Politechnika Warszawska
Wydział Elektroniki i Technik Informacyjnych

Warszawa, 28 marca 2017 r.

D z i e k a n a t

Uprzejmie informuję, że na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej odbędzie się w dniu 11 kwietnia 2017 r. publiczna obrona rozprawy doktorskiej

mgr inż. Marcina Pawłowskiego

temat: *„Lightweight, scalable and manageable link-layer authentication for security of the process of acquiring network access for the Internet of Things devices”.*

promotor – prof. dr hab. inż. Maciej Ogorzałek z Uniwerystetu Jagiellońskiego

recenzenci:
prof. dr hab. inż. Adam Dąbrowski z Politechniki Poznańskiej
prof. dr hab. inż. Jacek Kitowski z Akademii Górniczo-Hutniczej

Obrona odbędzie się w dniu 11 kwietnia 2017 r. w sali 116 na Wydziale Elektroniki i Technik Informacyjnych – Gmach im. Janusza Groszkowskiego, Warszawa, ul. Nowowiejska 15/19; początek godz. 10^{30}.

Po adresem: **www.elka.pw.edu.pl/Wydzial/Rada-Wydzialu/Harmonogram-obron-doktorskich-streszczenia-i-recenzje** zapewniony jest na stronie Wydziału dostęp do tekstów streszczenia rozprawy i recenzji, jak również do tekstu rozprawy umieszczonej w Bazie Wiedzy Politechniki Warszawskiej.

Dziekan

prof. dr hab. inż. Krzysztof Zaremba

Tytuł rozprawy:

Lekkie, skalowalne i zarządzalne uwierzytelnianie w warstwie łącza dla bezpieczeństwa procesu uzyskiwania dostępu do sieci urządzeń Internetu Rzeczy

Autor:

mgr inż. Marcin Piotr Pawłowski

Promotor:

Prof. dr hab. inż.. Maciej Ogorzałek *(Uniwersytet Jagielloński)*

Streszczenie rozprawy:

Dysertacja porusza kwestie bezpieczeństwa Internetu Rzeczy (Obiektów) z naciskiem na zaprojektowanie i optymalizacje mechanizmów uwierzytelniania warstwy łącza. Praca jest podzielona na trzy części.

Pierwsza część poświęcona jest zaprojektowaniu oraz optymalizacji zestawu protokołów warstwy łącza IEEE 802.15.4. Rzeczone protokoły bazują na standardzie uwierzytelniania IEEE 802.1X i są zoptymalizowane pod katem zminimalizowania liczby wykorzystywanych bajtów podczas uwierzytelniania oraz zwiększenia dostępnej przestrzeni przeznaczonej na dane uwierzytelniające.

Druga cześć pracy jest poświęcona zaprojektowaniu jak i optymalizacji zbioru mechanizmów i algorytmów uwierzytelniających. Wyniki tej części pracy są, komplementarne do zaprojektowanych protokołów warstwy łącza przedstawionych w pierwszej części pracy. Tym samym stworzone jest całościowe rozwiązanie uwierzytelniające warstwy łącza zabezpieczające proces uzyskiwania dostępu do sieci w Internecie Rzeczy.

Trzecia cześć pracy jest poświęcona zaprojektowaniu a także optymalizacji metod uzyskiwanie liczb losowych z wbudowanych sensorów urządzeń Internetu Rzeczy w celu poprawienia bezpieczeństwa generatorów liczb losowych ograniczonych urządzeń Internetu Rzeczy.

Prof. dr hab. inż. Adam Dąbrowski
tytuł, stopień, imię i nazwisko

Poznań, 30.01.2017 r.
data

miejsce pracy
Politechnika Poznańska
Wydział Informatyki
Pracownia Układów Elektronicznych
i Przetwarzania Sygnałów

KWESTIONARIUSZ- RECENZJA ROZPRAWY DOKTORSKIE J DLA RADY WYDZIAŁU ELEKTRONIKI I TECHNIK INFORMACYJNYCH POLITECHNIKI WARSZAWSKIEJ

Tytuł rozprawy: Lightweight, scalable manageable link-layer authentication for security of the process of acquiring network access for the Internet of Things devices

Autor rozprawy: mgr inż. Marcin Piotr Pawłowski

1. Jakie zagadnienie naukowe jest rozpatrzone w pracy /teza rozprawy/ i czy zostało ono dostatecznie jasno sformułowane przez autora? Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?

