Algoritmi za detekciju anomalija u sistemu za prečišćavanje vode (SWaT)

Babić Zorana
Departman za energetiku, elektroniku i telekomunikacije
Fakultet tehničkih nauka, Univerzitet u Novom Sadu
Novi Sad, R. Srbija
zbabic@uns.ac.rs

Sažetak — **Konvergencija poslovnih i operativnih (SCADA) mreža je doprinela sve većem broju hakerskih napada na sajber-fizičke sisteme. Stoga je razvoj i distribucija kvalitetnih rešenja za detekciju upada i sistema za prevenciju ovakvih napada od presudne važnosti. Ovaj rad sadrži uporednu analizu nekoliko rešenja za detekciju anomalija u oblasti sajber-fizičkih sistema i kritičnih infrastruktura. Analiza je bazirana na SWat (Secure Water Treatment Testbed) skupu podataka. Diskutovano je o korisnosti višestrukih tehnika za otkrivanje anomalija, i procenjena je optimalna vrste neuronske mreže prilikom korišćenja ovog specifičnog skupa.**

Ključne reči - Sajber-fizički sistemi; Secure Water Treatment Testbed (SwaT); detekcija anomalija; neuronske mreže; (key words)

I. UVOD

Sajber-fizički sistemi (Cyber-Physical Systems - CPS) predstavljaju kompleksne sisteme koji su u intenzivnoj vezi sa fizičkim svetom koji nas okružuje, ovakvi sistemi se mogu okarakterisati kao fizički i inženjerski sistemi čije se operacije nadgledaju, kontrolišu, koordinišu i integrišu, gde je interakcija od ključne važnosti. Stoga je veoma bitno razumeti ne samo fizičke i računske komponente već i to na koji način se razvija interakcija između ovih komponenti. CPS se mogu pronaći u kritičnim infrastrukturama kao što su transport, distribucija struje i vode, i ovi sistemi se sastoje od fizčkih procesa koje kontrolišu industrijski kontrolni sistemi [1].

Detekcija anomalija u CPS je veoma kompleksna, neophodno je voditi računa kako o mreži tako i o fizičkom delu sistema. Anomalije mogu da se jave usled napada na sam sistem, kao i usled greške nekog od operatera. Anomalije mogu da se manifestuju na nivou mreže i na fizičkom nivou i iz tog razloga je neophodno uzeti sve parametre u obzir.

U ovom radu su analizirane mogućnosti koje pružaju neke od vrsta neuronskih mreža prilikom detekcije anomalija u CPS. Podaci nad kojima je vršena analiza su prikupljeni sa sistema koji predstavlja infrastrukturni sistem u okviru kog se vrši prečišćavanje vode (SWaT) i koji je napravljen kako bi podržao istraživanja vezana za sigurnost CPS.

II. RELEVANTNI RADOVI

Neuronske mreže predstavljaju modele za proračune koji su inspirisani biološkim sistemom. Sastoje se od veštačkih neurona, koji se najčešće zovu čvorovi, i veza koje nastaju između čvorova. Svaki od čvorova poseduje određene informacije na osnovu kojih je definisano njegovo ponašanje, ove informacije čvorovi dobijaju prilikom obučavanja mreže.

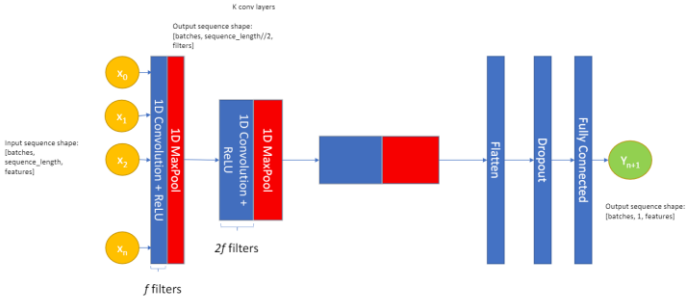
A. *Implementacija jednodimenzionalne konvolucione neuronske mreže*

U radu [2] autori razmatraju korišćenje konvolucionih neuronskih mreža (KNM) za detekciju napada. KNM predstavlja jednu od najčešće korišćenih dubokih neuronskih mreža, i ona spada u *feedforward* neuronske mreže. KNM poseduje sloj koji se zove konvolucioni sloj i on predstavlja najbitniji sloj koji umesto izračunavanja cele slike odjednom vrši podelu na male regione koji se koriste kao ulaz.

