Warszawa, 14 grudnia 2023 r.

Dr hab. inż. Halina Tarasiuk
Instytut Telekomunikacji
Politechnika Warszawska
ul. Nowowiejska 15/19
00-665 Warszawa

Recenzja rozprawy doktorskiej dla Rady Naukowej IITiS PAN

Tytuł rozprawy: „Samo-nadzorujące się uczenie w czasie rzeczywistym dla wykrywania włamań w Bezpiecznym Internecie Rzeczy" (ang.: "Online Self-Supervised Learning Intrusion Detection Towards Secure Internet of Things")

Autor rozprawy: mgr Mert Nakip

Promotor rozprawy: prof. dr Erol Gelenbe

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

Tematyka rozprawy dotyczy Internetu Rzeczy (ang. Internet of Things, IoT) i zabezpieczenia go przed włamaniami. Elementami IoT najbardziej podatnymi na włamania są urządzenia końcowe, takie jak czujniki. W konsekwencji włamania do tych urządzeń przyczyniają się do uruchamiania ataków typu DoS, DDoS. W atakach tych zainfekowane urządzenia mogą doprowadzać do unieruchomienia sieci IoT. Rozprawa doktorska proponuje rozwiązanie, które ma pozwolić na automatyzację procesu wykrywania włamań na podstawie systemu uczącego się prawidłowego działania sieci IoT, aby na tej podstawie automatycznie wykrywać ataki z zainfekowanych urządzeń IoT w sieci. W tym celu zaproponowano rozwiązanie, które stanowi istotną część Systemu IDS (ang. Intrusion Detection System). Tematyka rozprawy jest bardzo aktualna i jest ściśle związana z rozwojem dyscypliny, a włączenie do rozwiązania algorytmów sztucznej inteligencji jest obecnie przedmiotem intensywnych prac na świecie.

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

Problem naukowy podjęty przez Autora to zaproponowanie systemu wykrywania włamań dla sieci IoT w czasie rzeczywistym, czyli w tzw. trybie on-line na podstawie automatycznego uczenia się prawidłowych charakterystyk ruchu i porównywania ich z ruchem bieżącym w sieci. Główne wyzwania, to małe zasoby obliczeniowe elementów IoT, które są poddawane zabezpieczeniu przed złośliwym ruchem, w związku z tym analiza ruchu w czasie rzeczywistym stosowana dla typowych sieci telekomunikacyjnych nie ma szans powodzenia. Zatem, w mojej ocenie, problem został słusznie sformułowany.

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

Autor na bazie analizy teoretycznej i sprawdzenia wybranych metod uczenia maszynowego znanych z literatury wraz z zaproponowanymi oryginalnymi zestawami metryk pomiarowych rozwiązał postawiony problem badawczy. Sprawdzenie zastosowanych metod zostało przeprowadzone dla publicznie dostępnych pomiarowych baz danych uwzględniających ataki w sieciach IoT. Zastosowanie metod teoretycznych i danych pomiarowych reprezentatywnych dla różnego rozmiaru sieci IoT jest właściwym podejściem, jednakże nie pozwala na ostateczną ich ocenę ze względu na brak możliwości uwzględnienia uwarunkowań systemu IDS działającego w środowisku rzeczywistym lub demonstracyjnym. Chodzi tu głównie o wyliczanie w czasie rzeczywistym metryk poddawanych do algorytmów uczenia maszynowego. Zaproponowane rozwiązania są również ukierunkowane na wybrane typy ataków i w ten sposób wskazano ich skuteczność. Rozwiązanie nie uwzględnia uniwersalnego podejścia, które można rozwijać generycznie dodając wykrywanie kolejnych typów ataków, jak to ma miejsce w rzeczywistym systemie. Należy jednak podkreślić, że nie zmniejsza to wartości zaproponowanych rozwiązań, natomiast otwiera obszar dla dalszych badań.

4. **Na czym polega oryginalny wkład Autora w dyscyplinę?**

Oryginalny wkład autora w dyscyplinę polega na zaproponowaniu następujących oryginalnych rozwiązań:

- zaproponowanie rozwiązania polegającego na samo-nadzorującym się uczeniu w czasie rzeczywistym dla wykrywaniu złośliwego ruchu. Oryginalność rozwiązania polega na tym, że system nie wymaga wcześniejszego gromadzenia danych, na podstawie których jest przeprowadzane uczenie się zainfekowanego ruchu, tylko rozwiązanie pozwala na podstawie uczenia się ruchu prawidłowego w czasie rzeczywistym porównywać go z ruchem bieżącym w celu wyrywania włamań. W ramach rozwiązania zastosowano metody uczenia maszynowego znane z literatury, zaś metryki wg których stosowane jest uczenie się stanowią oryginalne rozwiązanie problemu.

- Na podstawie wykrywania wybranych ataków, w kolejnym kroku, rozwiązanie umożliwia identyfikację zainfekowanych urządzeń IoT, tzw. botów.

- Zaproponowane rozwiązanie może również działać w tzw. trybie offline lub quasi-online. Skuteczność tych dwóch trybów była badana w pracy w pierwszej kolejności, badania przeprowadzono dla ataku typu Mirai.

- Niewątpliwą zaletą proponowanego rozwiązania jest możliwość zastosowania go bez konieczności wcześniejszego gromadzenia danych wejściowych dla metod uczenia maszynowego. Z tego punktu widzenia można przyjąć, że jest to rozwiązanie generyczne i nie ogranicza skali zastosowania.