Oceniana rozprawa doktorska jest poświęcona nowatorskim zagadnieniom rozwijania technologii tzw. Internetu rzeczy (inaczej przedmiotów, ang. Internet of Things) i jako taka ma charakter teoretyczny, chociaż omawiane pomysły, metody i algorytmy dotyczące poprawy efektywności, zarządzania i bezpieczeństwa danych, przy jednoczesnym obniżaniu kosztów poszczególnych węzłów sieci, powiązanych z identyfikowalnymi przedmiotami, w tym ograniczaniu oferowanych w nich zasobów obliczeniowych, są sprawdzane doświadczalnie.

Głównym celem przeprowadzonych rozważań było badanie oraz poszukiwanie nowych rozwiązań problemów związanych z bezpieczną autentykacją i akwizycją danych, z niezawodnym dostępem do sieci, przy założeniu ograniczeń dotyczących poboru energii, a także zapewnieniu skalowalności, efektywności działania i w pełni automatycznej obsługi.

Doktorant w szczególności zajął się minimalizacją ilości transmitowanych danych, koniecznych do autentykacji urządzeń w celu nawiązywania bezpiecznych połączeń i uzyskania dostępu do zasobów Internetu rzeczy.

2. Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł / w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle /świadczący o dostatecznej wiedzy autora. Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?

Nad zagadnieniami przedstawionymi w ocenianej rozprawie Doktorant pracował w dużych międzynarodowych zespołach badawczych, skupionych w wiodących międzynarodowych ośrodkach badawczych, np. w Hiszpanii, Szwajcarii, Luksemburgu i innych. Analiza źródeł literaturowych została więc przeprowadzona wzorowo z uwzględnieniem wszystkich najnowszych osiągnięć poznawczych, aplikacyjnych i przemysłowych w skali światowej. Bogaty spis literatury (101 pozycji podsumowujących sam autoreferat) jak i wyczerpujące spisy literatury w załączonych publikacjach i wynikająca z nich obszerna analiza stanu wiedzy i zastosowań Internetu rzeczy świadczy o dużej wiedzy i wysokich kompetencjach Doktoranta.

3. **Czy autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?**

W rozprawie zaprezentowane zostały nowe rozwiązania architektoniczne i algorytmiczne do tworzenia bezpiecznych połączeń np. w warstwach sieciowych i łącza danych do zastosowań w nowoczesnych technologiach Internetu rzeczy.

Doktorant zaproponował ulepszenia mechanizmów autentykacji przedmiotów / podmiotów nawiązujących połączenie i mechanizmów komunikacyjnych prowadzące do minimalizacji ilości przesyłanych w tym celu nadmiarowych danych (ang. minimum data transmission overhead), przy zachowaniu skalowalności transmisji danych np. według protokołu IEEE 802.IX.

Rozważania prowadzono uwzględniając trzy integralnie związane i wzajemnie uzupełniające się aspekty: schematy protokołów, metody transmisji koniecznych danych i entropię przesyłanych proponowanych danych.

Dlatego z pełnym przekonaniem oceniam, że Doktorant zaproponował skuteczne rozwiązania rozważanych problemów i w pełni zrealizował zakładane cele rozprawy.

