Bydgoszcz, 22.01.2025

Prof. dr hab. inż. Michał Choraś
Wydział Telekomunikacji, Informatyki i Elektrotechniki
Politechnika Bydgoska im. J.J. Śniadeckich, Bydgoszcz

Recenzja rozprawy doktorskiej

Data sample optimisation for network traffic classification using machine learning methods,

której Autorem jest Pan

mgr inż. Jacek Krupski

realizowanej na Politechnice Warszawskiej

1. Wprowadzenie.

Niniejsza recenzja rozprawy doktorskiej, której Autorem jest Pan mgr inż. Jacek Krupski, została wykonana na zlecenie Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Politechniki Warszawskiej (Uchwała nr 760/2024 z dnia 22 października 2024 r.) oraz na podstawie zawiadomienia o wyznaczeniu na Recenzenta w postępowaniu o nadanie stopnia doktora podpisanego przez Przewodniczącego RDN ITT Politechniki Warszawskiej Pana prof. dr hab. inż. Jarosława Arabasa (z dnia 9 grudnia 2024 r.).

Rozprawę odebrałem w dniu 17.12.2024 r., a recenzję wysłałem przed wyznaczonym terminem w styczniu 2025 r.

Promotorem niniejszej rozprawy jest Pan dr hab. inż. Marcin Iwanowski, profesor uczelni. Na promotora pomocniczego wyznaczono Pana dr inż. Waldemara Graniszewskiego.

Praca doktorska składa się ze streszczenia, spisów, dziewięciu rozdziałów oraz bibliografii.

Niniejsza recenzja (poza wprowadzeniem i wnioskiem) zawiera odpowiedzi na siedem pytań dotyczących rozprawy doktorskiej.

2. Jaki jest problem naukowy (teza) rozprawy? Czy został on trafnie i jasno sformułowany? Jaki charakter ma rozprawa?

Rozprawa, której Autorem jest Pan mgr inż. Jacek Krupski, dotyczy cyberbezpieczeństwa, a w szczególności metod analizy danych oraz cech pochodzących z ruchu sieciowego w celu klasyfikacji i wykrywania ataków sieciowych.

Niniejsza praca naukowa ma charakter teoretyczny oraz koncepcyjno-eksperymentalny.

Problemy i zagadnienia naukowe rozprawy zostały odpowiednio sformułowane przez Autora, a także podjęto próbę ich rozwiązania.

Teza rozprawy znajduje się w rozdziale 1.1 na stronie 12. Teza jest dość ogólna, ale mimo to trafnie sformułowana. W pracy nie wyznaczono i nie zaprezentowano celów szczegółowych pracy, ani problemów badawczych (tzw. *research questions*).

Poniżej tezy, Autor wymienił dwa wątki prac, które pogłębił w rozprawie: analizę surowego ruchu sieciowego oraz analizę cech ruchu.

3. **Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł, w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle? Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?**

Analiza literatury została przeprowadzona przede wszystkim w Rozdziale 2 *„Literature review"*. Autor przeprowadził analizę literatury głównie na opublikowanych już pracach przeglądowych, m.in. takich jak: *Getman, A. and Ikonnikova, M., „A survey of network traffic classification methods using machine learning," Programming and Computer Software, vol. 48, no. 7, pp. 413–423, 2022.*

Niestety Autor nie podszedł do przeglądu literatury w sposób metodologiczny: nie podano kryteriów doboru prac do analizy, ani nie wykorzystano żadnej z metodologii takich jak np. PRISMA. Nie wiadomo dlaczego w Rozdziale 2, Autor omówił wybrane prace, a pominął szereg innych. Dla przykładu, nie wyjaśniono dlaczego Autor z chęcią powołuje się i omawia wymienioną wyżej pracę (autorów z Federacji Rosyjskiej), która nie odbiła się dużym echem w środowisku (mało cytowań, mała liczba pobrań), pomijając o wiele szersze przeglądy literatury dot. cyberbezpieczeństwa i analizy cech ruchu.

Do analizy stanu wiedzy, zaliczyć należy także kolejne Rozdziały, które omawiają podstawowe elementy dot. ruchu sieciowego oraz uczenia maszynowego:

- Rozdział 3: *„Network traffic"*
- Rozdział 4: *„Machine learning"*
- Rozdział 5: *„Network traffic datasets"*

Tym samym struktura pracy i jej balans są dość dziwne, gdyż po pięciu rozdziałach i 70 stronach rozprawy, wciąż nie wiadomo co zrobił jej Autor.

W Rozdziałach 2-5 zabrakło krytycznej analizy przeglądu literatury, wyciągnięcia wniosków dotyczących braków oraz luk w aktualnych podejściach oraz motywacji dla swoich prac nad rozprawą.

Ponadto, część treści jest dość oczywista i trywialna i mogła zostać pominięta przez Autora na rzecz jego własnych wniosków (np. podrozdziały 3.1, 3.2, 4.3 przedstawiające ISO-OSI, czy znane metryki). W mojej opinii połączenie treści z Rozdziałów 2-4 w jeden rozdział przeglądowy byłoby korzystniejszym rozwiązaniem.

