao što su ARP Spoofing i SYN Flood, što je fokus ovog rada.

Značajan doprinos detekciji anomalija u mrežnom saobraćaju dao je *Protić i saradnici* **[9]**, koji su predstavili detektor baziran na XOR tehnici za rešavanje sukoba između odluka donetih od strane više klasifikatora. Njihov metod je upoređivao rezultate težinskih k-najbližih suseda i unapred prosleđenih neuronskih mreža, pokazujući da rešavanje konflikata poboljšava tačnost detekcije mrežnih anomalija. Njihovi rezultati su naglasili važnost skaliranja karakteristika i hiperboličkih tangens transformacija u smanjenju vremena obrade, što je unapredilo performanse. Iako su postigli značajan napredak u poboljšanju detekcije anomalija, nisu se bavili detekcijom u realnom vremenu u bežičnim mrežama, niti su se fokusirali na specifične napade kao što su SYN ili PING Flood.

Kako bi se rešio specifičan izazov detekcije ARP Spoofing napada, *Kponyo i saradnici* **[10]** su razvili sistem za detekciju anomalija zasnovan na analizi ARP saobraćaja. Primenom modela mašinskog učenja, poput Support Vector Classification (SVC) i Gaussovog Naivnog Bajesa, postigli su impresivnu tačnost detekcije od 99,72%. Njihov rad je pružio dragocene uvide u ranjivosti ARP saobraćaja i otvorio put ka detekciji MITM napada u realnom vremenu, kako u žičnim, tako i u bežičnim mrežama. Međutim, njihov pristup je bio ograničen na analizu ARP saobraćaja, ostavljajući prostor za dalje istraživanje sistema koji mogu obraditi različite vrste napada.

Sukkar i saradnici **[11]** su predložili inovativan mehanizam odbrane protiv ARP Spoofing-a nadgledanjem promena u ARP tabelama i automatskim resetovanjem nevažećih unosa. Njihovo Python rešenje, korišćenjem Scapy biblioteke, pružilo je zaštitu u realnom vremenu protiv ARP Spoofing napada. Iako je efikasan u ublažavanju napada specifičnih za ARP, njihov rad se nije proširio na druge uobičajene napade u bežičnim mrežama, poput SYN Flood ili PING Flood, koje naša istraživanja obrađuju primenom mašinskog učenja za detekciju više vrsta napada.

U skorije vreme, Michelena i saradnici **[12]** su se fokusirali na detekciju MITM napada u IoT okruženjima koristeći veštačke neuronske mreže (ANN) i protokol za telemetrijski transport poruka (MQTT). Njihov model je postigao tačnost od 99,2\%, čime je pokazao potencijal ANN rešenja za osiguranje IoT mreža. Međutim, njihova istraživanja nisu pokrila širi set napada, kao što su SYN Flood ili PING Flood, niti su istražili potencijal modela mašinskog učenja kao što su CatBoost ili Gradient Boosting za sigurnost mreža, što je fokus našeg istraživanja.

Iako su ove studije značajno doprinele poboljšanju sigurnosti mreža, većina se fokusirala na specifične vektore napada ili ograničena okruženja. Ovo istraživanje se nadovezuje na ove nalaze predlaganjem sveobuhvatnog pristupa koji integriše više modela mašinskog učenja, uključujući CatBoost, LightGBM, Random Forest i Naivni Bajes, za detekciju širokog spektra napada (ARP Spoofing, SYN Flood i PING Flood) u bežičnim mrežama. Ovaj rad proširuje postojeće metodologije testiranjem modela u realnim uslovima, obezbeđujući robusne performanse u različitim vrstama mrežnih upada.

3 METODOLOGIJA

Ova studija simulira tri uobičajena sajber napada—ARP Spoofing, SYN i PING Flood—od kojih svaki cilja različite slojeve OSI modela, konkretno slojeve veze i transporta. Tokom simulacija, Wireshark je korišćen za prikupljanje normalnog i zlonamernog mrežnog saobraćaja **[13]**. Skup podataka je prošao kroz faze pretprocesiranja, uključujući selekciju karakteristika, normalizaciju i smanjenje dimenzionalnosti primenom analize glavnih komponenti (PCA) **[14]**. Zatim su obučeni i evaluirani različiti modeli mašinskog učenja, uključujući CatBoost, LightGBM, Random Forest, Gradient Boosting, Logističku regresiju, XGBoost, Naivni Bajes i K-najbliže susede (KNN). Da bi se rešio problem neuravnoteženosti klasa, korišćene su metode Synthetic Minority Oversampling Technique (SMOTE) **[15]** i Tomek Links **[16]**. Performanse modela su ocenjene na osnovu tačnosti, preciznosti, recall-a, F1 skora i površine ispod ROC-AUC krive.

Mrežni saobraćaj je prikupljan tokom regularnih operacija, dok su napadi ARP Spoofing, SYN Flood i PING Flood simulirani. Simulacije su uključivale strimovanje video sadržaja, SSH sesije i pretraživanje interneta kako bi se kreirali realistični obrasci saobraćaja. Ciljajući ranjivosti u ARP, TCP i ICMP protokolima, simulirani su napadi kako bi se što verodostojnije prikazali realni scenariji ugrožavanja mrežne bezbednosti.

Nakon prikupljanja podataka, izvršena je selekcija karakteristika i imputacija nedostajućih vrednosti. PCA je korišćena za smanjenje dimenzionalnosti uz očuvanje ključne varijanse. Modeli su potom obučeni za klasifikaciju mrežnog saobraćaja kao benignog ili zlonamernog, pri čemu je izvršena sveobuhvatna evaluacija svakog modela u detekciji ovih specifičnih tipova napada.

