dr hab. inż. Wojciech Mazurczyk, profesor uczelni
Instytut Informatyki, Wydział Elektroniki i Technik Informacyjnych
Politechnika Warszawska
ul. Nowowiejska 15/19
00-665 Warszawa
wojciech.mazurczyk@pw.edu.pl

Warszawa, 15.09.2020

Recenzja osiągnięcia naukowego oraz istotnej aktywności naukowej w postępowaniu habilitacyjnym dr inż. Janusza Furtaka

w dziedzinie nauk technicznych w dyscyplinie informatyka techniczna i telekomunikacja

Przedmiotem recenzji jest dorobek naukowy i aktywność naukowa dr inż. Janusza Furtaka, pracownika Instytutu Teleinformatyki i Cyberbezpieczeństwa, Wydziału Cybernetyki Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego. Recenzja została przygotowana w ramach postępowania habilitacyjnego dr inż. Janusza Furtaka prowadzonego przez Radę Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego w Warszawie. Formalną podstawą do przedłożenia niniejszej recenzji było pismo nr WYCH/OGL/01423/2020 Zastępcy Przewodniczącego Rady Dyscypliny Naukowej ITiT dr hab. inż. Zbigniewa Piotrowskiego, prof. WAT z dnia 15 lipca 2020, w oparciu o uchwałę Rady Dyscypliny Naukowej ITiT Wojskowej Akademii Technicznej nr 21/RDN ITiT/2020 z dnia 14 lipca 2020 r oraz pismo Rady Doskonałości Naukowej Z2.4000.10.2020.2.BR z dnia 30 czerwca 2020.

Niniejsza recenzja została opracowana zgodnie z obecnym porządkiem prawnym na podstawie przekazanej dokumentacji zawierającej wniosek dr inż. Janusza Furtaka, jego autoreferat, kopię dyplomu stwierdzającego nadanie stopnia doktora nauk technicznych, wykaz opublikowanych prac naukowych oraz informacji o osiągnięciach dydaktycznych, współpracy naukowej i popularyzacji nauki, oświadczeń współautorów publikacji wchodzących w skład osiągnięcia oraz kopii publikacji stanowiących przedłożone osiągnięcie naukowe.

1. Ocena osiągnięcia naukowego

Dr inż. Janusz Furtak jako swoje główne osiągnięcie naukowe wskazał zbiór powiązanych tematycznie 11 artykułów naukowych, który nosi tytuł „Metody podnoszenia poziomu bezpieczeństwa bezprzewodowych sieci sensorowych”. Przedłożone artykuły zostały opublikowane w latach 2014-2019 i są to następujące pozycje (w nawiasach podano m.in. deklarowany udział Habilitanta wg załączonych oświadczeń oraz liczbę punktów za publikację wg list punktacji MNiSW):

1. Janusz Furtak, Jan Chudzikiewicz, The concept of authentication in WSNs using TPM. FedCSIS (Position Papers) 2014: 183-190 (**PKT=5, udział Habilitanta: 60%)**

2. Jan Chudzikiewicz, Janusz Furtak, Zbigniew Zielinski, Secure protocol for wireless communication within internet of military things. WF-IoT 2015: 508-513 (**indeksowana w bazie WoS, PKT=15, udział Habilitanta: 60%)**

3. Janusz Furtak, Jan Chudzikiewicz, Securing transmissions between nodes of WSN using TPM. FedCSIS 2015: 1059-1068 (**indeksowana w bazie WoS, PKT=15, udział Habilitanta: 70%)**

4. Janusz Furtak, Zbigniew Zielinski, Jan Chudzikiewicz, Security techniques for the WSN link layer within military IoT. WF-IoT 2016: 233-238 **(indeksowana w bazie WoS, PKT=15, udział Habilitanta: 60%)**

5. Janusz Furtak, Jan Chudzikiewicz, Secure Transmission in Wireless Sensors' Domain Supported by the TPM, in Advances in Network Systems: Architectures, Security, and Applications, 2017, vol. 461, pp. 129–148 **(PKT=20, udział Habilitanta: 60%)**

6. Janusz Furtak, Zbigniew Zielinski, Jan Chudzikiewicz, Secured Domain of Sensor Nodes - A New Concept. I4CS 2018: 207-217 **(PKT=20, udział Habilitanta: 70%)**

