4-52/'23
28.03.2023.

UNIVERZITET SINGIDUNUM

Departman za poslediplomske studije

Danijelova 32, Beograd

Veću Departmanu za poslediplomske studije

Odlukom Veća Departmana poslediplomskih studija Univerziteta Singidunum, donetoj na sednici održanoj 26.01.2023. godine, određeni smo za članove Komisije za odbranu doktorske disertacije pod nazivom "XOR detektor konfliktnih odluka o anomalijama u računarskim mrežama", kandidata Danijele Protić o čemu podnosimo sledeći

I Z V E Š T A J

1. Biografski podaci o kandidatu i doktorskoj disertaciji

Danijela Protić rođena je 1970. godine u Varaždinu. IV beogradsku gimnaziju završila je 1988. godine. Osnovne akademske studije završila je 1995. godine na Fakultetu tehničkih nauka Univerziteta u Novom Sadu, na odseku Elektrotehničke struke i računarstva, smer Elektronika i telekomunikacije, i stekla zvanje diplomiranog inženjera elektrotehnike. Magistarske studije završila je 2001. godine na Elektrotehničkom fakultetu Univerziteta u Beogradu i, odbranom magistarske teze pod nazivom „Analiza neuronskih modela vokala srpskog jezika", stekla akademsko zvanje Magistar elektrotehničkih nauka – oblast telekomunikacije. Izbor u zvanje Stručni savetnik stekla je na osnovu odluke Naučnog veća Tehničkog opitnog centra, 2021. godine.

Više od dve decenije radi u Centru za primenjenu matematiku i elektroniku u Beogradu. U svom naučno – istraživačkom radu objavila je preko 30 naučnih i stručnih radova u časopisima internacionalnog i nacionalnog značaja. Učestvovala je na dva naučna projekta Matematičkog instituta SANU i na jednom projektu CPME. Prvi je autor na listi Vojnotehničkog glasnika po broju radova, čitanosti i citiranosti, a njeni radovi vidljivi su u bazama kao što su: MDPI, Web of Science, IEEEXplore, ResearchGate, Google Schoolar, Academia i dr. Član je IEEE asocijacije od 2022. godine.Kandidatkinja ima objavljen rad kategorije M22 čime je ispunjen preduslov za odbranu doktorske disertacije:

Protic, D., Gaur, L., Stankovic, M., Rahman, M.A. Cybersecurity in smart cities: Detection of opposing decisions of anomalies in the computer network behavior. Electronics, Vol. 11, 3718, 2022. https://doi.org/10.3390/electronics11223718 (M22)

Kandidat je prvi autor i tema rada je direktno povezana sa sadržajem doktorske disertacije.

Kandidat takođe ima niz radova i saopštenja objavljenih na domaćim i međunarodnim naučnim konferencijma

Doktorska disertacija kandidata Danijele Protić je bila podvrgnuta proveri softverom za ustanovljavanje preklapanja i plagijarizma (iThenticate Plagiarism Detection Software). Kada se eliminišu poklapanja u nazivima literature i opštih pojmova koji su košišćeni, stepen preklapanja je jako mali.

2. Predmet i cilj istraživanja

Predmet istraživanja ove disertacije je detekcija konfliktnih odluka o anomalijama u računarskim mrežama. Pojava anomalije u mrežnom saobraćaju je evidentna u svakodnevnom radu računarskih mreža, a anomaliju predstavlja poznata ili nepoznata malicioznost, greške u prenosu podataka, uticaj ljudskog faktora na ponašanje mreže, i niz drugih pojava. Prednost u detekciji anomalija je prepoznavanje nepoznatog malicioznog napada, što se izvodi poređenjem sa statističkim modelom normalnog mrežnog saobraćaja. Osnovni problem u ovom slučaju je što je za evaluaciju modela normalnog ponašanja računarske mreže potrebna velika količina podataka. Binarni klasifikatori bazirani na nadgledanom mašinskom učenju pokazali su se dobrim rešenjem ovog problema. U radu je prikazano pet visoko preciznih modela nadgledanog mašinskog učenja: k-najbližih suseda, k-najbližih suseda sa težinskim koeficijentima, stabla odlučivanja, modeli vektora potpore i feedforward neuronska mreža.

