Poznań, 11.09.2020

Dr hab. inż. Adam Wójtowicz, prof. UEP
Katedra Technologii Informacyjnych
Uniwersytet Ekonomiczny w Poznaniu
Al. Niepodległości 10, 61-875 Poznań
awojtow@kti.ue.poznan.pl

Recenzja w postępowaniu w sprawie nadania stopnia doktora habilitowanego – ocena osiągnięć naukowych dr. inż. Janusza Furtaka

Niniejsza recenzja została przygotowana w odpowiedzi na pismo dr. hab. inż. Zbigniewa Piotrowskiego, Zastępcy Przewodniczącego Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Wojskowej Akademii Technicznej z dnia 15.07.2020 informujące, że Rada Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja powołała mnie na recenzenta i członka komisji w postępowaniu w sprawie nadania stopnia doktora habilitowanego dr. inż. Januszowi Furtakowi.

Recenzja została przygotowana w oparciu o przesłaną dokumentację obejmującą: wniosek o przeprowadzenie postępowania, kopię dyplomu doktorskiego, autoreferat, wykaz osiągnięć naukowych, oświadczenia wnioskodawcy i współautorów cyklu publikacji tworzących osiągnięcie naukowe oraz kopie publikacji tworzących osiągnięcie naukowe.

Obecnie obowiązująca ustawa określa dwa główne warunki nadania stopnia doktora habilitowanego osobie posiadającej stopień doktora: posiadanie w dorobku osiągnięć naukowych stanowiących znaczny wkład w rozwój dyscypliny (1) oraz wykazanie się istotną aktywnością naukową (2). Zatem w recenzji ustosunkuję się najpierw do osiągnięcia naukowego dr. inż. Janusza Furtaka, a następnie przedstawię opinię na temat aktywności naukowej. W ostatniej sekcji sformułuję podsumowanie oceny.

1. Ocena osiągnięcia naukowego

1.1. Ocena publikacji wchodzących w skład osiągnięcia

Dr inż. Janusz Furtak w swoim wniosku o przeprowadzenie postępowania w sprawie nadania stopnia doktora habilitowanego jako osiągnięcie naukowe uzyskane po otrzymaniu stopnia doktora zgłosił cykl powiązanych tematycznie artykułów naukowych, zgodnie z art. 219 ust. 1 pkt. 2 ustawy oraz przepisami wprowadzającymi ustawę w okresie przejściowym. Osiągnięcie to nosi tytuł „Metody podnoszenia poziomu bezpieczeństwa bezprzewodowych sieci węzłów sensorowych" i obejmuje 11 artykułów wieloautorskich opublikowanych w latach 2014–2019, po uzyskaniu przez wnioskodawcę stopnia doktora. W ośmiu z jedenastu publikacji dr inż. Janusz Furtak jest pierwszym autorem, a w dziewięciu posiada kluczowy wkład w ich zawartość (w przedziale 60%–70%).

Artykuły wchodzące w skład osiągnięcia (oznaczone w dokumentacji wnioskodawcy symbolami C1-C11) zostały opublikowane jako:

- [C9] Artykuł w czasopiśmie *Concurrency and Computation: Practice and Experience* (wyd. Wiley) znajdującym się w aktualnym ministerialnym wykazie czasopism naukowych; w wykazie

czasopismo ma przypisaną dyscyplinę „informatyka techniczna i telekomunikacja" i 100 punktów; publikacja indeksowana w *Web of Science*, *Impact Factor* 1,17;

