Prof. dr hab. inż. Ryszard Tadeusiewicz
rtad@agh.edu.pl; www.tadeusiewicz.pl; 30-059 Kraków, al. Mickiewicza 30
Katedra Biocybernetyki i Inżynierii Biomedycznej wydziału EAIiIB AGH
Doktor Honoris Causa czternastu uczelni krajowych i zagranicznych
Członek Polskiej Akademii Nauk; Członek Polskiej Akademii Umiejętności;
Były Rektor AGH; Były Prezes Krakowskiego Oddziału PAN; Były członek CK
Członek Akademii Inżynierskiej, член Российской Академии Естественных Наук
Participe Pleno Jure Academiae Europensis Scientarum Artium Litterarumque
Fellow of World Academy of Art and Science; Euro-engineer FEANI
Senior Member of IEEE; professional member of ACM; member of SPIE

Kraków, 02.05.2023

Recenzja rozprawy doktorskiej mgr inż. Jarosława Homy

Przedmiotem niniejszej recenzji jest rozprawa doktorska mgr inż. Jarosława Homy zatytułowana „Implementacja algorytmów synchronizacji urządzeń sieciowych bazujących na paradygmacie programowalnych sieci komputerowych". Promotorem rozprawy jest prof. dr hab. inż. Aleksander Nawrat, a funkcję promotora pomocniczego pełnił dr inż. Krzysztof Daniec. Praca została opracowana na Wydziale Automatyki, Elektroniki i Informatyki Politechniki Śląskiej na kierunku Informatyka. Przewód jest prowadzony wg. zasad określonych w „starej" Ustawie, więc rozprawa może być broniona w dyscyplinie Informatyka.

Rozprawa ma objętość 93 stronic, a jej treść podzielona jest na 5 rozdziałów, wliczając w to „Wstęp" oraz „Podsumowanie i wnioski".

Przedstawię teraz omówienie poszczególnych części pracy, dokonując wstępnej oceny ich wartości z punktu widzenia wymagań stawianych ustawowo i zwyczajowo rozprawom doktorskim.

Wstęp naświetla znaczenie problematyki podjętej w ocenianej pracy. Jest bardzo profesjonalnie napisany i dowodzi ogromnej wiedzy Doktoranta w obszarze problemowym, w którym ulokowana jest rozprawa. Dodatkowo na stronie 12 owego Wstępu zdefiniowana jest **teza** pracy, która brzmi:

> *Możliwe jest opracowanie systemu mitygacji ataków sieciowych, opartego o rozwiązanie programowalnych sieci komputerowych SDN, wykorzystującego nowatorskie algorytmy sterowania i synchronizacji urządzeń, w tym analizę uzyskaną za pomocą algorytmów sztucznej inteligencji AI.*

Autor dodatkowo wskazuje, że głównym celem jego wysiłku jest detekcja ataków sieciowych z rodziny DDoS.

Uważam, że sformułowana teza odpowiada ustawowym i zwyczajowym wymaganiom, jakie wiąże się z zagadnieniem naukowym formułowanym i rozwiązywanym w ramach rozprawy doktorskiej.

Doceniam wartość naukową, jaką wniesie udowodnienie (w treści rozprawy) prawdziwości owej tezy, ponieważ powstaną (jak deklaruje Autor) nowatorskie algorytmy sterowania i synchronizacji urządzeń, dające kolejnym badaczom nowe narzędzie do rozwiązywania różnych problemów wiążących się z używaniem programowalnych sieci komputerowych SDN. Naukową wartość dostrzegam też w badaniu przydatności algorytmów sztucznej inteligencji w kontekście zadań rozważanych w rozprawie. Doceniam także wartość praktyczną oczekiwanych wyników rozprawy, ponieważ implementacja algorytmów synchronizacji urządzeń sieciowych w sieciach SDN z pewnością będzie użyteczna dla administratorów takich sieci. Stwierdzam także, iż problem badawczy zdefiniowany w ocenianej tezie jest w pełni oryginalny, nie znam bowiem żadnych opracowań innych autorów (krajowych czy zagranicznych), które by formułowały podobne problemy i sygnalizowały podobne rozwiązania.