3.1 *Prikupljanje podataka*

Prikupljanje podataka je od ključnog značaja u ovom radu jer pruža uvid u mrežni saobraćaj pre, tokom i nakon izvršenja sajber napada. Wireshark je korišćen za prikupljanje i analizu mrežnih aktivnosti u realnom vremenu, obuhvatajući raznovrsne podatke poput strimovanja YouTube videa, SSH sesija, Google Meet poziva, razmene e-pošte i opšteg pretraživanja interneta. Ova raznovrsnost aktivnosti omogućava kreiranje uzoraka regularnog saobraćaja, kao i razvoj obrazaca saobraćaja koji se odnose na sajber napade. Eksperimenti su sprovedeni u simuliranom okruženju bežične mreže koje je emuliralo praktične scenarije. Normalni i zlonamerni saobraćaj generisan je u kontrolisanom testnom okruženju pomoću hardverskih i softverskih konfiguracija koje su verno odražavale realne uslove, čime su rezultati postali primenljivi u praksi. Napadi koji su simulirani uključuju ARP Spoofing, SYN i PING Flood, koji mogu naneti značajnu štetu bežičnim mrežama.

Svi ovi testovi rezultirali su velikim skupom podataka od 439.171 unosa, koji obuhvataju različite scenarije mrežnog saobraćaja, od zlonamernih napada do normalnih aktivnosti. Konkretno, bilo je 4.219 unosa za ARP Spoofing, 1.499 za PING Flood i 2.016 za SYN Flood. Preostalih 431.437 unosa odnosi se na regularno ponašanje mreže. Neprekidno prikupljanje podataka putem Wireshark-a omogućilo je beleženje detaljnih varijacija u mrežnom saobraćaju, što je omogućilo precizno prikupljanje i klasifikaciju podataka. To je stvorilo čvrstu osnovu za dalju analizu korišćenjem tehnika mašinskog učenja, čime su omogućeni razvoj i testiranje robusnih modela u prirodnim okruženjima bežičnih mreža.

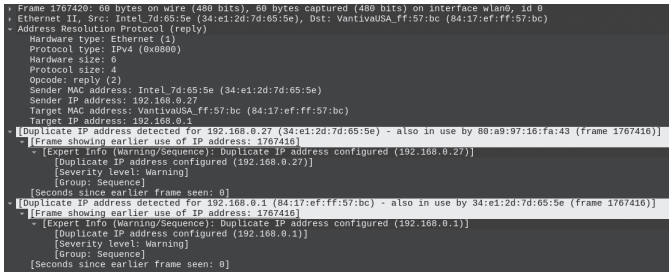
3.2 *Izvođenje eksperimenata*

Ova sekcija opisuje metodologiju korišćenu za izvođenje sajber napada na dva sloja OSI referentnog modela: sloj veze i transportni sloj. Prvo ćemo objasniti kako je ARP Spoofing, koji eksploatiše slabosti u ARP protokolu, korišćen za napade na sloj veze. Zatim ćemo analizirati SYN i PING Flood napade na transportni sloj, koji iskorišćavaju ranjivosti u TCP i ICMP protokolima. Ovi eksperimenti prikazuju praktične primene alata za bezbednost mreže i njihov potencijalni uticaj na integritet mreže.

3.2.1 Sloj veze

ARP (Address Resolution Protocol) je mrežni protokol koji prevodi IP adresu u odgovarajuću MAC adresu, omogućavajući komunikaciju unutar iste lokalne mreže. Prema OSI modelu, ARP funkcioniše na drugom sloju, sloju veze **[17]**. Međutim, ARP ima značajne sigurnosne slabosti zbog nedostatka autentifikacije ARP poruka, što ga čini ranjivim na različite napade.

Jedan od najopasnijih napada koji eksploatišu ove slabosti je ARP Spoofing, poznat i kao ARP trovanje. U ovom napadu, napadač šalje lažne ARP poruke preko mreže, povezujući svoju MAC adresu sa IP adresom legitimnog uređaja. To omogućava napadaču da presreće ili manipuliše saobraćajem namenjenim legitimnom uređaju **[18]**. Standardni alati za pokretanje ARP Spoofing napada uključuju `arpspoof`, `ettercap` i `bettercap`. Za potrebe ovog eksperimenta, korišćen je `bettercap` za izvođenje ARP Spoofing napada **[19]**. Alat je slao zlonamerne ARP poruke preko mreže, ciljajući uređaje i „trujući" njihove ARP keš memorije kako bi presreo mrežni saobraćaj. Prikupljeno je 4.219 instanci ARP Spoofing napada pomoću Wireshark-a, što je omogućilo detaljniju analizu.



Slika 1: *Detekcija duplih IP adresa uzrokovana ARP Spoofing napadom.*

Na slici 1 prikazana je instanca ARP Spoofing napada otkrivena pomoću Wireshark-a. Više uređaja tvrdi da ima istu IP adresu, što može izazvati prekid u mreži. Generalni mehanizmi odbrane od ARP Spoofing napada uključuju S-ARP (Secure ARP) i DAI (Dynamic ARP Inspection). S-ARP primenjuje kriptografsku verifikaciju ARP poruka, dok DAI proverava ARP pakete u odnosu na poverljivu bazu podataka, osiguravajući da zlonamerni ARP saobraćaj bude blokiran pre nego što može uticati na mrežu **[20]**.

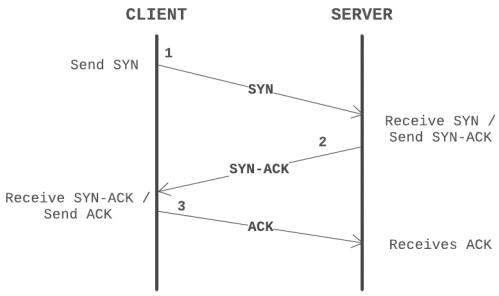
Mašinsko učenje unapređuje sigurnost mreža omogućavajući sistemima da efikasnije analiziraju obrasce saobraćaja, čime se detektuju različiti tipovi napada, kao što je ARP Spoofing. Ovaj proaktivan i adaptivan pristup može pružiti otpornija rešenja protiv razvijajućih sajber pretnji.

