prof. dr hab. inż. Janusz Górski, prof. zw. Politechniki Gdańskiej
Katedra Inżynierii Oprogramowania
Wydział Elektroniki, Telekomunikacji i Informatyki
Politechniki Gdańskiej

Recenzja
cyklu publikacji oraz o dorobku naukowego, organizacyjnego i dydaktycznego
dra inż. Rafała Kozika

Niniejsza recenzja została przygotowana na potrzeby przewodu habilitacyjnego prowadzonego przez Wydział Informatyki Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie.

Recenzja została przygotowana na podstawie otrzymanej przeze mnie dokumentacji obejmującej wymagany ustawowo zakres, w tym cykl publikacji, na podstawie których dr inż. Rafał Kozik, pracownik Wydziału Telekomunikacji, Informatyki i Elektrotechniki Uniwersytetu Technologiczno-Przyrodniczego w Bydgoszczy ubiega się o nadanie mu stopnia doktora habilitowanego w dziedzinie nauk technicznych w dyscyplinie *informatyka*.

Ocenę osiągnięć dra inż. Rafała Kozika dokonałem kierując się kryteriami zawartymi w Rozporządzeniu Ministra Nauki i Szkolnictwa Wyższego z dnia 1 września 2011 roku.

1. Ocena osiągnięcia naukowego przedstawionego w cyklu publikacji

Opiniowany wniosek dotyczy osiągnięcia naukowego zatytułowanego *Techniki analizy i klasyfikacji danych dla celów zwiększenia bezpieczeństwa aplikacji i sieci teleinformatycznych.*

Osiągnięcie zostało udokumentowane w 11 publikacjach, w tym 7 z listy JCR. Spośród przedstawionych publikacji 10 jest współautorskich a jedna autorska (lista JCR, 100% wkładu habilitanta). W publikacjach współautorskich udział habilitanta jest w większości dominujący (4 publikacje - 50%-65%, 6 publikacji - 70%-85%). Łączny *Impact Factor* wynosi IF=7,223. Z sumarycznej liczby 220 punktów ministerialnych, po uwzględnieniu procentowego udziału współautorów, na habilitanta przypada 151 punktów.

Prace wchodzące w skład osiągnięcia zostały opublikowane w następujących czasopismach: *Security and Communication Networks* (IF=0,904), *Pattern Recognition Letters* (IF=1,952), *Journal of Parallel and Distributed Computing* (IF=1,815), *Lecture Notes in Computer Science*, *Advances in Intelligent Systems and Computing*, *Logic Journal of the IGPL* (IF=0,461, IF=0,575, IF=0,449 - zależnie od roku publikacji), *IEEE Conference Publishing Service*s oraz *Lecture Notes in Artificial Intelligence*.

1.1 Wybór tematyki i cel naukowy

Oceniany wniosek dotyczy aspektów bezpieczeństwa sieci informatycznych oraz aplikacji webowych. Jest to problematyka bardzo aktualna ze względu na burzliwy rozwój zastosowań sieci i posadowionych na nich aplikacji, a z drugiej strony również burzliwy rozwój różnorodnych sposobów zagrażania bezpieczeństwu przechowywanych, przetwarzanych i przekazywanych danych.

W badaniach objętych wnioskiem habilitant skupił się na dwóch celach:

1. Poprawie bezpieczeństwa w sieci poprzez wykrywanie anomalii w ruchu sieciowym oraz identyfikowanie zainfekowanych hostów, na podstawie analizy zagregowanego ruchu sieciowego.
2. Ochronie aplikacji webowych przed cyberatakami na podstawie analizy kierowanych do nich żądań.

Pierwszy z wybranych celów dotyczy bezpieczeństwa ruchu w sieci, podczas gdy drugi dotyczy bezpieczeństwa aplikacji webowych posadowionych w środowisku sieciowym. Szczególnie drugi z tych celów jest wart zainteresowania ze względu na to, że gwałtownie rośnie liczba różnorodnych aplikacji webowych, zróżnicowanych technologicznie i funkcjonalnie oraz często nieodpowiednio zabezpieczonych. Stanowią one atrakcyjny cel dla atakujących, w domniemaniu łatwiejszy do pokonania niż środki bezpieczeństwa infrastruktury sieciowej.

Uważam zarówno wybór tematyki jak i wybór konkretnych celów za dobrze wpasowane w obecne potrzeby i wynikające z nich wyzwania badawcze.

1.2 Metoda badawcza i zakres osiągnięcia

Wyniki badań ukierunkowanych na osiągnięcie celu pierwszego zostały udokumentowane w trzech publikacjach z przedłożonego zestawu (wszystkie z listy JCR, jedna autorska, i dwie współautorskie). W publikacjach współautorskich deklarowany wkład habilitanta obejmował całościową propozycję koncepcyjną oraz znaczny udział w eksperymentach mających na celu zweryfikowanie tych koncepcji.