7. Niranjan Suri, Zbigniew Zielinski, Mauro Tortonesi, Christoph Fuchs, Manas Pradhan, Konrad S. Wrona, Janusz Furtak, Dragos Bogdan Vasilache, Michael Street, Vincenzo Pellegrini, Giacomo Benincasa, Alessandro Morelli, Cesare Stefanelli, Enrico Casini, Michal Dyk, Exploiting smart city IoT for disaster recovery operations. WF-IoT 2018: 458-463 **(PKT=15, udział Habilitanta: 6%)**

8. Frank T. Johnsen, Zbigniew Zieliński, Konrad Wrona, Niranjan Suri, Christoph Fuchs, Manas Pradhan, Janusz Furtak, Bogdan Vasilache, Vincenzo Pellegrini, Michał Dyk, Michał Marks, Mateusz Krzysztoń, Application of IoT in military operations in a smart city, 2018 International Conference on Military Communications and Information Systems (ICMCIS), Warsaw, 2018, pp. 1-8, DOI: 10.1109/ICMCIS.2018.8398690. **(PKT=15, udział Habilitanta: 8%)**

9. Janusz Furtak, Zbigniew Zielinski, Jan Chudzikiewicz, Procedures for sensor nodes operation in the secured domain. Concurr. Comput. Pract. Exp. 32(13) (2020) **(IF=1,17, PKT=100, udział Habilitanta: 70%)**

10. Janusz Furtak, Zbigniew Zielinski, Jan Chudzikiewicz, A Framework for Constructing a Secure Domain of Sensor Nodes. Sensors 19(12): 2797 (2019) **(IF=3,03, PKT=100, udział Habilitanta: 70%)**

11. Janusz Furtak, Zbigniew Zieliński, Jan Chudzikiewicz, Security Domain for the Sensor Nodes with Strong Authentication, in: 2019 International Conference on Military Communications and Information Systems, 2019, ISBN 978-1-5386-9384-1, pp. 1-6, DOI:10.1109/ICMCIS.2019.8842766 **(PKT=20, udział Habilitanta: 60%)**

Na jedenaście z przedłożonych publikacji wymienionych powyżej w ośmiu Habilitant jest pierwszym autorem. Ponadto, udział Habilitanta w dziewięciu publikacjach jest bardzo wysoki i wynosi pomiędzy 60% a 70% (co potwierdzają oświadczenia samego Habilitanta jak i współautorów). Brak jest natomiast publikacji jednoautorskich. Dodatkowo, trzy z prezentowanych w ramach osiągnięcia artykułów naukowych zostało napisanych przez dwóch współautorów ([1], [3], [5]), sześć jest napisanych przez trzech współautorów ([2], [4], [6], [9], [10], [11]), a dwie są napisane przez więcej niż dwunastu współautorów ([7], [8]). Pięć publikacji jest indeksowanych w bazie WoS ([2], [3], [4], [9], [10]), natomiast dwie z nich ([9] i [10]) zostały opublikowane w prestiżowych czasopismach z tzw. listy filadelfijskiej (lista JCR) posiadających współczynnik *Impact Factor* (łączny IF tych publikacji wynosi 4,2), natomiast pozostałych sześć zostało zaakceptowanych i przedstawionych na konferencjach międzynarodowych lub zamieszczonych jako rozdział w monografii ([1], [5], [6], [7], [8], [11]).

Warto podkreślić, że dziedzina badawcza, w której badania naukowe prowadzi Habilitant, czyli szeroko pojęte bezpieczeństwo bezprzewodowych sieci sensorowych (w tym sieci IoT w zastosowaniach wojskowych) jest obecnie jednym z istotnych obszarów cyberbezpieczeństwa, w którym prace prowadzi wiele zespołów naukowych z wiodących instytucji naukowych w Europie i na świecie.

W autoreferacie Habilitant stwierdza, że celem przedłożonego osiągnięcia naukowego jest „(…) przedstawienie kompleksowego rozwiązania zapewniającego wysoki poziom bezpieczeństwa bezprzewodowych sieci węzłów sensorowych". W dalszej części dr Furtak wskazuje, że w szczególności istotne zaproponowane tam rozwiązania obejmują trzy główne elementy: dwa modele domen węzłów sensorowych (Model I i II), opis architektury węzła sensorowego oraz zestawy odpowiednich procedur uzupełnione o stosowny demonstrator.

