Prof. dr hab. inż. Jerzy Baranowski
Profesor, AGH w Krakowie
Wydział Elektrotechniki, Automatyki,
Informatyki i Inżynierii Biomedycznej
Katedra Automatyki i Robotyki
jb@agh.edu.pl, 605-439-587

Kraków, 9.02.2025

Recenzja rozprawy doktorskiej mgr inż. Wiktora Sędkowskiego pt.: „Threat Modeling methods and detecting vulnerabilities in 5G networks"

Podstawa formalna opracowania recenzji

Umowa o dzieło nr 70/DN/2024 między recenzentem a Politechniką Opolską, reprezentowaną przez przewodniczącego Rady Dyscypliny Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne (AEEiTK) Politechniki Opolskiej dr hab. inż. Andrzeja Waindoka, prof. uczelni.

Dane uzupełniające o pracy

Promotor: dr hab. inż. Rafał Stanisławski, prof. PO
Rozprawa doktorska była realizowana w ramach programu „Doktorat wdrożeniowy"/

Ocena formalna pracy

Przedłożona do oceny rozprawa doktorska (licząca 129 stron) składa się z pięciu rozdziałów oraz spisów skrótów i oznaczeń, literatury oraz tabel i rysunków. Praca została napisana w języku angielskim.

Pierwszy rozdział nosi tytuł „Introduction" i jak sama nazwa wskazuje jest wprowadzeniem do pracy. Jest on podzielony na osiem sekcji, każda poświęcona osobnemu obszarowi, takim jak sformułowanie problemu badawczego, zakres pracy, teza pracy, cel pracy, metodologia badawcza, wkład autora, struktura pracy oraz opis źródeł. Teza pracy jest sformułowana w sposób nieskładny i niekonkretny. Autor rozwodzi się nad „płodnym gruntem dla zagrożeń bezpieczeństwa" i roli rozwiązań heurystycznych opartych o AI (czyli nie do końca wiadomo jakich). Na tych niezbyt konkretnych podstawach sformułowano dwie hipotezy badawcze, które są bardziej precyzyjne. Pierwsza z nich mówi, że jest możliwe modelowanie i priorytetyzowanie zagrożeń występujących w sieciach 5G, zaś druga to, to że da się to zrobić za pomocą automatycznych i adaptacyjnych algorytmów obliczeniowych pracujących w czasie rzeczywistym. Następna sekcja, jako cel nie stawia jednak weryfikacji tych hipotez, a „udowodnienie, że AI może odgrywać rolę w bezpieczeństwie nowowczesnych sieci oraz implementację takich rozwiązań". Sekcja „contribution" opisująca wkład doktoranta jest również niezbyt klarowna, ale należy wnioskować, że doktorant określa swój wkład jako przeprowadzenie analizy

jakościowo-ilościowej charakteru zagrożeń w sieciach 5G oraz opracowanie prototypowych narzędzi.
Rozdziały drugi – „5G Network" i trzeci „State-of-the-art in threat modeling" mają w zasadzie charakter przeglądu literatury i nie wymagają szczególnej dyskusji. Wyjątkiem jest jednak podrozdział 2.4, który stanowi dość głęboką analizę modelowania zagrożeń w odniesieniu do sieci 5G co stanowi element osiągnięcia doktoranta. Doktorant dodatkowo sekcji 3.4 opisuje narzędzia do automatycznej generacji modeli zagrożeń, oraz jak potencjalnie można je wykorzystać w sieciach 5G. Podrozdział ten jest powiązany z pracą [56], którą autor wraz ze współautorem Łukaszem Basą opublikował jako rozdział w podręczniku do cyberbezpieczeństwa.

Rozdział czwarty pt. „Automating threat modeling process" obejmuje pierwszą część zasadniczej pracy autora. Omawiane są w nim zagadnienia generacji graficznych modeli zagrożeń oraz opisów zagrożeń. Rozdział nie jest przesadnie czytelny, zawiera np. duży fragment pliku YAML opisującego środowisko programowe, który rozciąga się na 6 stron, bez szczególnego uzasadnienia i co gorsza bez dobrej interpretacji. Następnie przeprowadzona jest krótka analiza efektywności automatycznej generacji diagramów, ze wskazaniem, że w zasadzie ono nie działa bez manualnych poprawek. Należy zwrócić uwagę na brak analizy narzędzi AI w tym zakresie, które są publicznie dostępne. Druga część rozdziału omawia zagadnienie generacji opisu zagrożeń w oparciu o dane. Poprzedza je analiza jakościowa z użyciem ankiet (20 osób, brak szczegółowych informacji na ich temat oprócz przynależności do specjalistycznych grup w mediach społecznościowych). Analiza została przeprowadzona w ramach pracy [90]. Charakter analizy pozostawia wiele do życzenia, gdyż przeprowadzono wyłącznie analizę średniej odpowiedzi, przy czym ocena miała charakter 1-10, co w przypadku oceny przez ludzi powinno być traktowane jako zmienna niemetryczna. Brak również informacji o związku proponowanego zagadnienia SQL injection w kontekście sieci 5G. Następnie autor podejmuje próbę wykorzystania narzędzi LLM do automatycznego generowania opisów. Tutaj widoczny jest największy wkład doktoranta, który pozyskał dane a następnie skonstruował rozwiązanie w postaci pre-promptingu w pythonie, które ma współpracować z modelem GPT. Analiza wyników pozostawia nieco do życzenia, jako że 7.5% wyników było bezużytecznych, zaś bliżej nieokreślona liczba opisów została określona przez autora jako „vague and generic". Przeprowadzono następnie analizę porównawczą z niepromptowanym modelem GPT, alternatywnym rozwiązaniem STRIDE-GPT oraz dwoma ekspertami (bliżej nieznanymi). Przedstawiono procentową analizę podobieństwa modeli językowych do eksperta (sposób oceny podobieństwa nie został opisany).