Da bi bilo smanjeno vreme procesuiranja, uz minimalnu degradaciju tačnosti modela, korišćeno je preprocesuiranje kojeg čine dve faze: izbor numeričkih atributa i skaliranje atributa u simetrične granice, uz primenu tangens hiperboličke funkcije i damping strategije Levenberg-Marquardt algoritma. Za prikaz pozitivnog uticaja ovakvog preprocesuiranja na vreme evaluacije i tačnost klasifikatora korišćena je Kyoto 2006+ baza podataka snimljena na pet računarskih mreža unutar i izvan Univerziteta u Kyoto-u, u periodu od 10 godina. Ova baza je jedina javno dostupna baza realnog mrežnog saobraćaja namenjena isključivo za istraživanje detekcije anomalija u računarskim mrežama.

Za izabrane klasifikatore, najveću brzinu procesuiranja ima feedforward neuronska mreža a, iako svi klasifikatori pokazuju izuzetno visoku tačnost, model k-najbližih suseda s težinskim koeficijentima se pokazao najpreciznijim u smislu tačnosti i broja lažnih alarma. Iz tog razloga su ova dva klasifikatora iskorišćena kao osnov za „ekskluzivno ili“ (XOR) detekciju. Kada klasifikatori rade u paraleli na istom mestu u računarskoj mreži oni bi istovremeno trebali ili da detektuju anomaliju ili da mrežni saobraćaj smatraju normalnim. Međutim, s vremena na vreme, dolazi do različite procene o anomaliji, odnosno normalnom saobraćaju, tj. nastaje konflikt. Detektor konflikta je baziran na primeni operacije XOR na izlaze, odnosno odluke klasifikatora. Ukoliko su oba klasifikatora istovremeno detektovala anomaliju ili prepoznala saobraćaj kao normalan, njihova odluka je da konflikta nema. U suprotnom detektovan je konflikt.

U okviru ove disertacije prikazane su mogućnosti poboljšanja tačnosti i procesnog vremena, i mogućnosti dodatne detekcije anomalija koja se izvodi XOR detekcijom. Osnovna hipoteza istraživanja prikazanog u disertaciji glasi:

H: „XOR detekcijom konfliktnih odluka o anomalijama moguće je povećati stepen prepoznavanja malicioznosti i grešaka u računarskim mrežama."

Pojedinačne hipoteze koje su korišćene glase:

H1: „Izborom skaliranja tipa hiperboličkog tangensa i damping strategije Levenberg-Marquardt algoritma moguće je više od dva puta smanjiti vreme procesuiranja bez značajne degradacije tačnosti binarnih klasifikatora."

H2: „Nelinearni binarni klasifikatori sa težinskim koeficijentima pokazuju najbolje karakteristike za primenu u XOR detekciji konfliktnih odluka o anomalijama u računarskim mrežama."

Ciljevi istraživanja

Osnonvi cilj istraživanja je formirati detektor konfliktnih odluka o anomalijama koji je baziran na XOR operaciji primenjenoj na vrednostima izlaza binarnih klasifikatora. Da bi ovaj cilj bio ostvaren, prvo je potrebno izvršiti preprocesuiranje izborom numeričkih atributa iz Kyoto 2006+ baze podataka. Nakon toga je potrebno skalirati izabrane atribute tangens hiperboličkom prenosnom funkcijom sa pravilima koja važe za damping strategiju Levenberg-Marquardt algoritma. Cilj je, u zavisnosti od tačnosti i vremena procesuiranja, izabrati binarne klasifikatore bazirane na nadgledanom mašinskom učenju koji pokazuju najveću tačnost i najmanje vreme procesuiranja, za korišćenje u XOR detekciji. Na kraju, cilj je dokazati da XOR detektor konfliktnih odluka o anomalijama predstavlja značajan alat u dodatnoj detekciji potencijalnih malicioznosti ili grešaka u računarskim mrežama.

Primenjene metode istraživanja

U toku naučno-istraživačkog rada primenjen je niz metoda kako bi bili zadovoljeni metodološki zahtevi za pouzdanost, objektivnost, sistematičnost i ponovljivost rezultata.

U skladu sa izabranom problematikom istraživanja, definisanim ciljevima i postavljenim hipotezama, radi definisanja naučnih i stručnih zaključaka i pronalaženja mogućih rešenja, prvo je izvršeno temeljno istraživanje javno dostupnih referenci i baza podataka.