W mojej ocenie przedstawione osiągnięcie naukowe mimo tego, że zawiera pewne walory merytoryczne nie może jednak zostać uznane za kompleksowe z następujących powodów. Po pierwsze, zarówno dla Modelu I jak i Modelu II nie opracowano, nie zaimplementowano i nie zbadano wszystkich niezbędnych procedur. Dla Modelu I (wykazującego znaczące wady funkcjonalne wskazane przez Habilitanta na str. A-18 autoreferatu) brak jest procedur 8-11 (str. A-17 autoreferatu). Natomiast w przypadku Modelu II brak jest części procedur związanych z normalną pracą domeny (procedury 11, 13-17 str. A-24). Po drugie, nie przeprowadzono dogłębnych badań eksperymentalnych pokazujących w sposób przekonujący, że zaproponowane rozwiązania rzeczywiście zapewniają wysoki poziom bezpieczeństwa, są wydajne, skalowalne i nadają się rzeczywiście do zastosowań w sieciach IoT. Należy też nadmienić, że wyniki badań przedstawione w publikacjach C1-C11 zostały przeprowadzone w dość ograniczonym środowisku eksperymentalnym (zaledwie kilka elementów sieci), w bardzo okrojonym zakresie, bez jednoznacznego wskazania użytej metodyki badawczej oraz bez odniesienia i porównania się (także eksperymentalnego) z innymi rozwiązaniami zaproponowanymi dotychczas w literaturze. Ponadto, warto zauważyć, że w przedstawionym cyklu artykułów mamy do czynienia z negatywnymi zjawiskami takimi jak:

- tzw. *academic salami slicing*, czyli publikowanie prac naukowych na praktycznie ten sam temat z minimalną bądź żadną wartością dodaną w stosunku do poprzednich publikacji tego samego autora/ów oraz

- wielokrotnego wykorzystywania elementów jednego artykułu (obrazków, fragmentów tekstu i wyników) w tej samej lub bardzo zbliżonej formie w kolejnych publikacjach bez odpowiedniego cytowania czy adnotacji.

Poniżej przedstawiono syntetyczne omówienie ocenianego osiągnięcia naukowego w podziale na poszczególne publikacje ze szczególnym uwzględnieniem mankamentów wskazanych powyżej.

W pracy [1] opublikowanej w materiałach konferencji *FedCSIS* przeznaczonych dla tzw. position papers (czyli nie w głównych materiałach konferencyjnych), tj. artykułach dokumentujących prace badawcze będące w toku, zawarto jedynie ogólną koncepcję nowej metody uwierzytelnienia w sieciach WSN oraz zdefiniowano role i sposób wymiany danych dla węzłów M, rM i S. Głównym elementem gwarantującym bezpieczeństwo jest w tym przypadku dobrze znany zewnętrzny układ TPM (Trusted Platfom Module). Warto podkreślić, że w artykule brakuje m.in. przeglądu literatury jasno pokazującego czym to co autorzy proponują różni się od tego co już dotychczas zaproponowano, co jest nowatorskim aspektem badawczym, brak także przeprowadzenia

badań eksperymentalnych choćby z wykorzystaniem symulacji i dyskusji wyników. W ocenie recenzenta artykuły zawierające jedynie opis koncepcji rozwiązania bez eksperymentalnego udowodnienia jego skuteczności w zastosowaniu, do którego był przewidziany ma niską wartość naukową.

Dopiero w publikacji [2] zaprezentowanej na konferencji *World Forum on Internet of Things* w 2015 roku autorzy przedstawiają rozwinięcie koncepcji przedstawionej w [1] wzbogaconej o implementację i realizację sprzętową (choć ograniczoną do jedynie dwóch węzłów – jednego urządzenia S i jednego M) oraz wstępne wyniki eksperymentalne. Niestety, także w tej pracy zabrakło przeglądu literatury wskazującego nowatorskość podjętego przez autorów problemu badawczego oraz wyjaśnienia czym to co proponują różni się od tego co już opublikowano w literaturze. Ponadto, przedstawiono wyniki badań eksperymentalnych nie podając szczegółów zastosowanej metodyki badawczej, czyli jak dokładnie zostały przeprowadzone eksperymenty, np. w jaki sposób badano zużycie energii czy zajętość pamięci przez poszczególne komponenty, ile razy były powtarzane badania dla każdego punkty pomiarowego, czy zaprezentowane wartości są wartości średnimi, jakie jest odchylenie standardowe, itd. Brakuje większej liczby i bardziej pogłębionych badań np. jak rola danego węzła wpływa na szybkość zużycia energii zakładając przykładowo typowe źródła energii dla urządzeń IoT, jaka jest skalowalność rozwiązania, jaka jest eksperymentalna odporność na różnego rodzaju ataki jakim podlegać mogę sieci sensorowe, itp.

