Prof. dr hab. inż. Franciszek Seredyński
Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
Instytut Informatyki
Wydział Matematyczno – Przyrodniczy. SNŚ
ul. Wóycickiego 1/3, 01-938 Warszawa
f.seredynski@uksw.edu.pl

Warszawa, 17.09.2020

Recenzja
osiągnięcia naukowego dr inż. Janusza Furtaka nt.

Metody podnoszenia poziomu bezpieczeństwa bezprzewodowych sieci sensorowych (na podstawie cyklu 11 publikacji powiązanych tematycznie)

w związku z Jego wystąpieniem o nadanie stopnia naukowego doktora habilitowanego w dziedzinie Nauk Inżynieryjno-Technicznych w dyscyplinie „Informatyka Techniczna i Telekomunikacja"
oraz
ocena Jego dorobku naukowego i organizacyjnego

Niniejsza recenzja została przygotowana w odpowiedzi na pismo dr. hab. inż. Zbigniewa Piotrowskiego, prof. WAT, z-cy Przewodniczącego Rady Dyscypliny Naukowej *Informatyka Techniczna i Telekomunikacja* z dn. 15.07.2020 w związku z postępowaniem habilitacyjnym dr inż. Janusza Furtaka.

Habilitant pracuje na stanowisku adiunkta - dyrektora Instytutu Teleinformatyki i Cyberbezpieczeństwa, Wydział Cybernetyki, Wojskowa Akademia Techniczna (WAT). Tytuł magistra inżyniera informatyki uzyskał na WAT, Wydział Cybernetyki w 1982 r. Dyplom doktora nauk technicznych w dyscyplinie Informatyka również uzyskał na WAT, Wydział Cybernetyki w 1999 r.

Jego zainteresowania badawcze w okresie przygotowywania rozprawy doktorskiej związane były z zagadnieniami orientacji przestrzennej na podstawie obrazu z ruchomej kamery. W pierwszym okresie po obronie pracy doktorskiej Habilitant prowadził swoje badania dotyczące zagadnień efektywności i bezpieczeństwa transmisji danych w środowisku sieciowym z wykorzystaniem protokołów IPv4 i IPv6. W późniejszym okresie podjął się badań dotyczących tematyki sieci bezprzewodowych, a w szczególności sieci sensorowych, skupiając się na zagadnieniach bezpieczeństwa tych sieci w różnych zastosowaniach, w tym wojskowych. Badania prowadzone przez Habilitanta były realizowane w większości we współpracy z innymi badaczami.

1. Opis osiągnięcia naukowego – monotematycznego cyklu publikacji nt.

Metody podnoszenia poziomu bezpieczeństwa bezprzewodowych sieci sensorowych

Monotematyczny cykl publikacji składa się z 11 artykułów o łącznej liczbie 121 stron opublikowanych w latach 2014-2019. Dwa artykuły opublikowano w dobrych czasopismach znajdujących się w bazie *JCR* (*Journal Citation Reports*), a pozostałe artykuły w materiałach konferencyjnych opublikowanych przez wydawnictwa *IEEE* (5 artykułów), *Springer* (4 artykuły) oraz *PTI* (1 artykuł). Wszystkie artykuły to publikacje wieloautorskie. Przedstawiona dokumentacja zawiera oświadczenia współautorów wskazująca rodzaj ich udziału w tych pracach. Z informacji Habilitanta zawartej w Autoreferacie wynika, że Jego udział procentowy w realizacji większości tych prac waha się w granicach od 60% do 70%.