Metoda kompleksnog posmatranja i analiza sadržaja primenjena je prilikom obrade rezultata istraživanja u onim delovima predložene teme koji se odnose na karakteristike i primenu prikazanih binarnih klasifikatora, koji su dostupni u svetskoj praksi.

Kvantitativna istraživanja i analiza korišćena su za prikaz istraživačkih procedura, kontrolu faktora koji imaju uticaj na tok istraživačkog procesa i obradu podataka. Prikazan je izbor Kyoto 2006+ baze podataka, na osnovu komparativne analize sa 15 drugih baza podataka koje se koriste za evaluaciju sistema za detekciju napada na računarske mreže. Statističke metode normalizacije i standardizacije korišćene su da se pokaže pozitivan uticaj hiperboličkog tangensa i damping strategije na skaliranje atributa.

Eksperimentima su utvrđene karakteristike grupa klasifikatora i, na osnovu parametara koji su dostupni u programskom paketu MATLAB: Classification Learner, izabrano je pet partikularnih modela za izvođenje eksperimenata. Na osnovu rezultata eksperimenata primenjene su metode analize dobijenih klasifikatora, na osnovu kojih je izvršen izbor najpovoljnijih rešenja za XOR detekciju.

Za svaku od eksperimentalnih faza izvedena je vizuelizacija sa pratećim komentarima. Rezultati su prikazani tabelarno i grafički

3. Sadržaj disertacije

Doktorska disertacija podeljena je u sledeća poglavlja:

Prvo poglavlje disertacije je uvodno razmatranje u kojem je ukratko izložen problem koji će biti razmatran u ovoj disertaciji. Uvod sadrži opšte podatke o značaju i primeni detekcije anomalija u računarskoj mreži. Uvod takođe sadrži i opšti prikaz detektora konfliktnih odluka o anomalijama u računarskim mrežama koji je baziran na primeni XOR operacije. Predmet, ciljevi, hipoteze i metodološki pristup, predstavljaju poseban deo uvodnog razmatranja.

U okviru drugog poglavlja definisani su pojmovi vezani za detekciju anomalija. Opisana je relacija između biološkog i veštačkog imunog sistema. Prikazane su osnovne karakteristike anomalija i detekcije anomalija u računarskim mrežama i dat je opis sistema za detekciju anomalija.

Treće poglavlje daje prikaz mašinskog učenja, s posebnim naglaskom na sledećih pet modela nadgledanog mašinskog učenja: model k-najbližih suseda, model k-najbližih suseda sa težinskim koeficijentima, model vektora potpore, stabla odlučivanja i feedforward neuronska mreža. Posebno je prikazano nadgledano mašinsko učenje u detekciji anomalija u računarskoj mreži.

Četvrto poglavlje opisuje prenos podataka u računarskim mrežama i način na koji je moguće detektovati malicioznosti ili greške u ponašanju računarske mreže. U ovom poglavlju prikazan je i izbor i karakteristike Kyoto 2006+ baze podataka.

Peto poglavlje daje prikaz binarne klasifikacije, s posebnim osvrtom na binarnu klasifikaciju u detekciji anomalija, kada su binarni klasifikatori modeli nadgledanog mašinskog učenja. Opisan je proces binarne klasifikacije koji uključuje preprocesuiranje, obučavanje klasifikatora i postprocesuiranje sa vizuelizacijom. U okviru preprocesuiranja posebno su opisani: izbor atributa, skaliranje atributa, tangens hiperbolička normalizacija i Levenberg-Marquardt algoritam.

Šesto poglavlje opisuje odstupanje u detekciji anomalija. Posebno je obrađena XOR detekcija. Poglavlje takođe opisuje značaj konfliktnih odluka o anomalijama kod klasifikatora visoke tačnosti.

