Dr hab. inż. Jerzy Domżał, prof. uczelni

Wydział Informatyki, Elektroniki i Telekomunikacji

Instytut Telekomunikacji

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie

Kraków, 05.12.2023 r.

Recenzja rozprawy doktorskiej pt. „Samo-Nadzorujące się Uczenie w Czasie Rzeczywistym dla Wykrywania Włamań w Bezpiecznym Internecie Rzeczy"

Autor rozprawy doktorskiej: mgr inż. Mert Nakip

Promotor: prof. dr Erola Gelenbe

Niniejszą recenzję opracowano na zlecenie Instytutu Informatyki Teoretycznej i Stosowanej Polskiej Akademii Nauk, 44-100 Gliwice, ul. Bałtycka 5, reprezentowanego przez Dyrektora IITiS PAN dr hab. inż. Krzysztofa Grochlę z dnia 11.10.2023 r.

1. Czy tematyka rozprawy jest aktualna i jak jest związana z rozwojem dyscypliny?

Tematyka rozprawy doktorskiej jest związana z zagadnieniami dotyczącymi analizy danych na potrzeby wykrywania i przeciwdziałania atakom sieciowym z zastosowaniem modeli uczenia maszynowego w sieciach IoT (Internet of Things). Autor rozprawy opracował autorski system wykrywania włamań (IDS), który uczy się na podstawie zadanych wzorców ruchu w sieciach IoT i wykrywa zarówno złośliwe pakiety, jak i zainfekowane urządzenia. Opracowany system zbudowany jest w oparciu o model Deep Random Neural Network (DRNN) rozbudowany o klasyfikator ruchu bazujący na określonych metrykach. Przeprowadzone badania testowe wykazały, że opracowane rozwiązanie cechuje się akceptowalną skutecznością i krótszym czasem wykrywania ataków typu DoD/DDoS oraz ataków typu zero-day w porównaniu z rozwiązaniami konkurencyjnymi bazującymi na uczeniu maszynowym. Autor pracy zaproponował również rozszerzenie opracowanego rozwiązania. Przedstawiono nową strukturę samonadzorowanego wykrywania włamań (SSID - Self-Supervised Intrusion Detection), która umożliwia zbieranie i oznaczanie pakietów na podstawie decyzji systemu IDS, bez dodatkowej ingerencji z zewnątrz.

Tematyka rozprawy niewątpliwie wpisuje się w aktualne trendy badawcze w dyscyplinie informatyka techniczna i telekomunikacja. Zagadnienia związane z bezpieczeństwem sieciowym, w tym w sieciach IoT wpisują się w aktualne i istotne obszary badawcze podejmowane przez badaczy na całym świecie.

2. **Jaki jest problem naukowy podejmowany przez Autora i czy został on trafnie sformułowany?**

Problemem naukowym, którego rozwiązania podjął się Doktorant było opracowanie rozwiązania umożlwiającego skuteczne wykrywanie anomalii sieciowych, w tym ataków DoS/DDos, zero-day z użyciem modeli uczenia maszynowego, niewymagających interwencji z zewnątrz (samouczących się).

Doktorant wskazał, że jego celem było opracowanie algorytmu wykrywania włamań, działającego w środowisku, które nie wymaga dużych obciążeń obliczeniowych i jednocześnie odpowiednio skutecznego. Doktorant wyjaśnił, że obecnie aktualnym wyzwaniem badawczym jest opracowanie i wdrożenie kompleksowych i zaawansowanych metod zabezpieczeń, takich jak system wykrywania włamań (IDS – Intrusion Detection System), opartych na uczeniu maszynowym (ML – Machine Learning) w środowisku zbudowanym w oparciu o urządzenia IoT.

W rozprawie trafnie wskazano trzy argumenty przemawiające za zasadnością prowadzenia prac badawczych we wskazanym obszarze:

1) niskie moce obliczeniowe urządzeń IoT nie są wystarczające, by wykonywać złożone obliczenia na potrzeby istniejących algorytmów,

2) algorytmy oparte na analizie dużych zbiorów danych (np. algorytmy oparte na uczeniu maszynowym) wymagają odpowiednio dużych zasobów obliczeniowych,

3) algorytmy uczenia maszynowego wymagają dostosowania do konkretnego systemu lub sieci, do pracy w której są przeznaczone, gdyż ich parametry są bezpośrednio optymalizowane dla tego systemu.