- [C10] Artykuł w czasopiśmie *Sensors* (wyd. MDPI) znajdującym się w aktualnym ministerialnym wykazie czasopism naukowych; w wykazie czasopismo ma przypisaną dyscyplinę „informatyka techniczna i telekomunikacja" i 100 punktów; publikacja indeksowana w *Web of Science*, *Impact Factor* 3,03;
- [C6] Artykuł opublikowany w materiałach konferencyjnych konferencji *Innovations for Community Services* znajdującej się w aktualnym ministerialnym wykazie konferencji naukowych z dyscypliny „informatyka techniczna i telekomunikacja" i mającej przypisane 20 punktów;
- [C2][C4][C7] 3 artykuły opublikowane w materiałach konferencyjnych *IEEE World Forum on Internet of Things* wydanych przez wydawnictwo IEEE; publikacje indeksowane w *Web of Science*;
- [C3] Artykuł opublikowany w materiałach konferencyjnych *Federated Conference on Computer Science and Information Systems* wydanych przez wydawnictwo IEEE; publikacja indeksowana w *Web of Science*;
- [C5] Artykuł opublikowany w materiałach konferencyjnych konferencji *Advances in Network Systems*, które się ukazały jako rozdział w książce serii *Advances in Intelligent Systems and Computing* wydanej przez wydawnictwo Springer; publikacja indeksowana w *Web of Science*;
- [C8][C11] 2 artykuły opublikowane w materiałach konferencyjnych *International Conference on Military Communications and Information Systems* wydanych przez wydawnictwo IEEE; w chwili obecnej wcześniejsza z publikacji jest zaindeksowana w *Web of Science*;
- [C1] Artykuł typu „position paper" opublikowany w materiałach konferencyjnych *Federated Conference on Computer Science and Information Systems* wydanych przez wydawnictwo PTI.

Jak wynika z przedstawionego wyżej zestawienia, publikacje wchodzące w skład zgłoszonego cyklu, z wyjątkiem publikacji [C1], posiadają dobrą międzynarodową i rozpoznawalną rangę lub – w przypadku publikacji [C9] i [C10] – bardzo dobrą międzynarodową i szeroko rozpoznawalną rangę. Oceniając charakter czasopism oraz konferencji, w których wnioskodawca publikował, poprawna jest kwalifikacja osiągnięcia naukowego wnioskodawcy do dyscypliny informatyka techniczna i telekomunikacja w dziedzinie nauk inżynieryjno-technicznych. Publikacje merytorycznie kluczowe dla osiągnięcia, tj. [C9], [C10] i [C6] (por. sekcja 1.2) znajdują się w aktualnym „wykazie czasopism naukowych i recenzowanych materiałów z konferencji międzynarodowych wraz z przypisaną liczbą punktów".

Reasumując, z punktu widzenia publikacyjnego pozytywnie oceniam osiągnięcie naukowe dr. inż. Janusza Furtaka jako cykl powiązanych tematycznie publikacji pt. „Metody podnoszenia poziomu bezpieczeństwa bezprzewodowych sieci sensorowych".

1.2. Ocena szczegółowa

Zakres tematyczny osiągnięcia obejmuje zagadnienia związane z zapewnieniem bezpieczeństwa w dziedzinie bezprzewodowych sieci sensorowych (ang. *Wireless Sensor Network*, *WSN*). Dziedzina ta jest częścią szerszego pola badań i zastosowań technologii nazywanego Internetem Rzeczy (ang. *Internet of Things*, *IoT*). Bezpieczeństwo Internetu Rzeczy jest obecnie jednym z największych wyzwań naukowych i technologicznych w dziedzinie cyberbezpieczeństwa, stanowiącym warunek rozwoju całej gałęzi nowych usług i rozwiązań, znajdujących zastosowania nie tylko w dziedzinie technologii militarnych.

W swoich badaniach wnioskodawca analizuje wiele różnych wymagań bezpieczeństwa stawianych przed systemami Internetu Rzeczy, które można klasyfikować do ogólnych atrybutów bezpieczeństwa,

takich jak: poufność, integralność, dostępność, autentyczność, niezaprzeczalność i rozliczalność. Wnioskodawca identyfikuje najważniejsze podatności sieci Internetu Rzeczy związane z ww. atrybutami bezpieczeństwa, a także analizuje istniejące już rozwiązania, nakreślając panoramę stanu wiedzy z zakresu zabezpieczeń mobilnych sieci sensorowych.