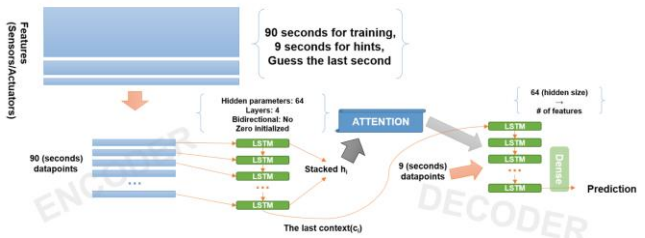
Ideja je bila da se upotrebi jednodimenzionalna KNM (Slika 1) gde se prilikom detekcije anomalija koristi detekcija bazirana na prozoru (*windows-based*). Na samom početku neophodno je bilo iskoristiti model kako bi se predvidelo koje vrednosti se očekuju, ovo predviđanje se vršilo na osnovu prethodnih vrednosti i korišćen je model koji na osnovu sekvence predviđa sekvecu (*sequence-to-sequence* - seq2seq).

Seq2seq model se smatra efikasnim metodom kad je u pitanju učenje semantike i konteksta na osnovu podataka tokom određenog vremena.

Sama evaluacija detekcije performansi je bazirana na broju napada koji su uspešno detektovani (*attack-based*), a neuronska mreža je nahranjena sekvencama veličine n+1, prolazeći kroz LSTM slojeve. Testirana je kombinovana arhitektura koja se sastojala iz kovolucionih slojeva čiji su izlazi prosleđivani u LSTM slojeve, koji su potom vršili predviđanje [2].



Slika 1 – Model 1D KNM [2]



Slika 2 – Model učenja korišćenjem seq2seq modela [6]

LSTM je model koji je predstavljen u radu pod istim nazivom [3], ovaj model je napravljen primarno da prevaziđe probleme nestajućeg gradijenta. Implementiran je tako što standardnu rekurentnu neuronsku mrežu proširuje jednim skrivenim slojem u kom se svaki čvor zamenjuje memorijskom ćelijom. Svaka memorijska ćelija je povezana sa svojom rekurentnom ivicom fiksne težine jedan. Jedna memorijska jedinica sastavljena je od ulaznog čvora, ulazne kapije, internog stanja i izlazne kapije pomoću kojih se utvrđuje na koji način određena jedinica treba da se ponaša.

B. Implementacija neuronske mreže vislojnog perceptrona

U radu [4] je dat predlog na koji način uz pomoć neuronske mreže koja koristi genetske algoritme se može pronaći odgovarajuća mrežna arhitektura na osnovu skupa podataka.

Kada je u pitanju proces traženja optimalne arhitekture on se sastoji iz dva dela, prvi je da eksperti analiziraju arhitehturu i odluče koja arhitektura najviše pogoduje datom skupu podataka, nakon toga se vrše ručna podešavanja nad arhitekturom kako bi ona bila odgovarajuća za dati skup podatak. U ovom radu autori su razmatrali pristup automatskog traženja odgovarajuće arhitekture. Pre početka same analize bilo je neophodno kreirati šablon na osnovu kog se formira optimalna arhitektura. Ovaj šablon sadrži podatke o optimizaciji (zajedno sa parametrima), inicijalizatorima težine, maksimalnom broju slojeva, gde se za svaki sloj definiše lista mogućih tipova slojeva, aktivacione funkcije kao i moguće veličine slojeva.

Kako bi se unapredio kvalitet detekcije anomalija korišćeno je nekoliko tehnika. *Exponentially Weighted Smoothing* je tehnika koja je omogućila da se smanji broj lažno pozitivnih detekcija. *Measuring Prediction Error* je takođe tehnika koja omogućava smanjenje broja lažno pozitivnih detekcija. Ova tehnika vrednost greške diže na p stepen gde je prilikom odabira ovog stepena neophodno voditi računa o tome da stepen ne bude premali, a ni preveliki. Za ovaj konkretan skup izabrana je vrednost 6 za stepen p. *Weighted p-Powered Error* je tehnika kojom se daje težina tagovima na osnovu toga da li je vrednost nekog taga teže ili lakše predvideti. Četvrta tehnika koja je korišćena je *Disjoint Forecasting Window* koja vrši predviđanje vremenskog prozora koji je na određenoj udaljenosti od drugog vremenskog prozora na kom se zasniva prognoza, ova tehnika pomaže u tome da se na osnovu trenutnih podataka predvidi šta će se desiti i sve to u nekom vremenskom okviru, ono što je bitno da se uzme u obzir je to da što je dužina vremenskog prozora kraća to je tačnost predviđanja veća.

