Warszawa, 5 października 2020 r.

Prof. dr hab. inż. Ewa Niewiadomska-Szynkiewicz
Instytut Automatyki i Informatyki Stosowanej
Wydział Elektroniki i Technik Informacyjnych
Politechnika Warszawska

Recenzja
osiągnięcia naukowego oraz istotnej aktywności naukowej
Pana dr inż. Janusza Furtaka
w związku z postępowaniem o nadanie stopnia doktora habilitowanego
w dziedzinie nauk inżynieryjno-technicznych, w dyscyplinie Informatyka Techniczna i Telekomunikacja

1. Informacje ogólne

Recenzja została opracowana na zlecenie Zastępcy Przewodniczącego Rady Dyscypliny Naukowej *Informatyka Techniczna i Telekomunikacja* Wojskowej Akademii Technicznej dr hab. inż. Zbigniewa Piotrowskiego, profesora WAT. Recenzję opracowano zgodnie z wytycznymi ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz.U.2020.85 t.j.).

Przedmiotem recenzji jest ocena osiągnięcia naukowego oraz dorobku naukowego, dydaktycznego i organizacyjnego doktora inżyniera Janusza Furtaka, uzyskanego po nadaniu mu stopnia doktora nauk technicznych. Recenzja została opracowana w związku z toczącym się postępowaniem o nadanie Panu dr Januszowi Furtakowi stopnia doktora habilitowanego w dziedzinie nauk inżynieryjno-technicznych, w dyscyplinie Informatyka Techniczna i Telekomunikacja prowadzonym przez Radę Dyscypliny Naukowej *Informatyka Techniczna i Telekomunikacja* Wojskowej Akademii Technicznej.

2. Sylwetka Habilitanta

Dr inż. Janusz Furtak ukończył studia wyższe w 1982 roku na Wydziale Cybernetyki Wojskowej Akademii Technicznej. W 2000 roku uzyskał stopień doktora nauk technicznych w dyscyplinie Informatyka, broniąc na tym samym wydziale rozprawę doktorską pt. „Orientacja przestrzenna na podstawie obrazu z ruchomej kamery".

Od roku 1994 do chwili obecnej dr inż. Janusz Furtak jest zatrudniony na Wydziale Cybernetyki Wojskowej Akademii Technicznej, początkowo na stanowisku asystenta, a od 2000 roku na stanowisku adiunkta. Do chwili obecnej pełnił funkcje: kierownika zakładu (2003 –2006), zastępcy dyrektora Instytutu Teleinformatyki i Automatyki (2006 – 2016), dyrektora tego instytutu (2016 – 2019), a od 2019 roku jest dyrektorem Instytutu Teleinformatyki i Cyberbezpieczeństwa.

W latach 1999 - 2005 Habilitant pracował również w Prywatnej Wyższej Szkole Biznesu i Administracji, kolejno na stanowiskach: asystent, adiunkt, docent. Dr Janusz Furtak ukończył kursy w zakresie systemów do symulacji sieci teleinformatycznych *System Riverbed Modeler*. Uzyskał również certyfikat CCNA (Cisco) i uprawnienia instruktorskie w zakresie kursów CCNA, CCNA *Security* i *Security in IoT*.

3. Ocena osiągniecia naukowego

Osiągnięcie naukowe dr inż. Janusza Furtaka stanowiące podstawę do ubiegania się o stopień doktora habilitowanego w dziedzinie nauk inżynieryjno-technicznych, w dyscyplinie Informatyka Techniczna i Telekomunikacja składa się z dwóch części:

- teoretycznej, stanowiącej jednotematyczny cykl publikacji zatytułowany „Metody podnoszenia poziomu bezpieczeństwa w bezprzewodowych sieciach węzłów sensorowych'',
- praktycznej, stanowiącej demonstrator bezpiecznej domeny sensorów, który służy badaniom rozwiązań z zakresu bezpieczeństwa sieci sensorowych, w tym opracowanych przez Habilitanta.