Wnioskodawca, biorąc pod uwagę specyficzne wymagania bezpieczeństwa dla bezprzewodowych sieci sensorowych, dynamiczny rozwój Internetu Rzeczy, szerokie spektrum zastosowań takich sieci, fakt istnienia bardzo istotnych podatności użytkowanych aktualnie sieci Internetu Rzeczy i brak kompleksowych rozwiązań bezpieczeństwa w tym zakresie stawia sobie ogólny cel badawczy: opracowanie kompleksowego rozwiązania zapewniającego wysoki stopnień bezpieczeństwa bezprzewodowych sieci sensorowych. Rozwiązania zaprezentowane w cyklu publikacji obejmują dwa modele domen (klastrów) węzłów sensorowych (oznaczanych jako Model I i Model II), definicję architektury węzła sensorowego oraz zestawy procedur. Dodatkowo wnioskodawca opisuje opracowany prototyp typu *proof of concept* nazywany w dokumentacji „demonstratorem sieci węzłów sensorowych", którego przeznaczeniem jest weryfikacja poprawności działania sieci WSN i zbadanie ich własności.

W badaniach wnioskodawcy bezprzewodowe sieci sensorowe składają się z węzłów sensorowych pełniących rolę pomiarową, wykonawczą lub bram sieciowych. Są one wyposażone w mikrokontroler/procesor i moduł komunikacyjny, a także w element wykonawczy mogący mieć funkcjonalność pomiarową lub aktuatora. Specyficzne ograniczenia sieci WSN wynikają z faktu, że mogą być one oparte na urządzeniach sprzętowych dysponujących ograniczonymi zasobami takimi jak przestrzeń pamięciowa, moc obliczeniowa, energia zasilania i zasięg lub przepustowość łącza bezprzewodowego. Ograniczenia te wpływają negatywnie na możliwości wykorzystania istniejących zaawansowanych rozwiązań bezpieczeństwa, takich jak infrastruktura jednostek certyfikujących. Dlatego wnioskodawca w swoich badaniach proponuje rozwiązania zapewniające wymagany poziom zaufania lokalnie w klastrach (domenach) węzłów sensorowych (opisał je w artykule [C6]), z wykorzystaniem sprzętowo-programowych modułów TPM (ang. *Trusted Platform Module*).

W zaproponowanym Modelu I (opisanym przez wnioskodawcę w artykułach [C1], [C2], [C3] i [C5]) założono, że ten sam węzeł sensorowy jest odbiorcą danych generowanych przez węzły domeny (pełni rolę bramy sieciowej) i równocześnie jest autorytetem bezpieczeństwa dla domeny. Wykorzystywana jest kryptografia asymetryczna w większości procedur wykonywanych w domenie, a w szczególności do uwierzytelniania węzłów i zabezpieczania danych przesyłanych między węzłami. Z kolei kryptografia symetryczna jest wykorzystywana do zabezpieczania wewnętrznych zasobów węzłów sensorowych – co wnioskodawca opisuje w publikacji [C5]. Wnioskodawca definiuje szczegółowo role poszczególnych węzłów w wymianie danych, w tym do celów zapewniania bezpieczeństwa, a także procedury rejestracji nowych węzłów w domenie i ich uwierzytelniania. Zdefiniowane są również procedury przejmowania nowych ról przez węzły w przypadkach awaryjnych. Ponadto wnioskodawca szczegółowo zdefiniował wymagania związane z poszczególnymi komponentami sprzętowymi węzła, a także zdefiniował poszczególne komponenty architektury pamięciowej przechowującej materiał kryptograficzny i inne dane wrażliwe.

W celu zapewnienia uwierzytelnienia węzłów w domenie, poprawnego zabezpieczenia kryptograficznego transmisji danych i zwiększenia odporności sieci na ataki typu *DoS* zaproponowano jedenaście procedur, które adresują wszystkie ważniejsze wymagania funkcjonalne oraz niefunkcjonalne (bezpieczeństwa) w analizowanej dziedzinie (inicjowanie domeny sensorów, rejestrowanie węzła, transfer danych sensorowych, usuwanie węzła z domeny, wzajemna weryfikacja uwierzytelnień, testy integracji domeny, odnawianie kluczy kryptograficznych oraz cztery procedury związane z transformacją ról węzłów

np. po awarii lub skutecznym ataku). Niestety, cztery ostatnie procedury nie zostały w pełni opublikowane w artykułach składających się na oceniane osiągnięcie.