Modeli korišćeni u ovom istraživanju su prilagođeni za detekciju napada na osnovu njihovih osnovnih mehanizama. Boosting modeli, kao što su CatBoost i LightGBM, se ističu u detekciji napada kao što su SYN Flood jer mogu obrađivati velike količine strukturiranih podataka i identifikovati složene obrasce. Kod SYN Flood napada, ovi modeli efikasno detektuju ponavljajuće SYN zahteve i nedostatak odgovarajućih ACK odgovora. S druge strane, modeli poput Random Forest-a, sa svojim ansambl učenjem, pogodni su za detekciju ARP Spoofing napada jer uspešno obrađuju neuravnotežene skupove podataka i hvataju karakteristične karakteristike na nivou paketa, kao što su neslaganja u MAC adresama ili IP dodelama. Ove prilagođene sposobnosti omogućavaju svakom modelu da optimalno funkcioniše u zavisnosti od tipa napada koji se analizira.

3.2.2 Transportni sloj

TCP (Transmission Control Protocol) je jedan od najvažnijih protokola u okviru internet protokola, koji omogućava pouzdani prenos podataka između dva uređaja preko mreže. TCP funkcioniše na četvrtom sloju OSI modela, Transportnom sloju **[21]**.

TCP uspostavlja konekciju pomoću procesa poznatog kao trosmerni handshake, što je prikazano na slici 2. U ovom procesu, klijent šalje SYN paket serveru. Server odgovara sa SYN-ACK paketom, a klijent kompletira uspostavljanje veze slanjem ACK paketa **[22]**.



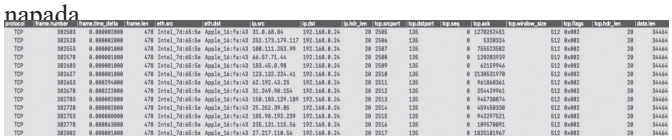
Slika 2: *Proces TCP trosmernog handshake-a, kako je definisano u RFC 793* ***[21]****.*

Međutim, jedna od glavnih slabosti TCP-a je njegova ranjivost na SYN Flood napade. U SYN Flood napadu, napadač šalje veliki broj SYN zahteva serveru, ali nikada ne završava proces slanjem ACK odgovora. Kao rezultat, server biva preopterećen poluotvorenim konekcijama, što troši njegove resurse i sprečava ga da obradi legitimne zahteve.

Slika 3: *Statistika mrežnog saobraćaja tokom SYN Flood napada.*

Slika 3 prikazuje statistiku mrežnog saobraćaja prikupljenu tokom SYN Flood napada. Grafikon ukazuje na značajan porast dolaznih paketa, uz mali broj izlaznih odgovora. U ovom eksperimentu, korišćen je alat `hping3` za pokretanje SYN Flood napada, poznat alat za slanje velikog broja SYN zahteva ka ciljanom serveru **[23]**. Wireshark je korišćen za praćenje i snimanje mrežnog saobraćaja, jasno pokazujući ogroman broj SYN zahteva i rezultirajuće uskraćivanje usluge.

Detaljnija analiza prikupljenog saobraćaja otkriva razmere poplave SYN zahteva, prikazujući snagu i uticaj ove vrste napada.



Slika 4: *SYN Flood napad snimljen Wireshark-om.*

Slika 4 prikazuje SYN Flood napad uhvaćen u Wireshark-u, gde mrežni saobraćaj pokazuje veliki broj ponavljajućih SYN zahteva bez odgovarajućih ACK odgovora. Ovaj obrazac paketa naglašava prirodu napada, gde je server preplavljen pokušajima povezivanja, što dovodi do iscrpljivanja resursa. Konzistentne dužine frejmova i odredišni portovi dodatno ukazuju na ponavljajuću prirodu napada, čineći ga lakim za detekciju pomoću modela mašinskog učenja, poput *CatBoost*-a, koji identifikuju anomalije u protoku saobraćaja.

Slično tome, sproveden je PING Flood napad koristeći isti alat, šaljući veliki broj ICMP Echo zahteva (PING) kako bi se preplavila mreža. Ovaj napad je rezultirao ozbiljnim kašnjenjem u mreži i gubitkom paketa. Wireshark je snimio i analizirao napad, potvrđujući visoko kašnjenje i značajan gubitak paketa, što su uobičajeni indikatori PING Flood napada **[24]**.

protocol	frame.number	frame.time_delta	frame.len	eth.src	eth.dst	ip.src	ip.dst	ip.hdr_len	icmp.type
ICMP	776	0.351392000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	811	0.535928000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	812	1.024157000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	813	0.983132000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	826	0.649353000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	839	0.176153000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	852	0.315215000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	870	0.585751000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	871	0.921780000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	1628	0.053767000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	2151	0.135025000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	2239	0.007052000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	2256	0.409440000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	5000	0.000671000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	5670	0.049695000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	5889	0.033557000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	6098	0.178842000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	7182	0.009766000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	7473	0.004942000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	7579	0.037493000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	7782	0.005068000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	7859	0.044336000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0
ICMP	7881	0.000002000	42	Intel_7d:65:5e	Apple_16:fa:43	192.168.0.23	192.168.0.16	20	0

Slika 5: Rezultati snimanja mrežnog saobraćaja tokom PING Flood napada.

Slika 5 prikazuje mrežni saobraćaj snimljen tokom PING Flood napada. U ovom slučaju, Wireshark otkriva veliki broj ICMP Echo zahteva (PING-ova) koji su brzo poslati sa jednog izvora, uz minimalan odgovor cilja. Ponavljajuća priroda ICMP zahteva, zajedno sa kratkim intervalima između paketa, čini ovaj napad prepoznatljivim modelima kao što je *Naivni Bajes*, koji su izuzetno efikasni u identifikovanju statističkih anomalija u distribuciji paketa.

3.3 Konsolidacija podataka

Ovaj proces je doveo do integracije prikupljenih podataka u jedinstven skup podataka, u kojem su svi uspešni napadi zabeleženi. Svaka sesija je dalje ručno analizirana kako bi se filtrirali nebitni podaci, a relevantni paketi su izvezeni. Na taj način, označen skup podataka je jasno odvojio normalne mrežne aktivnosti od saobraćaja generisanog napadima.