Rozwijając myśli zawarte w tezie rozprawy mgr Homa wskazuje, jakie technologie zamierza stosować i jak rozplanował realizację celów rozprawy.

Drugi rozdział ocenianej rozprawy zawiera – zgodnie z tytułem – przegląd literatury. Jest on przeprowadzony przez Doktoranta w sposób wzorowy i z pewnością umożliwia mi (jako opiniodawcy) wystawienie bardzo pozytywnej opinii na temat rozległości i szczegółowości wiedzy mgra Homy w obszarze problematyki wiążącej się z tezą ocenianej rozprawy. Informacje literaturowe zebrane przez Autora są aktualne, dobrze dobrane i poprawnie omówione. Doktorant wprowadza i obszernie omawia sieci komputerowe SDN, bardzo nowoczesne i w sumie mniej znane, niż tradycyjne sieci komputerowe, więc ta część rozprawy jest dla czytelnika bardzo wartościowa. Opis odpowiednio: koncepcji SDN, architektury referencyjnej sieci, protokołu Open Flow, przełącznika Open Flow, kontrolera sieci i jej bezpieczeństwa – są przygotowane perfekcyjnie. Sugeruję, że ten bardzo dobrze napisany rozdział warto by było opublikować (najlepiej online) jako materiał informacyjny przydatny dla wielu osób. Do decyzji Autora pozostaje wybór formy takiej publikacji: artykuł open access, wpis na blogu, załącznik w mediach społecznościowych itp. Ale publikacja byłaby bardzo przydatna.

W dalszej części omawianego drugiego (literaturowego) rozdziału dysertacji Doktorant omówił techniki wykrywania ataków DDoS. Opisano metody oparte na teorii informacji, techniki oparte na regułach oraz techniki wykorzystujące uczenia maszynowe. Zwłaszcza te ostatnie są bardzo ciekawe, bo nawiązują do zapowiedzianego w tezie rozprawy wykorzystania algorytmów sztucznej inteligencji.

Podsumowując moją opinię na temat zawartości drugiego rozdziału recenzowanej rozprawy mogę (w kontekście wymagań stawianych rozprawie doktorskiej) mogę przedstawić następujący pogląd: Na zawarte w kryteriach pytanie o zasoby wiedzy Doktoranta mogę z całą stanowczością

odpowiedzieć pozytywnie. Natomiast zawartości tego rozdziału, opartego głównie na analizie i dyskusji wyników prac innych autorów, nie mogę zaliczyć do **oryginalnych własnych osiągnięć naukowych Kandydata**, zatem nie mogę włączyć tej pozytywnej oceny do argumentów przemawiających za nadaniem stopnia naukowego. Trzeba bowiem mieć na uwadze fakt, że stopień naukowy nadaje się za własny wkład naukowy Doktoranta do dyscypliny, w której ulokowana jest oceniana rozprawa. W tym rozdziale owego **własnego wkładu naukowego** mgra Homy nie dostrzegłem.

Całkiem inna sytuacja jest związana z zawartością trzeciego rozdziału rozprawy, zatytułowanego „Proponowane rozwiązanie problemu". Z czysto redakcyjnego punktu widzenia jestem zdania, że byłoby dobrze w tym miejscu przypomnieć, co jest owym rozwiązywanym **problemem**, bo od stronicy nr 12, na której zapisana została teza rozprawy i problem był bardzo wyraźnie zarysowany, czytelnik musiał „przebić się" przez cały bardzo bogaty w treści rozdział 2 i już trochę zatarła się świadomość, ku czemu konkretnie Doktorant zmierza.