Wskazany przez Habilitanta cykl publikacji obejmuje następujące prace:

[P1] Furtak J., Chudzikiewicz J. (2014). The concept of authentication in WSNs using TMP. In Ganzha M., Maciaszek L., Paprzycki M. (Eds.), Position Papers of the 2014 Federated Conference on Computer Science and Information Systems. Warsaw, Poland, *PTI*, pp. 183-190;
punkty *MNiSW (PM) PM*=5;

[P2] Chudzikiewicz J., Furtak J., Zieliński Z. (2015). Secure protocol for wireless communication within Internet of Military Things, 2015 2nd IEEE World Forum on Internet of Things, Milano, Italy, *IEEE*;
PM=15;

[P3] Furtak J., Chudzikiewicz J. (2015). Securing transmission between nodes of WSN using TMP. 2015 Federated Conference on Computer Science and Information Systems, Łódź, Poland, *IEEE*, pp. 1059-1068;
PM=15;

[P4] Furtak J., Zieliński Z., Chudzikiewicz J. (2016). Security Techniques for the WSN Link Layer Within Military IoT. 2016 3rd IEEE World Forum on Internet of Things, Reston, VA, USA, *IEEE*, pp. 233-238;
PM=15;

[P5] Furtak J., Chudzikiewicz J. (2017). Secure Transmission in Wireless Sensors Domain Supported by the TPM. In M. Grzenda, A.I. Awad, J. Furtak, J. Legierski (Eds.). Advances in Network Systems. Advances in Intelligent Systems and Computing, vol. 461, *Springer International Publishing*, pp. 129-148;
PM=20;

[P6] Furtak J., Zieliński Z., Chudzikiewicz J. (2018). Secured Domain of Sensors Nodes – A New Concept. In Hodon M., Eichler G., Erfurth C., Fahrnberger G. (Eds.). Innovations for Community Services. I4CS 2018. Communications in Computer and Information Science vol. 863. *Springer International Publishing AG*, pp. 207-217;
PM=20;

[P7] Suri N., Zielinski Z., Tortonesi M., Fuchs C., Pradhan M., Wrona K., Furtak J., Vasilache B., Street M., Pellegrini V., Benibcasa G., Morelli A., Stefanelli C., Casini E., Dyk M. (2018). Exploiting smart city IoT for disaster recovery operations. 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, Singapore, *IEEE*, pp. 458-463;

PM=15;

[P8] Johnsen F.T., Zielinski Z., Wrona K., Suri N., Fuchs C., Pradhan M., Furtak J., Vasilache B., Pellegrini V., Dyk M., Marks M., Krzyszton M. (2018), Application of IoT in Military Operations in a Smart City. 2018 International Conference on Military Communications and Information Systems, Warsaw, Poland, *IEEE*, pp. 163-169;
PM=15;

[P9] Furtak J., Zieliński Z., Chudzikiewicz J. (2019). Procedures for sensor nodes operation in the secured domain. **Concurrency and Computation: Practice and Experience**, pp. e5183;
Impact Factor (IF) IF= 1.17; *PM*=100;

[P10] Furtak J., Zieliński Z., Chudzikiewicz J. (2019). A Framework for Constructing a Secure Domain of Sensor Nodes. **Sensors** 19(12);
IF= 3.03; *PM*=100;

[P11] Furtak J., Chudzikiewicz J. (2019). Security Domain for the Sensor Nodes with Strong Authentication. 2019 International Conference on Military Communications and Information Systems, Budva, Montenegro, IEEE, pp. 1-6;
PM=5.

2. Ocena osiągnięcia naukowego

Przedłożony cykl publikacji stanowiący osiągnięcie naukowe prezentuje wyniki badań Habilitanta mających na celu opracowanie kompleksowego rozwiązania problemu bezpieczeństwa bezprzewodowych sieci sensorowych, spełniających w szczególności wymagania bezpieczeństwa w zastosowaniach, w których te sieci są elementami infrastruktury krytycznej państwa. Na kompleksowość zaproponowanych rozwiązań składają się takie elementy jak architektura węzła sensorowego, modele bezpiecznej domeny węzłów sensorowych wraz z towarzyszącymi procedurami funkcjonowania oraz demonstrator sieci węzłów przedstawiający sobą implementację zaproponowanych koncepcji bezpieczeństwa umożliwiający ich praktyczną weryfikację. Koncepcja bezpieczeństwa opiera się na założeniu, że sieć sensorowa tworzona jest na bazie małych lokalnych klastrów węzłów sieci, a budowanie lokalnej struktury zaufania między sensorami odbywa się z wykorzystaniem mechanizmów zaufania oferowanych przez specjalny moduł TPM (ang. Trusted Platform Module) mający charakter ogólnie przyjętego zaimplementowanego zestawu standardów kryptograficznych w dziedzinie bezpieczeństwa transmisji i przetwarzania danych, a obecność tego modułu w systemie jest obligatoryjna.