Tokom faze pretprocesiranja, podaci su analizirani na osnovu vremenskih intervala između paketa i zastavica vezanih za protokole. Visoka multikolinearnost unutar varijanse skupa podataka je od suštinskog značaja, jer se koristi korelaciona matrica za procenu povezanosti atributa. Ovaj pristup omogućava da se obezbedi kvalitetna selekcija karakteristika kako bi performanse modela bile optimizovane. Detalji o kolonama u skupu podataka prikazani su u tabeli 1.

Atribut	Opis
protokol	Identifikuje protokol korišćen u paketu (TCP, ARP, ICMP).
frame.number	Broj frejma u listi paketa, prati redosled komunikacije.
frame.time_delta	Razlika u vremenu između uzastopnih paketa, otkriva anomalije.
frame.len	Dužina frejma u bajtovima.
eth.src	MAC adresa izvora, identifikuje poreklo saobraćaja.
eth.dst	MAC adresa odredišta, prati komunikaciju uređaja.
arp.src.proto_ipv4	Izvorna IPv4 adresa u ARP zahtevima, ključna za detekciju napada.
arp.dst.proto_ipv4	IPv4 adresa u ARP zahtevima, identifikuje neovlašćene mape.

arp.src.hw_mac	Izvorna MAC adresa u ARP zahtevima, proverava autentičnost ARP-a.
arp.dst.hw_mac	MAC adresa odredišta u ARP zahtevima, detektuje ARP trovanje.
arp.opcode	Označava da li je ARP poruka zahtev ili odgovor.
ip.src	Izvorna IP adresa, određuje poreklo saobraćaja.
ip.dst	Odredišna IP adresa, prati destinaciju saobraćaja.
tcp.srcport	Izvorni TCP port, ukazuje na uslugu kojoj se pristupa.
tcp.dstport	TCP port odredišta, detektuje neovlašćene pokušaje pristupa.
tcp.seq	TCP redni broj, održava redosled paketa.
tcp.ack	TCP broj potvrde, prati status sesije.
tcp.window_size	TCP veličina prozora, detektuje zagušenja ili napade u mreži.
tcp.flags	TCP zastavice koje označavaju stanje konekcije, ključne za SYN flood.
ip.hdr_len	Dužina IP zaglavlja, detektuje taktike izbegavanja.
tcp.hdr_len	Dužina TCP zaglavlja, osigurava pravilnu funkcionalnost sesije.
data.len	Dužina korisničkih podataka, detektuje napade prepunjavanja bafera.
icmp.type	Tip ICMP poruke, identifikuje PING flood napade.
oznaka	Binarna oznaka: 0 za benigni saobraćaj, 1 za zlonamerni.

Tabela 1: *Atributi skupa podataka za analizu saobraćaja napada i normalnog saobraćaja.*

4 EKSPERIMENTI I REZULTATI

U sledećoj sekciji prikazan je pregled eksperimentalne postavke i rezultata klasifikacije i detekcije sajber napada u bežičnoj mreži korišćenjem modela mašinskog učenja. U radu se koristi metrika *Receiver Operating Characteristic Area Under the Curve (ROC-AUC)* za evaluaciju performansi modela. ROC kriva prikazuje odnos između stope tačno pozitivnih (senzitivnosti) i stope lažno pozitivnih (1-specifičnosti) za različite pragove klasifikacije. AUC se odnosi na površinu ispod ROC krive, sa vrednostima u rasponu od 0 do 1, pri čemu vrednost bliža 1 označava bolje performanse modela u razlikovanju klasa **[25]**.

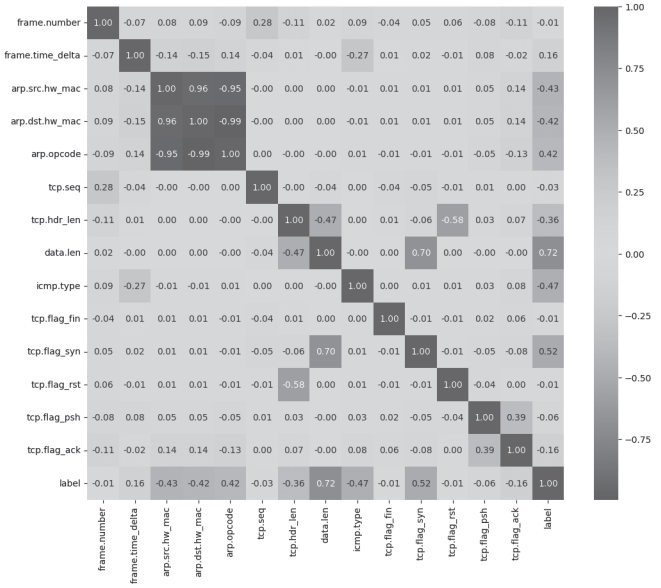
Skup podataka je generisan simulacijom napada, kombinovanjem regularnog saobraćaja sa specifičnim tipovima napada. Glavni cilj ove studije je procena sposobnosti modela da identifikuju i klasifikuju različite vrste napada, uz održavanje mogućnosti generalizacije na nepoznate podatke.

Korišćeni su različiti modeli, uključujući CatBoost, LightGBM, Random Forest, Gradient Boosting, Logističku regresiju, XGBoost, Naivni Bajes i KNN. Ovi modeli pružaju uvid u efikasnost svakog pristupa za detekciju različitih sajber napada, od jednostavnih obrazaca do složenijih napada koji zavise od vremena. Sledeće sekcije opisuju razvijene modele, korišćene metode pretprocesiranja i rezultate performansi eksperimenata.

4.1 Pretprocesiranje

Pretprocesni postupak primenjen na skupove podataka za napade ARP Spoofing, SYN Flood i PING Flood bio je od ključnog značaja za obezbeđivanje visokokvalitetnih podataka za modele mašinskog učenja, sa fokusom na čišćenje, transformaciju i balansiranje podataka kako bi se obezbedila optimalna obuka i testiranje modela. Ovaj sveobuhvatan postupak omogućio je adekvatnu pripremu mrežnih podataka, koji su obično sastavljeni od mnogobrojnih mrežnih karakteristika, kao što su tipovi protokola, izvorne i odredišne adrese, brojevi portova i TCP zastavice.