Prilikom optimizacije su korišćeni genetski algoritmi, koji su zasnovani na mehanizmima prirodne selekcije, ideja za ove algoritme je došla iz biološkog sistema i kombinuje darvinovsko preživljavanje najsposobnijih u okviru binarnih stringova sa struktuiranim podacima, koji vrše razmenu podataka na slučajan način.

Genetski algoritmi se sastoje iz tri glavne operacije. Prva operacija koja se izvršava je reprodukcija i ona predstavlja proces tokom kog se vrši selekcija niza bitova koji će da nastave u naredni proces. Svaki od niza bitova je rangiran na slučajan način i što je rangiranje veće, veća je verovatnoća da će ta vrednost biti prosleđena u sledeći proces. Drugi poces, proces ukrštanja, se izvršava u dva koraka, gde se u prvom koraku parovi bitova spajaju na slučajan način kako bi se dobio par roditelja, dok se u drugom delu vrše ukrštanja bitova dva novostvorena roditelja kako bi se dobila deca, ovaj proces pokušava da reprezentuje proces dobijanja DNK deteta u biološkom svetu. Takođe u ovom procesu postoji mogućnost da se vrši spajanje više od dve jedninke kako bi se dobilo dete. Treći i poslednji proces je mutacija koja služi kako bi se povećala slučajnost odabira vrednosti, ovaj proces podrazumeva jednostavnu promenu nekih od bitova iz 0 u 1 i obrnuto [5]. U okviru ovog rada autori su podesili inicijalnu veličinu populacije N do 10, dok su za proces ukrštanja uzeli tri roditelja što se dokazalo kao dovoljno efikasno.

Prilikom analize SWaT skupa podataka korišćena su tri dobro poznata arhitekturalna šablona: višeslojni perceptron, konvolucione mreže i rekurentna neuronska mreža. Kako bi se ustanovilo koja od mreža je dala najbolji rezultat autori su se odlučili za NAB skaliranje, razloga što su autori izabrali NAB skaliranje jeste taj što NAB uzima u obzir sve anomalije bez obzira koliko su one trajale, pošto je vecina napada u SWaT skupu podataka trajala svega nekoliko minuta, ovo skaliranje je dalo najverodostojnije rezultate. NAB skaliranje daje rezultat 100 za idealnu detekciju sve do 0 za nula detekcija. Najbolji rezultat je dala neuronska mreža višeslojnog perceptrona (multilayer perceptron - MLP) koja je imala NAB rezultat 69,612, dok su druge dve arhitekture dale znatno manje rezultate.

C. Implementacija rekurentne neuronske mreze bazirana na seq2seq modelu

U radu [6] je predstavljena detekcija anomalija bazirana na dubokom učenju rekurentne neuronske mreže (RNM) korišćenjem seq2seq modela. Za normalizaciju podataka korišćena je min-max normalizacija. Dok su na osnovu LSTM memorijskih ćelija, koje imaju funkciju koja daje izlaz (0,1), za normalizaciju izabrane vrednosti 0 i 1. Izabrana je Seq2seq mreža sa akcenatom na obuci i evaluaciji, gde je prilikom obučavanja korišćen vremenski prozor u trajanju od 90 sekundi. Prilikom implementacije dodat je i dekoder pošto su uz pomoć dekodera dobijeni tačniji rezultati. Prilikom obučavanja mreže korišćen je nezavistan model nad svakim potprocesom, s tim što je u svakom od potprocesa korišćena ista LSTM arhitektura.

Prilikom implementacije modela korišćena je tehnika *Measuring Prediction Error*, koja je takođe korišćena u radu [4], s razlikom što su se ovde autori odlučili za vrednost p = 4.

Predloženi model je smatrao da je sistem pod napadom ukoliko stanje koje je pristiglo do sada nije ni jednom viđeno. Iz tog razloga za određene napade sistem nije mogao sa sigurnošću da tvrdi da su se dogodili.

D. Sličnosti poređenih implementacija

Prlikom obučavanja mreže kod MLP modelovan je ceo sistem, dok je kod KNM i RNM za svaki potproces pravljen poseban model, ono po čemu su se razlikovali ovi modeli jeste da je kod RNM za svaki potproces korišćena ista LSTM arhitektura, dok kod KNM to nije bio slučaj.