Na cykl publikacyjny składa się 11 prac opublikowanych w latach 2014 – 2019. W skład tego cyklu wchodzą:

- 2 publikacje w czasopismach: *Sensors* oraz *Concurrency and Computation: Practice and Experience* (indeksowane w bazie JCR)
- 2 rozdziały w monografiach wydanych przez *Springer International Publishing*.
- 5 prac opublikowanych w materiałach międzynarodowych konferencji takich jak: *IEEE World Forum on Internet of Things*, *Federated Conference on Computer Science and Information Systems*, *International Conference on Military Communications and Information System*, (indeksowane w bazie Web of Science).
- 2 prace opublikowane w materiałach międzynarodowych konferencji, które nie są indeksowane w bazie Web of Science.

Należy podkreślić, że pozycje zamieszczone w cyklu prezentują wyniki badań z ostatnich 5 lat. Większość publikacji to prace dwóch lub trzech autorów, przy czym w 8 z nich Habilitant jest pierwszym autorem, w jednej drugim. Wartości jego udziału są w zakresie 60% do 70%. Dwie zamieszczone prace zostały przygotowane przez większe zespoły i udział Habilitanta wynosi odpowiednio 6 i 8%. W przedłożonym cyklu znajdują się dwie pozycje opublikowane w czasopismach indeksowanych w bazie JCR o sumarycznym wskaźniku IF 4,20. Do 9 publikacji zostały załączone deklaracje współautorów o procentowym udziale w powstaniu wymienionych prac oraz o zakresie prac wykonanych przez poszczególnych autorów. W przypadku 2 wieloautorskich prac zostały dołączone deklaracje współautorów, którzy potwierdzili zakres prac wykonanych przez Habilitanta. Każda z prac zawartych w cyklu została omówiona w autoreferacie, ze zwróceniem szczególnej uwagi na autorski wkład Habilitanta.

Web of Science Core Collection [odczyt z 5 października 2020 r.] wykazuje 15 publikacji dr J. Furtaka w latach 2015-2020, co wskazuje na znaczne zwiększenie aktywności publikacyjnej Kandydata w ostatnich 5 latach. Z drugiej strony, fakt iż najważniejsze publikacje, w tym zawarte w cyklu, ukazały się stosunkowo niedawno, co jest prawdopodobnie powodem, że nie zdążyły one zebrać wysokiej liczby cytowań.

Sumaryczna punktacja publikacji stanowiących osiągnięcie naukowe wynosi 325, a sumaryczny Impact Factor 4.2. Ranga bibliograficzna podstawowego cyklu publikacji nie jest zatem wysoka i raczej wskazuje na minimalne spełnienie wymagań stawianych wnioskom habilitacyjnym. Warto jednak nadmienić, że w roku 2020, już po wszczęciu postępowania, ukazały się dwie nowe prace Habilitanta w czasopismach indeksowanych

w bazie JCR, o sumarycznej wartości 200 pkt. i sumarycznym wskaźniku IF 4,20. Jedna z nich jest samodzielną pracą Habilitanta.

Wskazany cykl publikacji jest skoncentrowany na tematyce bezpieczeństwa bezprzewodowych sieci sensorowych. Jest to spójny materiał. Biorąc pod uwagę zakres tematyczny czasopism i konferencji, w których były publikowane prace wchodzące w skład osiągnięcia naukowego dr inż. J. Furtaka, to jego kwalifikacja w dyscyplinie Informatyka Techniczna i Telekomunikacja jest właściwa. Pewnym mankamentem jest powielanie się części rozważań naukowych oraz prezentacji wyników badań w przedstawionych publikacjach, np. prace [C2], [C3] i [C5], czy [C6] i [C9].

Szczegółowa analiza osiągniecia naukowego

Dr inż. Janusz Furtak od czasu uzyskania stopnia doktora koncentruje swoje zainteresowania naukowe na zagadnieniach cyberbezpieczeństwa sieci teleinformatycznych. Cykl publikacji wskazany jako główne osiągnięcie naukowe dotyczy problematyki zapewnienia bezpieczeństwa w bezprzewodowych sieciach sensorowych, konkretnie odpowiedniego zabezpieczania urządzeń stanowiących węzły tego typu sieci. Poruszana tematyka, w dobie upowszechniania się rozwiązań IoT, stanowi ważny, ciekawy i perspektywiczny kierunek rozwoju w zakresie nowoczesnych systemów sieciowych.