Prvi korak uključivao je učitavanje sirovih podataka u okruženje, nakon čega je sledila početna selekcija karakteristika. Iako određene karakteristike, poput izvornih i odredišnih adresa ili identifikatora paketa, ponekad mogu doprineti curenju informacija ili pretreniravanju modela, mnoge od ovih karakteristika su zadržane zbog njihove važnosti u identifikaciji zlonamernih obrazaca u mrežnom ponašanju. Ovaj korak je obezbedio zadržavanje ključnih karakteristika potrebnih za detekciju različitih mrežnih napada, uz eliminaciju nebitnih ili previše prediktivnih kolona, čime se smanjio rizik od pristrasnosti modela.



Slika 6: *Korelaciona matrica skupa podataka.*

Nakon selekcije ključnih karakteristika, fokus je prebačen na obradu nedostajućih vrednosti. Za numeričke kolone, nedostajuće vrednosti su imputirane korišćenjem prosečne vrednosti svake kolone. Kategorizovani podaci, kao što su tipovi protokola, imputirani su najčešće korišćenim vrednostima. Ovaj proces imputacije obezbedio je integritet podataka bez stvaranja veštačkih pristrasnosti koje bi mogle ometati sposobnost modela da se generalizuje.

Zatim su numeričke karakteristike normalizovane na standardnu skalu, što je naročito važno za modele poput Logističke regresije i K-najbližih suseda (KNN), koji su osetljivi na relativno skaliranje ulaznih karakteristika. Ovaj korak je sprečio dominaciju karakteristika sa većim opsegom vrednosti tokom procesa obuke i omogućio balansirano učenje svih ulaznih karakteristika.

Takođe, kategorizovane karakteristike su kodirane korišćenjem one-hot kodiranja, pretvarajući ih u binarne vektore kako bi

postale kompatibilne sa algoritmima mašinskog učenja. Ova transformacija je omogućila modelima kao što su Random Forest i Gradient Boosting da efikasno obrađuju kategorizovane podatke.

Kako bi se dalje optimizovao skup podataka i smanjila složenost obrade, primenjena je analiza glavnih komponenti (PCA). Ova tehnika smanjenja dimenzionalnosti zadržala je 95\% varijanse podataka dok je uklonila neinformativne ili šumne karakteristike. Kao rezultat, podaci su postali kompaktniji, smanjujući šanse za pretreniravanje uz zadržavanje visokih performansi predikcije. PCA je bila posebno korisna u smanjenju računarskog opterećenja prilikom obuke modela na podacima visoke dimenzionalnosti.

Zbog izrazito neuravnoteženih podataka u mrežnom saobraćaju, posebno za detekciju napada, primenjene su tehnike poput SMOTE i TomekLinks. Ove metode su pomogle u balansiranju skupa podataka generisanjem sintetičkih uzoraka za manjinsku klasu (zlonamerni saobraćaj) i uklanjanjem preklapajućih uzoraka, čime su modeli mogli učiti iz regularnog i napadačkog saobraćaja bez pristrasnosti prema većinskoj klasi. Ovaj balans bio je ključan za poboljšanje recall-a (sposobnosti detekcije napada), uz zadržavanje preciznosti.

Poslednji korak pretprocesiranja uključivao je podelu skupa podataka na trening i test setove u odnosu 80:20, kako bi se osiguralo da modeli budu trenirani i testirani na različitim podskupovima podataka. Podela je bila stratifikovana, što znači da su trening i test setovi zadržali originalnu raspodelu klasa, omogućavajući reprezentativnu evaluaciju performansi modela.

Nakon pretprocesiranja, podaci su bili spremni za obuku i testiranje modela, a sve transformacije su sačuvane radi buduće reproduktivnosti i implementacije modela.

4.1.1 Detekcija SYN Flood napada

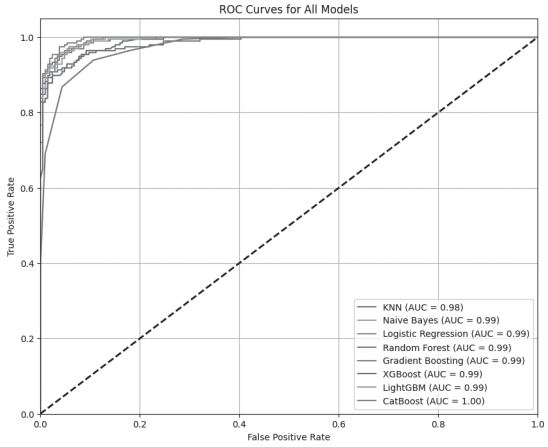
U zadatku detekcije SYN Flood napada, modeli su pokazali snažne performanse prema svim metrikama, pri čemu su se CatBoost i Logistička regresija posebno istakli. CatBoost je postigao tačnost od 96.53\% i izvanredan ROC-AUC od 0.9961, što ukazuje na visoku sposobnost razlikovanja. Logistička regresija je pratila sa tačnošću od 96.03\% i ROC-AUC rezultatom od 0.9945, pokazujući sličnu efikasnost. Ostali modeli, poput Gradient Boosting-a i Naivnog Bajesa, takođe su se dobro pokazali sa stopama tačnosti od 95.28\% i 94.29\%, respektivno, pružajući pouzdane i konzistentne rezultate. Iako je KNN pokazao relativno nižu tačnost (89.08\%), postigao je respektabilan ROC-AUC od 0.9759, što naglašava njegovu sposobnost da efikasno rešava specifične scenarije. Sledeća tabela prikazuje ključne metrike performansi za sve modele:

Model	Tačnost	Preciznost	Recall	F1 Skor	ROC-AUC
CatBoost	0.965261	0.959799	0.969543	0.964646	0.996057
Logistička regresija	0.960298	0.973822	0.944162	0.958763	0.99448
Gradient Boosting	0.952854	0.968421	0.93401	0.950904	0.992805
Naivni Bajes	0.942928	0.910377	0.979695	0.943765	0.994012
LightGBM	0.942928	0.953125	0.928934	0.940874	0.993495
XGBoost	0.935484	0.943005	0.923858	0.933333	0.987568
Random Forest	0.935484	0.947644	0.918782	0.93299	0.986447
KNN	0.890819	0.837004	0.964467	0.896226	0.975975

Tabela 2: *Rezultati detekcije SYN Flood napada.*

Kao što je prikazano, boosting modeli poput CatBoost-a i Gradient Boosting-a su se posebno istakli u detekciji SYN Flood napada, postižući visoke rezultate tačnosti i ROC-AUC skorova. Logistička regresija je takođe pokazala izvanredne rezultate, demonstrirajući svoju sposobnost da upravlja velikim skupovima podataka i efikasno razlikuje napadački saobraćaj od benignog.

