dr hab. inż. Sławomir Hanczewski

Instytut Sieci Teleinformatycznych

Wydział Informatyki i Telekomunikacji

Politechnika Poznańska

Poznań, 12.02.2025

RECENZJA ROZPRAWY DOKTORSKIEJ
DLA RADY DYSCYPLINY
AUTOMATYKA, ELEKTRONIKA, ELEKTROTECHNIKA I TECHNOLOGIE KOSMICZNE
POLITECHNIKI OPOLSKIEJ

Autor rozprawy doktorskiej: mgr inż. Wiktor Sędkowski

Tytuł rozprawy doktorskiej: „Threat Modeling methods and detecting vulnerabilities in 5G networks"

Promotor: dr hab. inż. Rafał Stanisławski, profesor PO

1. Ocena wyboru tematu i tezy naukowej rozprawy

Obecnie obserwujemy bardzo dynamiczny rozwój technologii w każdej dziedzinie życia. Praktycznie niczym nie ograniczona możliwość komunikacji, pozwalająca na łączenia ze sobą różnych systemów, niesie ze sobą korzyści ale również i niebezpieczeństwa. Problem bezpiecznego działania współczesnych systemów staje się zatem multidyscyplinarny. Z tym problemem postanowił zmierzyć się Doktorant, decydując się na przygotowanie rozprawy pt. „Threat modeling methods and detecting vulnerabilities in 5G networks". Temat ten, jest bardzo aktualny i wpisuje się w szeroki obszar badań aktualnie prowadzonych na świecie, zwłaszcza z biorąc pod uwagę możliwości wykorzystania do rozwiązania rozważanego problemu narzędzi bazujących sztucznej inteligencji (SI). Dlatego uważam, że rozprawa wpisuje się obszar dyscypliny naukowej Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne.

Doktorant postawił następujące hipotezy badawcze:

1) Możliwe jest skuteczne modelowanie i ustalanie priorytetów zagrożeń występujących w sieciach 5G, uwzględniając zmienność struktury sieci.

2) Możliwe jest wykorzystanie zautomatyzowanych, adaptacyjnych algorytmów obliczeniowych działających w czasie rzeczywistym do modelowania i priorytetyzacji zagrożeń.

Tak postawione hipotezy badawcze jasno określają ogólny cel rozprawy: opracowanie metod pozwalających na zwiększenie bezpieczeństwa sieci 5G, będącej obecnie podstawą budowy różnych systemów użytkowych lub służącej jedynie jako sieć dostępowa do internetu.

Moim zdaniem, mimo pewnych niedociągnięć (które przytoczono w dalszej części recenzji), zostały one udowodnione przez Doktoranta w wyniku przeprowadzonych przez niego badań, których rezultaty zostały przedstawione w rozprawie (także w trzech publikacjach).

Według mojej opinii mgr inż. Wiktor Sędkowski rozwiązał postawiony problem naukowy w zakresie adekwatnym do postawionych hipotez, stosując prawidłowe metody badawcze.

2. Charakterystyka rozprawy

Rozprawa składa się z 129 stron a jej treść została podzielona na 5 rozdziałów. Rozprawę uzupełnia bibliografia oraz spis tabel i rysunków. Rozprawa została przygotowana w języku angielskim.

Pierwszy rozdział pracy stanowi wstęp do rozprawy, w którym przestawiony został problem badawczy, zakres, hipotezy i cel pracy. Rozdział ten zawiera również krótką charakterystykę metod zastosowanych podczas badań.

W rozdziale drugim została zawarta charakterystyka sieci 5G. Uwzględnia ona np. właściwości interfejsu radiowego wraz z wykorzystywanymi tam technologiami, takimi jak kształtowanie wiązki (beamforming), masywne MIMO (massive MIMO). Omówione zostały również podstawowe komponenty sieci. Rozdział ten uwzględnia także w architekturę opartą na usługach 5G, zidentyfikowane zagrożenia dla sieci 5G oraz wskazuje na krytyczne (z punktu widzenia bezpieczeństwa) elementy sieci 5G.

Rozdział trzeci to przegląd istniejącej literatury dotyczącej metodologii modelowania zagrożeń. W rozdziale tym Doktorant odniósł się również do problemu wykorzystania sztucznej inteligencji w modelowaniu zagrożeń a także do automatyzacji tego procesu.

Rozdział czwarty skupia się na automatyzacji procesu modelowania zagrożeń. W rozdziale tym omówiono źródła danych do automatycznego modelowania zagrożeń, automatyzację przygotowywania diagramów zagrożeń oraz wyzwania związane z opisywaniem zagrożeń. Analizuje również wykorzystanie GPT do opisywania zagrożeń, w tym gromadzenie danych, próby wdrożenia rozwiązania i porównania z podobnymi narzędziami. W tym rozdziale Doktorant powołuje się na swoją publikację.

Rozdział 5 dotyczy automatyzacji wykrywania podatności w zabezpieczeniach, począwszy od wykrywania zasobów i przewidywania zagrożeń. Szczegółowo opisano w nim procesy gromadzenia danych wykorzystywanych do uczenia modeli, opracowywania modeli sztucznej inteligencji do przewidywania podatnych zasobów oraz przewidywania wzorców wykorzystania podatności. Rozdział kończy się prezentacją wyników badań.