Rozwiązania Modelu I zapewniają pewien poziom bezpieczeństwa informacji w zakresie sześciu głównych atrybutów bezpieczeństwa (poufność, integralność, autentyczność, aktualność, odporność sieci i uwierzytelnianie urządzeń). Bezpieczeństwo to nie jest jednak pełne. W szczególności istotna jest możliwość przeprowadzenia ataku typu *spoofing* (podszywanie się) skutkująca zarejestrowaniem fałszywego węzła w domenie czy możliwość przejęcia części kluczy w procedurze rejestracyjnej. Ryzyka te wynikają z niedostatecznego zabezpieczenia procedury inicjowania i rejestrowania węzłów w domenie, które to czynności odbywają się w niezaufanym środowisku i przez niezaufany kanał komunikacyjny. Inne ryzyka wynikają z obecności pojedynczego krytycznego punktu awarii w domenie (którym jest węzeł pełniący rolę autorytetu bezpieczeństwa), czy z braku ochrony parametrów łącza bezprzewodowego w zasobach węzła, co powoduje możliwość przechwycenia i modyfikacji parametrów łącza mogących skutkować udanymi atakami MitM lub DoS. Poza ograniczeniami bezpieczeństwa zaproponowany Model I ma również ograniczenia funkcjonalne, np. węzły będące autorytetami bezpieczeństwa nie są w stanie obsługiwać swoich elementów wykonawczych, a także ograniczenia związane z wydajnością i skalowalnością, wynikające z czasochłonnych procedur szyfrowania/deszyfrowania asymetrycznego.

Wnioskodawca, będąc świadomym ww. ograniczeń zaproponowanego modelu w nowszych i kluczowych publikacjach wchodzących w skład osiągnięcia ([C6], [C9] i [C10], a także [C4]), zaproponował Model II bezpiecznej domeny węzłów sensorowych. W tym modelu wszystkie dane przesyłane z węzłów sensorowych i dane przechowywane w zasobach węzłów są zabezpieczane kryptograficznie: bazą zabezpieczeń kryptograficznych są efektywne algorytmy symetryczne, a algorytmy asymetryczne są wykorzystywane tylko w trakcie procedury rejestracji węzłów w bezpiecznej domenie. Wszystkie procesy zabezpieczania kryptograficznego są wspomagane przez moduły TPM. Domena jest przygotowana do uruchamiania procedur diagnostycznych weryfikujących poprawność działania poszczególnych węzłów i całej domeny, co umożliwia budowanie samoorganizujących się sieci węzłów sensorowych uodpornionych na awarie, włamanie czy przejęcie. W zaproponowanym Modelu II każdy węzeł sensorowy domeny jest w stanie wykonywać podobne funkcje użytkowe: pozyskiwać i wstępnie przetwarzać dane pochodzące od elementów wykonawczych zainstalowanych w węźle sensorowym, uczestniczyć w bezpiecznej transmisji wewnątrz domeny i uwierzytelnianiu węzłów w domenie, uczestniczyć w odbieraniu danych pozyskanych z węzłów sensorowych domeny i bezpiecznym przesyłaniu tych danych do innych domen, a także uczestniczyć w diagnozowaniu domeny i rekonfigurowaniu węzłów domeny. Zostało to przedstawione w artykułach [C6], [C9] i [C10].

Wnioskodawca definiuje dwie domeny: domenę bezpieczeństwa i domenę przesyłania danych sensorowych. Domena bezpieczeństwa ma topologię gwiazdy, węzły wymieniają w niej dane wykorzystywane do uwierzytelniania węzłów, a autorytetem bezpieczeństwa jest pojedynczy węzeł. Jednak rolę tę są w stanie przejąć pozostałe węzły w przypadku awarii/skompromitowania węzła. W domenie bezpieczeństwa realizowane są również procedury diagnostyczne mające na celu weryfikację bezawaryjności węzła w aspekcie funkcjonalnym, a także w aspekcie bezpieczeństwa, jego dostępność komunikacyjną, a także, jeśli zachodzi taka potrzeba, zdolność do przejęcia nowej roli czy uruchamiania procedury elekcji węzła, który przejmie rolę pełnioną przez niedziałający/skompromitowany węzeł. W domenie przesyłania danych odbiorcą danych, które pochodzą od węzłów sensorowych, jest jeden z węzłów domeny pełniący rolę bramy sieciowej. Węzeł ten jest również odpowiedzialny za bezpieczny transfer danych pochodzących z domeny do adresatów spoza domeny.