ROC krive za sve modele, prikazane na slici 7, vizuelno upoređuju stvarnu stopu pozitivnih rezultata naspram lažno pozitivnih rezultata. Krive potvrđuju da boosting modeli i Logistička regresija zadržavaju superiorne performanse klasifikacije sa visokim vrednostima AUC. Nasuprot tome, drugi modeli poput KNN-a, iako ostvaruju niže rezultate po nekim metrikama, i dalje nude respektabilne sposobnosti detekcije u specifičnim scenarijima.



Slika 7: *ROC krive za sve modele u zadatku detekcije SYN Flood napada.*

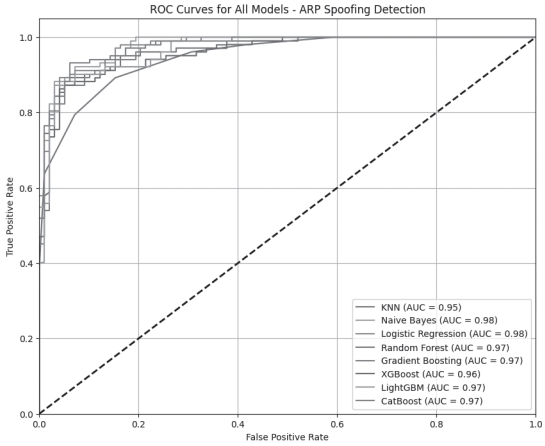
4.1.2 Detekcija ARP Spoofing napada

U eksperimentima za detekciju ARP Spoofing napada, Random Forest je postigao najvišu tačnost od 97.00\%, uz preciznost od 0.98, što odražava njegovu sposobnost da precizno razlikuje regularni od lažnog saobraćaja. Naivni Bajes je ostvario slične rezultate sa tačnošću od 96.5\% i preciznošću od 0.98, ali je njegov recall (95.1\%) bio nešto niži u poređenju sa Random Forest-om, što ukazuje na manji kompromis u osetljivosti. CatBoost je takođe postigao visoke rezultate, usklađujući se sa Random Forest-om po pitanju tačnosti i recall-a (97.06\%), dok je Logistička regresija postigla konkurentne rezultate sa tačnošću od 96.00\% i solidnim performansama prema svim metrikama. Ostali modeli, poput Gradient Boosting-a, KNN-a i LightGBM-a, postigli su respektabilne tačnosti između 95\% i 96\%, pri čemu se KNN posebno istakao po visokom recall-u (99.02\%), iako je njegova preciznost bila nešto niža. XGBoost, iako nešto iza po tačnosti (94.5\%), i dalje je pokazao pouzdane performanse prema svim ključnim metrikama.

Model	Tačnost	Preciznost	Recall	F1 Skor	ROC-AUC
CatBoost	0.97	0.970588	0.970588	0.970588	0.994498
Random Forest	0.97	0.98	0.960784	0.970297	0.992297
Naivni Bajes	965	0.979798	0.95098	0.965174	0.992797
Logistička regresija	0.96	0.97	0.95098	0.960396	0.991497
Gradient Boosting	955	0.942857	0.970588	0.956522	0.991196
KNN	0.95	0.918182	0.990196	0.95283	0.985194
LightGBM	0.95	0.933962	0.970588	0.951923	0.991897
XGBoost	945	0.933333	0.960784	0.94686	0.989196

Tabela 3: *Rezultati detekcije ARP Spoofing napada.*

ROC krive za sve modele testirane u zadatku detekcije ARP Spoofing napada prikazane su na slici 8. ROC-AUC vrednosti za sve modele ukazuju na izuzetne performanse klasifikacije, pri čemu većina modela postiže ROC-AUC skorove iznad 0.97. KNN, iako ima visok recall, pokazuje nešto niži ROC-AUC od 0.95, što ukazuje na manji kompromis u preciznosti u poređenju sa drugim modelima, kao što su Naivni Bajes i Logistička regresija.



Slika 8: *ROC krive za sve modele - Detekcija ARP Spoofing napada.*

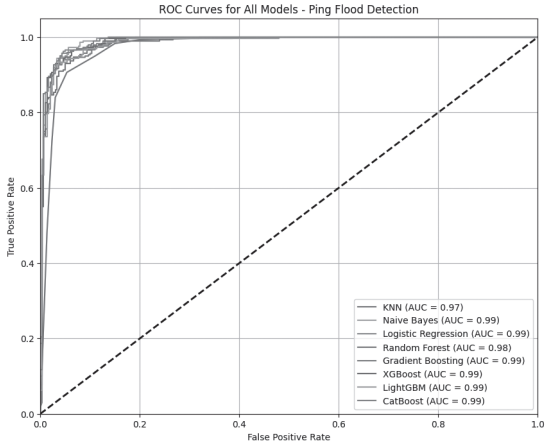
4.1.3 Detekcija PING Flood Napada

U zadatku detekcije PING Flood napada, XGBoost i Naivni Bajes su pokazali uporedive performanse. XGBoost je postigao tačnost od 96.67\% uz F1 skor od 0.9668, što naglašava njegove snažne sposobnosti generalizacije. Naivni Bajes je postigao nešto bolje rezultate sa tačnošću od 97.83\% i F1 skorom od 0.9784, što ukazuje na njegovu efektivnu ravnotežu između preciznosti i recall-a. CatBoost i Logistička regresija su takođe postigli visoke rezultate, oba sa tačnošću od 97.17\%, iako su bili nešto slabiji u poređenju sa XGBoost i Naivnim Bajesom. KNN se istakao izuzetnim recall-om od 99.33\%, mada sa nešto nižom preciznošću, što je rezultiralo ukupnom tačnošću od 97.67\%. Ostali modeli, poput Random Forest i LightGBM, takođe su pokazali dosledne performanse sa tačnostima između 96.17\% i 96.33\%, pružajući pouzdane, ali nešto niže rezultate u poređenju sa najboljim modelima.