Sličnosti koje pronalazimo kod KNM i RNM jesu da se u obe implementacije koristi LSTM i Seq2seq model. Još jedna sličnost koja se uočava jeste da MPL i RNM radi bolje optimizacije detekcije anomalija koriste *Measuring Prediction Error* tehniku.

III. KARAKTERISTIKE SWAT SKUPA PODATAKA

Sistem za prečišćavanje vode (SWaT) je sistem koji je napravljen od strane inženjera laboratorije iTrust, centra za istraživanja sajber bezbednosti, koji se nalazi u okviru singapurskog univerziteta za tehnologiju i dizajn.

SWaT skup podataka je jedan od skupova podataka koji su pogodni za analizu detekcije napada, s toga postoji nekolicina radova u kojoj su autori analizirali detekciju anomalija upotrebom neuronskih mreže, nad ovim konkretnim skupom podataka.

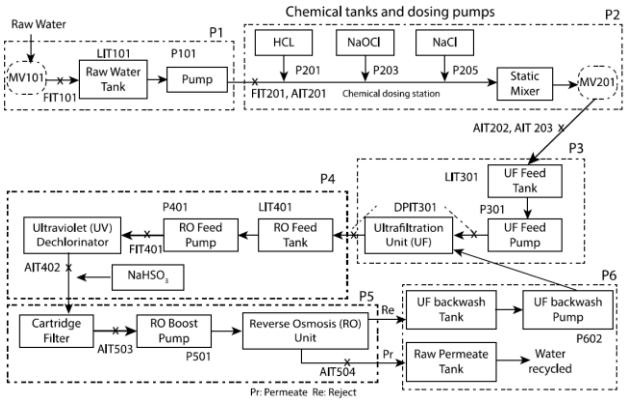
Sam sistem prečišćavanja vode je proces koji se sastoji od šest potprocesa (P1 do P6). Svaki od ovih potprocesa kontroliše set dualnih PLC-ova, od kojih je jedan primarni, a drugi sekundarni (u stanju pripravnosti), samo stanje PLC-ova se prati uz pomoć sistema za nadgledanje i prikupljanje podataka (SCADA).

Na Slici 3 su prikazani svi potprocesi koji se odvijaju u ovom sistemu. Proces prečišćavanja vode počinje sa uzimanjem sirove vode i njenim skladištenjem u cisternu, nakon toga voda prolazi kroz drugi potproces tokom kog se vrši doziranje određenih hemikalija kako bi se povećao kvalitet vode, naredna dva potprocesa vrše prečišćavanje izbacujući nepoželjne materije. Nakon filtriranja voda se prosleđuje u pretposlednji potproces gde se vrši njena demineralizicija. Poslednji, šesti potproces, vodi računa o tome da li voda zadovoljava određene uslove, ukoliko ih zadovoljava ona se skladišti, u suprotnom se vraća u treći potproces kako bi se jos jednom izvršilo njeno filtriranje.

Imena komponenti su dodeljivana u zavisnosti od toga čemu komponenta služi, kao i u kom potprocesu se nalazi. U toku analize napada je ovo bilo od velikog značaja jer se na osnovu naziva moglo zaključiti u kom potprocesu je započet napad i na koji potproces je imao uticaj.

Nomenklatura analognih komponenti: LIT (Level Indicator Transmitter) – indikator nivoa vode, FIT (Flow Indicator Transmitter) – indikator protoka, AIT (Analyzer Indicator Transmitter) – indikator analize, PIT (Presure Indicator Transmitter) – indikator pritiska, DPIT (Differential Pressure Indication Transmitter) – indikator diferencijalnog pritiska.

Nomenklatura digitalnih komponenti: P (Pump) – pumpa, MV (Motorised Valve) – motorizovani ventil, UV (UltraViolet Module) – ultraviolentni modul.



Slika 3 - Prikaz SWaT Sistema [7]

U okviru SWaT skupa podataka praćene su aktivnosti koje su se dešavale na mreži i aktivnosti fizičkog dela sistema. U okviru podataka koji se tiču fizičkog dela sistema sakupljene su vrednosti senzora i aktuatora koji se nalaze u SWaT sistemu.