Wnioskodawca przyjął założenie, że krytyczne z punktu widzenia bezpieczeństwa procedury przygotowania nowego węzła sensorowego są wykonywane w bezpiecznym i kontrolowanym środowisku

poza obszarem normalnej pracy węzła. Takie podejście pozwala na bezpieczną inicjalizację węzłów do pracy w domenie niezależnie od normalnego działania domeny. Inicjalizacja węzłów domeny wykonywana jest przez specjalny węzeł, nazywany w artykułach węzłem „B node". Jest on odpowiedzialny za generowanie asymetrycznych kluczy domeny, definiowanie parametrów domeny, generowanie identyfikatorów dla węzłów domeny oraz definiowane parametrów transmisji łącza sieciowego. Wnioskodawca zaproponował szczegółową architekturę węzła „B node", a także węzła sensorowego, w publikacjach [C6], [C9] i [C10]. Ponadto w Modelu II wnioskodawca zdefiniował siedemnaście procedur bezpieczeństwa, które zostały przypisane do trzech faz: przygotowawczej [C9], wdrożeniowej [C10] i normalnej pracy [C10]. Procedury takie są kluczowym elementem zagwarantowania bezpieczeństwa w całym cyklu życia każdego węzła i domeny. Podobnie jak w przypadku Modelu I pewnym mankamentem przedstawionego osiągnięcia jest fakt, że sześć z siedemnastu wymienionych procedur nie zostało opublikowanych. Z kolei na pozytywną uwagę zasługuje fakt, że opublikowane procedury zostały nie tylko opracowane i poddane teoretycznej ewaluacji, ale również zaimplementowane i przebadane za pomocą prototypu nazwanego „demonstratorem bezpiecznej domeny węzłów sensorowych".

Analiza bezpieczeństwa Modelu II opisana w artykule [C11] obejmuje podstawowe atrybuty bezpieczeństwa danych: poufność danych, integralność danych, dostępność danych, a także autentyczność danych. Dodatkowo przeanalizowano odporność na fizyczne ataki, co jest istotnym wymaganiem charakterystycznym dla dziedziny Internetu Rzeczy, oraz diagnozowalność systemu. Poufność danych jest zapewniona dzięki zastosowaniu odpowiednich algorytmów kryptograficznych – zarówno dla danych w transmisji, jak i w składowaniu, gdzie wykorzystywane są dodatkowo mechanizmy modułu TPM. Również integralność danych jest zapewniona zgodnie z przyjętymi standardami za pomocą danych kontrolnych, funkcji skrótu, numerów sekwencyjnych oraz mechanizmu noncji. Różne rodzaje kluczy kryptograficznych są wykorzystywane do szyfrowania danych w różnych domenach lub podczas realizacji specyficznych procedur. Z kolei pewnym ograniczeniem przedstawionego osiągnięcia jest brak szczegółowej analizy wpływu proponowanych mechanizmów bezpieczeństwa na atrybut dostępności danych/węzłów.

W zakresie zapewnienia autentyczności danych przez mechanizmy uwierzytelnienia poziom bezpieczeństwa jest wysoki dzięki wykorzystaniu tzw. drzew zaufania. Są one zabezpieczane dzięki mechanizmom modułu TPM w zasobach pierwszego węzła podczas procedury inicjowania domeny. Podejście to wydaje się właściwe z punktu widzenia bezpieczeństwa, w pewnym stopniu odpowiada sprawdzonym mechanizmom hierarchicznej infrastruktury klucza publicznego i certyfikatów znanych z ogólnych rozwiązań powszechnie wykorzystywanych w sieci Internet.