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

Znaczenie poznawcze wkładu autora wskazuje na możliwość zastosowania metod samo-nadzorującego się uczenia maszynowego dla sieci IoT w celu wykrywania wybranych ataków DoS i DDoS. W pracy zawarto wyniki dla wybranych danych pomiarowych udostępnianych publicznie.

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

Rozprawa świadczy o dobrej wiedzy autora w obszarze sieci IoT, systemów bezpieczeństwa, włamań i ataków w obszarze cyberprzestrzeni, metod sztucznej inteligencji i posługiwania się aparatem matematycznym. Na potrzeby rozprawy Autor przywołuje 220 pozycji literaturowych, które wskazują na bardzo dobre rozeznanie Autora w obszarze stanu sztuki.

7. Jakie są słabe strony rozprawy?

Do słabych stron rozprawy można zaliczyć:

- skuteczność zastosowanych metryk dla uczenia maszynowego została potwierdzona wynikami dla przykładowych danych z publicznie dostępnych baz danych dla ataku typu Mirai, natomiast przy ich zastosowaniu dla jednocześnie występujących innych ataków warstwy transportowej wskazano w rozprawie słabszą skuteczność, co stanowi jeden z wniosków w rozprawie.

- brak odniesienia się do konsekwencji zastosowanych metryk i ich pomiaru w rzeczywistym systemie dla działania rozwiązania w tzw. trybie online. W rozprawie zaznaczono, że to wymaga dalszych prac związanych z implementacją rzeczywistego systemu. Szkoda, że nie podjęto próby implementacji demonstratora w zakresie umożliwiającym sprawdzenie wpływu rzeczywistego pomiaru na wydajność proponowanych metod.

- brak w rozprawie analizy krytycznej dla założenia w punkcie „5.2.3 Representativeness of Learned Traffic", że długość pakietów w procesie porównawczym ruchu bieżącego z ruchem reprezentatywnym, jest opisana rozkładem wykładniczym.

- brak wyraźnie zaznaczonych wniosków dla rozprawy w na końcu rozdziałów 2. i 3. Autor przywołuje szereg pozycji literaturowych, jednakże nie wskazuje wprost, np. z którymi rozwiązaniami będzie porównywał swoje rozwiązanie. Jedynym wnioskiem wpisanym przy okazji analizy literaturowej jest wskazanie na zastosowanie uczenia maszynowego jako powszechnie stosowanej metody.

8. Ocena układu rozprawy doktorskiej, w tym informacje o jej poszczególnych częściach składowych

Rozprawa doktorska składa się z sześciu rozdziałów, zawiera 92 strony. Układ rozprawy doktorskiej jest czytelny, z wyłączeniem uwagi dotyczącej braku wniosków na końcu rozdziałów 2. i 3.

Rozdział 1. stanowi wprowadzenie, w którym m.in.: sformułowano problem podjęty w rozprawie oraz zawarto publikacje związane z rozprawą i pozostałe publikacje Autora.

Rozdział 2. przedstawia stan sztuki w obszarze bezpieczeństwa sieci, w tym rodzaje ataków dla tego środowiska oraz znane metody zabezpieczeń systemów sieciowych przed atakami. Następnie na tym tle wskazano problemy związane z zastosowaniem metod bezpieczeństwa i występowania ataków w sieciach IoT, w tym podział na typy występujących ataków dla modelu warstwowego systemów IoT.

W rozdziale 3. Autor skupił się na metodach wykrywania włamań w sieciach IoT wskazując na różne rozwiązania z tym związane prezentowane w literaturze.

Rozdział 4. zawiera propozycję rozwiązań związanych z uczeniem maszynowym typu offline i quasi-online dla ruchu prawidłowego w celu porównania go z ruchem bieżącym, aby wykrywać nieprawidłowości związane z atakiem typu Mirai.

W rozdziale 5. Autor zaproponował rozwiązanie typu online, działające w czasie rzeczywistym, które pozwala na samo-nadzorujące uczenie maszynowe, umożliwiające wykrywanie włamań do sieci poprzez wykrywanie nieprawidłowego ruchu, i w konsekwencji wykrywanie zainfekowanych urządzeń IoT.

Rozdział 6. stanowi podsumowanie rozprawy.

9. Podsumowanie

Rozprawa zawiera oryginalne rozwiązania, które pozwalają na wskazanie, że problem naukowy sformułowany w rozprawie można uznać za rozwiązany, tzn. zaproponowano rozwiązanie, które może pozwolić na zastosowanie samo-nadzorującego się systemu uczenia się dla bezpieczeństwa sieci IoT, z uwzględnieniem, że elementy tych sieci mają ograniczone zasoby obliczeniowe. Mimo, iż zaproponowane rozwiązanie wymaga dalszych prac, zaś przyjęte założenia uszczegółowienia dla specyfiki rzeczywistych systemów IoT, to należy uznać, że jest to bardzo dobry przyczynek dla dalszych prac. Wyniki przedstawione w rozprawie zostały opublikowane w 6 artykułach, w tym 2 w czasopismach i 4 w materiałach konferencyjnych. Ponadto, Autor jest współautorem wielu artykułów, które nie są bezpośrednio związane z rozprawą. **Podsumowując, w mojej ocenie rozprawa spełnia wymagania odnoszące się do obowiązujących przepisów w zakresie prac doktorskich.**

Tomasz