Autor rozprawy trafnie wskazał obszar badań i sam problem naukowy, a także trafnie sformułował istniejące ograniczenia.

Minusem jest brak jednoznacznie określonej hipotezy badawczej.

3. **Czy Autor rozwiązał postawiony problem i czy wykorzystał w tym celu właściwe metody?**

W wyniku realizacji prac badawczych Autora rozprawy został opracowany system SSID, umożliwiający implementację samonadzorowanych rozwiązań typu IDS opartych na uczeniu maszynowym. Rozwiązanie to umożliwia samodzielne uczenie się systemów IDS w zakresie wykrywania ataków sieciowych. Wśród wykazanych zalet systemu można wymienić:

- łatwe dostosowywanie się do zmieniających się charakterystyk ruchu sieciowego,
- brak potrzeby gromadzenia danych w trybie offline,
- wyeliminowanie błędów ludzkich w etykietowaniu danych,
- wyeliminowanie kosztów pracy związanych z uczeniem modeli i gromadzeniem danych.

Na potrzeby funkcjonowania systemu opracowano odpowiednie metryki umożliwiające ocenę skuteczności działania systemu.

Autor w swoich badaniach zastosował głębokie sieci neuronowe w celu porównywania wzorców ruchu sieciowego i znajdowania odwzorowań z pierwotnie określonymi metrykami ruchu. Opracowano algorytm klasyfikacji o nazwie Statistical Whisker based Benign Classifier

(SWBC), który identyfikuje szkodliwy ruch, porównując ruch rzeczywisty z ruchem wzorcowym. Opracowane metryki bazują wyłącznie na informacjach z nagłówków pakietów ruchu. Dzięki temu uzyskano wysoką skuteczność analizy wpływu ataków botnetów na ruch sieciowy oraz w zakresie przechwytywania sygnatur hosta atakującego. Dzięki powyższemu opracowano nowy system identyfikacji urządzeń IoT, które uległy atakom sieciowym, bazując wyłącznie na ruchu sieciowym, bez konieczności dostępu do samych urządzeń.

Autor pracy, w założonym zakresie, rozwiązał przedstawiony problem.

Autor rozprawy w ramach swoich badań stosował różne metody badawcze. Opracowano dwa algorytmy uczenia maszynowego typu offline i quasi-online, a także algorytm podejmowania decyzji, umożliwiający klasyfikację ruchu sieciowego jako złośliwego lub łagodnego na podstawie wyłącznie wyników z autorskiego systemu IDS z użyciem rozwiązania Auto-Associative DRNN (AADRNN). Eksperymenty praktyczne wykonano z użyciem komputera wyposażonego w procesor AMD 3.7 (Ryzen 7 3700X) i 32 GB pamięci RAM. Algorytmy zostały zaimplementowane w języku Python. Użyto powszechnie dostępnych zbiorów danych, zawierających odpowiednie przebiegi ruchu sieciowego niezbędnego do analizy. W ramach badań wykorzystano analizy bazujące na korelacji Pearsona i wariancji (ANOVA F-score). System AADRNN był porównywany z metodami Simple Thresholding, Lasso czy KNN. Użyte metody badawcze były w pełni adekwatne do przeprowadzenia zaplanowanych badań i osiągnięcia zakładanych rezultatów.

Tym samym należy stwierdzić, że Autor rozwiązał postawiony problem badawczy i wykorzystał w tym celu właściwe metody badawcze.