Habilitant, prowadząc analizę literaturową, zwrócił uwagę na brak ujęcia problematyki zapewnienia bezpieczeństwa węzłów sieci sensorowych w sposób kompleksowy, uwzględniający różne podatności oraz potencjalne zagrożenia. Stąd, główny wysiłek skoncentrował na opracowaniu rozwiązania, które pozwala na zapewnienie wysokiego poziomu bezpieczeństwa statycznych i mobilnych sieci sensorowych i może znaleźć zastosowanie w innych systemach Internetu rzeczy. Zaproponowane podejście zakłada zastosowanie technik i mechanizmów dość powszechnie używanych w systemach IoT. Jego innowacyjność polega na odpowiedniej ich integracji w celu opracowania rozwiązania, które spełnia wszystkie wymagania bezpieczeństwa: uwierzytelnienie, dostępność, poufność, integralność, niezaprzeczalność, rozliczalność oraz ochronę zasobów przed nieautoryzowaną aktywnością. Pozwala na minimalizację ryzyka wykorzystania najważniejszych podatności tego typu systemów. Ponadto jest rozwiązaniem o stosunkowo niewielkich kosztach realizacji.

Podsumowując, do najważniejszych osiągnięć Habilitanta zawartych w cyklu publikacji stanowiących istotny wkład w rozwój dyscypliny naukowej Informatyka Techniczna i Telekomunikacja zaliczam:

1. Propozycję dekompozycji sieci na bezpieczne klastry oraz zaproponowanie struktury i ustalenie ról urządzeń tworzących klastry, nazywane w cyklu publikacji „domenami węzłów sensorowych".
2. Propozycję architektury bezpiecznego węzła sensorowego oraz opracowanie procedur bezpiecznego przesyłania i odbierania danych.
3. Zbudowanie demonstratora do testów zaproponowanego rozwiązania oraz opracowanie scenariuszy testów i analizę ich wyników.

Ad. 1.

W przedstawionych publikacjach [C4], [C6] Habilitant stwierdza, że rozwiązania, których celem jest zapewnienie bezpieczeństwa sieci sensorowych, zarówno ze względu na ograniczone zasoby obliczeniowe i energetyczne urządzeń oraz medium komunikacyjne,

powinny być konstruowane lokalnie, w obrębie niewielkich klastrów sieci (domen). Stąd propozycja dekompozycji sieci na grupy złożone z współpracujących urządzeń. Zdaniem recenzenta proponowane podejście jest zasadne. Niemniej, z przedstawionego cyklu publikacji nie wynikają jasno kryteria przydziału węzłów do klastrów. Zapewne jest to zasięg komunikacji radiowej. Brakuje w zamieszczonych pracach opisu procesu klasteryzacji, odniesienia się do licznych algorytmów uwzględniających nie tylko zasięgi radiowe, ale też aktualne zasoby energetyczne i obliczeniowe węzłów. Natomiast dość dokładnie są opisane role poszczególnych węzłów w domenie oraz procedura zmiany ról w przypadkach infekcji, awarii lub wyłączenia węzła [C1]. Wskazane byłoby dodatkowo opracowanie procedury dynamicznego reagowania na zmieniające się warunki w sieci związane z zużywaniem wspomnianych wcześniej mocy i zasobów urządzeń oraz oddziaływaniem środowiska.