Następnie w artykule [3], który został opublikowany w materiałach konferencji *Conference on Computer Science and Information Systems* w 2015 roku Habilitant wykorzystał z bardzo małymi modyfikacjami w zasadzie połowę zawartości pracy [1] (np. rozdziały II, III) oraz fragmenty z [2] (np. część rozdziału IV) bez odpowiedniego cytowania – w pracy zawarto jedynie informację w formie przypisu, że koncepcja tego rozwiązania była prezentowana na konferencji FEDCSIS 2014 (co w żadnym wypadku nie dopuszcza skopiowania znacznych części artykułu [1]). Także środowisko badawcze pozostało zasadniczo bez zmian choć autorzy wskazują bardzo ogólnie w rozdziale IV, że wykorzystano *kilka* sensorów z TPM oraz *kilka* stacji roboczych (choć rysunki środowiska badawczego także zostały przekopiowane z [1]). Ponadto, to co autorzy prezentują jako wyniki badań trudno uznać za rezultaty eksperymentów niosących jakąś wartość naukową i poznawczą – są to zrzuty opisów poszczególnych węzłów wskazujące w ten sposób, że dochodzi do transmisji danych pomiędzy nimi.

Z kolei w pracy [4] zaakceptowanej na konferencję *World Forum on Internet of Things* w roku 2016 autorzy bardziej szczegółowo zdefiniowali koncepcję domeny bezpieczeństwa sensorów dla zastosowań wojskowych, stwierdzając także, że ogólne wymagania bezpieczeństwa dla zastosowań cywilnych i wojskowych są w zasadzie są takie same. Artykuł ten jest bardzo krótki (6 stron) i oprócz omówienia implementacji sprzętowej (w skład której wchodzą te same elementy co w artykułach [1-3]) nie zawarto w nim praktycznie żadnych wyników badań oprócz powtórzenia rezultatów zużycia energii poprzednio umieszczonych także w artykule [2] (Rys. 14). Ponownie jednak nie zawarto informacji na temat metodyki badawczej tych eksperymentów. Dziwi także fakt umieszczenia tego artykułu w tym miejscu cyklu, gdyż odnosi się już do Modelu II (który wykorzystuje głównie kryptografię symetryczną, co pozwala na wykorzystanie większej liczby sensorów w jednej domenie), a który opisano także w pracach [6], [9-10]. Warto także zauważyć, że Model I (oparty głównie na kryptografii asymetrycznej) jest opisany w pracach [1-3] oraz [5] przedłożonego osiągnięcia naukowego, zatem logiczniejszym rozwiązaniem byłoby ułożenie artykułów w cyklu najpierw tych opisujących Model I, następnie Model II, a na końcu scenariusze zastosowań (np. obecne prace [7] i [8]).

Publikacja [5], która jest rozdziałem w monografii *Advances in Network Systems: Architectures, Security, and Applications* (której dr Furtak jest także jednym z edytorów naukowych) dotyczy ponownie zagadnień związanych z Modelem I i jest w zasadzie najpełniejszym tego rozwiązania oraz powiązanych z nim koncepcji. Z drugiej strony, dziwi jednak fakt, że Habilitant poświęcił aż tyle publikacji [1-3] oraz [5] Modelowi I, który wykazujące znaczące wady funkcjonalne wskazane m.in. na str. A-18 autoreferatu. Niemniej jednak należy zauważyć, że ten artykuł od strony edytorskiej jest zasadniczo kompilacją poprzednio opublikowanych prac [2-4] zarówno jeśli chodzi o fragmenty tekstu (np. str. 133-134 zwierają części artykułu [3]), obrazki (Rysunki 5 i 6 z bardzo małymi modyfikacjami lub żadnymi są przeniesione z [2]; Rys. 7 pochodzi z [4]; Rys. 8-11 z [3]), a co najgorsze wyniki badań eksperymentalnych (w całości zaczerpnięte z [2] wyniki z Rys. 16 oraz Tabeli 3, natomiast wyniki w Tabelach 1-2 różnią się nieznacznie w granicach 0,01-4% i na ich podstawie wyciągnięte są te same co w [2] wnioski). Podsumowując, publikacji tej nie można uznać z naukowego punktu widzenia za zawierającą jakieś nowe, zasadnicze elementy, a nosi ona raczej znamiona tzw. autoplagiatu.

