UNIVERZITET CRNE GORE

PRIRODNO-MATEMATIČKI FAKULTET, PODGORICA

UNIVERZITET CRNE GORE
PRIRODNO-MATEMATIČKI FAKULTET
Broj 2025/01-311
Podgorica: 17.02.2025 god.

Vijeću Prirodno-matematičkog fakulteta Univerziteta Crne Gore

Predmet: Izvještaj komisije o pregledu i ocjeni master rada Damira Delijića

Vijeće Prirodno-matematičkog fakulteta na sjednici održanoj 08. 11. 2024. godine, donijelo je Odluku o imenovanju komisije za ocjenu master rada "Detekcija *SIMBox* prevare u telekomunikacionim sistemima", kandidata Damira Delijića, u sastavu:

Prof. dr Savo Tomović, redovni profesor PMF – mentor;

Doc. dr Igor Jovančević, docent PMF – član;

Prof. dr Milenko Mosurović, redovni profesor PMF – član.

Kandidat Damir Delijić je dana 29. 11. 2024. godine predao rukopis master rada na uvid javnosti i ocjenu. Nakon uvida u podneseni materijal, a u vezi sa članom 22 Pravila studiranja na master studijama, podnosimo sljedeći

IZVJEŠTAJ

Master rad pod nazivom "Detekcija *SIMBox* prevare u telekomunikacionim sistemima", kandidata Damira Delijića je iz oblasti računarskih nauka, a uže oblasti rada su rudarenje podataka i detekcija anomalija. Rad je napisan na 60 strana kucanog teksta. Sastoji se iz pet glava, zaključka i literature sa 28 bibliografskih jedinica. Svaka glava je podijeljena na više poglavlja u kojima se obrađuje jedna logička cjelina.

Prva glava je uvodnog karaktera. U ovoj glavi ukratko je opisan domen problema. Pored toga navedene su metode i algoritmi detekcije anomalija koji se koriste u radu. Navedeno je da rad doprinosi rješavanju problema nedostatka *ground truth*-a kod *SIMBox* prevare.

U drugoj glavi izložen je pregled literature. Literatura se u ovom dijelu odnosi na šire pojmove telekomunikacionih prevara i detekcije anomalija, ali i na uže kao što je detekcija konkretno *SIMBox* prevare i algoritme detekcije anomalija. Osim toga navedeni su i sajtovi na kojima se mogu naći provajderi usluga terminacije saobraćaja, za potrebe analize njihovih metoda.

U trećoj glavi se pruža teorijska osnova koja je neophodna za razumijevanje *SIMBox* prevare i metoda detekcije. U prvom dijelu poglavlja se vrši upoznavanje sa telekomunikacionim ekosistemom i daje se pregled telekomunikacionih elemenata i procesa koji su relevantni za ovu vrstu prevare: mreže, rutiranje poziva i zapisi poziva. Drugi dio poglavlja odnosi se na telekomunikacione prevare u najširem smislu, najzastupljenijim tipovima, metodama detekcije i izazovima prilikom

detekcije. Treći dio odnosi se konkretno na *SIMBox* prevaru i daje detaljan pregled bitnih pojmova, metoda detekcije, izazova, metoda izbjegavanja detekcije i najčešće korišćenih arhitektura. Na kraju se nalazi uvod u osnove procesa detekcije anomalija.

Četvrta glava odnosi se na metodologiju rada koja uključuje testiranje algoritama detekcije nad skupom podataka koji predstavljaju zapise poziva. Poglavlje sadrži pojašnjena procesa konsolidacije, selekcije, čišćenja i agregacije podataka u vektor karakteristika. Zatim prikazuje korak ekploracione analize koji se ogleda u vizualizacijama *dataset*-a i analizi korelacija. Na kraju poglavlja se nalazi faza modeliranja i opisan je korak ispravljanja krivih distribucija i uklanjanje izuzetaka.

U petoj glavi analiziraju se rezultati implementacije navedenih algoritama i metoda.

Ovaj master rad istražuje problem detekcije *SIMBox* prevara u telekomunikacionim sistemima, koristeći nenadgledane algoritme mašinskog učenja. Ova prevara se nalazi među najzastupljenijim telekomunikacionim prevarama i primarni motiv joj je finansijski benefit koji se zasniva na razlici cijena lokalnih i internacionalnih poziva. Realizuje se preusmjeravanjem internacionalnih poziva sa regularnih ruta na kompromitovane i terminiranjem poziva kao lokalnog. Glavni cilj ovog istraživanja je ispitivanje primjene algoritama detekcije anomalija u kontekstu otkrivanja *SIMBox* prevare na osnovu podataka o korisničkom pozivnom saobraćaju.