W pracach [C1] – [C11] Habilitant szczegółowo omawia zaproponowane przez siebie modele domen węzłów sensorowych. Wskazuje na dwie kluczowe role wybranych węzłów – węzeł *Master*, który pełni rolę nadzorcy w domenie – autoryzuje węzły oraz węzeł *Gateway* odpowiedzialny za wymianę danych między domenami. Jako pierwszy proponowany jest prosty model domeny Model I, w którym przyjmuje się, że ten sam węzeł realizuje zadania przypisane *Master* i *Gateway*. Modyfikacją Modelu I jest Model II, w którym role te są rozdzielone między różne węzły, co pozwala na zwiększenie odporności sieci i podniesienie poziomu bezpieczeństwa. Należy podkreślić, że zaproponowane podejścia są dokładnie omówione w publikacjach. Przedstawione są również zadania realizowane przez wspomniane węzły i procedury bezpieczeństwa oraz oceny zdolności węzłów do realizacji kluczowych ról i wymiany węzłów *Master* i *Gateway*. Procedury bezpieczeństwa obejmują: bezpieczne inicjowanie domeny i rejestrację węzła w domenie, weryfikację uwierzytelnień, aktualizację danych oraz bezpieczny transfer danych. Habilitant prezentuje skuteczność i wydajność rozwiązania na przykładzie testowych domen – klastrów o rozmiarach 11 węzłów [C5] i 4 węzły [C6]. Pewnym mankamentem rozwiązania są narzuty czasowe związane z tworzeniem bezpiecznej domeny, szczególnie w przypadku większych sieci o liczniejszych klastrach. Około 20-65 sekund zajmuje rejestracja węzła w domenie. W trybie operacyjnego działania narzuty nie zależą tak silnie od wymiaru sieci. W pracy [C10] przedstawione są dość dokładne oszacowania zależności liczby przesyłanych podczas konstrukcji domeny ramek w zależności od wielkości domeny (liczby sensorów) wskazujące na liniową zależność. Niemniej, zastosowanie szyfrowania przesyłanych danych wpływa na czas transmisji (średni narzut – 60%, tabele 1 i 2 [C5]), natomiast wbudowany algorytm AES w niewielkim stopniu zwiększa zużycie zasobów energetycznych. W prezentowanym cyklu publikacji brakuje dokładniejszych analiz (np. symulacyjnych) pokazujących wpływ rozmiaru i złożoności sieci na skuteczność i wydajność rozwiązania, jego odporność na zakłócenia transmisji (np. zjawiska odbić, interferencji itd.) oraz przykładu współpracy wielu domen, przy założeniu znacznego rozmiaru, rozproszenia węzłów i rozległości sieci.

Oczywistą zaletą przedstawionych badań jest prezentacja działania zaproponowanych metod zwiększenia poziomu bezpieczeństwa na fizycznych urządzeniach. Przykłady zastosowań bezprzewodowej sieci sensorów z uwierzytelnianiem do budowania świadomości sytuacyjnej przez pozyskiwanie danych z systemów IoT są opisane w pracach [C7] i [C9]. Rozwiązanie Habilitanta zostało sprawdzone w dwóch demonstratorach technologii zbudowanych w ramach uczestnictwa w pracach grupy NATO. Rozważano dwa scenariusze: 1) odzyskiwanie ciągłości działania po dużych katastrofach [C7], 2) wzbogacanie świadomości sytuacyjnej dowódcy wielonarodowych sił zbrojnych po katastrofie w środowisku miejskim [C8].

Ad 2.

W pracach [C1], [C2] i [C3] prezentowana jest architektura węzła sieci sensorowej typowa dla Modelu I domeny, a w pracach [C4] i [C6] dla Modelu II. W obu przypadkach kluczowym komponentem jest moduł TPM (*Trusted Platform Module*) wykorzystany do budowy lokalnej struktury zaufania w klastrze. Habilitant proponuje proste konstrukcje węzłów oparte o układy mikrokontrolerów, moduły radiowe i odpowiednie adaptery. Głównym wyzwaniem przy oprogramowaniu węzła było opracowanie i realizacja biblioteki funkcji organizujących współpracę mikrokontrolera Arduino z modułem TPM. Trudność zadania wynikała z bardzo małych zasobów pamięci mikrokontrolera (8 KB).

Ad 3.

Na potrzeby prezentacji opracowanych metod podnoszenia bezpieczeństwa sieci sensorowych Habilitant zbudował w laboratorium demonstrator bezpiecznej domeny [C5]. Pozwala on na prowadzenie badań różnych rozwiązań wspierających bezpieczeństwo IoT. Składa się z trzech komponentów umożliwiających: przygotowanie urządzenia – węzła sieci sensorowej, zbudowanie domeny (klastra) z uwierzytelnianiem, prowadzenie badań – uruchomienie węzłów, zbieranie pomiarów i przesyłanie danych. Wykorzystanie demonstratora prezentują prace [C7] i [C8].