Analizując publikacje tego cyklu można stwierdzić, że widoczne są w nim trzy główne nurty badawcze. Poniżej przedstawiam zwięzłą analizę uzyskanych przez Habilitanta wyników przedstawionych w pracach tych nurtów tworzących cykl publikacji.

Nurt 1: Prosty model bezpieczeństwa domeny węzłów sensorowych (Model I).

Prace tego cyklu obejmują publikacje [P1], P[2], P[3] oraz P[5].

W pracy [P1] zaproponowano koncepcję architektury systemu bezpieczeństwa bezprzewodowej sieci sensorowej wykorzystującej mechanizmy zaufania zawarte w module TPM umożliwiającym uwierzytelnienie węzłów sieci. Sieć składa się z węzłów trzech typów: węzła M (ang. Master – M) zarządzającego danymi służącymi do uwierzytelnienia pozostałych węzłów domeny, węzłów S

(ang. Slave – S) będących źródłami danych oraz węzłów R umożliwiających przejęcie roli węzła M w przypadku jego awarii. W tym modelu bezpieczeństwa do uwierzytelnienia węzłów domeny i komunikacji między węzłami stosowana jest kryptografia z kluczem publicznym (kryptografia asymetryczna), natomiast do zabezpieczenia zasobów wewnętrznych węzłów sensorowych stosowana jest kryptografia symetryczna. Umożliwia to moduł TPM, w który wyposażony jest każdy węzeł domeny. Artykuł zawiera szczegółowy opis procedur przyłączania/odłączania węzłów sieci oraz ich uwierzytelnienia. Model tak realizowanego bezpieczeństwa domeny sensorów określana jest przez Habilitanta jako Model I.

W pracy [P2] zaproponowano protokół bezpiecznej transmisji danych w bezprzewodowej sieci sensorowej o architekturze bezpieczeństwa przedstawionej w pracy [P1]. Protokół został zaimplementowany jak też dokonano w oparciu o sprzęt Arduino i system transmisji danych XBee implementacji sprzętowej prostego wariantu sieci zawierającego jeden węzeł typu M, jeden węzeł typu S oraz dodatkowy węzeł pełniący rolę obserwatora ruchu sieciowego. Wykonano badania eksperymentalne systemu mające na celu weryfikację zaproponowanego protokołu bezpieczeństwa. Badano wydajność sieci mierząc takie parametry jak zużycie energii, czas inicjalizacji węzła M, czas autoryzacji węzła S oraz wpływ kosztów czasowych algorytmu szyfrowania AES na opóźnienie czasu transmisji danych.

Praca [P3] stanowi rozszerzenie koncepcji przedstawionych w pracy P[2] dzięki zwiększeniu liczby węzłów sieci i przeprowadzeniu szerokiego wachlarza badań eksperymentalnych z użyciem mechanizmów bezpieczeństwa modułu TPM. Pozwoliły one na określenie realnych warunków funkcjonowania domeny sieci sensorowej z punktu widzenia jej bezpieczeństwa jak też ujawniły pewne istniejące ograniczenia pamięciowe związane z modułami architektury sprzętowej Arduino.