W zakresie odporności węzłów na atak fizyczny podwyższony stopień bezpieczeństwa został osiągnięty dzięki wykorzystaniu specjalnych rejestrów w modułach TPM. Za pomocą tych rejestrów węzeł sensorowy może zostać zdalnie lub automatycznie zablokowany. W przypadku nieautoryzowanej modyfikacji zasobów węzła dzięki tym rejestrom można również usuwać przechowywany materiał kryptograficzny. Istotną cechą zaprojektowanego systemu w Modelu II jest możliwość przeprowadzania zautomatyzowanych testów diagnostycznych w dziedzinie bezpieczeństwa. Węzły sensorowe przeprowadzają wzajemne testowanie, po zakończeniu którego można z pewnymi ograniczeniami identyfikować węzły niedziałające poprawnie.

Zatem ograniczenia Modelu I w zapewnieniu wysokiego poziomu bezpieczeństwa, takie jak łatwość zarejestrowania fałszywego węzła w domenie, pojedyncze krytyczne punkty awarii w domenie, możliwość przejścia części klucza, dostępność dla atakującego niezabezpieczonego interfejsu fizycznego, problemy z wydajnością kryptografii czy możliwość przechwycenia/modyfikacji parametrów łącza zostały w znacznym stopniu zaadresowane w zaproponowanym Modelu II, co wnioskodawca opisał w artykułach [C10] i [C11].

Niewątpliwie wartość zaproponowanych rozwiązań podnosi fakt, że na ich podstawie opracowano prototyp bezpiecznej domeny węzłów sensorowych, który został poddany ewaluacji oraz był prezentowany na konferencjach naukowych poświęconych technologiom informacyjnym i telekomunikacyjnym w zastosowaniach militarnych. Ponadto rozwiązania te znalazły swoje praktyczne zastosowania w dwóch scenariuszach wzbogacania świadomości sytuacyjnej przez pozyskiwanie informacji z urządzeń sieci IoT, które zostały opisane w artykułach [C7] i [C8]. Jednak trzeba zaznaczyć, że w tych dwóch pracach indywidualny wkład naukowy wnioskodawcy był znacznie mniejszy niż w pozostałych, a także ich obszar badań w większym stopniu odbiega od meritum osiągnięcia.

1.3. Podsumowanie oceny osiągnięcia naukowego

Podsumowując, stwierdzam, że przedstawione osiągnięcie naukowe w postaci cyklu powiązanych tematycznie artykułów naukowych stanowi znaczny wkład w ważny i dynamicznie rozwijający się obszar informatyki technicznej, jakim jest bezpieczeństwo Internetu Rzeczy. Charakter badań jest motywowany praktycznymi potrzebami w zakresie bezpieczeństwa bezprzewodowych sieci sensorowych. Indywidualny wkład wnioskodawcy w 9 z 11 publikacji (w tym w publikacje o najwyższej randze [C9] i [C10]) jest kluczowy – na poziomie 60%-70%. Warto odnotować, że wnioskodawca drogą analizy bezpieczeństwa identyfikuje luki poszczególnych rozwiązań i modeli – także własnych – i proponuje w konsekwencji udoskonalone modele a także prototypy. Wsparcie teoretycznych metod wnioskodawcy stworzonymi i przebadanymi prototypami dodatkowo podnosi ocenę zgłoszonego osiągnięcia. Mimo wskazanych niedociągnięć, z naukowego punktu widzenia uważam indywidualne osiągnięcie wnioskodawcy za znaczne i wystarczające do pozytywnego zakwalifikowania go jako osiągnięcia w postępowaniu habilitacyjnym.

2. Ocena aktywności naukowej

2.1. Publikacje naukowe i osiągniecia projektowe, technologiczne i konstrukcyjne

Wnioskodawca jest autorem lub współautorem 41 publikacji naukowych z dziedziny informatyki opublikowanych po uzyskaniu stopnia doktora oraz 12 publikacji naukowych z dziedziny informatyki opublikowanych przed uzyskaniem stopnia doktora. Na jego łączny dorobek 53 publikacji naukowych składa się 1 samodzielna monografia, 24 artykułów w czasopismach naukowych, 13 rozdziałów w monografiach i 15 artykułów konferencyjnych (z czego 9 indeksowanych w bazie WoS). Ponadto wnioskodawca jest współautorem skryptu i redaktorem jednej monografii naukowej.