Przechodząc do podsumowania osiągnięcia naukowego dr inż. Janusza Furtaka stwierdzam, że osiągnięcie zatytułowane „Metody podnoszenia poziomu bezpieczeństwa bezprzewodowych sieci sensorowych" jest tematycznie spójne. Stwierdzam również, że spełnia ono wymagania stawiane osiągnięciom naukowym stanowiącym podstawę do uzyskania stopnia naukowego doktora habilitowanego.

Do pozytywów przedstawionego osiągnięcia zaliczam opracowanie spójnej koncepcji rozwiązania, jego realizację w środowisku zbudowanym z fizycznych urządzeń, rzetelną weryfikację eksperymentalną oraz opublikowanie badań w dwóch rozpoznawalnych czasopismach dziedzinowych o zasięgu globalnym oraz materiałach konferencji międzynarodowych.

Do mankamentów zaliczam brak opracowania szerszego ujęcia problematyki bezpieczeństwa sieci sensorowych, co sugeruje tytuł osiągnięcia. Habilitant mówi o kompleksowym rozwiązaniu, niemniej w proponowanym podejściu brakuje uwzględnienia kilku ważnych aspektów, takich jak: weryfikacja poprawności przesyłanych danych, ochrona przed atakami wolumetrycznymi, reputacja węzłów, możliwość utraty spójności sieci. Mankamentem jest również niewielka liczba publikacji w renomowanych czasopismach (poprawiają ten wyniki dwie ostatnie publikacje z 2020 roku) oraz stosunkowo niskie wskaźniki bibliometryczne (IH=3 w WoS, IH=4 w Scopus).

4. Ocena pozostałego dorobku naukowego

Do dokumentacji przewodu, Habilitant dołączył także opis osiągnięć konstrukcyjnych i technologicznych obejmujących prace z zakresu cyberbezpieczeństwa oraz protokołów komunikacyjnych. Pierwsze są związane z budową specjalizowanego systemu zabezpieczającego stanowiska komputerowe do zastosowań specjalnych (m.in. wojskowych). Opis sytemu był prezentowany na konferencji *International Conference on Secure and Trust Computing , Data Management and Application.*

Badania nad protokołami komunikacyjnymi koncentrowały się na opracowaniu spójnej metodyki oceny mechanizmów integracji sieci IPv4 i IPv6. Metodyka został przedstawiona

przez Habilitanta i współpracowników w artykule do Biuletynu Automatyki i Robotyki pt. „Metodyka oceny mechanizmów integracji sieci IPv4 i IPv6".

5. Ocena aktywności naukowej i współpracy z otoczeniem społecznym i gospodarczym

Na podstawie przedłożonej dokumentacji stwierdzam, że dr inż. Janusz Furtak jest aktywnym uczestnikiem społeczności naukowej. Habilitant prezentuje wyniki swoich badań na krajowych i międzynarodowych konferencjach. Wykonał recenzje 77 prac naukowych w czasopismach (w tym z IF), monografiach oraz materiałach konferencji i 2 recenzje projektów badawczych finansowanych przez NCBiR i MON.

Istotnym obszarem aktywności naukowej Kandydata jest udział w krajowych i międzynarodowych zespołach realizujących programy i projekty naukowe i badawczo-rozwojowe. W sumie uczestniczył w 10 projektach:

- trzech projektach finansowanych przez NCBiR w drodze konkursów krajowych,
- jednym projekcie finansowanym przez KBN,
- jednym projekcie finansowanym przez MON,
- pięciu projektach finansowanych przez WAT.

Habilitant jest aktywny w naukowym środowisku międzynarodowym. Od 2016 roku prowadzi badania naukowe w ramach programów NATO Science and Technology Organization:

- *Federated Interoperability of Military C2 and IoT Systems* (grupa robocza: IST-176/RTG).
- *Military Applications of Internet of Things* (grupa robocza IST-147/RTG.