4. **Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu techniki reprezentowanych przez literaturę światową?**

Rozważania zawarte zarówno w autoreferacie napisanym przez Doktoranta (rozdziały 1 – 4) jak i w przedłożonych czterech artykułach (zamieszczonych w rozdziałach 5 – 8 i w dodatku A) opublikowanych np. w czasopiśmie IEEE Journal of Selected Areas in Communications, indeksowanym w bazie JCR i innych wiodących czasopismach a także w czterech komunikatach konferencyjnych, których Doktorant jest współautorem (w większości przypadków pierwszym lub wiodącym współautorem), świadczą o dużym, oryginalnym dorobku Doktoranta, nawiązującym do zarówno światowego stanu wiedzy jak i światowego poziomu techniki w zakresie wybranych rozwiązań technologicznych stosowanych w urządzeniach Internetu rzeczy.

Na wysoką ocenę zasługują zwłaszcza trzy oryginalne hipotezy badawcze sformułowane i uzasadnione przez Doktoranta: tworzenie rozszerzalnego protokołu autentykacji jest możliwe za pomocą opracowanego adaptacyjnego algorytmu warstwy łącza (hipoteza 1), opracowany mechanizm autentykacji pozwala na redukcję ilości transmitowanych danych (hipoteza 2), ten mechanizm pozwala zaś na redukcję danych podczas procesu autentykacji dzięki właściwemu doborowi protokołu transmisyjnego po stronie serwera autentykacji (hipoteza 3).

5. **Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników /zwięzłość, jasność, poprawność redakcyjna rozprawy/?**

Zarówno poziom naukowy rozprawy jak i znaczny dorobek naukowy Doktoranta oceniam bardzo wysoko. Wysoko oceniam także pracę zespołową Doktoranta w zespołach międzynarodowych i umiejętność prezentowania wyników badań w postaci wartościowych artykułów naukowych, lokowanych w czasopismach o wysokiej randze naukowej jak i w postaci tekstów referatów umieszczonych w materiałach wiodących konferencji naukowych.

Dość zwięzły ale ogólnikowy, chaotyczny i mało przekonujący tekst autoreferatu zawartego w rozdziałach 1 – 4 rozprawy, o czym piszę bardziej szczegółowo w p. 6 niniejszej recenzji, uważam jednak za słabszą część ocenianej rozprawy.

6. Jakie są słabe strony rozprawy i jej główne wady?

Słabą stroną recenzowanej rozprawy jest tekst autoreferatu Doktoranta zawarty na stronach od 7 do 55 tekstu rozprawy, podzielony na rozdziały od 1 do 4. Tekst ten jest napisany chaotycznie. Zawiera zbyt wiele ogólnie znanych informacji wprowadzających. W części zawierającej opis dokonań Doktoranta jest zaś powierzchowny i zbyt ogólnikowy.

Ponadto kompozycja i struktura tego tekstu jest niezrozumiała i utrudnia zaznajamianie się z zawartymi w nim informacjami ze względu na szereg powtórzeń tych samych nazw podrozdziałów a także ze względu na kończenie poszczególnych części tekstu licznymi częściowymi podsumowaniami, zaciemniającymi śledzenie osiągnięć Doktoranta. Najczęstszymi powtarzającymi sie tytułami podrozdziałów są np.: „security", „methods", „entropy".

7. Jaka jest przydatność rozprawy dla nauk technicznych?

Mimo przedstawionych i opisanych powyżej pewnych słabych stron i wad tekstu rozprawy, osiągnięte przez Doktoranta wyniki, jak już to wcześniej podkreśliłem, oceniam bardzo wysoko. Opracowane algorytmy zwłaszcza dotyczące autentykacji danych są moim zdaniem bardzo ważnym etapem rozwoju technologicznego nowoczesnego Internetu rzeczy i mają dużą potencjalną przydatność praktyczną.

Ocenianą przeze mnie rozprawę, dzięki dużemu zaangażowaniu Doktoranta, promotora Pana Profesora Macieja Ogorzałka i innych współpracowników kilku znakomitych ośrodków badawczych, z którymi obydwaj współpracują, można wręcz zaliczyć do prac o charakterze pionierskim.