Zastosowana metoda badawcza polegała na zaproponowaniu innowacyjnych rozwiązań dotyczących pozyskiwania i klasyfikacji strumieni danych reprezentujących przepływy sieciowe oraz ich analizy pod kątem wykrywania występujących w nich anomalii, które mogą świadczyć o zagrożeniu bezpieczeństwa. W celu oceny tych propozycji zostały zaprojektowane i wdrożone rozwiązania techniczne wykorzystujące dostępne komponenty i technologie oraz dostępne zbiory danych. W szczególności wykorzystano technologie BigData, rozwiązania NIDS (Network Intrusion Detection Systems), środki modelowania sieci informatycznych, sieci neuronowe, obliczenia w chmurze i inne. Umożliwiło to ocenę zarówno pod kątem adekwatności funkcjonalnej (to znaczy sprawdzenie, czy zaproponowane mechanizmy są zdolne do osiągania założonego celu) jak i pod kątem skalowalności, a więc dla sytuacji gdy liczba węzłów analizowanej sieci odzwierciedla rozmiar sieci spotykanych w praktyce.

Wyniki badań ukierunkowanych na osiągnięcie celu drugiego zostały udokumentowane w ośmiu publikacjach z przedłożonego zestawu (w tym 4 z listy JCR). Wszystkie te publikacje są współautorskie. W publikacjach tych deklarowany wkład habilitanta obejmował całościową propozycję koncepcyjną (w 7 publikacjach) lub kluczowy udział w opracowaniu takiej koncepcji (w jednej publikacji). W zdecydowanej większości habilitant również deklaruje albo pełny albo istotny udział w opracowaniu scenariuszy badawczych mających na celu eksperymentalną weryfikację tych koncepcji.

Zastosowana metoda badawcza polegała na analizie scenariuszy ataków na aplikacje webowe i zaproponowaniu odpowiednich środków wzmacniających ochronę przed takimi atakami. Kluczowym jest tu mechanizm klasyfikacji żądań umożliwiający wychwytywanie żądań „złośliwych". Habilitant (i współpracownicy) zaproponowali architekturę i algorytmy takiego klasyfikatora umożliwiające selekcję i ekstrakcję istotnych cech żądań wysyłanych do serwera aplikacji, doskonalenie klasyfikatora z pomocą technik uczenia maszynowego, oraz uwzględnili różne protokoły komunikacji klient-serwer oraz różne sposoby reprezentacji żądań.

1.3 Ocena wyniku naukowego

Poddane ocenie wyniki naukowe dotyczą zagadnień aktualnych, mających duże (i rosnące) znaczenie praktyczne. Poprawa bezpieczeństwa sieci zarówno na poziomie infrastruktury jak i na poziomie aplikacji ma zasadnicze znaczenie dla wzmacniania bezpieczeństwa i budowy zaufania do usług i systemów realizowanych środkami technologii informatycznych. Zarówno cele badawcze jaki i sposób ich osiągnięcia nie budzą zastrzeżeń. Opublikowanie tych wyników w renomowanych publikatorach świadczy o tym, że z sukcesem przeszły one ocenę krytyczną ze strony środowiska ekspertów w dziedzinie, której dotyczą. Wyniki te należy uznać z wartościowe, a zakres dokonanej w stosunku do nich oceny eksperymentalnej potwierdza ich potencjalną przydatność praktyczną.

Trzeba jednak zaznaczyć, że prezentowane wyniki są w zdecydowanej większości współautorskie, a więc zawarty jest w nich również wkład pozostałych współautorów. Dla każdej przedłożonej do oceny publikacji przedstawiono jednak wyraźne określenie wkładu autorskiego ze strony habilitanta oraz współautorów wraz z oceną procentową tego wkładu. Na tej podstawie mogę stwierdzić, że wkład ze strony habilitanta był w wielu przypadkach dominujący i nigdy nie był niższy niż 50%.

Głównymi osiągnięciami naukowymi habilitanta w ocenianym zakresie są opracowanie innowacyjnych metod analizy zagregowanego ruchu sieciowego oraz metod oceny tego ruchu z punktu widzenia wykrywania anomalii wskazujących na zagrożenia bezpieczeństwa, opracowanie nowych technik detekcji ataków na podstawie analizy żądań oraz metod poprawy skuteczności wykrywania cyberataków na podstawie analizy dotychczasowych żądań. Warto również podkreślić, że zaproponowane metody zostały poddane rzetelnej weryfikacji eksperymentalnej, potwierdzającej ich skuteczność oraz możliwość praktycznej implementacji.

1.4 Podsumowanie

Uważam, że poddany ocenie wynik naukowy zawarty w przedłożonym cyklu publikacji spełnia kryteria dla przewodów habilitacyjnych.