Następnie w artykule [6], który opublikowano w materiałach konferencyjnych *International Conference on Innovations for Community Services* w 2018 roku autorzy rozwijają koncepcję Model II, który jest ulepszoną wersją Modelu I w większym stopniu opartym na kryptografii symetrycznej i poprawiającą większość niedostatków Modelu I (m.in. to, że węzeł M jest pojedynczym krytycznym punktem awarii w domenie, możliwe było przejęcie części publicznej klucza DK, gdyż był przesyłany w postaci jawnej, czy w prosty sposób zarejestrować fałszywy węzeł w domenie). Z tej perspektywy, w tej pracy w odróżnieniu od części wcześniej omawianych artykułów widoczny jest nowatorski wkład naukowy. Ponadto, rozwinięte zostało środowisko badawcze (choć jedynie do 4 węzłów), natomiast na każdy węzeł składają się w zasadzie te same komponenty fizyczne co w poprzednich publikacjach. Niemniej jednak praca [6] posiada także szereg mankamentów, a najważniejsze z nich to: brak opisu i implementacji kompletnego rozwiązania tzn. brakuje implementacji procedur 7-10, poza tym w pracy tej nie ma informacji nt. sposobu działania procedur 1-6. Co więcej, zawarto tam bardzo mało wyników eksperymentalnych – jest jedynie jedna tabela zawierająca wyniki dla węzła G dokumentująca opóźnienie wprowadzane przy zabezpieczeniu przesyłanych ramek (analogiczne tabele umieszczano dla innych węzłów w poprzednich pracach opisujących Model I). Poza tym brakuje także tych samych elementów co w artykułach [1-5] tzn. brak jest analizy i porównania eksperymentalnego z rozwiązaniami znanymi z literatury (w tym z Modelem I), brak jest opisu metodyki badawczej wykorzystywanej przy przeprowadzaniu eksperymentów i w końcu brakuje rzetelnej i systematycznej analizy proponowanego rozwiązania z wykorzystaniem badań eksperymentalnych w przedstawionym środowisku badawczym.

Z kolei prace: [7], którą opublikowano na konferencji *World Forum on Internet of Things* oraz [8] zaprezentowaną na konferencji *International Conference on Military Communications and Information Systems* (obie w 2018 roku) mają zupełnie inny charakter w porównaniu z pozostałymi publikacjami przedłożonego cyklu. Po pierwsze, udział Habilitanta w tych pracach jest znikomy (6% w [7] – 15 współautorów i 8% w [8] – 12 współautorów przy założeniu równomiernego udziału, co nie jest potwierdzone oświadczeniami). Już tak niski udział stawia pod znakiem zapytania stosowność ich zamieszczenia w przedstawionym przez Habilitanta osiągnięciu naukowym. Po drugie, są to jedyne prace w całym dorobku dr Furtaka, które są napisane we współpracy międzynarodowej (w ramach prac w grupie NATO RTG IST-147). Po trzecie, prace te w zasadzie nie zawierają sformułowania nowatorskiego problemu badawczego a następnie jego rozwiązania, a koncentrują się na przedstawieniu wysokopoziomowych scenariuszy

wykorzystania sensorów inteligentnego miasta do zwiększenia świadomości sytuacyjnej w tracie operacji militarnych bądź po wystąpieniu katastrof naturalnych. W obu artykułach nie przedstawiono jednak żadnych wyników badań eksperymentalnych, zatem ich wartość naukowa jest znikoma – wspomniane jest tak kilka narzędzi np. ATAK, ale jedynie hasłowo. Ponadto, fragmenty artykułu [7] znajdują się także w pracy [8] (np. praktycznie cała 2 i 4 strona razem ze znajdującymi się tam obrazkami). Podsumowując, lepszym rozwiązaniem byłoby w opinii recenzenta umieszczenie w cyklu, zamiast jednego bądź obu tych artykułów publikacji wskazanej w autoreferacie jako [23], której Habilitant jest współautorem, a która dotyczy opisu procedury diagnostycznej dla bezpiecznej domeny sensorów.