Praca [P5] jest ostatnią pracą tego nurtu związanego z badaniem modelu bezpieczeństwa sieci sensorowej określanego jako Model I. W pracy w sposób kompleksowy przedstawiono kwestie uwierzytelnienia węzłów w domenie sieci. Opisano struktury danych, które są przechowywane w zasobach węzłów, jak też opisano działanie bezpiecznych procedur w domenie obejmujących różne aspekty funkcjonowania węzłów mające wpływ na bezpieczeństwo domeny. Przeprowadzone badania eksperymentalne umożliwiły modyfikacje procedur funkcjonowania sieci mające na celu zwiększenie odporności oprogramowania na możliwe ataki jak też zaproponowanie większej integracji zaproponowanych rozwiązań z używanym systemem komunikacyjnym XBee w celu redukcji opóźnień transmisji danych.

Nurt 2: Zaawansowany model bezpieczeństwa domeny węzłów sensorowych (Model II).

Prace tego cyklu obejmują publikacje [P4], P[6], P[9], P[10]] oraz P[11].

W pracy P[4] zaproponowano nową architekturę sieci sensorowej spełniającej wymagania bezpieczeństwa dla zastosowań wojskowych oraz odpornej na uszkodzenia. Sieć składa się z pewnej liczby klastrów, a elementami pojedynczego klastra są mobilne węzły sensorowe SN (ang. sensor node) zbierające lokalnie informację i komunikujące się między sobą lub z SN innych klastrów przez wyróżniony w klastrze koordynujący węzeł CSN (ang. Collecting Sensor Node). Funkcjonowanie tej sieci opiera się na nowym modelu (Model II), który jest rozszerzeniem poprzedniego Modelu I. Każdy węzeł CSN jest wyposażony w moduł TPM, który umożliwia wykonywanie w domenie bezpieczeństwa funkcji odpowiadających funkcjonalnie węzłowi typu Master (M) lub (albo jednocześnie) wykonywać funkcje bramy G (ang, Gate) w domenie transmisji danych sensorycznych. Zaproponowany model bezpieczeństwa zakłada, że w sieci złożonej z klastrów kontrolowanych przez CSN-y aktualnie tylko jeden z nich pełni rolę węzła typu M i ten wybór odbywa się dzięki algorytmowi elekcji. Pozostałe węzły CSN pełnią rolę replik węzła M i w przypadku odkrycia błędnego funkcjonowania węzła M gotowe są do podjęcia się tej roli. Za bezpieczeństwo klastra odpowiada związany z nim CSN, który dzięki modułowi TSM i wykorzystaniu technik kryptografii symetrycznej umożliwia bezpieczne przechowywanie

wrażliwych danych jak też bezpieczną zaszyfrowaną komunikację między węzłami sieci. Funkcje uwierzytelnienia węzłów sieci realizowane są z użyciem kryptografii asymetrycznej przez węzeł typu M. Artykuł zawiera informację o implementacji na bazie sprzętowej Arduino systemu składającego się z 3 węzłów oraz wstępne wyniki testowe systemu.

Praca P[6] prezentuje opis wariantu rozwiązania budowy bezpiecznej domeny sieci sensorowej zapewniającej wewnątrz niej bezpieczną komunikację, zgodnie z koncepcją przedstawioną w pracy P[4]. Podstawowe elementy tej sieci to mobilne sensory generujące dane przesyłane lokalnie do węzłów sensorowych typu R pełniących wg. koncepcji z P[4] rolę koordynatora klastra oraz węzeł M pełniący główną rolę organizacji bezpieczeństwa domeny. Dane mogą być przesyłane do innych węzłów typu R przy użyciu modułu komunikacyjnego XBee lub przesyłane do środowiska znajdującego się poza siecią z użyciem modułu komunikacyjnego LoRA i specjalnego węzła G pełniącego rolę bramy. Za przygotowanie bezpiecznej domeny sieciowej odpowiada specjalny węzeł B inicjujący hierarchiczną strukturę bezpieczeństwa, które opiera się na dystrybucji kluczy kryptograficznych do zweryfikowanych węzłów typu R wyposażonych w moduł TPM umożliwiających bezpieczny dostęp do danych oraz bezpieczną komunikację. Praca zawiera również opis stanowiska laboratoryjnego składającego się z czterech węzłów sensorowych realizujących sieć zgodnie z przedstawioną architekturą oraz wyniki badań związane z opóźnieniami w transmisji danych z wykorzystaniem węzła typu G.