Sumaryczna liczba punktów za publikacje po uzyskaniu stopnia doktora wg listy czasopism wynosi 563, wg zasad ewaluacji wynosi 326,75, a z uwzględnieniem udziałów współautorskich 284,65. Publikacje wnioskodawcy były cytowane 23 razy w bazie Web of Science, 89 razy w bazie Scopus i 142 razy w bazie Google Scholar. Łączny współczynnik wpływu (Impact Factor) wynosi 4,2.

Ponadto na uwagę zasługuje fakt, że wnioskodawca jest autorem 4 osiągnięć konstrukcyjnych związanych tematycznie z przedstawionym osiągnięciem naukowym. Wnioskodawca jest autorem osiągnięcia konstrukcyjnego „Demonstrator bezpiecznej domeny sensorów" (2018), był kierownikiem zespołu, który zrealizował osiągnięcie „Opracowanie rekomendacji wykorzystania metodyk do oceny podatności i narzędzi do oceny podatności systemów teleinformatycznych" (2016), jest współautorem osiągnięcia technologicznego „Bezpieczna stacja do zastosowań specjalnych" (2012) wykonanego w ramach współpracy w konsorcjum Wojskowej Akademii Technicznej (lider) z trzema innymi instytucjami

oraz jest jednym z trzech współautorów osiągnięcia projektowego „Metodyka oceny mechanizmów integracji sieci IPv4 i IPv6" (2010).

2.2. Aktywność w instytucjach naukowych, projektach i zespołach badawczych

Dr inż. Janusz Furtak uzyskał tytuł magistra inżyniera na kierunku informatyka w Wojskowej Akademii Technicznej w roku 1982, a stopień doktora nauk technicznych w dyscyplinie informatyka w roku 1999 (specjalność: inżyniera systemów). W latach 1990-2000 był zatrudniony w Wojskowej Akademii Technicznej na Wydziale Cybernetyki na stanowisku asystenta, a od roku 2000 – jest zatrudniony na stanowisku adiunkta. W latach 2006-2016 pełnił funkcję zastępcy dyrektora Instytutu Teleinformatyki i Automatyki, a w latach 2016-2019 – dyrektora Instytutu Teleinformatyki i Automatyki. Od roku 2019 pełni funkcję dyrektora Instytutu Teleinformatyki i Cyberbezpieczeństwa.

W ramach aktywności w zagranicznych instytucjach naukowych od 2016 roku wnioskodawca aktywnie uczestniczy w pracach *NATO Science and Technology Organisation* w panelach *Information Systems Technology*, w grupach roboczych *Military Appliaction of the Internet of Things* oraz *Federated Interoperability of Military C2 and IoT Systems*, pełniąc funkcję przedstawiciela RP. Prace w tym zakresie owocują wynikami publikowanymi w międzynarodowych czasopismach naukowych i prezentowanymi na międzynarodowych konferencjach, których współautorem był wnioskodawca w ośmiu przypadkach. Jako członek grupy roboczej został uhonorowany wyróżnieniem *IST Panel – Team Excellence Award*. Na uwagę zasługuje tutaj międzynarodowy charakter pracy w grupach roboczych, gdzie aktywnie uczestniczą przedstawiciele dziesięciu państw NATO. Ponadto wnioskodawca odbył sześciotygodniowy staż naukowy na wyższej uczelni na Słowacji.

Wnioskodawca kierował zespołem na poziomie instytucji w konsorcjum projektowym w dwóch projektach finansowanych przez Narodowe Centrum Badań i Rozwoju, a w jednym tego typu projekcie pełnił funkcję wykonawcy. Wnioskodawca kierował pięcioma projektami badawczymi realizowanymi na zlecenie Wojskowej Akademii Technicznej oraz jednym projektem badawczym realizowanym na zlecenie Komitetu Badan Naukowych. Wnioskodawca pełnił rolę wykonawcy w jednym projekcie badawczym, którego zleceniodawcą było Ministerstwo Obrony Narodowej. Ponadto wnioskodawca w ramach współpracy z sektorem gospodarczym realizował dziewięć projektów z sześcioma różnymi podmiotami w dziedzinie bezpieczeństwa systemów IT.