Bibliografia zawiera listę wszystkich źródeł i odniesień wykorzystanych w rozprawie (łącznie 106 pozycji, choć nie udało mi się znaleźć odwołania w tekście do pozycji nr 88). Obejmuje ona książki, artykuły w czasopismach, materiały konferencyjne i inne istotne materiały wspierające badania.

W mojej ocenie struktura rozprawy doktorskiej jest w zasadzie prawidłowa. Przyjęty układ wskazuje na przemyślane działanie Doktoranta w trakcie procesu przygotowania rozprawy. Dotyczy to zwłaszcza pierwszych rozdziałów wprowadzających czytelnika w tematykę rozprawy. Jedyna uwaga dotycząca struktury rozprawy dotyczy podrozdziału 5.3 Conclusions, który w mojej opinii powinien stanowić oddzielny rozdział. Samo zaś podsumowanie rozprawy nie powinno być jedynie streszczeniem wcześniejszych rozdziałów. Pierwsze zdanie z rozdziału 5.3 również wydaje się niefortunne z punktu widzenia przeprowadzonych badań (This dissertation has presented an overview of topics related to threat modeling and vulnerability detection in modern systems.).

Biorąc pod uwagę przygotowanie edycyjne rozprawy, Doktorant mógłby poświęcić więcej czasu na jej opracowanie. W pracy pojawiają się bowiem rysunki do których nie ma odwołania w tekście rozprawy (np. rysunek nr 19), zdarzają się błędnie odwołania do tablic (strona 104, jest Table 2 powinno być Table 14) czy też różny zapis np. source own (Own z

kropka lub bez). Również zamieszczone a wykorzystywane przez Doktoranta kod programów mogłyby być choć w małym stopniu opisane. Uważam również, że dodatkowe przeczytanie rozprawy przed jej oddaniem mogłoby rozwiązać wiele takich problemów, choć wiadomo, że uniknięcie wszystkich niedociągnięć nie jest możliwe.

3. Ocena wartości naukowej rozprawy

Za największe osiągnięcie pracy uważam opracowanie metod automatyzacji procesu modelowania zagrożeń z wykorzystaniem do tego celu sztucznej inteligencji a także opracowanie i implementacja narzędzia do automatycznego wykrywania podatności a także przeprowadzenie analizy porównawczej efektywności działania mechanizmów sztucznej inteligencji z metodami konwencjonalnymi modelowania zagrożeń realizowanymi przez eksperta. Przedstawione przez Doktoranta rozwiązania pozwalają na poprawę bezpieczeństwa sieci 5G a tym samym i innych systemów korzystających z sieci 5G co nie jest problemem trywialnym. Niestety, opis w rozprawie tych rozwiązań, moim zdaniem, nie jest pełny. Na czym sama rozprawa traci. Doktorant powinien w jasno i przede wszystkim szczegółowo przedstawić swoje rozwiązania. Pewną nonszalancją można nazwać odsyłanie czytelnika rozprawy do artykułu w celu znalezienia więcej szczegółów. Artykuły, których Doktorant jest współautorem sią dostępne w bazie IEEExplore do której nie każdy ma dostęp. Nie mniej jednak należy podkreślić, że z punktu widzenie idei doktoratów wdrożeniowych, przeprowadzona implementacja własnego rozwiązania ma zasadnicze znaczenie.

Do mniej znaczących osiągnięć zaliczam: przeprowadzenie analizy istniejących metod modelowania zagrożeń oraz ich wykorzystania w sieciach 5G, szczegółowa analiza mechanizmów i elementów sieci 5G (z uwzględnieniem interfejsu radiowego i części core).

4. Uwagi szczegółowe i dyskusyjne.

Przestawiona rozprawa porusza istotny dla współczesnego świata problem cyberbezpieczeństwa. Jej lektura zrodziła następujące pytania, komentarze:

1. Jak wyglądało środowisko badawcze?
2. Jak wyglądała realizacja eksperymentów, których rezultaty przedstawiono w tabeli 16?
3. W jaki sposób przeprowadzona została analiza, której wynikiem jest rysunek 17?

4. Proszę o komentarz dotyczący zaproponowanych przez Doktoranta rozwiązań w kontekście najnowszych rozwiązań LLM?
5. Czym jest GMS z tabeli 1?
6. Jeśli nie Python to co?
7. Co zdaniem Doktoranta jest jego dotychczasowym największym osiągnięciem?

5. Wniosek końcowy

Biorąc pod uwagę przedstawione w recenzji uwagi krytyczne i polemiczne a także wymagania zawarte w Ustawie z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2023 r. poz. 742, z późn. zm.), uważam, że rozprawa doktorska mgr. inż. Wiktora Sędkowskiego pt. „Threat Modeling methods and detecting vulnerabilities in 5G networks" zawiera oryginalne rozwiązania problemu naukowego oraz dowodzi, że Autor posiada ogólną wiedzę teoretyczną w dyscyplinie Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne oraz posiada umiejętność samodzielnego prowadzenia pracy naukowej.

Wnoszę o dopuszczenie rozprawy doktorskiej Pana mgr. inż. Wiktora Sędkowskiego pt. „Threat Modeling methods and detecting vulnerabilities in 5G networks" do publicznej obrony.

Sławomir Hanczewski