4. Na czym polega oryginalny wkład Autora w dyscyplinę?

Oryginalny wkład Autora stanowi przede wszystkim opracowany system IDS z użyciem modelu Auto-Associative DRNN (AADRNN). System ten został zbudowany w oparciu o model Deep Random Neural Network (DRNN) rozbudowany o klasyfikator ruchu bazujący na określonych metrykach. Co więcej, Doktorant opracował dwa algorytmy uczące offline and quasi-online, a także opracował autorski algorytm podejmowania decyzji pozwalający na klasyfikację ruchu sieciowego jako złośliwego lub użytecznego bazując wyłącznie na wyniku działania modelu AADRNN. Opracowany system, dzięki temu, jest w stanie wykryć ataki różnego typu, w tym ataki typu Botnet, równolegle ataki różnego typu, a także wskazać zaatakowane urządzenia. Doktorat zaproponował też autorski system uczenia nienadzworowanego - Self-Supervised Intrusion Detection (SSID). System ten pozwala na współpracę z różnymi typami systemów IDS, w tym w szczególności ich trenowanie bez ingerencji z zewnątrz ze strony użytkownika. Proces uczenia jest podzielony na dwa etapy – uczenie wstępne i uczenie typu online pozwalające na łatwe aktualizacje parametrów. Wszystkie zaproponowane rozwiązania pozwalają na zwiększenie skuteczności systemów bezpieczeństwa przewidzianych dla sieci z urządzeniami IoT.

Zagadnienia związane z zapewnianiem bezpieczeństwa w sieciach IoT są ważne i aktualne. Istnieją systemy pozwalające wykrywać zagrożenia w tego typu sieciach i skutecznie przeciwdziałające atakom. Zastosowanie metod uczenia maszynowego w sposób ograniczający zużycie zasobów pozwoliło na zwiększenie skuteczności wykrywania ataków. Stanowi to nowy wkład w dyscyplinę informatyka techniczna i telekomunikacja.

5. **Jakie jest znaczenie poznawcze oraz znaczenie praktyczne wkładu Autora?**

Doktorant w ramach swojej pracy zajmował się zagadnieniami związanymi z analizą danych na potrzeby opracowania modeli uczenia maszynowego wykorzystywanych w procesie przeciwdziałania atakom sieciowym, głównie w sieciach IoT. Opracowanie rozwiązań zaprezentowanych w pracy wymagało poznania mechanizmów działania systemów IDS, jak i samych ataków sieciowych. Zrozumienia wymagały użyte metody uczenia maszynowego i analizy danych. Z pewnością duże znaczenie poznawcze miało opracowanie nowych metryk służących do klasyfikacji typu ruchu bazujących wyłącznie na informacjach z nagłówków pakietów.

Rozprawa ma przede wszystkim znaczenie praktyczne. Zaproponowany system IDS może być stosowany z powodzeniem w sieciach IoT, a więc w sieciach cechujących się niskim poborem mocy. To stanowiło istotne ograniczenie w zakresie opracowywanych rozwiązań. Pokonanie tej bariery, jednocześnie zachowując wysoką skuteczność wykrywania ataków, świadczy o dużym potencjale praktycznym opracowanego rozwiązania. Co więcej, zastosowanie metod uczenia maszynowego znacząco poprawiło skuteczność rozwiązania względem innych systemów obecnych na rynku i opisanych w literaturze. Z całą pewnością rozwiązanie Doktoranta może znaleźć swoje miejsce na rynku IT i może być dalej rozwijane zgodnie z sugestiami zawartymi w samej rozprawie.

6. **Czy rozprawa świadczy o dostatecznej wiedzy Autora w zakresie nauk technicznych i szczegółowej wiedzy w tematyce odpowiadającej zakresowi badań?**

Tematyka pracy jest związana z dyscypliną naukową informatyka techniczna i telekomunikacja. Doktorant wykazał się dobrze ugruntowaną wiedzą techniczną w tematyce pracy. Przedstawiona analiza obecnego stanu wiedzy jest prawidłowa i pełna. Opracowanie rozwiązań zaprezentowanych w rozprawie nie byłoby możliwe bez posiadania gruntownej wiedzy w tematyce pracy. Doktorant wykazał się znajomością tematyki związanej z bezpieczeństwem sieciowym, ale też zastosowaniem metod uczenia maszynowego. Doktorant potwierdził znajomość narzędzi badawczych, w tym symulatora sieciowego.