Prace P[9] oraz P[10] łącznie przedstawiają pełną wersję rozwiązania problemu budowy bezpiecznej domeny sieci sensorowej zainicjowanej w pracy P[6]. W pracy P[9] przedstawiono szczegółowo koncepcję bezpiecznej domeny jak też koncepcję zabezpieczenia kryptograficznego węzłów sensorowych. Szczególną uwagę poświęcono przedstawieniu zaproponowanych procedur inicjalizacji bezpiecznej domeny sieci sensorowej z użyciem węzła B. Praca P[10] jest swoistym dopełnieniem pracy P[9]. Przedstawiono w niej szczegółowo kwestie danych przechowywanych w węźle sensorowym, mechanizmy ich zabezpieczania oraz procedury tworzenia bezpiecznej domeny w powiązaniu ze strukturami danych węzłów sensorowych. W artykule przedstawiono również wyniki badań kilkuwęzłowej sieci sensorowej realizującej koncepcje Modelu II. Wykazano odporność sieci na różnorodne możliwe ataki sieciowe jak też pokazano jej dobrą skalowalność.

Praca P[11] ma charakter zwięzłego podsumowania prac prowadzonych w ramach tworzenia bezpiecznej domeny sieciowej zgodnej z Modelem II.

Nurt 3: Zastosowanie sieci sensorowych w operacjach usuwania skutków katastrof.

Prace tego cyklu obejmują publikacje [P7] oraz P[8]. Mają one charakter koncepcyjny i dotyczą wykorzystania narzędzi Internetu Rzeczy, w tym bezpiecznych domen sieci sensorowych w sytuacjach kryzysowych spowodowanych skutkami poważnych katastrof. Istotnym elementem usuwania skutków takich katastrof jest uzyskanie wiarygodnej informacji o sytuacji po katastrofie, czyli uzyskanie tzw. świadomości sytuacyjnej, w celu podjęcia efektywnych skoordynowanych działań zespołów ratowniczych zorientowanych na usunięcie skutków katastrofy.

W pracy P[7] zaproponowano architekturę systemu Internetu Rzeczy przeznaczonego do zbierania i przetwarzania dużej ilości wiarygodnej informacji w celu tworzenia świadomości sytuacyjnej umożliwiającej podjęcie akcji ratunkowej w hipotetycznej sytuacji kryzysowej w środowisku miasta Helsinki. Zwrócono uwagę na kwestię integracji systemów wojskowych, w tym dotyczących zagadnień bezpiecznej domeny sieci sensorowych z narzędziami Internetu Rzeczy dostępnych w ramach tzw. inteligentnego miasta.

Praca P[8] rozpatruje hipotetyczną sytuację zaistniałą po katastrofie w jednym z miast sojuszu NATO i związaną z koniecznością rozmieszczenia w miejscu katastrofy niewielkich międzynarodowych oddziałów wojskowych. Tworzenie świadomości sytuacyjnej ma tu istotne znaczenie dla ustalenia priorytetów w redystrybucji dostępnych środków dla najbardziej potrzebujących poszkodowanych w wyniki katastrofy. Artykuł przedstawia koncepcję systemu

uwzględniającą zagadnienia techniczne mające na celu współpracę z urządzeniami Internetu Rzeczy będącymi elementami inteligentnego miasta. Celem takiej współpracy będzie pozyskanie informacji, bieżące monitorowanie stanu żołnierzy-ratowników oraz budowanie zaufania i bezpiecznej wymiany danych między systemami wojskowymi a systemami inteligentnego miasta.

Najważniejsze wyniki osiągnięcia naukowego, jego podsumowanie i ocena.