Model	Tačnost	Preciznost	Recall	F1 Skor	ROC-AUC
Naivni Bajes	0.9783	0.9767	0.98	0.9784	0.9978
KNN	0.9767	0.9613	0.9933	977	0.9983
Logistička regresija	0.9717	0.9639	0.98	0.9719	0.9952
CatBoost	0.9717	967	0.9767	0.9718	0.9954
XGBoost	0.9667	0.9636	0.97	0.9668	0.9951
Random Forest	0.9633	0.9696	0.9567	0.9631	0.9949
LightGBM	0.9617	0.9571	0.9667	0.9619	0.9944
Gradient Boosting	0.9533	0.9533	0.9533	0.9533	0.9942

Tabela 4: *Rezultati detekcije PING Flood napada.*

ROC krive dalje potvrđuju visoke performanse svih modela u detekciji PING Flood napada. Gotovo svi modeli su prikazali izvanredne ROC-AUC vrednosti iznad 0.99. Naivni Bajes i KNN su pokazali izuzetne sposobnosti klasifikacije sa ROC-AUC rezultatima od 0.997 i 0.998, respektivno. Logistička regresija, CatBoost i XGBoost su takođe pokazali pouzdane performanse, sa ROC-AUC rezultatima između 0.995 i 0.996. Iako je Gradient Boosting imao najniži AUC od 0.994, i dalje je pokazao visoku sposobnost razlikovanja napadačkog od regularnog saobraćaja. ROC krive podržavaju rezultate tačnosti i F1 skora, naglašavajući sposobnost modela da efikasno detektuju PING Flood napade.



Slika 9: *ROC krive za sve modele - Detekcija PING Flood napada.*

5 ZAKLJUČAK

Na osnovu rezultata i nalaza, ovo istraživanje je dokazalo da su modeli mašinskog učenja, posebno metode ansambla poput CatBoost, Random Forest i algoritmi za boosting, izuzetno efikasni u detekciji i prevenciji mrežnih napada poput ARP spoofing, SYN flood i PING flood u bežičnim mrežama. Visoke vrednosti tačnosti, F1 skora i ROC-AUC metrika različitih modela ukazale su na njihovu sposobnost razlikovanja između normalnog i zlonamernog saobraćaja.

U detekciji SYN Flood napada, CatBoost je postigao tačnost od 96.53%, dok je Logistička regresija imala tačnost od 96.03%, sa ROC-AUC rezultatima od 0.9961 i 0.9945. Random Forest je pružio najbolje rezultate u detekciji ARP Spoofing napada, sa ROC-AUC rezultatom od 0.9700 i 0.9923. U

detekciji PING Flood napada, Naivni Bajes je postigao tačnost od 97.83% sa ROC-AUC rezultatom od 0.9977, dok je KNN ostvario recall od 99.33\% i ROC-AUC od 0.9983.

Dalja validacija modela je potvrđena kroz ROC krive za svaki napad, gde su gotovo svi modeli ostvarili ROC-AUC vrednosti iznad 0.99, što ukazuje na njihovu sposobnost da efikasno klasifikuju neuravnotežene skupove podataka, što je ključni zahtev za bezbednost mreža u realnom vremenu.

Ovi rezultati podržavaju tvrdnju da modeli mašinskog učenja, poput CatBoost-a i Gradient Boosting-a, u kombinaciji sa tradicionalnim modelima, mogu predstavljati osnovu za napredne sigurnosne okvire. Takvi okviri će biti ključni u kontekstu rastućih sajber pretnji unutar IoT i BYOD okruženja.

Buduća istraživanja mogu predložiti hibridne pristupe detekciji anomalija, integrišući mašinsko učenje sa tehnikama dubokog učenja, kao što su one zasnovane na RNN-ovima. Ovi radovi će biti ključni za velike mreže, gde pretnje evoluiraju i zahtevaju gotovo trenutni nadzor. Ova studija postavlja temelje za buduća istraživanja o primeni mašinskog učenja u bezbednosti mreža.

6 LITERATURA

[1] A. A. Khan, A. A. Laghari, Z. A. Shaikh, Z. D. Pikiewicz, and S. Kot, "Internet of Things (IoT) Security With Blockchain Technology: A State-of-the-Art Review," IEEE Access, vol. 10, pp. 122679-122695, Nov. 2022, doi: 10.1109/ACCESS.2022.3223370.

[2] R. Palanisamy, A. A. Norman, and M. L. M. Kiah, "Compliance with bring your own device security policies in organizations: A systematic literature review," Computers & Security, vol. 98, p. 101998, Nov. 2020, doi: 10.1016/j.cose.2020.101998.

[3] M. I. Ali, S. Kaur, A. Khamparia, D. Gupta, S. Kumar, A. Khanna, and F. A. Turjman, "Security Challenges and Cyber Forensic Ecosystem in IoT Driven BYOD Environment," IEEE Access, vol. 8, pp. 172770-172782, Sep. 2020, doi: 10.1109/ACCESS.2020.3024784.

[4] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller, "Landscape of IoT security," Computer Science Review, vol. 44, art. no. 100467, May 2022, doi: 10.1016/j.cosrev.2022.100467.

[5] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," Journal of Big Data, vol. 7, no. 41, Jul. 2020, doi: 10.1186/s40537-020-00318-5.