8. Do której z następujących kategorii Recenzent zalicza rozprawę:

a/ nie spełniająca wymagań stawianych rozprawom doktorskim przez obowiązujące przepisy

b/ wymagająca wprowadzenia poprawek i ponownego recenzowania

c/ spełniająca wymagania

d/ spełniająca wymagania z wyraźnym nadmiarem

e/ wybitnie dobra, zasługująca na wyróżnienie ×

Powyższe pytania mają charakter pomocniczy. Wskazane jest takie formułowanie treści recenzji, by można j ą było odczytywać bez przeczytania pytań.

podpis

Adam Dąbrowski

Prof. dr hab. inż. Jacek Kitowski
Katedra Informatyki
Wydział Informatyki, Elektroniki i Telekomunikacji
Akademia Górniczo-Hutnicza
Al. Mickiewicza 30, 30-059 Kraków

Kraków, 9.12.2016

RECENZJA ROZPRAWY DOKTORSKIEJ DLA RADY WYDZIAŁU ELEKTRONIKI I TECHNIK INFORMACYJNYCH POLITECHNIKI WARSZAWSKIEJ

Tytuł rozprawy: Lightweight, scalable and manageable link-layer authentication for security of the process of acquiring network access for the Internet of Things devices

Autor rozprawy: mgr inż. Marcin Piotr Pawłowski

1. *Jakie zagadnienie naukowe jest rozpatrywane w pracy (teza rozprawy) i czy zostało ono dostatecznie jasno sformułowane przez autora? Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?*

Rozprawa dotyczy współczesnej problematyki zastosowań informatyki w odniesieniu do tzw. Internetu Rzeczy, czyli możliwie szerokiego wykorzystania Internetu do połączenia i zapewnienia współpracy obiektów bądź przedmiotów wcześniej za sobą nie współpracujących. Jest to zagadnienie aktualne, rozwijane w wielu ośrodkach naukowych i przemysłowych na świecie, jak również będące przedmiotem tematyki konkursów ogłaszanych przez różnorodne instytucje, w tym Komisję Europejską. Sama koncepcja wydaje się już być wystarczająco rozwinięta, niemniej szereg elementów wymaga dalszego rozwoju. Jednym z podstawowych elementów każdej infrastruktury bądź aplikacji rozproszonej jest zapewnienie odpowiedniego poziomu bezpieczeństwa usług, najczęściej rozumianych jako ochrona przed niepowołanym dostępem lub dodatkowo -- w przypadku usług udostępniania danych – ochrona przed utratą lub zniszczeniem.

Doktorant skupił się w swoich badaniach na zaprojektowaniu i optymalizacji zbioru mechanizmów i algorytmów uwierzytelnienia warstwy łącza. Stanowi to rozwiązanie całościowe, wsparte dodatkowo metodami uzyskiwania liczb losowych z sensorów urządzeń Internetu Rzeczy, jako niezbędnych dla realizacji protokołu uwierzytelnienia. Biorąc pod uwagę standard uwierzytelnienia IEEE 802.1X zaproponowano metodologię badań uwzględniającą kategorie związane z protokołem, metodami oraz entropią i na tej podstawie

sformułowano jasno i trafnie szczegółowe hipotezy badawcze, będące przedmiotem rozważań kolejnych części pracy. Zatem tematyka Rozprawy jest ważna i współczesna.

Rozprawę stanowi zbiór 4 publikacji współautorskich opublikowanych w roku 2015 w dobrych czasopismach z wysokim wskaźnikiem wpływu (Web of Science *Impact Factor*) oraz jednego doniesienia konferencyjnego przedstawionego na międzynarodowej konferencji (indeksowanego wysoko przez prestiżowy serwis (http://www.conferenceranks.com/). Część wprowadzająca do zbioru nie zawiera tezy, natomiast wspomniane powyżej hipotezy badawcze układają się w spójną całość, nadając Rozprawie charakter teoretyczno-projektowy, której wyniki potwierdzają postawione hipotezy.