W ramach przedstawionego cyklu publikacji stanowiących osiągnięcie naukowe uzyskano oryginalne wyniki dotyczące rozwoju nowych technologii informatyczno-komunikacyjnych wnoszące istotny wkład do dyscypliny Informatyka Techniczna i Telekomunikacja, w dziedzinie Nauk Inżynieryjno-Technicznych. Do najważniejszych uzyskanych wyników zaliczam:

- opracowanie architektury systemu bezpieczeństwa domeny bezprzewodowej sieci sensorowej opartej na wykorzystaniu mechanizmów zaufania zawartych w module TPM – Model I,
- zaproponowanie protokołu bezpiecznej transmisji danych w bezprzewodowej sieci sensorowej o architekturze bezpieczeństwa odpowiadającej Modelowi I,
- realizacja sprzętowo-programistyczna modelu laboratoryjnego domeny zgodnej z Modelem I oraz przeprowadzenie badań testowych modelu laboratoryjnego,
- opracowanie zmodyfikowanej architektury systemu bezpieczeństwa domeny bezprzewodowej sieci sensorowej opartej na wykorzystaniu mechanizmów zaufania zawartych w module TPM, określanej jako Model II,
- opracowanie w ramach Modelu II nowej, zoptymalizowanej do możliwości sprzętowych bezprzewodowej sieci sensorowej, hierarchicznej struktury bezpieczeństwa domeny sieci, poprzez zbalansowany wybór algorytmów kryptografii asymetrycznej oraz symetrycznej zapewniających jednocześnie wysoki stopień bezpieczeństwa oraz efektywną i bezpieczną transmisję danych,
- opracowanie w ramach Modelu II interesującej koncepcji utrzymywania odporności sieci na uszkodzenia jej węzłów w trakcie jej funkcjonowania,
- opracowanie i implementacja szeregu algorytmów funkcjonowania sieci w różnych cyklach jej życia,
- realizacja sprzętowo-programistyczna modelu laboratoryjnego bezpiecznej domeny sieciowej zgodnej z Modelem II oraz przeprowadzenie badań testowych modelu laboratoryjnego,
- eksperymentalne wykazanie, że zaproponowana i zrealizowana bezpieczna domena sieci sensorowych jest odporna na aktualnie znane ataki sieciowe,
- zaproponowanie opracowanych rozwiązań bezpiecznych technologii informatyczno-komunikacyjnych do tworzenie systemów budowania świadomości sytuacyjnej w sytuacjach katastrof humanitarnych i usuwania ich skutków.

W moim przekonaniu wyniki badań przedstawionych w ramach cyklu publikacji tworzących osiągnięcie naukowe wnoszą istotny wkład w rozwój informatyki technicznej i telekomunikacji proponując innowacyjne technologie informatyczno-komunikacyjne, które mogą być wykorzystywane w różnych zastosowaniach cywilnych, ale też ze względu na wysoki stopień gwarantowanego bezpieczeństwa mogą być stosowane z powodzeniem w operacjach wojskowych bądź mogą być elementami infrastruktury krytycznej państwa.

Podsumowanie parametryczne publikacji przedłożonego osiągnięcia naukowego jest następujące. Liczba artykułów opublikowanych w czasopismach indeksowanych w bazie *JCR* wynosi 2, a ich sumaryczny *IF* wynosi 4.20 (*IF 5* wynosi 4.45), a *SNIP* (wg. *Scopus*) wynosi 3.02.

Sumaryczna liczba punktów ministerialnych cyklu publikacji wynosi 325. Są to dobre wartości świadczące o randze cyklu publikacji.

Dokonując końcowego podsumowania oceny osiągnięcia naukowego Habilitanta stwierdzam, że ma ono oryginalny, twórczy charakter oraz w moim przekonaniu spełnia wymagania formułowane przez obowiązującą ustawę w stosunku do osób ubiegających się o nadanie stopnia doktora habilitowanego.