Podobnie jak w przypadku działalności publikacyjnej warto podkreślić znaczne zwiększenie aktywności dr inż. J. Furtaka w pracach zespołów badawczych w ostatnich 5 latach.

Habilitant realizując projekty NCBiR współpracował z firmami reprezentującymi sektor ICT. Wykonał również kilka ekspertyz dla MON i NCBiR.

6. Ocena działalności organizacyjnej i aktywności na rzecz społeczności naukowej

Habilitant aktywnie uczestniczy w pracach organizacyjnych dla środowiska naukowego oraz macierzystej uczelni. Pełnił i pełni funkcje kierownicze na Wydziale Cybernetyki WAT: kierownik zakładu (2003 –2006), zastępca dyrektora Instytutu Teleinformatyki i Automatyki (2006 – 2016), dyrektor tego instytutu (2016 – 2019), a od 2019 roku dyrektor Instytutu Teleinformatyki i Cyberbezpieczeństwa.

Był kierownikiem zespołów badawczych z WAT w dwóch projektach NCBiR, kierownikiem projektu finansowanego przez KBN oraz kierownikiem pięciu projektów WAT. Od 2016 roku jest z nominacji MON przedstawicielem Polski w wymienionych powyżej programach NATO Science and Technology Organization (grupy robocze: IST-146/RTG i IST-147/RTG).

Na szczególną uwagę zasługuje również zaangażowanie Habilitanta w organizację krajowych i międzynarodowych konferencji obejmujących tematykę z zakresu dyscypliny Informatyka Techniczna i Telekomunikacja. Był członkiem Komitetów Programowych

i Organizacyjnych 28 konferencji. Od 2013 roku regularnie organizuje sesje poświęcone IoT oraz systemom i aplikacjom sieciowym w ramach międzynarodowej konferencji *Federated Conference on Computer Science and Information Systems* (FedCSIS). Materiały konferencji są indeksowane m.in. w bazie WoS.

Podsumowując, uważam, że aktywność Habilitanta w zakresie działań organizacyjnych w macierzystej jednostce oraz na rzecz krajowej i międzynarodowej społeczności naukowej jest na wysokim poziomie.

7. Ocena dorobku dydaktycznego

Habilitant od wielu lat bierze czynny udział w procesie dydaktycznym w macierzystej uczelni, na studiach I i II stopnia oraz studiach podyplomowych. Przygotował i prowadził wykłady i ćwiczenia laboratoryjne z 12 przedmiotów, z zakresu sieci komputerowych, systemów operacyjnych, systemów IoT i cyberbezpieczeństwa. Prowadzi również zajęcia dydaktyczne na kursach przygotowawczych MON. Dodatkowo wykładał w Prywatnej Wyższej Szkole Biznesu i Administracji. W sumie, w obu uczelniach, wypromował około 140 inżynierów i magistrów inżynierów.

Aktywnie uczestniczył i uczestniczy w opracowywaniu programu studiów I i II stopnia na Wydziale Cybernetyki WAT jako członek komisji ds. trzech kierunków studiów z zakresu informatyki i telekomunikacji.

Habilitant był również członkiem zespołu, który powołał Akademię Cisco na Wydziale Cybernetyki WAT, jest organizatorem i instruktorem kursów. Opracował niezbędne materiały dydaktyczne.

Podsumowując, uważam, że aktywność Habilitanta w zakresie dydaktyki jest na ponadprzeciętnym poziomie.

8. Ocena końcowa wniosku habilitacyjnego

Podsumowując przedstawione powyżej oceny dorobku naukowego, organizacyjnego i dydaktycznego stwierdzam, że dorobek dr inż. Janusza Furtaka spełnia wymagania Ustawy o Stopniach i Tytule Naukowym stawiane w przewodzie o nadanie stopnia naukowego doktora habilitowanego i wnosi znaczny wkład w rozwój dyscypliny naukowej Informatyka Techniczna i Telekomunikacja. W związku z tym, wnioskuję o nadanie stopnia doktora habilitowanego.