W rozdziale piątym autor zajmuje się zagadnieniem automatycznego wykrywania podatności. Rozdział rozpoczyna się od analizy dostępnych narzędzi open source. Następnie omówione jest zagadnienie przewidywania zagrożeń. Autor przeprowadza w nim analizę modelu, o którym wiadomo jedynie, że był to pretrenowany model o architekturze transformera połączony z nieokreślonym modelem uczenia maszynowego. Następnie bez podania źródeł autor stwierdza „Research proves that this approach can be used in cloud environments for fast

identification of targets which should be prioritized for full vulnerability scan." Dalsza część rozdziału omawia modele wykrywania wzorców podatności. Jest to skrócone podsumowanie pracy [105]. Ponownie brak jakichkolwiek szczegółów o specyfice modelu, brak ich również w cytowanej pracy. Jednocześnie, zwracając uwagę, że praca [105] jest współautorska, pewien niedosyt stanowi brak informacji o tym za jakie elementy pracy odpowiadał autor. Rozdział kończy dwustronicowe podsumowanie całej rozprawy doktorskiej, które stanowi streszczenie wszystkich rozdziałów. Widoczny jest brak próby osadzenia badań w szerszym kontekście naukowym.

Spis literatury liczy 106 pozycji obejmuje podręczniki, artykuły w czasopismach, referaty konferencyjne, rozdziały w książkach i odniesienia do stron internetowych. Przegląd literatury jest bardzo wyczerpujący i zawiera zarówno prace ugruntowane jak też i te z bieżącego roku.

Przedstawiony układ pracy doktorskiej jest generalnie logiczny, i w większości zgodny z zasadą hierarchizacji treści oraz przejrzysty. Niedosyt budzi brak szerszego podsumowania i dyskusji oraz określenia podstawowych ograniczeń uzyskanych wyników i możliwości ich rozwoju. Jakość wykonanych ilustracji (wykresów) jest w większości akceptowalna, jednak ich czytelność pozostawia sporo do życzenia, część z nich powtórzono jeden do jeden z prac bez odpowiedniego cytowania. Opisy rezultatów pozostawiają wiele do życzenia, zwłaszcza że w zasadzie jedyna analiza porównawcza została przeprowadzona dla metod opisu zagrożeń.

Na podstawie rozprawy można uznać, że doktorant posiada wiedzę teoretyczną, niezbędną do poprawnego prowadzenia badań i wnioskowania badawczego.

Ocena merytoryczna pracy

Tematyka i zakres wykonanej pracy lokują ją w dyscyplinie Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne w obszarze na styku cyberbezpieczeństwa, automatyki i modelowania. Szczególnie dotyczy to wykorzystania uczenia maszynowego do usprawnienia bezpieczeństwa. Problematyka pracy jest ważna i aktualna.

Należy jednoznacznie stwierdzić, że hipoteza postawiona w pracy nie została zweryfikowana. Nie pokazano zdolności do pełnej automatyzacji, adaptacji algorytmów ani też ich pracy w czasie rzeczywistym. Cel pracy natomiast, który tę hipotezę osłabia został zrealizowany. Pokazano możliwość wykorzystania narzędzi AI zarówno teoretycznie jak też i przykładowymi metodami, które mogą analizę bezpieczeństwa wspierać. W pracy zdecydowanie brak szczegółów dotyczących przeprowadzonych badań, zwłaszcza użytych algorytmów uczenia maszynowego i pogłębionych analiz. Braki te powinny zostać uzupełnione podczas publicznej obrony.