Jednoznacznie stwierdzam, że zakres rozprawy świadczy o dostatecznej wiedzy Autora w zakresie nauk technicznych i potwierdza jego szczegółową wiedzę w tematyce odpowiadającej zakresowi badań.

7. **Jakie są słabe strony rozprawy?**

W mojej ocenie słabą stroną rozprawy jest brak jednoznacznie zdefiniowanej hipotezy badawczej. Doktorant wskazał na obszar badawczy i zagadnienia, które stanowiły podstawę jego działań naukowych. Wskazano jaki problem jest planowany do rozwiązania. Jednakże, klasyczna struktura rozprawy doktorskiej wymaga postawienia wprost hipotezy badawczej i planowanej metodyki jej wykazania. Tego, według mnie, zabrakło w rozprawie, choć nie umniejsza to rangi osiągnięcia naukowego Doktoranta.

Przedstawione wyniki podane zostały bez błędów pomiarowych. Czasami podano odchylenie standardowe (jak w tabeli 4.6), jednak to jest niewystarczające do dokonywania porównań. W mojej ocenie, wyciągnięcie wniosków na podstawie danych z tabeli 4.6 jakoby średni czas

nauczania modelu AADRNN był krótszy niż w przypadku Lasso jest nieuprawnione. Takiego porównania można dokonać biorąc pod uwagę błędy pomiarowe, zgodnie z wybranym rozkładem prawdopodobieństwa i poziomem ufności. Również w przypadku innych porównań zabrakło tego typu analiz. Nie umniejsza to wyciągniętym wnioskom bazującym na obserwowanych trendach.
Dane, które posłużyły do analizy wykrywania szkodliwego ruchu w różnego typu atakach (dataset KDD Cup"99) mają już 24 lata. Od tego czasu powstało wiele nowych ataków i wiele rodzajów szkodliwego ruchu. Nie wyjaśniono w rozprawie dlaczego posłużono się tak już jednak starym i nieaktualnym wzorcem, a nie jakimś młodszym.

Praca zawiera drobne błędy językowe. Przykładowo:
In this results → In these results
The results in this figure show that of the AADRNN with offline learning clearly outperforms → The results in this figure show that the AADRNN with offline learning clearly outperforms
32 Gb RAM → 32 GB RAM

Wskazane wyżej słabe strony rozprawy nie są na tyle istotne, by umniejszyć pozytywną ocenę rozprawy jako całości.

8. Podsumowanie

Recenzowana rozprawa doktorska stanowi spójny, dobrze opracowany dokument. Doktorant podjął się pracy nad niełatwym tematem dotyczącym zabezpieczania sieci IoT i wykrywania pojawiających się nieprawidłowości. Opracowane rozwiązania stanowią znaczący wkład w rozwój dyscypliny naukowej informatyka techniczna i telekomunikacja. Istnieje realna szansa na kontynuację prac przedstawionych w rozprawie doktorskiej i komercyjne wdrożenie opracowanych rozwiązań.
Doktorant jest autorem wielu publikacji naukowych. Tematyka doktoratu stanowiła podstawę dwóch publikacji, z których jeden został opublikowany w czasopiśmie IEEE Access, a drugi został zgłoszony do czasopisma (aktualnie jest umieszczony w bazie arXiv). Dodatkowo z tematyką doktoratu są związane cztery publikacje konferencyjne (LANMAN, GLOBECOM, EuroCybersec, MASCOTS). Są to znane i cenione konferencje. Dodatkowo, Doktorant jest autorem wielu innych publikacji w czasopismach (w tym z listy JCR) i konferencyjnych, których tematyka nie jest bezpośrednio związana z doktoratem.
Biorąc pod uwagę powyższe stwierdzenia uznaję, że recenzowana rozprawa doktorska spełnia ustawowe wymagania stawiane rozprawom doktorskim. Wnioskuję o jej dopuszczenie do obrony. Ze względu na wysoką merytoryczną wartość zaprezentowanych wyników oraz znaczący dorobek publikacyjny Doktoranta, wnioskuję o wyróżnienie rozprawy.

Elektronicznie podpisany przez
Jerzy Domżał
Data: 2023.12.05 15:22:43 +01'00'