2. *Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł (w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle), świadczący o dostatecznej wiedzy autora? Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonujący?*

Lektura Rozprawy nie pozostawia wątpliwości co do wiedzy Autora w odniesieniu do zagadnień Internetu Rzeczy, a bardziej szczegółowo – do problematyki bezpieczeństwa i autentykacji w tym zakresie problemowym. Ze względu na strukturę rozprawy analiza źródeł przedstawiona została w dwóch miejscach – w sposób ogólny w Rozdziale wstępnym (101 pozycji cytowanych) oraz szczegółowo w publikacjach stanowiących kolejne rozdziały Rozprawy. Ze względu na zakres tematyczny Rozprawy szczególną wagę przywiązano w przeglądzie literatury do bezpieczeństwa wstępnych procedur nawiązywania połączenia między obiektami sieci Internetu Rzeczy (*bootstrapping security*) wykazując niedostatki istniejących rozwiązań. Zwrócono uwagę na stosunkowo niską przydatność protokołu IP ze względu na narzut komunikacyjny i potencjalnie wysokie zużycie energii, mające znaczenie w urządzeniach o niewielkich zasobach energetycznych oraz problem adresacji. Wskazano na potrzebę rozwiązań „lżejszych", wykorzystujących tokeny autoryzacyjne i/lub modyfikację implementacji protokołów ECC (*elliptic curves cryptography*). Wnioski z przeglądu literatury przedmiotu przedstawione są jasno i przekonująco.

3. *Czy autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?*

W Rozprawie wyróżnić można trzy podstawowe zagadnienia, którym jest ona poświęcona, a to: projekt protokołów warstwy łącza IEEE 802.15.4 z wykorzystaniem standardu IEEE 802.1X, projekt mechanizmów i optymalizacji algorytmów uwierzytelniających oraz projekt i optymalizacja generacji liczb losowych uzyskiwanych z obiektów Internetu Rzeczy.

Pierwsze zagadnienie wraz z wynikami przedstawione zostało w Rozdziale 5 (z najważniejszymi wynikami umieszczonymi na Rys. 4-5 i Rys. 6-9), pokazując oszczędności w długości nagłówka i poprawę w wykorzystaniu sieci (co jest rezultatem opracowania warstwy Slim EAPOL), jak również w Rozdziale 7 (Rys. 6-7), w którym uzyskano obniżenie długości nagłówka w protokole EAP poprzez redukcję nadmiarowości w nagłówku. Dodatkowo, zmniejszenie liczby pakietów osiągnięto poprzez analizę protokołu RADIUS vs. EAP skutkujące zwiększeniem przepływności 9-10% (dyskutowane w Dodatku A, Tabela 1). Drugie zagadnienie w kontekście autentykacji i autoryzacji jest częściowo dyskutowane w Rozdziale 5 (Rys. 10-11), a szerzej w Rozdziale 6, gdzie zaproponowano kombinację lekkiego protokołu

autentykacji z protokołem ECC. W przekonaniu recenzenta główny ciężar naukowy tego fragmentu polega na teoretycznych badaniach dotyczących optymalizacji ECC i ich użyciu w schemacie Schnorra. Dla kompletności badań, został także zaadoptowany i zbadany protokół EAP-TEPANOM, wstępnie opracowany na University of Applied Sciences (Szwajcaria), wykazując dużą redukcję w zakresie liczby przesyłanych pakietów i danych (omówiony w Rozdziale 7) . Ten fragment osiągnięć wskazuje bezpośrednio na korzyści płynące z możliwej współpracy z wytwórcą. Ostatnie z zagadnień, ważne ze względu na ograniczone zazwyczaj zasoby obiektów Internetu Rzeczy, stanowi przedmiot szczegółowych badań zawartych w Rozdziale 8. Opracowana metoda charakteryzuje się bardzo wysoką entropią, co korzystnie wpływa na zagadnienia uwierzytelnienia w warstwie łącza.