Za szczególnie znaczące aspekty rozprawy uważam następujące osiągnięcia:

1. **Usystematyzowanie technik modelowania zagrożeń** – analiza istniejących metod modelowania zagrożeń, ich mocnych i słabych stron oraz potencjalnego zastosowania w sieciach 5G.
2. **Wpływ architektury 5G na bezpieczeństwo sieci** – szczegółowa analiza nowoczesnych rozwiązań w sieciach 5G, takich jak wirtualizacja RAN, architektura oparta na usługach (SBA) czy separacja płaszczyzny sterowania i użytkownika (CUPS), w kontekście ich podatności na zagrożenia.
3. **Opracowanie metod automatyzacji procesu modelowania zagrożeń** – zaproponowanie wykorzystania sztucznej inteligencji (AI) do generowania opisów zagrożeń na podstawie danych.
4. **Implementacja narzędzia do automatycznego modelowania zagrożeń** – stworzenie prototypowego rozwiązania, które łączy AI z istniejącymi bazami wiedzy o zagrożeniach w celu tworzenia predykcji. Brak jednak szczegółów tego rozwiązania.
5. **Porównawcza analiza skuteczności automatyzowanego opisywania zagrożeń** – przeprowadzenie badań porównujących skuteczność podejścia AI z tradycyjnymi metodami modelowania zagrożeń (przez eksperta).

Praca ma pewne niedociągnięcia. Dotyczą one przede wszystkim szczegółowości opisu przeprowadzonych badań. Autor powinien zdecydowanie bardziej dogłębnie opisać stosowane techniki, eksperymenty oraz precyzyjniej przeprowadzić analizę ilościową i jakościową.

Uwagi krytyczne i dyskusyjne

Praca jest interesująca i dotyczy ważnych problemów, są jednak pewne zagadnienia, w stosunku do których oczekiwałbym głębszego wyjaśnienia podczas publicznej obrony.

1. Czy proponowane narzędzia wykorzystujące AI nie działałyby lepiej gdyby wykorzystywać techniki strukturalizowanej generacji (structured generation)?
2. Czy narzędzia typu PyMTGPT nie rozwiązują znacznej części problemów w sekcjach 4.1 i 4.2?
3. Proszę szczegółowo opisać modele uczenia maszynowego opisane w sekcji 5.2.
4. Proszę przedstawić wyniki badań potwierdzających prawdziwość zdania „Research proves that this approach can be used in cloud environments for fast identification of targets which should be prioritized for full vulnerability scan."

Mam również pewne uwagi o charakterze redakcyjnym:

1. Język pracy jest trudny, zdania są przesadnie „kwieciste", słownictwo co prawda bogate to jednak nienaturalne w odbiorze. Te efekt sugeruje wykorzystanie do przygotowania części dokumentu tzw. Dużych modeli językowych. Samo to w sobie nie jest naganne, jednak autor powinien we wstępie zaznaczyć wykorzystanie takich narzędzi w dokumencie. Dodatkowo, po poddaniu dokumentu analizie pod kątem wykorzystania LLM, na szczególnie charakterystyczne do manieryzmów AI wskazano opisy metod

modelowania zagrożeń, podsumowania wyników eksperymentów, opisy podatności oraz podsumowanie.

2. Autor w bibliografii wykorzystuje cytowanie w kolejności odwołań, co nie jest przesadnie czytelne. Jednocześnie jednak nie wszystkie pozycje literatury są cytowane w treści rozprawy. Dzieje się tak np. przy pozycji [88]. Jednocześnie cytowania nie są przygotowane spójnie, stosując niejednorodne style.
3. W bibliografii można też znaleźć nieścisłości jeśli chodzi o kolejność autorów. Przykładowo w pracy [56] autor jest wymieniony, jako pierwszy autor, co nie jest zgodne z informacjami na stronie wydawnictwa.

Poprawienie tych kwestii znacząco poprawiłoby czytelność i profesjonalny wygląd rozprawy.

Wniosek końcowy

Przedłożoną do oceny pracę doktorską pod względem formalnym i merytorycznym, pomimo uwag krytycznych i dyskusyjnych, oceniam pozytywnie.

Uważam, że rozprawa doktorska mieści się w dyscyplinie naukowej „Automatyka, Elektronika, Elektrotechnika i Technologie Kosmicznie" oraz spełnia wszystkie wymagania w art. 187 ustawy z dnia 20 lipca 2018 r.(Dz.U.2024.1571 t.j. z dnia 2024.10.24) Prawo o szkolnictwie wyższym i nauce, bowiem prezentuje ogólną wiedzę teoretyczną autora w dyscyplinie Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne, umiejętność samodzielnego prowadzenia pracy naukowej oraz jest oryginalnym rozwiązaniem problemu naukowego.

W związku z powyższym wnioskuję do Rady Dyscypliny Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne Politechniki Opolskiej o dopuszczenie rozprawy doktorskiej Pani mgr inż. Wiktora Sędkowskiego, pt. *„Threat Modeling methods and detecting vulnerabilities in 5G networks"* do publicznej obrony oraz procedowania dalszych etapów procedury nadawania stopnia doktora.