2. Ocena dorobku naukowego

2.1 Dorobek publikacyjny

Dorobek naukowy zgromadzony przez habilitanta przed uzyskaniem stopnia doktora obejmuje: publikacje z listy JCR (1 publikacja) i publikacje z WoS (21 publikacji). Sumaryczny *Impact Factor* wynosi 0.814, liczba cytowań (bez samocytowań) = 13, *h-index* równy 2.

Po uzyskaniu stopnia doktora, w okresie 2013-2018, dorobek naukowy habilitanta obejmuje: publikacje z listy JCR (14 publikacji) i publikacje z WoS (58 publikacji). Sumaryczny *Impact Factor* wynosi 14.945, liczba cytowani (bez samocytowań) = 86, *h-index* równy 6.

Dorobek ten zarówno w zakresie ilościowym jak i jakościowym spełnia oczekiwania habilitacyjne w dyscyplinie naukowej, z którą związany jest habilitant. Stwierdzam również, po uzyskaniu stopnia doktora habilitant w znacznym stopniu powiększył swój dorobek naukowy.

2.2 Zakres zainteresowań badawczych

Początkowo (przed uzyskaniem stopnia doktora) zainteresowania badawcze habilitanta dotyczyły metod analizy i przetwarzania obrazów i ich zastosowań.

Po uzyskaniu stopnia doktora habilitant rozszerzył zakres swoich zainteresowań, który oprócz problemów dotyczących bezpieczeństwa sieci i aplikacji webowych (główne osiągnięcie badawcze przedstawione w ocenianym wniosku) obejmuje również ochronę infrastruktur krytycznych, jakość procesów wytwarzania oprogramowania, przetwarzanie rozproszone i zastosowania metod analizy danych i uczenia maszynowego. Publikacje dokumentujące wyniki uzyskane w tych obszarach są głownie współautorskie. Wśród tych publikacji, w każdym z wymienionych obszarów, znajdują się pozycje z listy JCR.

Warto podkreślić, że wymienione wyżej obszary aktywności naukowej habilitanta nie są oderwane tematycznie od jego głównego nurtu zainteresowań. Przeciwnie, tworzą szerszy kontekst dla obszaru, w którym ten główny nurt jest realizowany. Uważam to za wartościowe, gdyż lokuje główne osiągnięcia w szerszej perspektywie, zarówno od strony potencjalnych zastosowań (na przykład ochrona infrastruktur krytycznych) jak również od strony stosowanych narzędzi i środków technicznych (na przykład przetwarzanie rozproszone czy metody uczenia maszynowego).

2.3 Udział w projektach badawczych

Habilitant udokumentował szeroki zakres swojego uczestnictwa w projektach badawczych, w tym w projektach międzynarodowych finansowanych z programów Unii Europejskiej takich jak H2020 (2 projekty), FP7 (5 projektów, w tym 3 przed doktoratem), DG Home (1 projekt) i z innych źródeł (4 projekty). W większości z tych projektów wnosił wkład jako wykonawca ale, co warto szczególnie podkreślić, w dwóch projektach z programu H2020 pełnił również role kierownika projektu (po stronie partnera w projekcie) oraz lidera pakietu roboczego, przyjmując tym samym odpowiedzialność za wyniki uzyskiwane przez (międzynarodową) grupę badaczy zaangażowanych w realizację danego pakietu oraz za integrację tych wyników w ramach całej struktury zadaniowej realizowanej w ramach projektu. Oznacza to w szczególności, że habilitant uczestniczył aktywnie nie tylko w realizacji projektów ale również w zdefiniowaniu ich celów, zakresu i struktury.

Uważam, że jest to dorobek i doświadczenie ponadstandardowe na tym etapie rozwoju naukowego świadczące o tym, że habilitant daje sobie świetnie radę w zespołowych przedsięwzięciach badawczych realizowanych w środowisku międzynarodowym.

2.4 Rozpoznawalność w środowisku naukowym

Niewątpliwie o rozpoznawalności habilitanta w środowisku naukowym dobrze świadczą jego udział i pełnione role w międzynarodowych projektach badawczych. Udział w konsorcjach składających propozycje projektów (szczególnie tych finansowanych ze źródeł europejskich) oznacza, że habilitant był traktowany jako atrakcyjny partner wnoszący istotną wartość dodaną do składanej propozycji. Wziąwszy pod uwagę, że średnio szansa na powodzenie aplikacji o projekt międzynarodowy lokuje się na poziomie 10%, udział habilitanta w kilku finansowanych projektach wskazuje, że jego aktywność na polu przygotowywania propozycji projektów była szczególnie wysoka.

Do tego dochodzi praca w komitetach programowych licznych (kilkunastu) konferencji, głównie w latach 2015-2018, co świadczy o rosnącej rozpoznawalności habilitanta na międzynarodowym forum wymiany doświadczeń i dyskusji naukowej.