3. Ocena całościowego dorobku naukowego

Aktualny dorobek publikacyjny Habilitanta wg. podanych przez Niego danych zamyka się liczbą 53 publikacji. Spośród nich 42 publikacje powstały po uzyskaniu stopnia doktora. Struktura tych publikacji jest następująca: jedna monografia naukowa (po doktoracie), 13 rozdziałów w monografiach naukowych (12 z nich po doktoracie), 24 artykuły w czasopismach naukowych (18 z nich po doktoracie), w tym 2 z nich opublikowano w czasopismach z bazy *JCR* (po doktoracie). Habilitant posiada również 4 osiągnięcia projektowe, konstrukcyjne i technologiczne.

Sumaryczny *IF* publikacji z bazy *JCR* to 4.20, a sumaryczna liczba punktów MNiSW wynosi 563. Sumaryczna liczba cytowań (bez autocytowań) to 14 (wg. *WoS)*, 56 (wg. *Scopus*) oraz 142 (wg. *Google Scholar, GS*), a wartość indeksu *h* to 3 wg. *WoS*, 6 wg. *Scopus* oraz 7 wg. *GS*.

Habilitant brał udział w realizacji 3 projektów badawczych finansowanych przez NCBiR. W dwóch z nich pełnił funkcję kierownika zespołu. Brał udział w 7 projektach badawczych zlecanych przez *WAT, MON* oraz *KBN*, w tym 6 razy pełnił funkcję kierownika projektu. Dwukrotnie był przedstawicielem Polski (nominacja MON) w grupach roboczych programu *NATO Science and Technology Organization*. Współpracował z otoczeniem społecznym i gospodarczym, m.in. z Wojskowym Instytutem Łączności, Enamor Sp. z o.o., Enigma Systemy Ochrony Informacji Sp. z o.o., FILBICO Sp. z o.o., TRANSBIT Sp. z o.o. oraz z Naukową i Akademicką Siecią Komputerową. Wykonywał recenzje i ekspertyzy dla MON, MON DNiSW oraz NCBiR.

Habilitant odbył kilkutygodniowy staż naukowy na Słowacji .

Całościowy dorobek naukowy Habilitanta oceniam jednoznacznie pozytywnie. W związku z tym stwierdzam, że całościowy dorobek publikacyjny dr inż. Janusza Furtaka mieści się z powodzeniem w dziedzinie Nauk Inżynieryjno-Technicznych, w dyscyplinie Informatyka Techniczna i Telekomunikacja.

4. Ocena dorobku dydaktycznego i organizacyjnego

Habilitant aktywnie uczestniczył w międzynarodowych i krajowych konferencjach naukowych. Był zapraszany około 20 razy do komitetów programowych konferencji jak też wielokrotnie pełnił funkcję przewodniczącego sesji.

Wielokrotnie recenzował artykuły dla międzynarodowych i krajowych czasopism, w tym dla czasopism z listy *JCR*.

Habilitant był promotorem około 130 prac inżynierskich i magisterskich. Jego dyplomanci byli dwukrotnie laureatami krajowych konkursów „Seeds for the Future 2018" oraz „Forum Młodych Mistrzów".

Habilitant prowadził na WAT oraz w Prywatnej Wyższej Szkole Businessu i Administracji" zajęcia dydaktyczne o następującej tematyce:

- *Administrowanie sieciami komputerowymi,*
- *Administrowanie systemem UNIX,*
- *Bezpieczeństwo w sieciach IPv6,*

- *IPv6 networks,*
- *Konfigurowanie serwerów usług internetowych,*
- *Podstawy sieci komputerowych,*
- *Podstawy użytkowania systemu UNIX,*
- *Projektowanie serwerów i aplikacji WWW,*
- *Security mechanisms in the Linux environment,*
- *Sieci IPv6,*
- *Sieci komputerowe,*
- *Sieci komputerowe i telekomunikacyjne,*
- *Sprzęt i technologie sieciowe,*
- *Systemy bezpieczeństwa sieciowego,*
- *Systemy operacyjne,*
- *Systemy operacyjne UNIX,*
- *Techniki sieciowe w bezpieczeństwie,*
- *Techniki sieciowe urządzeń IoT,*
- *Technologie i techniki sieci komputerowych,*
- *Usługi sieciowe w systemie UNIX,*
- *Użytkowanie i administrowanie sieciami komputerowymi,*
- *Zaawansowane techniki sieciowe.*

Habilitant prowadził również zajęcia dydaktyczne na kursach dokształcających dla MON.