Sedmo poglavlje prikazuje eksperimentalne rezultate. Opisana je selekcija numeričkih atributa iz Kyoto 2006+ baze podataka, sa rezultatima koji potvrđuju da je moguće, smanjenjem atributa sa ukupno 24 na 9 numeričkih atributa, postići smanjenje vremena procesuiranja za više od dva puta, sa malom degradacijom tačnosti, za sve izabrane klasifikatore. U sledećoj fazi eksperimenata prikazane su prednosti skaliranja hiperboličkim tangensom u odnosu na Z-score standardizaciju, Min-Max normalizaciju u granice [0,1] i Min-Max normalizaciju u granice [-1,1]. Proces izbora i evaluacije klasifikatora takođe je prikazan u ovom delu eksperimenata. Posebno je prikazana struktura XOR detektora sa obrazloženjem korišćenja najbržeg i najpreciznijeg klasifikatora u detekciji konfliktnih odluka o anomalijama. Prikazani su rezultati procene ukupnog broja kontradiktornih odluka o anomalijama.

Zaključak rada daje kratak prikaz dobijenih rezultata, osvrt na dokaz postavljenih hipoteza i moguće pravce razvoja u ovoj oblasti. Na kraju rada dat je spisak korišćenih referenci.

4. Postignuti rezultati i naučni doprinos doktorske disertacije

Naučni doprinos se ogleda u još jednom potentnom istraživanju za rešenja koja mogu pomoći u predviđanju i sprečavanju ergonomskih rizika povezanih sa povredama na radnom mestu.

Motivacija je bila da se multidisciplinarno istraži integraciju nosivih senzora i njihovoj primeni u regularnim odevnim predmetima, uzimajući u obzir prikladne materijale za finalne proizvode koji su antropometrijski ugrađeni tako da se mogu koristiti kao alat za procenu stanja rizika od ergonomije sa u skladu sa ustanovljenim ergonomskim metodama procena rizika.

Drugačiji pristup sve svodi na dizajn senzora za detekciju pragova ergonomskih rizika baziranim na rastezljivim elektroprovodljivim bojama na fleksibilnim tekstilnim površinama u cilju detekcije pokreta tela. Naglasak je stavljen na minimalno ometanje korisnika kako se kvalitet prikupljenih podataka ne bi ugrozio zbog toga što se radnik oseća nelagodno ili ima smetnje pri radu. Ovo

podiže potencijal za svakodnevnu upotrebu u stvarnom scenariju koji bi neizbežno smanjio obolenja vezana za radne aktivnosti uzrokovane lošim ergonomskim navikama i okruženjem.

Mikrokontroler senzora je otvorene arhitekture, on se može nadograditi modulima bežične veze, efektivno transformišući ceo proizvod u nosivu IoT platformu koja pruža mogućnost daljinske procene i nadgledanje. Istovremeno, testiran je novi alat koji može pomoći i olakšati upotrebu reprezentativnih metoda usmerenih na procenu ergonomskih rizika pri obavljanju radnih zadataka. Senzor kao takav, omogućava čak i manje iskusnim ergonomistima da kvalitetnoje obavljaju zadatke procene rizika i dizajna radnog mesta. Radnik takođe dobija trenutnu povratnu informaciju, što rezultira bržom obukom i usvajanjem dobrih ergonomskih navika, a samim tim direktno doprinosi bezbednosti na radu.

Očekivani rezultat, odnosno ishod koji će se dobiti nakon sprovedenog istraživanja jeste da će se postavljene hipoteze dokazati ili opovrgnuti.

6.Mišljenje i predlog Komisije o doktorskoj disertaciji

Na osnovu svega izloženog Komisija je mišljenja da doktorska disertacija kandidata Danijele Protić po svojoj temi, pristupu, strukturi i sadržaju rada, kvalitetu i načinu izlaganja, metodologiji istraživanja, načinu korišćenja literature, relevantnosti i kvalitetu sprovedenog istraživanjai donetim zaključcima zadovoljava kriterijume zahtevane za doktorsku disertaciju, te se može prihvatiti kao podobna za javnu odbranu.

Sagledavajući ukupnu ocenu disertacije kandidata Danijele Protić pod nazivom "XOR detektor konfliktnih odluka o anomalijama u računarskim mrežama" predlažemo Veću departmana za poslediplomske studije i Senatu Univerziteta Singidunum da prihvati napred navedenu doktorsku disertaciju i odobri njenu javnu odbranu

Beograd, 27mart, 2023

Prof. dr Marina Marjanović,

Univerzitet Singidunum, Beograd

Prof. dr Marko Tanasković,

Univerzitet Singidunum, Beograd

Prof. dr Petar Spalević,

Univerzitet u Prištini sa sedištem u Kosovskoj Mitrovici