Ale poza tą uwagą redakcyjnej natury – zawartość rozdziału 3 niesie te wartości, które składają się na naukowe (i praktyczne) osiągnięcie, będące kluczem do nadania Panu Jarosławowi Homie stopnia naukowego doktora. Głównym osiągnięciem jest stworzenie koncepcji, a następnie także implementacji systemu STRAINER, który służy do wykrywania i mitygacji dwóch podstawowych grup ataków sieciowych z rodziny DDoS. Doktorant podkreśla przy tym, że projektując system dedykowany do **wykrywania** ataków DDoS wchodzi na nowy grunt badawczy i nie dubluje prac wcześniejszych badaczy, którzy skupiali uwagę na **odpieraniu** ataków typu DoS. Następnie lokuje swój system STRAINER wśród innych systemów chroniących przed atakami DDoS i podkreśla oryginalne rozwiązania opracowanego przez siebie systemu mitygacji ataków DDoS w podrozdziale 3.2. Na tej podstawie prezentowany jest opis architektury systemu oraz jego modułów. Za szczególnie ciekawy uważam moduł MOD2 wykorzystujący koncepcję losowego lasu złożonego z losowych lasów (vide rysunek 16 na stronicy 59), opisany w podrozdziale 3.4.2, oraz moduł MOD3 oparty na metodzie głębokiego uczenia z wykorzystaniem akceleracji za pomocą kart GPU.

Uważam, że rozdział 3 rozprawy wnosi bardzo wiele oryginalnych i wartościowych koncepcji, będących wynikiem przemyśleń i doświadczeń Autora, więc zdecydowanie jego zawartość traktuję jako **wartościowy wkład naukowy** (i praktyczny) mgra Homy do dziedziny mitygacji ataków sieciowych, znacząco posuwających naprzód wiedzę na ten temat oraz praktykę tworzenia systemów ochronnych programowalnych sieci komputerowych SDN. Jest to pierwsza z bardzo mocnych przesłanek przemawiających za tym, żeby Kandydatowi nadać stopień naukowy doktora.

Dalszych argumentów zmierzających do tego samego wniosku dostarcza rozdział 4. Opisuje on zastosowane środowisko testowe oraz testy weryfikacyjne systemu. Przeprowadzenie takich testów było konieczne dla domknięcia dowodu prawdziwości zaproponowanej tezy rozprawy. W tezie tej bowiem stwierdzono:

Możliwe jest opracowanie systemu mitygacji ataków sieciowych (...)

Dla dowiedzenia tej tezy nie wystarczyło pokazanie struktury proponowanego systemu (co nastąpiło w rozdziale 3), ale trzeba było także wykazać, że system taki naprawdę może się przyczyniać do mitygacji rozważanej klasy ataków. Doktorant podszedł do tego zadania bardzo profesjonalnie. Stworzył odpowiednie środowisko testowe, przeprowadził symulowane ataki i badał skuteczność systemów mitygacji. Opis tych testów na stronicach 67 i 68 rozprawy jest dla mnie nieczytelny, bo Doktorant posługuje się skrótami i nazwami, których nie byłem w stanie odszyfrować i zweryfikować. Zakładam jednak, że testowanie zostało przeprowadzone poprawnie, a wyniki podane w podrozdziale 4.2 są wiarygodne. Na szczęście wyniki te, zestawione w tabelach o numerach od 5 do 7 były dla mnie czytelne i zrozumiałe (w odróżnieniu od wskazanych wyżej opisów), więc upewniłem się, że stworzony przez mgra Homę system naprawdę jest w stanie wykrywać ataki (tym skuteczniej, im są one intensywniejsze). Podobnie jako prawidłowe odbieram wyniki zestawione w podrozdziale 4.3 (tabela 8), więc cały rozdział 4 opiniuję pozytywnie, a zawarte w nim wyniki uważam za wartościowy wkład Doktoranta do uprawianej dyscypliny naukowej.