Habilitant był członkiem komisji do spraw przygotowania programu studiów I i II stopnia prowadzonych na Wydziale Cybernetyki WAT dla kierunków *Informatyka* (od 2009 r), *Kryptologia i cyberbezpieczeństwo* (od 2014 r) oraz *Informatyka w medycynie* (w latach 2014 – 2019).

Habilitant był członkiem zespołu, który powołał do życia lokalną Akademię Cisco w Instytucie Teleinformatyki i Automatyki Wydziału Cybernetyki WAT. Był organizatorem i instruktorem kursów CCNA w lokalnej Akademii Cisco. Był również członkiem zespołu instruktorów Akademii Cisco w latach 2013-2015, który tłumaczył materiały kursów Cisko.

Habilitant w latach 2003-2006 był kierownikiem Zakładu na Wydziale Techniki Wojskowej WAT. W latach 2006-2008 był zastępcą dyrektora Instytutu Teleinformatyki i Automatyki, a w latach 2008-2012 był zastępcą dyrektora z powierzeniem obowiązków dyrektora Instytutu. W latach 2016-2019 pełnił funkcję dyrektora Instytutu Teleinformatyki i Automatyki, a od 2019 r do chwili obecnej pełni funkcję dyrektora Instytutu Teleinformatyki i Cyberbezpieczeństwa.

Za swoją działalność naukową, dydaktyczną i organizacyjną Habilitant był nagradzany: przez Prezydenta Rzeczypospolitej Polskiej srebrnym i złotym Krzyżem Zasługi w latach 1997 i 2000, odpowiednio; przez Ministra Obrony Narodowej medalem „Siły Zbrojne w służbie Ojczyzny" – brązowym (1987 r), srebrnym (1994 r) oraz złotym (1999 r); przez Rektora WAT – odznaczeniem „Zasłużony Nauczyciel WAT) (2002 r) oraz przez Dziekana Wydziału Cybernetyki WAT odznaczeniem „ Zasłużony dla Wydziału Cybernetyki WAT".

Habilitant jest od 2016 r. członkiem IEEE (Institute of Electrical and Electronics Engineers).

Przedstawiony wyżej dorobek dydaktyczno-organizacyjny świadczy o znacznej aktywności zawodowej Habilitanta i jego uznaniu jako wartościowego naukowca przez środowiska naukowe krajowe jak i zagraniczne.

5. Konkluzja

W perspektywie całościowej oceniam dorobek dr inż. Janusza Furtaka jako bardzo wartościowy zarówno pod względem poznawczym jak też aplikacyjnym. Dokonania przedstawione w osiągnięciu naukowym składają się na oryginalny i twórczy wkład w dziedzinie Nauk Inżynieryjno-Technicznych, w dyscyplinie Informatyka Techniczna i Telekomunikacja, a w szczególności istotny dla problematyki bezpieczeństwa bezprzewodowych sieci sensorowych. Posiadają one duże znaczenie dla dalszego rozwoju problematyki Internetu Rzeczy, zarówno w aspekcie teoretycznym jak i praktycznym, w tym w obszarze bezpieczeństwa sieci oraz zastosowań wojskowych lub związanych z infrastrukturą krytyczną państwa. Jego działalność naukowo-badawcza oraz dydaktyczno-organizacyjna w sferze nauki potwierdza wysokie predyspozycje badawcze Habilitanta.

W konkluzji z pełnym przekonaniem stwierdzam, że przedłożone osiągnięcie naukowe oraz całokształt dorobku naukowego i organizacyjnego dr inż. Janusza Furtaka spełniają wymogi aktualnie obowiązującej Ustawy o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki do nadania mu stopnia doktora habilitowanego Nauk Inżynieryjno-Technicznych, w dyscyplinie Informatyka Techniczna i Telekomunikacja.