Tokom 11 dana, koliko su prikupljani podaci, nije bilo prekida u radu sistema. Prvih sedam dana sistem je radio u normalnom okruženju, kako bi se rad sistema ustalio, dok su poslednja četiri dana vršeni napadi na sistem. Izvršen je 41 napad na sistem od kojih 5 nisu imali nikakvog uticaja na sistem i stoga ovi napadi nisu analizirani.

Napadi su podeljeni u četiri kategorije i razlikuju se po tome da li je napad vršen na jednu ili više tačaka i da li je fokusiran da ima uticaj na jedan ili na više potprocesa u sistemu [7].

IV. ANALIZA REZULTATA

Analizirana su tri rada koja su detaljno opisana u poglavlju II. u kojima su se autori bavili detekcijom anomalija nad ovim konkretnim skupom podataka.

Napadi 5, 9, 12, 15 i 18 nisu razmatrani iz razloga što nisu imali uticaja na fizički deo sistema.

A. Analiza uspešnosti detekcije anomalija

U Tabeli I. se nalazi spisak svih napada sa informacijom koja od prethodno pomenute tri implemntacije je imala uspeha u detekciji napada.

Minus (-) označava da napad nije detektovan, plus (+) da napad jeste detektovan i kosa crta (/) da određeni napad nije ni razmatran.

Napad 3 – Kao metu ovaj napad je imao LIT101 i nije detektovan od strane MLP i RNM, prilikom detekcije RNM je imala rezultat od 65% da je u pitanju napad i iz tog razloga nije bilo moguće sa sigurnošću tvrditi da se napad zaista desio.

Napad 4 – Nijedan predloženi model nije detektovao napad 4. U ovom napadu meta je bila MV504, razlog zašto nijedan model nije detektovao ovaj napad je taj što vrednost MV504 ne postoji u skupu podataka i nije postojao način da se ovaj napad detektuje. Iz kog razloga se ova vrednost ne nalazi u skupu podataka nije poznato.

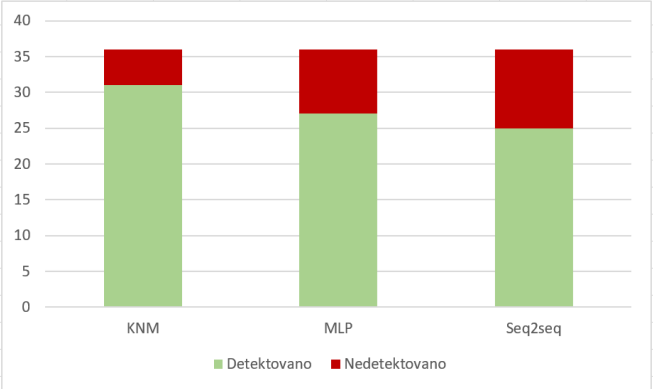
Napad 13 – Ovaj napad je imao minimalni uticaj na sistem i zbog toga je bio veoma težak za detekciju, meta je bio MV304, odnosno njegovo zatvaranje, vrednost MV304 se nije promenila i ovaj napad nije detektovao ni jedan od modela.

TABELA I. PRIKAZ REZULTATA

napad	Meta	Detekcija napada		
		1D KNM [1]	MLP [3]	RNM [5]
1	MV101	+	-	+
2	P102	+	+	+
3	LIT101	+	-	-
4	MV504	-	-	-
6	AIT202	+	+	+
7	LIT301	+	+	+
8	DIPIT301	+	+	+
10	FIT401	+	+	+
11	FIT401	+	+	+
13	MV304	-	-	-
14	MV303	-	-	-
16	LIT301	+	+	+
17	MV303	+	-	+
19	AIT504	+	+	-
20	AIT504	+	-	+
21	MV101, LIT101	+	+	-
22	UV401, AIT502, P501	+	+	+
23	P602, DIT301, MV302	+	+	+
24	P203, P205	+	+	-
25	LIT401, P401	+	+	-
26	P101, LIT301	+	+	+
27	P302, LIT401	+	-	+
28	P302	+	+	+
29	P201, P203, P205	-	+	-
30	LIT101, P101, MV201	+	+	+
31	LIT401	+	+	-
32	LIT301	+	/	+
33	LIT101	+	/	+
34	P101	+	+	+
35	P101, P102	-	+	-
36	LIT101	+	+	+
37	P501, FIT502	+	+	+
38	AIT402, AIT502	+	+	+
39	FIT401, FIT502	+	+	+
40	FIT401	+	+	+
41	LIT301	+	-	+

Napad 14 – Meta ovog napada je bio ventil MV303, zamisao je bila da se ne dozvoli otvaranje ventila, napad nije bio uspešan iz razloga što je cisterna T301 bila već puna, i napad nije imao uticaja na fizički deo sistema, ovaj napad takođe nije detektovao ni jedan od modela.