Zdecydowanie pozytywnie oceniam też rozdział 5 („Podsumowanie i wnioski") w którym Autor skrótowo podsumował zebrane informacje literaturowe, opisał swoje dzieło w postaci systemu STRAINER, opisał syntetycznie ten system i jego moduły, wykazując, że zbudowany system ma szereg zalet, a także nawiązał do wyników przeprowadzonych testów. Owo podsumowanie kończy mgr Homa stwierdzeniem, że *„Zaimplementowane rozwiązania w systemie STRAINER w pełni realizują postawioną w pracy tezę"*. Zgadzam się z tym stwierdzeniem, chociaż dla porządku odnotuję, że tezę się dowodzi, a nie realizuje.

Podsumowując tę recenzję stwierdzam, że moja ocena merytoryczna opiniowanej rozprawy jest zdecydowanie pozytywna.

Dla porządku odnotuję kilka mało ważnych uwag dyskusyjnych, jakie mi się nasunęły przy studiowaniu dysertacji. Oceniana praca jest generalnie napisana na bardzo wysokim poziomie i żadnych merytorycznych błędów mnie nie udało się odnaleźć. Dodam, że bardzo się z tego cieszę, bo z całej pracy wynikał wniosek, że Autor jest osobą bardzo kompetentną, rzetelną

i kreatywną. Natomiast mam wrażenie, że praca była pisana dość długo, w wyniku czego niektóre zawarte w niej **marginalne** stwierdzenia uległy dezaktualizacji.
Na przykład na dole stronicy 11 Autor pisze: „(...) *Polska nazwała ustawę o cyberbezpieczeństwie KSC – (ustawa o Krajowym Systemie Cyberbezpieczeństwa). Dokumenty te są aktualnie w fazie uzgodnień i aktualizacji* (...)" Tymczasem Ustawa o Krajowym Systemie Cyberbezpieczeństwa została **uchwalona** 5 lipca 2018 roku (Dz.U. 2018 poz. 1560) i **obowiązuje** – jakkolwiek (jak każdy akt prawny) będzie z pewnością podlegać aktualizacji. Dodam, że obecnie projekt nowelizacji tej Ustawy znajduje się w wykazie prac legislacyjnych i programowych Rady Ministrów. Ale Ustawa **jest** i działa!

Niewątpliwą zaletą ocenianej pracy jest obszerny Słownik Skrótów i Oznaczeń. Ponieważ poszczególne hasła są objaśniane dość obszernie – jest to bez mała mikro-podręcznik terminologii używanej w zagadnieniach cyberbezpieczeństwa. Jednak próba skorzystania z tego słownika w kontekście skrótów i oznaczeń zawartych w pracy pokazała, że jest on wysoce niekompletny. Na przykład na stronie 12 pracy Autor pisze o agregatorach zdarzeń SIEM – ale tego skrótu nie ma we wspomnianym słowniku. Dalej wymienia analizatory SOAR, ale tego skrótu także bezskutecznie szukałem w słowniku. O zaporach FW i NG, wymienianych wśród narzędzi na stronicy 12, też w słowniku ani słowa. Tak więc po entuzjastycznym odnotowaniu obecności w pracy wspomnianego Słownik Skrótów i Oznaczeń - byłem potem bardzo rozczarowany jego nieprzydatnością przy czytaniu tekstu rozprawy...

Wydaje mi się, że wykryłem drobny błąd literowy w tytule podrozdziału 3.4.2. Jest Random Forest o Random Forest, a powinno być chyba: Random Forest **of** Random Forest**s.**

Ale przytoczone uwagi w najmniejszym stopniu nie umniejszają wartości rozprawy, więc **wniosek końcowy** tej recenzji jest taki, że rekomenduję Radzie Dyscypliny Informatyka Techniczna i Telekomunikacja Politechniki Śląskiej **przyjęcie** rozprawy i dopuszczenie jej autora, mgr. inż. Jarosława Homy do jej obrony, a po pozytywnym (mam nadzieję) odbyciu tej obrony będę wnioskował o nadanie mu stopnia naukowego doktora.