Ostali ciljevi istraživanja uključuju: 1) inžinjering karakteristika koje daju adekvatan opis korisnika u datom kontekstu i koje se izračunavaju brzo i efikasno za velik broj korisnika, 2) optimizaciju inžinjeringa karakteristika kreiranjem atributa koji su nezavisni od vremenskog konteksta koji analiza obuhvata, 3) primjenu algoritama nenadgledanog učenja za detekciju anomalija, kao što su LOF (*Local Outlier Factor*), IF (*Isolation Forest*), OCSVM (*One-Class Support Vector Machine*) nad realnim skupovima podataka u kombinaciji sa vještački generisanim instancama, 4) evaluaciju performansi algoritama uz pomoć standardnih metrika kao što su preciznost, odziv i slične.

Kako bi se ostvarili postavljeni ciljevi i dali odgovori na istraživačka pitanja korišćene su različite metode. Osnovna metoda prati standardne korake implementacije modelaza detekciju anomalija: prikupljanje i analiza podataka, obrada i prepocesiranje podataka, implementacija odgovarajućeg modela, testiranje i analiza rezultata. Za upoređivanje performansi implementiranih modela korišćene su metrike poput preciznosti, odziva i F1 mjere. Algoritmi su testirani prvo nad podacima koji obuhvataju period od mjesec dana. U radu je navedeno da je algoritmu koji je radio najduže trebalo u prosjeku oko tri minuta za detekciju anomalija.

Navedeni algoritmi su bili sposobni da prepoznaju prevarantske instance koje se značajno razlikuju od uobičajenih korisničkih obrazaca, pružajući time alternativu sistemima nadgledanog učenja koji zahtijevaju označene podatke, i tradicionalnim sistemima zasnovanim na pravilima koji često nisu prilagodljivi dinamičnim i sofisticiranim taktikama izvršilaca prevare. U okviru istraživanja, poseban fokus je stavljen na inženjering karakteristika, pri čemu je kreiran skup od 17 atributa koji opisuju različite aspekte korisničkih pozivnih navika. Konstrukcija skupa atributa za nekoliko stotina hiljada korisnika je u toku rada na praktičnom dijelu svedena na svega nekoliko minuta što ukazuje na visok stepen efikasnosti u praktičnoj primjeni. Algoritam koji se najbolje pokazao je *Isolation Forest*, ali to može biti posljedica načina kreiranja prevarantskih instanci i prirode algoritma. Eksperimentisanje sa različitim konfiguracijama parametara modela i procesima preprocesiranja podataka pokazalo je značajan uticaj ovih faktora na krajnje rezultate. Na primjer, prilagođavanje hiperparametara, kao što su broj susjednih tačaka za LOF ili broj izolacionih stabala za IF, imalo je direktan efekat na preciznost i osjetljivost modela. Poseban izazov u radu predstavljala je potreba za balansiranjem između složenosti modela i njihove interpretabilnosti. Iako su svi

algoritmi pružili kvantitativne mjere anomalija, dodatna analiza je bila potrebna kako bi se rezultati preveli u praktične uvide koji su korisni za operativno osoblje telekomunikacionih kompanija. Rezutati rada naglašavaju potencijal primjene nenadgledanih metoda u detekciji *SIMBox* prevara i ukazuju na potrebu za daljim istraživanjem, posebno u pravcu obogaćivanja *dataset*-ova realnim podacima o prevarama i unapređenja metoda za generisanje vještačkih instanci.

ZAKLJUČAK

Nakon pregledanog master rada komisija konstatuje da rad zadovoljava sve uslove propisane Pravilima studiranja na master studijama. Kandidat je pokazao da odlično poznaje naučnu problematiku, kao i da posjeduje značajan nivo istraživačkih sposobnosti. Stoga, komisija pozitivno ocjenjuje master rad pod nazivom "Detekcija *SIMBox* prevare u telekomunikacionim sistemima", kandidatka Damira Delijića.

Komisija predlaže Vijeću Prirodno-matematičkog fakulteta da rad pod nazivom "Detekcija *SIMBox* prevare u telekomunikacionim sistemima", kandidata Damira Delijića prihvati kao master rad i odobri njegovu javnu usmenu odbranu.

U Podgorici, 31.01.2025. godine

KOMISIJA

Prof. dr Savo Tomović, redovni profesor PMF – mentor;

Doc. dr Igor Jovančević, docent PMF – član;

Prof. dr Milenko Mosurović, redovni profesor PMF – član.