Napadi 19 i 20 – Ova dva napada su usko povezana iz dva razloga, prvi je taj što su napadi usledili jedan nakon drugog u veoma kratkom vremenskom intervalu i što je meta napada bila ista, AIT504, iz tog razloga neki od modela nisu mogli da detektuju oba napada. Tokom napada 19 vrednost AIT504 je trebala da se podesi na 16 µS/cm (gornja granica je 15), dok je u napadu 20 vrednost trebala da podesi na 255 µS/cm. RNM nije detektovala napad 19, 15% je bila mogućnost da se napad desio što nije dovoljno za njegovu detekciju, dok je napad 20 detektovan. Napad 19 nije detektovan iz razloga što je vremenska razlika između ova dva napada veoma mala i sistem je dobio utisak da je u pitanju jedan isti napad. Razlog za to je što se korišćen seq2seq model, gde je vrednost za vremenski prozor bila 90 sekundi. MLP za razliku od RNM nije detektovala napad 20 već napad 19. Razlog za detekciju samo jednog napada je ta što je prilikom implementacije



Grafikon 1 - Pikaz uspešnosti detekcije napada

korišćena tehnika *Disjoint Forecasting Window* koja takođe koristi vremeski prozor za predikciju.

Napad 21 – Tačke napada su bili MV101 i LIT101, napad je imao uticaj na sistem, ali nije detektovan od strane RNM, odnosno ovaj model je mogao da tvrdi samo sa 35% sigurnošću da se napad dogodio.

Napad 24 – Uticaj na sistem u ovom napadu je bio veoma mali i iz tog razloga je ovaj napad bio težak za detekciju. Pumpe P203 i P205 su pokrenute u tom momentu cisterna T101 je bila puna i došlo je do njenog zatvaranja i samim tim hemikalije nisu dozirane u vodu. Jedini model koji nije detektovao ovaj napad je RNM.

Napad 25 – Ovaj napad nije detektovan od strane RNM, tačnije detektovana je pogrešna tačka napada i samim tim se smatra da napad nije detektovan.

Napad 29 – Mete napada su bile tri pumpe za doziranje hemikalija P201, P202 i P203, odnosno njihovo otvaranje i puštanje hemikalija. Tri pumpe se nisu pokrenule zbog mehaničke blokade i samim tim nije došlo do uticaja na sistem. Jedini model koji je detektovao ovu anomaliju jeste MPL.

Napad 31 – Ovaj napad nije detektovan samo od strane RNM, napad je imao uticaja na sistem, tako da se ne zna tačan razlog zašto napad nije detektovan.

Napad 35 – Ovaj napad je podrazumevao gašenje obe pumpe iz prve faze. KNM i RNM nisu detektovali ovaj napad. Razlog je taj što mreža nije smatrala da je u pitanju napad. Prilikom obučavanja mreže pumpa P102 je bila stalno ugašena i to se nije smatralo kao nešto što nije uobičajeno. Cilj je bio držati obe pumpe, glavnu i rezervnu, zatvorene. Da bi sistem detektovao ovaj napad bilo je neophodno da ima informaciju o tome koja je veza između ove dve pumpe.

Napadi 1, 17, 27 i 41 nisu detektovani samo od strane MPL modela, razlog zašto ovi napada nisu detektovani nije poznat.

Sa grafikona 1. može se uočiti da je najveću uspešnost detekcije napada imala KNM koja nije detektovala svega 5 napada. MLP nije detektovala 9 napada, dok RNM nije detektovala čak 11 napada.

Jedini napad za koji model KNM nije izvršio detekciju, a imao je uticaja na fizički deo sistema je napad 35 kako bi ovaj napad bio detektovan bilo bi neophodno dodatno izvršiti obuku mreže vezano za odnose među komponentama, kako bi

mreža imala informacije u ovom slučaju o tome koja je glavna, a koja rezervna pumpa i mogla da zaključi kad dođe do napada.