Warto podkreślić, że przedstawione rezultaty badań, o dużych znaczeniu poznawczym i praktycznym, zostały opublikowane we wiodących czasopismach z zakresu telekomunikacji, a przedstawione w Rozprawie rozdziały 5-8 i dodatek A zawierają wprost ich treści. Z podsumowania załączonego do tekstu Rozprawy wynika przeważający udział Autora w załączonych publikacjach (o udziale odpowiednio: 40, 90, 60, 90 i 90%).

Na podstawie powyżej wymienionych faktów można zatem stwierdzić, że Doktorant rozwiązał postawione zagadnienia, a przyjęte założenia i metody były właściwe.

4. *Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu techniki reprezentowanych przez literaturę światową?*

Główne osiągnięcia Autora stanowią oryginalne rezultaty uzyskane przy weryfikacji postawionych hipotez badawczych. Do najważniejszych z nich zaliczam:

a. Zaprojektowanie oraz optymalizacja protokołów warstwy łącza IEEE 802.15.4 wykorzystujących uwierzytelnienie standardu IEEE 802.1X, co skutkuje minimalizacją liczby wykorzystanych bajtów i lepszym wykorzystaniem przestrzeni na dane uwierzytelniające. Redukcja kosztów transmisji danych potencjalnie wpływa na niższe zużycie energii podczas tego procesu.

b. Opracowanie algorytmów uwierzytelniających wykorzystujących zarówno uwierzytelnienie jak i autoryzację, a zatem dotyczących nawiązywania połączenia jak i jego operacyjności.

c. Optymalizacja ECC (*elliptic curve cryptography*) przewidziana do współpracy z protokołem warstwy łącza oraz wykorzystanie protokołu TEPANOM wskazującego na zasadność udziału wytwórcy w procesie tworzenia rozwiązań bezpiecznych i potencjalnym wykorzystaniem w środowiskach chmur obliczeniowych.

d. Przeprowadzenie badań i uzyskanie bardzo dobrych wyników w zakresie wykorzystania obiektów wchodzących w skład Internetu Rzeczy jako źródeł liczb pseudolosowych o wysokiej entropii.

Wymienione osiągnięcia są oryginalne i znaczące, na nich więc opieram *ogólnie pozytywną ocenę pracy*. Stanowią one odpowiedź na postawione problemy badawcze i wspierają rozwój Internetu Rzeczy w zakresie podniesienia poziomu bezpieczeństwa systemów i usług.

5. *Czy autor wykazał umiejętność poprawnego i przekonującego przedstawienia uzyskanych przez siebie wyników (zwięzłość, jasność, poprawność redakcyjna rozprawy)?*

Przedstawiona do recenzji Rozprawa, wydana drukiem przez Politechnikę Warszawską, napisana została w języku angielskim. Jest starannie przygotowana zarówno pod względem zarówno językowym jak i edytorskim. Liczy ona 156 stron tekstu i składa się z 8 rozdziałów, jednego dodatku oraz spisu 101 pozycji bibliograficznych z ostatnich lat. Pierwsze 4 rozdziały są oryginalne, pozostałe wraz z dodatkiem są opublikowanymi artykułami na podstawie których przygotowana jest Rozprawa.

W części wstępnej, oprócz wprowadzenia w tematykę Internetu Rzeczy nakreślono problemy i cele pracy wraz z przyjętą poprawnie metodologią oraz założonymi hipotezami badawczymi. Główny tekst poprzedza krótkie streszczenie w języku polskim, odzwierciedlające w sposób ogólny zasadniczy tekst Rozprawy. Rozdziały 3 i 4 stanowią przegląd uzyskanych wyników (omawianych szczegółowo w Rozdziałach 5-8 i Dodatku A) oraz zbiorcze wnioski i plany dalszych badań. Część wstępna dobrze przybliża szczegółowe zagadnienia, będące przedmiotem opublikowanych wcześniej artykułów i wchodzące w skład kolejnych rozdziałów, ułatwiając lekturę.

Podkreślić wysoki poziom teoretyczny prezentowanych badań, dobrze świadczący o dojrzałości Autora i jego przygotowaniu do pracy naukowej.