Kolejny artykuł [9], który został opublikowany w czasopiśmie *Concurrency and Computation: Practice and Experience* (lista JCR) kontynuuje tematykę podjętą w [6] (Model II). Warto jednak podkreślić, że naukowa wartość dodana w tej pracy jest bardzo mała i skupia się faktycznie na opisie 2 procedur fazy przygotowawczej, natomiast znacząca część rysunków (np. Rys. 1-5, 19-20) oraz fragmenty tekstu (np. na str. 4) zostały przekopiowane z pracy [6]. Co nietypowe dla artykułów w czasopismach na tym poziomie w całej publikacji cytowanych jest jedynie 6 prac, co wyklucza możliwość właściwego przedstawienia stanu prac badawczych na świecie w tej tematyce i wskazania na tym tle w czym tkwi nowatorskie podejście autorów. Brakuje także wyników badań, a przedstawione środowisko badawcze opisane jest jedynie hasło i jest w zasadzie identyczne z tym zawartym w [6] (por. Rys. 20). Podsumowując, w mojej ocenie praca [9] jest jedynym z przykładów negatywnego zjawiska w środowisku naukowym tzw. *academic salami slicing*. W końcu warto także nadmienić, że artykuł [9] został wydany w numerze specjalnym czasopisma, którego Habilitant był jednocześnie zaproszonym edytorem.

W pracy [10] opublikowanej w czasopiśmie *Sensors* Habilitant w dalszym ciągu uszczegóławia koncepcje przedstawione w [6] i [9] poprzez doprecyzowanie działania części procedur z fazy wdrażania. W końcu w tej pracy pojawia się dość wyczerpujący przegląd stanu istniejących prac badawczych, jednak w konkluzji nie wskazuje jednoznacznie czym artykuł [10] się od nich różni. Ponadto, jak w poprzednio przedstawionych pracach cyklu także i ta korzysta z zawartości uprzednio opublikowanych artykułów cyklu np. Rys. 1-3 i 5-6 (z małymi modyfikacjami) zostały przekopiowane z [6], natomiast Rys. 4 z [9], to samo dotyczy fragmentów tekstu np. zawartość podpunktu 3.2.3 można odnaleźć także w [9]. Poza tymi mankamentami w artykule tym znajduje się także trochę nowych wyników badań związanych z wydajnością i skalowalnością proponowanego systemu.

W końcu, na zakończenie cyklu umieszczono krótki artykuł [11], który ukazał się w materiałach konferencji *International Conference on Military Communications and Information Systems* w 2019 roku, a w którym oprócz kolejny raz przypomnienia czym jest bezpieczna domena sensorów przedstawiono wyniki porównawcze opóźnień w transmisji dla Modelu I oraz Modelu II, które w zasadzie dowodzą, że kryptografia symetryczna jest szybsza niż asymetryczna – choć oczywiście w takim zastosowaniu i przy takiej implementacji i tak warto to było zbadać. Nie jest natomiast jasne, dlaczego takiego porównania nie zawarto już w pierwszej publikacji wprowadzającej Model II, czyli [6]. Na koniec tej pracy autorzy konkludują, że nadal proponowane rozwiązanie nie jest kompletne, co potwierdza tezę recenzenta o tym, że mimo zapewnień Habilitanta w autoreferacie nie jest ono kompleksowe. Podsumowując, w mojej opinii najlepszym rozwiązaniem byłoby połączenie zawartości publikacji [6] i [9-11] i opublikowanie ich w jednym porządnym artykule, co wymagało by także uzupełnienia metodyki badawczej, opracowania systematycznego planu badań, przeprowadzenia eksperymentów oraz

przedstawienia i dyskusji wyników.