Wnioskodawca był współautorem 22 prezentacji konferencyjnych, z czego 16 razy osobiście prezentował artykuł. Konferencje, na których artykuły wnioskodawcy były prezentowane, zaliczają się do uznanych i rozpoznawalnych konferencji międzynarodowych, takich jak *IEEE World Forum on Internet of Things*, *International Conference on Military Communication and Information Systems*, czy *Federated Conference on Computer Science and Information Systems*. Wnioskodawca brał 7 razy udział w konferencjach międzynarodowych w roli *chairman* i 21 razy w roli członka komitetu programowego. Wnioskodawca zrecenzował 16 prac naukowych będących artykułami w czasopismach lub rozdziałami w monografiach. Wnioskodawca zrecenzował 61 artykułów konferencyjnych na rzecz 6 międzynarodowych cyklicznych konferencji naukowych. Wnioskodawca dwukrotnie pełnił rolę recenzenta wniosków projektowych na rzecz NCBiR oraz dwukrotnie opracował opinię ekspercką dla MON.

2.3. Aktywność dydaktyczna i popularyzatorska

W zakresie osiągnięć dydaktycznych trzeba podkreślić, że wnioskodawca jest od prawie trzydziestu lat nauczycielem akademickim i bierze czynny udział w procesie dydaktycznym na Wydziale Cybernetyki

Wojskowej Akademii Technicznej. Wnioskodawca opracowywał programy nauczania i prowadził zajęcia dydaktyczne (wykłady i ćwiczenia laboratoryjne na studiach I i II stopnia oraz studiach podyplomowych) z kilkunastu przedmiotów z zakresu informatyki, w zdecydowanej większości o charakterze technicznym i związanym z bezpieczeństwem informatycznym. Wnioskodawca kierował również pracami dyplomowymi – magisterskimi, inżynierskimi i podyplomowymi w sumarycznej liczbie 95 oraz był recenzentem wielu prac magisterskich i inżynierskich. Działalność dydaktyczną w zakresie informatyki wnioskodawca prowadził również w latach 1999–2004 w Prywatnej Wyższej Szkole Businessu i Administracji, gdzie prowadził zajęcia z 11 informatycznych przedmiotów i kierował 40 pracami dyplomowymi.

Działalność popularyzatorska wnioskodawcy była skoncentrowana na zagadnieniach związanych z sieciami komputerowymi. Wnioskodawca był członkiem zespołu powołującego do życia Akademię Cisco w Instytucie Teleinformatyki i Automatyki Wydziału Cybernetyki WAT, a także jest organizatorem i instruktorem kursów CCNA, gdzie przeprowadził około 80 kursów.

2.4. Podsumowanie aktywności naukowej

Aktywność naukową wnioskodawcy oceniam jako istotną. Zgodnie z wymogami ustawy jest ona realizowana w więcej niż jednej instytucji naukowej, w tym zagranicznej. Dorobek publikacyjny jest bogaty, po uzyskaniu stopnia doktora jest spójny tematycznie i ma charakter międzynarodowy. Współpraca naukowa wnioskodawcy realizowana była w ramach międzynarodowych grup roboczych a także w ramach krajowych konsorcjów instytucji realizujących wspólne projekty naukowo-badawcze. Niemal każdy tych projektów związany był tematycznie z obszarem badawczym będącym przedmiotem przedstawionego do recenzji osiągnięcia naukowego. Podobnie warta podkreślenia jest aktywność wnioskodawcy w organizowaniu oraz wsparciu naukowym międzynarodowych konferencji naukowych. Również wysoko należy ocenić dorobek wnioskodawcy w zakresie doświadczenia dydaktycznego.

3. Podsumowanie

Biorąc pod uwagę pozytywną ocenę osiągnięcia naukowego pt. „Metody podnoszenia poziomu bezpieczeństwa bezprzewodowych sieci sensorowych" oraz pozytywną ocenę aktywności naukowej, stwierdzam, że dr inż. Janusz Furtak spełnia wymagania określone w ustawie „Prawo o szkolnictwie wyższym i nauce" oraz w przepisach wprowadzających ustawę w okresie przejściowym. Dlatego popieram wniosek dr. inż. Janusza Furtaka o nadanie mu stopnia doktora habilitowanego w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja.

Adam Wojtowicz