Za bardzo istotny i potrzebny oceniam Rozdział 5 z analizą dostępnych i wykorzystanych przez Autora w rozprawie baz danych.

Sama bibliografia zawiera odpowiednią liczbę źródeł (169), w tym ponad połowa z nich została opublikowana po roku 2020 włącznie, co oceniam pozytywnie.

4. **Czy autor rozwiązał postawione zagadnienia? Czy użył do tego właściwych metod dowodząc, że posiadł umiejętności związane z metodyką i metodologią prowadzenia badań naukowych? Czy przyjęte założenia są uzasadnione?**

Generalnie, Autor w sposób odpowiedni rozwiązał problemy, których dotyczy rozprawa. Nie mam wątpliwości, iż Autor posiada dużą wiedzę dot. zagadnień związanych z pozyskiwaniem ruchu sieciowego, analizą cech ruchu sieciowego, analizą istotności poszczególnych cech, oraz cyberbezpieczeństwem.

Przyjęte założenia i teza są uzasadnione i merytorycznie poprawne.

Teza rozprawy została dowiedziona. Autor zaproponował oraz zaprezentował bardzo wiele analiz oraz wyników eksperymentalnych potwierdzających możliwości redukowania wykorzystywanych cech ruchu - jest to niewątpliwie dużą zaletą niniejszej rozprawy.

Autor posiada duże umiejętności w analizie oraz wykorzystywaniu cech ruchu sieciowego w celu wykrywania ataków sieciowych.

5. **Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu nauki reprezentowanych przez literaturę światową?**

Głównym elementem rozprawy jest autorska analiza oraz propozycja wyboru i redukcji cech ruchu sieciowego przy jednoczesnym utrzymaniu skuteczności wykrywania ataków sieciowych.

Głównymi osiągnięciami rozprawy oraz propozycjami Autora są:

- Sposoby anonimizacji ruchu sieciowego oraz metodologia poziomów anonimizacji,

- Analiza wpływu infrastruktury sieciowej na cechy ruchu sieciowego, oraz propozycja wykorzystania cech, na które infrastruktura sieciowa nie ma wpływu,
- Analiza dotycząca cech zawartych w znanych bazach danych zawierających ruch sieciowy (tzw. *benchmark datasets*) oraz analiza ich generalizacji i przydatności nauczonych na nich rozwiązań dla wykrywania ruchu sieciowego,
- Analiza dotycząca skuteczności klasyfikatorów i metod uczenia maszynowego oraz ich wpływu na wykrywanie ataków sieciowych w analizowanych bazach danych ruchu, a także analiza wpływu połączonych klasyfikatorów na skuteczność wykrywania.

Tym samym, Autor nie zaproponował nowych metod, ani rozwiązań uczenia maszynowego dla cyberbezpieczeństwa, ale przeprowadził szereg istotnych analiz oraz wyciągnął odpowiednie wnioski.

Autor wykonał szereg testów i prac eksperymentalnych w celu zbadania i porównania zaproponowanych analiz i rozwiązań, wkładając bardzo dużo pracy w tę część rozprawy oraz prezentując bogaty zestaw wyników i porównań (Rozdział 8 niniejszej rozprawy).

6. Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników? Jaka jest poprawność redakcyjna rozprawy?

Niniejsza rozprawa stanowi przykład profesjonalnie przygotowanej pracy doktorskiej. Praca napisana jest na odpowiednim poziomie edycyjnym, językowym oraz graficznym.

W pracy występują oczywiście drobne usterki, literówki i błędy językowe, ale jest ich niewiele i nie są znaczące. Dla przykładu, szereg skrótów nie została wytłumaczona i rozwinięta przy pierwszym użyciu (np. TCP, UDP, czy PCAP). Część ilustracji prezentujących wyniki nie jest zbyt wyraźna, a tym samym przedstawione rezultaty i wykresy są trudne do interpretacji.

Te drobne usterki nie zmieniają ogólnej opinii o dobrym i profesjonalnym poziomie językowym i edycyjnym rozprawy.

7. Jakie są słabe strony rozprawy i jej główne wady?

Rolą recenzenta jest zauważenie ewentualnych niedociągnięć i mankamentów przedstawianej pracy, oraz zgłoszenie uwag, które mogą być pomocne i przydatne w dalszych pracach.

Uwagi krytyczne to między innymi:

- Teza pracy jest dość ogólna, a w szczególności zabrakło w niej miar lub kwantyfikatorów.
- Autor używa metod uczenia maszynowego, jednak poświęcił zbyt mało miejsca na przedstawienie szczegółów wykorzystanych rozwiązań (np. parametrów itp.).