Konkludując, w mojej ocenie przedstawione osiągnięcie naukowe w postaci omówionego powyżej cyklu publikacji, mimo pewnych walorów merytorycznych, nie może zostać uznane za dojrzałe i kompletne. Jak dowiedziono powyżej w kolejnych prezentowanych artykułach Habilitant dokonuje wielokrotnego powtórzenia tych samych koncepcji z bardzo małym bądź żadnym rozszerzeniem w stosunku do uprzednio proponowanych prac. Nie zawiera w nich także informacji, co tak naprawdę jest nowatorskim wkładem naukowym (problemem badawczym) i nie przedstawia rzetelnego porównania swojej koncepcji z istniejącymi rozwiązaniami znanymi z literatury. Ponadto, przeprowadzone i udokumentowane w części z tych prac badania eksperymentalne zrealizowane zostały w prostym środowisku badawczym, które w zasadzie w całym cyklu prac nie ulega zmianie (jedyna zmiana następuje w momencie przejścia z Modelu I na Model II), bądź nie jest to wystarczająco udokumentowane. Dodatkowo, w artykułach tych nie zamieszczono szczegółów zastosowanej metodyki badawczej oraz eksperymentalnego porównania z najlepszymi rozwiązaniami znanymi z literatury. W mojej opinii, dużo lepiej byłoby zawrzeć i skondensować proponowane pomysły oraz uzyskane wyniki w 1-2 artykułach opublikowanych w wysoko punktowanych czasopismach bądź na prestiżowych konferencjach, gdyż obecnie wkład w ramach poszczególnych publikacji jest bardzo rozdrobiony i mało znaczący. W rezultacie jednak oznaczałoby to, że całość cyklu składałaby się nie z 11 a jedynie z 2-3 publikacji, co nie wystarcza na habilitacyjny cykl publikacji ze znaczącym wkładem naukowym w dyscyplinie informatyka techniczna i telekomunikacja.

Podsumowując, w mojej ocenie, **przedstawione we wniosku dr inż. Janusza Furtaka osiągnięcie naukowe, mimo pewnych walorów merytorycznych, nie spełnia kryterium znaczącego wkładu w rozwój nauk technicznych w dyscyplinie informatyka techniczna i telekomunikacja.**

2. Ocena istotnej aktywności naukowej, dorobku dydaktycznego, organizacyjnego i popularyzatorskiego

Oprócz przedłożonego osiągnięcia naukowego ocenionego powyżej Habilitant posiada w swoim dorobku także inne artykuły, które zostały opublikowane już po uzyskaniu stopnia doktora. Jest to łącznie 6 rozdziałów w monografiach w języku angielskim (punktacja MNiSW od 5 do 20pkt.) oraz 2 rozdziały w języku polskim (każda po 4 pkt. MNiSW), członkostwo w redakcji naukowej jednej monografii (20 pkt. MNiSW) oraz 16 artykułów w czasopismach (w tym jedynie 3 w języku angielskim i aż 13 w języku polskim, głównie w Biuletynie Instytutu Automatyki i Robotyki – 6 pkt. MNiSW). Biorąc pod uwagę, że Habilitant uzyskał stopień doktora w październiku 1999 roku i doliczając do niego 11 publikacji z przedłożonego cyklu (2 artykuły w czasopismach z listy JCR, 8 w materiałach konferencyjnych i 1 rozdział w monografii) nie można uznać tego dorobku za imponujący – wskazuje on raczej na dość umiarkowaną aktywność naukową dr Furtaka po uzyskaniu stopnia doktora. Dość dużym mankamentem dorobku jest bardzo niska liczba publikacji ze współautorami spoza Polski – w sumie są to jedynie 2 publikacje (oba włączone do przedłożonego osiągnięcia naukowego), które są efektem działalności Habilitanta w grupach roboczych NATO Science and Technology Organization (IST-176 oraz IST-147) w latach 2016-2020. W rezultacie dość niskiej liczby publikacji (w tym w języku angielskim) uzyskana liczba cytowań oraz indeks Hirscha dr Furtaka pozostają na niskim, jak na ten etap kariery naukowej, poziomie (baza WoS: 14 cytowań bez autocytowań, H=3; baza Scopus: 56 cytowań bez autocytowań, H=4; Google Scholar: 142 cytowania z autocytowaniami, H=7).