O rozpoznawalności habilitanta w międzynarodowym środowisku badaczy zajmujących się podobną tematyką świadczą też cytowania prac jego autorstwa lub współautorstwa. W momencie składania ocenianego wniosku bilans cytowań według bazy *Web of Science* obejmował 58 cytowanych prac, łącznie 131 cytowań, w tym 86 nie będących autocytowaniami.

Uważam, że dane te świadczą o znacznej rozpoznawalności habilitanta w międzynarodowym środowisku naukowym oraz o tym, że już obecnie jest on traktowany jako wartościowy partner przy definiowaniu i realizacji ambitnych przedsięwzięć naukowych realizowanych przez międzynarodowe grupy badaczy.

2.5 Podsumowanie

Uważam, że habilitant zgromadził dorobek naukowy kwalifikujący go do nadania stopnia doktora habilitowanego.

3. Ocena dorobku organizacyjnego i dydaktycznego

Habilitant wniósł wkład organizacyjny w realizację kilku konferencji naukowych pełniąc funkcję recenzenta i przewodniczącego sesji naukowych. Aktywnie uczestniczył w organizacji i pracy licznych konsorcjów naukowych związanych z międzynarodowymi projektami badawczymi (*Magneto, Q-Rapids, Camino, CIPRNet, Cipher*) realizowanymi w ramach programów H2020, FP7 czy DG Home). W niektórych z nich pełnił również funkcje kierownicze (na poziomie instytucji partnerskiej lub na poziomie dekompozycji na pakiety robocze). Z racji tych funkcji pełnił również rolę redaktora dokumentów powstających w ramach tych projektów (tzw. *deliverables*).

Szeroki zakres uczestnictwa w konsorcjach badawczych tworzy naturalną bazę dla upowszechniania wyników naukowych osiąganych przez habilitanta oraz dla pozyskiwania partnerów do dalszych badań. Wśród tych organizacji partnerskich są zarówno uczelnie (na przykład *University of Cyprus*, *University of Britisch Columbia*, *Universitta Bio-Medico di Roma*). instytuty badawcze (na przykład *European Commission Joint Research Centre – JRC*, *ENEA* we Włoszech czy *TNO* w Holandii) czy organizacje biznesowe (na przykład *ACRIS* w Szwajcarii czy *Deltares* w Holandii).

Habilitant pełnił rolę współredaktora 25. edycji periodyku naukowego *The European CIIP Newsletter* oraz jest zaproszonym redaktorem numeru specjalnego czasopisma *Security and Communication Networks*. Jest również zapraszany do recenzowania artykułów w renomowanych czasopismach, w tym również tych z *Impact Factor* oraz do wykonywania ekspertyz, co również świadczy o jego rozpoznawalności w środowisku naukowym.

Habilitant udziela się również w dwóch organizacjach międzynarodowych, *Camino Cyber Think Tank* oraz *Integrated Mission Group Security (Thematic Ares 7)*. Na podkreślenie zasługuje fakt zgodności tematycznej tych organizacji z głównym nurtem zainteresowań badawczych habilitanta.

W ramach działalności dydaktycznej habilitant prowadzi wykłady (*Techniki internetowe*) oraz projekty i laboratoria w ramach programu dydaktycznego realizowanego na zatrudniającej go uczelni. Warto również podkreślić, że poza tymi zajęciami angażuje się w przygotowanie i realizację wykładów otwartych (w ramach programów *CIPRNet Master Class* oraz *CIPRNet Training Lectures*) dotyczących tematyki cyberbezpieczeństwa, a więc tej która jest obecnie jego główną specjalnością. Jego kompetencje zostały również dostrzeżone przez lokalny świat mediów, o czy świadczą zaproszenia do udzielania wywiadów związanych z uprawianą przez niego tematyką. Warto również zaznaczyć, że w wyniku realizowanych pod jego kierunkiem prac magisterskich powstają wspólne z dyplomantami publikacje, co potwierdza jego umiejętność pracy z młodymi, początkującymi badaczami.

3.1 Podsumowanie

Uważam, że habilitant zgromadził dorobek dydaktyczny i organizacyjny w pełni kwalifikujący go do nadania stopnia doktora habilitowanego.

4. Wniosek

Biorąc pod uwagę ocenę przedstawionego osiągnięcia naukowego oraz ocenę dorobku naukowego, dydaktycznego i organizacyjnego dra inż. Rafała Kozika stwierdzam, że przedstawiony we wniosku dorobek spełnia wymagania Ustawy i na tej podstawie rekomenduję nadanie dr inż. Rafałowi Kozikowi stopnia naukowego doktora habilitowanego oraz wnoszę o dopuszczenie go do dalszych etapów przewodu habilitacyjnego.

Gdańsk, 30.01.2019r.