- Część wyników dowiedzionych przez Autora (np. duża skuteczność metod typu *Random Forest* w porównaniu to bardziej złożonych sieci) jest dość oczywista i tego typu wyniki były już publikowane.
- Autor w rozprawie dokonał analizy istotności cech. Nie wykorzystał jednak w tym celu metod tzw. wyjaśnialnej sztucznej inteligencji, czyli xAI (j.ang. *explainable Artificial Intelligence*) nawet tak prostych jak SHAP czy LIME. Nie jest dla mnie jasne jakie kryterium zdecydowało o odrzuceniu podejścia bazującego na metodach xAI?
- W pracy często brakuje głębszej dyskusji oraz metryk dotyczących weryfikacji oraz walidacji osiąganych rezultatów. Brakuje także głębszej analizy wad i ograniczeń wykorzystanych rozwiązań, metod oraz osiągniętych wyników i wniosków (tzw. *threats to validity*).
- Autor powinien przedstawić więcej metryk dotyczących osiągniętych rezultatów i przeprowadzonych badań. Tematyka miar dla systemów rozpoznawania, w tym w cyberbezpieczeństwie, jest dużo bardziej złożona i Autor powinien się z nią zapoznać.
- Zbyt mało dyskusji poświęcono zagadnieniu dotyczącemu zbalansowania klas.
- W pracy brakuje formalnej analizy dotyczącej istotności statystycznej różnic między osiągniętymi wynikami, parametrami, testami.
- W swojej pracy Autor wykorzystał bazy danych z ruchem sieciowym omówione w Rozdziale 5 „*Network traffic datasets*". Autor wykorzystał bazy danych, opierając się na jednej tylko pracy przeglądowej z roku 2019 (a więc sprzed około pięciu lat) nie podając żadnych kryteriów wyboru tych baz, ani niniejszej pracy: *Markus Ring, Sarah Wunderlich, Deniz Scheuring, Dieter Landes, Andreas Hotho: A survey of network-based intrusion detection data sets. Comput. Secur. 86: 147-167 (2019).*
- Autor pominął nowsze bazy danych ruchu sieciowego, w tym np. pochodzące z projektów europejskich bazy ruchu takie jak:
    - Pochodząca z projektu SPARTA (*Strategic programs for advanced research and technology in Europe*) baza ruchu LitNet-2020, dostępna i opisana m.in. w publikacji: *Damasevicius, R.; Venckauskas, A.; Grigaliunas, S.; Toldinas, J.; Morkevicius, N.; Aleliunas, T.; Smuikys, P. LITNET-2020: An Annotated Real-World Network Flow Dataset for Network Intrusion Detection. Electronics 2020, 9, 800.*
    - Pochodząca z koordynowanego przeze mnie projektu SIMARGL (*Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware*), w którym Politechnika Warszawska była partnerem, baza ruchu RoEduNet-SIMARGL2021, dostępna i opisana w publikacji: *Mihailescu, M.-E.; Mihai, D.; Carabas, M.; Komisarek, M.; Pawlicki, M.; Hołubowicz, W.; Kozik, R. The Proposition and Evaluation of the RoEduNet-SIMARGL2021 Network Intrusion Detection Dataset. Sensors 2021, 21, 4319.*

- W pracy zabrakło dyskusji na temat praktycznego wykorzystania zaproponowanych rozwiązań oraz głębszego ukazania przypadków użycia/scenariuszy ewentualnie podejmowanych decyzji, dotyczących np. anonimizacji lub wykorzystania badanych cech ruchu przez konkretnych użytkowników.

Pomimo wymienionych uwag krytycznych, często natury dyskursywnej, niniejszą pracę oceniam pozytywnie.

Warto zauważyć, że Doktorant jest także współautorem kilku opublikowanych oraz zgłoszonych artykułów naukowych wymienionych m.in. na str. 136 niniejszej rozprawy w podrozdziale *Bibliography*.

Niniejszy dorobek jest wystarczający na tym etapie kariery naukowej.

8. Jaka jest przydatność rozprawy dla nauk technicznych?

Praca dotyczy bardzo aktualnych i potrzebnych zagadnień nowoczesnej informatyki technicznej i telekomunikacji, a w szczególności cyberbezpieczeństwa.

Moim zdaniem temat niniejszej rozprawy, czyli szczegółowe zbadanie, które cechy ruchu należy analizować, będzie jeszcze zyskiwał na popularności oraz będzie ważną częścią szeroko rozumianego cyberbezpieczeństwa.

Tym samym, niniejsza rozprawa i przedstawione metody mogą być szczególnie interesujące i przydatne dla podmiotów i organizacji zajmujących się analizą ruchu sieciowego, takich jak CERT-y (j.ang. *Computer Emergency Response Team*), SOC-i (j.ang. *Security Operations Center*), CERT-y branżowe itp..

Niniejsza praca dobrze wpisuje się w konsultowaną aktualnie (w momencie pisania recenzji) Strategię Cyfryzacji Państwa, w której cyberbezpieczeństwo oraz metody sztucznej inteligencji są istotnymi zagadnieniami.

9. Wniosek

Biorąc pod uwagę przedstawioną przez Doktoranta rozprawę stwierdzam, że recenzowana praca **spełnia wymagania stawiane rozprawom doktorskim** przez obowiązujące przepisy.

Dlatego wnoszę o przyjęcie niniejszej rozprawy i **dopuszczenie** mgr inż. Jacka Krupskiego do publicznej obrony.

Prof. dr hab. inż. Michał Choraś