Z kolei, jeśli chodzi o granty badawcze to dr Furtak nie uczestniczył w projektach międzynarodowych, ale w czasie swojej kariery naukowej dwukrotnie był kierownikiem zespołu WAT w projektach realizowanych przez konsorcja naukowe a ufundowanych przez NCBiR (w latach 2008-2010 oraz 2015-2018) oraz był jednym z wykonawców projektu NCBiR (w latach 2010-2012). Był także sześciokrotnie kierownikiem prac zlecanych przez WAT. Ponadto, dr Furtak brał udział w opracowywaniu kilku recenzji oraz opinii dla MON i NCBiR. Habilitant w latach 2010-2018 uczestniczył także w charakterze (współ)autora, kierownika zespołu oraz członka zespołu przy opracowywaniu demonstratorów, mechanizmów, czy rekomendacji/metodyk związanych z bezpieczeństwem szeroko pojętych sieci komunikacyjnych (łącznie 4 razy).

Dr inż. Janusz Furtak, po uzyskaniu stopnia doktora, nie wygłaszał żadnych wykładów zaproszonych ani plenarnych, ale miał łącznie 10 wystąpień na konferencjach międzynarodowych oraz krajowych, 11 razy występował w roli „chairman" na międzynarodowych workshopach oraz 24 razy był członkiem komitetów programowych konferencji i recenzentem 16 czasopism międzynarodowych i krajowych oraz rozdziałów w monografiach.

Z kolei w odniesieniu do osiągnięć dydaktycznych Habilitant posiada bardzo bogaty dorobek. Prowadził w trakcie swojej kariery zawodowej ponad 20 przedmiotów na dwóch różnych uczelniach (WAT oraz Prywatna Wyższa Szkoła Businessu) oraz kursy dokształcające dla MON. Ponadto, był członkiem komisji do spraw przygotowania programu studiów I oraz II stopnia na Wydziale Cybernetyki WAT. Był promotorem łącznie ponad 100 pracy dyplomowych. Prowadzeni przez niego dyplomanci dwukrotnie na poziomie krajowym zdobywali nagrody (w 2018 i 2019 roku). W przypadku aktywności organizacyjnych dr Furtak pełnił funkcje kierownika Zakładu (2003-2006), następnie zastępca dyrektora Instytutu (2008-2016) oraz dyrektora Instytutu od 2016 roku. Ponadto, uczestniczył on w tworzeniu Lokalnej Akademii Cisco w Instytucie Teleinformatyki i Automatyki Wydziału Cybernetyki WAT oraz był jej instruktorem. Warto podkreślić, że za osiągnięcia dydaktyczne i organizacyjne dr Furtak otrzymał nagrodę „Zasłużony nauczyciel WAT" od Rektora WAT (2002) oraz nagrodę „Zasłużony dla Wydziału Cybernetyki WAT" od Dziekana Wydział Cybernetyki (2018).

Jeśli chodzi natomiast o aktywności Habilitanta popularyzujące naukę to w autoreferacie takich nie stwierdzono.

Reasumując, w przypadku istotnych aktywności naukowych pozostały dorobek należy ocenić jako niewystarczający, aktywności popularyzujących naukę Habilitant nie posiada, natomiast osiągnięcia dydaktyczne i organizacyjne dr inż. Janusza Furtaka są bardzo dobre. Należy zatem stwierdzić, że wymagania stawiane kandydatom do uzyskania stopnia naukowego doktora habilitowanego w tym aspekcie spełnione są jedynie częściowo.

3. Podsumowanie i wniosek końcowy

W mojej ocenie przedłożone osiągnięcie naukowe Habilitanta dr inż. Janusza Furtaka, którym jest zbiór publikacji pt. „Metody podnoszenia poziomu bezpieczeństwa bezprzewodowych sieci sensorowych" należy ocenić negatywnie, gdyż publikacje zaprezentowane w zawartym cyklu nie stanowią wystarczającego twórczego wkładu w dyscyplinę informatyki technicznej i telekomunikacji. Także, jeśli chodzi o istotną aktywność naukową jest ona w mojej ocenie niewystarczająca, natomiast dorobek organizacyjny i dydaktyczny oceniam jako bardzo dobry.

W związku z powyższym, moim zdaniem, przedstawiony dorobek Habilitanta nie spełnia kryteriów wymaganych do uzyskania stopnia doktora habilitowanego. Dlatego też nie popieram wniosku o nadanie Panu dr inż. Januszowi Furtakowi stopnia doktora habilitowanego w dziedzinie nauk technicznych, w dyscyplinie informatyka techniczna i telekomunikacja.

dr hab. inż. Wojciech Mazurczyk, prof. uczelni