6. *Jakie są słabe strony rozprawy i jej główne wady?*

Do formalnych niedostatków Rozprawy należy powołanie się w Tabeli 3.1 na pozycje literaturowe, które nie zostały dołączone do cyklu publikacji. Dotyczy to pozycji w częściach Protokół (konferencje 2 i 4), Metody (konferencja 2) i Entropia (konferencja 3). Ten sam problem dotyczy analizy danych umieszczonych w Tabeli 3.3 Rozprawy. Brak załączenia publikacji jest niekorzystny dla Autora, gdyż jego udział w wymienionych pracach jest oceniony na 90%. Pewnym mankamentem jest brak krótkiej charakterystyki udziału merytorycznego Autora w publikacjach zawartych w Tabelach 3.2 i 3.3.

W Rozdziale 3.2.3 wskazano na możliwość poprawy transmisji poprzez eliminację istniejących redundancji w nagłówkach protokołu EAP. Brakuje dyskusji poprawności takiej operacji, innymi słowy uzasadnienia, że eliminacja wskazanej redundancji nie spowoduje obniżenia funkcjonalności protokołu.

Do niedostatków Rozprawy również należy zaliczyć brak dyskusji na temat perspektyw zastosowania wyników badań w praktyce.

7. *Jaka jest przydatność rozprawy dla nauk technicznych?*

Problematyka badawcza dobrze wpisuje się we współczesny rozwój społeczeństwa informacyjnego, w którym wykorzystanie środków i narzędzi współczesnych technologii informatycznych jest już na tyle holistyczne, że – jak się wydaje – w najbliższej przyszłości stanie się niemal transparentne dla człowieka. W tym obszarze Internet Rzeczy zdobywa szybko coraz większa popularność, z czym wiąże się konieczność zapewnienia wysokiego

poziomu autonomiczności urządzeń, bezpieczeństwa komunikacji i sterowania oraz efektywnego zużycia zasobów energetycznych.

W tym obszarze problemowym dobrze lokuje się recenzowana praca, o dużym znaczeniu poznawczym w zakresie nauk technicznych i implementacyjnym, choć zapewne jeszcze ze stosunkowo odległym bezpośrednim zastosowaniu praktycznym. Wiąże się to z opracowaniem nowych protokołów komunikacyjnych i algorytmów, które powinny uzyskać akceptację środowiska. Propozycje przedstawione w Rozprawie są w kontekście przedstawionych trendów wartościowe i przydatne.

8. *Do której z następujących kategorii Recenzent zalicza rozprawę:*
   a. *Nie spełniającą wymagań stawianych rozprawom doktorskim przez obowiązujące przepisy*
   b. *Wymagająca poprawek i ponownego recenzowania*
   c. *Spełniająca wymagania*
   d. *Spełniająca wymagania z wyraźnym nadmiarem*
   e. *Wybitnie dobra, zasługująca na wyróżnienie*

Należy wyraźnie zaznaczyć, że podane w punkcie 6 recenzji słabe strony Rozprawy nie kwestionują słuszności przyjętych koncepcji ani też nie wpływają w sposób istotny na poznawcze i utylitarne wartości zrealizowanych badań. Ich uwzględnienie może okazać się korzystne w dalszej działalności naukowej dotyczącej zbliżonych zagadnień. W Rozprawie Autor proponuje całościowe podejście do zagadnienia bezpieczeństwa Internetu Rzeczy ze szczególnym uwzględnieniem projektu i optymalizacji mechanizmów uwierzytelnienia łącza proponując nowatorskie rozwiązania w zakresie protokołów i algorytmów uwierzytelniających wspartych optymalizacją metod generacji liczb losowych przez obiekty Internetu Rzeczy.

Uważam, że Rozprawa spełnia wymagania z wyraźnym nadmiarem i stawiam wniosek o dopuszczenie jej Autora do dalszych etapów przewodu doktorskiego.