B. Lažno pozitivne detekcije napada

Tokom detekcije anomalija dolazi i do detekcije lažno pozitivnih napada. Kod KNM došlo je do 3 lažno pozitivne detekcije, kod MPL do 7 lažno pozitivnih detekcija, dok je kod RNM došlo do čak 20 lažno pozitivnih detekcija. Na osnovu ovoga zaključujemo da je KNM imao i najmanji broj lažno pozitivnih detekcija.

V. ZAKLJUČAK

U ovom radu su analizirane tri različite implementacije za detekciju anomalija u kritičnim infrastrukturama. Tokom analize je korišćen poznat SWaT skup podataka namenski kreiran u laboratorijskom postrojenju za prečišćavanje vode.

Podaci koji se nalaze u SWaT skupu podataka su prikupljani sa fizičkog i mrežnog dela sistema. Prilikom detekcije anomalija korišćeni su podaci sa fizičkog dela sistema. Ovaj skup podataka je koncipiran tako da je tokom prvih sedam dana sistem radio u normalnim okolnostima kako bi se prikupio dovoljan broj podataka i kako bi se sistem ustalio, ai potom su tokom četiri poslednja dana vršeni napadi, gde izvršeno ukupno 41 napad. Jedan od razloga što je ovaj skup podataka pogodan da se koristi prilikom detekcije anomalija uz pomoć neurosnskih mreža, je taj da sadrži dovoljan broj podataka sa kojim mreža može da se obuči.

Analizirane su tri različite neuronske mreže. Jednodimenzionalna KNM koja koristi detekciju anomalija zasnovanu na prozoru uz pomoć seq2seq modela i ima LSTM sloj. Druga neuronska mreža je MLP koja za optimizaciju koristi genetske algoritme dok za predikciju koristi vremenski prozor i treća neuronska mreža je RNM koja je kao i KNM zasnovana na seq2seq modelu i poseduje LSTM sloj.

Jedan od predloga za izmenu postojećeg rešenja je da se prilikom obuke neuronske mreže kod MPL ne koristi jedan model za ceo sistem već da se vrši modelovanje posebno za svaki od potprocesa. Kod RNM iako je prilikom obučavanja mreže za svaki potproces korišćen različit model, ona nije pružila zadovoljavajuće performanse, stoga je predlog da se za svaki potproces ne koristi ista LSTM arhitekturu, već da se ona modeluje u zavisnosti od potprocesa.

Poređenjem rezultata tri konkretne implementacije dolazimo do zaključak je da je u slučaju SWaT skupa podataka najbolje rezultate dala jednodimenzionalna konvoluciona neuronske mreža koja koristi LSTM i seq2seq model.

LITERATURA

[1] L. Montesori, “Cyber-Physical Systems”, In: The International Academy for Production, Chatti S., Tolio T. (eds) CIRP Encyclopedia of Production Engineering. Springer, September 2018

[2] M. Kravchik, A. Shabtai, “Detecting cyber attacks in industrial control systems using convolutional neural networks”. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy, pages 72–83. ACM, 2018

[3] S. Hochreiter, J. Schmidhuber “Long short-term memory”, Neural Computation 9(8):1735-1780, 1997

[4] D. Shalyga, P. Filonov, A. Lavrentyev, “Anomaly Detection for Water Treatment System based on Neural Network with Automatic Architecture Optimization”, arXiv:1807.07282v1, Jul 2018

[5] R. Mahajan, G.Kaur, “Neural Networks using Genetic Algorithms”, International Journal of Computer Applications, Volume 77 – No.14, September 2013

[6] J. Kim, J. Yun, H. C. Kim, "Anomaly Detection for Industrial Control Systems Using Sequence-to-Sequence Neural Networks", Lecture Notes in Computer Science, 2020

[7] J. Goh, S. Adepu, K. N. Junejo, A. Mathur, “A dataset to support re-search in the design of secure water treatment systems”, International Conference on Critical Information Infrastructures Security, October 2016

ABSTRACT

The convergence of business and operational (SCADA) networks contributed to an ever increasing number of hacker attacks against cyber-physical systems. Therefore, it is of utmost importance to develop and deploy proper intrusion detection and prevention systems to counter these kinds of attacks. This paper contains a comparative analysis of several anomaly detection solutions in the fields of cyber-physical systems and critical infrastructures. The analysis was based on the Secure Water Treatment Testbed (SWat) dataset. We discussed the utility of multiple anomaly detection techniques, assessed which type of neural network is optimal to use with this specific dataset.

Algorithms for anomaly detection in Secure Water Treatment Testbed (SWaT)

Zorana Babić