[6] B. Ghimire and D. B. Rawat, "Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things," IEEE Internet of Things Journal, vol. 9, pp. 8229-8249, Jun. 2022, doi: 10.1109/JIOT.2022.3150363.

[7] W. B. W. Mariam and Y. N. Shiferaw, "Performance Evaluation of Machine Learning Algorithms for Detection of SYN Flood Attack," in IEEE Africon, Arusha, Tanzania, Sep. 2021, doi: 10.1109/AFRICON51333.2021.9570968.

[8] S. Al-Juboori, F. Hazzaa, Z. S. Jabbar, and S. Salih, "Man-in-the-middle and denial of service attacks detection using machine learning algorithms," Bulletin of Electrical Engineering and Informatics, vol. 12, no. 1, pp. 418-426, Feb. 2023, doi: 10.11591/eei.v12i1.4555.

[9] D. Protic and M. Stankovic, "XOR-Based Detector of Different Decisions on Anomalies in the Computer Network Traffic," Romanian Journal of Information Science and Technology, vol. 26, no. 3-4, pp. 323-338, Sep. 2023, doi: 10.59277/ROMJIST.2023.3-4.06.

[10] J. Kponyo, J. Agyemang, and G. S. Klogo, "Detecting End-Point (EP) Man-In-The-Middle (MITM) Attack based on ARP Analysis: A Machine Learning Approach," International Journal of Communication Networks and Information Security, vol. 12, no. 3, pp. 384-388, May 2020, doi: 10.22541/au.158938565.57807215.

[11] G. M. A. Sukkar, R. Salfan, S. Khwaldeh, and M. Maqableh, "Address Resolution Protocol (ARP): Spoofing Attack and Proposed Defense," Communications and Network, vol. 7, no. 3, pp. 118-130, Aug. 2016, doi: 10.4236/cn.2016.83012.

[12] A. Michelena, J. Aveleira, E. Jove, and M. Bayon, "A novel intelligent approach for man-in-the-middle attacks detection over internet of things environments based on message queuing telemetry transport," Expert Systems, vol. 41, no. 2, p. 15, Feb. 2023, doi: 10.1111/exsy.13263.

[13] V. Ndatinya, Z. Xiao, V. R. Manepalli, K. Meng, and Y. Xiao, "Network forensics analysis using Wireshark," International Journal of Security and Networks, doi: 10.1504/IJSN.2015.070421.

[14] M. Greenacre, P. J. F. Groenen, T. Hastie, A. I. d'Enza, A. Markos, and E. Tuzhilina, "Principal Component Analysis," Nature Reviews Methods Primers, vol. 2, no. 100, Dec. 2022, doi: 10.1038/s43586-022-00184-w.

[15] D. Dablain, B. Krawczyk, and N. V. Chawla, "DeepSMOTE: Fusing Deep Learning and SMOTE for Imbalanced Data," IEEE Transactions on Neural Networks and Learning Systems, vol. 34, pp. 6390-6404, Sep. 2023, doi: 10.1109/TNNLS.2021.3136503.

[16] F. Swana, W. Doorsamy, and P. Bokoro, "Tomek Link and SMOTE Approaches for Machine Fault Classification with an Imbalanced Dataset," Sensors, vol. 22, p. 3246, Apr. 2022, doi: 10.3390/s22093246.

[17] K. W. R. James and F. Kurose, Link-Layer Addressing and ARP, Computer Networking, Pearson, pp. 468-474, 2017.

[18] R. Kaur, G. Singh, and S. Khurana, "A Security Approach to Prevent ARP Poisoning and Defensive tools," International Journal of Computer and Communication System Engineering (IJCCSE), vol. 2, no. 3, pp. 431-437, Jun. 2015.

[19] Bettercap, "Bettercap," [Online]. Available: https://www.bettercap.org. [Accessed: 16-Aug-2024].

[20] F. P. E. Putra, U. Ubaidi, A. B. Tamam, and R. W. Efendi, "Implementation And Simulation Of Dynamic Arp Inspection In Cisco Packet Tracer For Network Security," Brilliance Research of Artificial Intelligence, vol. 4, no. 1, pp. 340-347, May 2024, doi: 10.47709/brilliance.v4i1.4199.

[21] J. Postel, "Transmission Control Protocol, RFC 793," [Online]. Available: https://datatracker.ietf.org/doc/html/rfc793. [Accessed: 16-Aug-2024].

[22] B. Dowling, M. Fischlin, F. Günther, and D. Stebila, "A Cryptographic Analysis of the TLS 1.3 Handshake Protocol," Journal of Cryptology, vol. 34, no. 37, Feb. 2023, doi: 10.1007/s00145-021-09384-1.

[23] Kali Linux Organization, "hping3," [Online]. Available: https://www.kali.org/tools/hping3. [Accessed: 16-Aug-2024].

[24] D. Stiawan, M. E. Suryani, Susanto, M. Y. Idris, M. N. Aldalaien, N. Alsharif, and R. Budiarto, "Ping Flood Attack Pattern Recognition Using a K-Means Algorithm in an Internet of Things (IoT) Network," IEEE Access, vol. 9, pp. 116475-116484, doi: 10.1109/ACCESS.2021.3105517.

[25] A. M. Carrington, D. G. Manuel, P. W. Fieguth, T. Ramsay, V. Osmani, B. Wernly, C. Bennett, S. Hawken, O. Magwood, Y. Sheikh, M. McInnes, and A. Holzinger, "Deep ROC Analysis and AUC as Balanced Average Accuracy, for Improved Classifier Selection, Audit and Explanation," IEEE Transactions On Pattern Analysis And Machine Intelligence, vol. 45, no. 1, pp. 329-341, Jan. 2023, doi: 10.1109/TPAMI.2022.3145392.

mast. inž. Aleksandar Rakić, student doktorskih akademskih studija na smeru Informacioni sistemi i tehnologije na Fakultetu organizacionih nauka, Univerziteta u Beogradu.
Kontakt: aleksandar.rakic@yahoo.com
Oblasti interesovanja: sajber bezbednost, mašinsko učenje, cloud tehnologije, detekcija sajber pretnji.