dr hab. inż. Wojciech Mazurczyk

Instytut Telekomunikacji
Wydział Elektroniki i Technik Informacyjnych
Politechnika Warszawska

Warszawa, 10.12.2018

RECENZJA ROZPRAWY DOKTORSKIEJ DLA RADY WYDZIAŁU
Department of Informatics, Polish-Japanese Academy of Information Technology
w Warszawie

Tytuł rozprawy: **Wieloaspektowe modelowanie rozproszonych ataków odmowy usługi dla architektury Internetu Rzeczy**

Autorka rozprawy: **mgr inż. Katarzyna Mazur**

1. Problematyka naukowa oraz przedmiot rozprawy

Tematyka rozprawy koncentruje się na wybranych aspektach bezpieczeństwa sieciowego, a w szczególności jej problematyka naukowa dotyczy wieloaspektowej analizy rozproszonych ataków odmowy usługi (Distributed Denial of Service, DDoS) w środowisku systemów Internet of Things (IoT). Zaproponowana w pracy przez Doktorantkę analiza wielopoziomowa pozwala dobrać parametry sieci w taki sposób, aby ograniczyć skutki tego typu ataków przy jednoczesnym zapewnieniu jak najwyższej dostępności sieci oraz zachowaniu odpowiedniego poziomu bezpieczeństwa.

Tematyka podjęta w rozprawie jest ważna i akutalna, gdyż w ostatnich latach można zaobserwować wręcz lawinowy wzrost udanych cyberataków typu (D)DoS na infrastrukturę sieciową firm, instytucji, państw, a także użytkowników indywidualnych. W przypadku utrzymania się takiego stanu rzeczy, realnym długoterminowym skutkiem może być spadek zaufania użytkowników do wykorzystywania sieci teleinformatycznych, a co za tym idzie potencjalne straty socjo-ekonomiczne.

Recenzowana rozprawa doktorska poświęcona jest w szczególności próbie scharakteryzowania nowych aspektów zagrożeń takich jak, przykładowo, DDoS w systemach z ograniczonymi zasobami takimi jak WSN, IoT, itp., co biorąc pod uwagę obecny trend rozwoju sieci teleinformatycznych i wykorzystywanych tam urządzeń świadczy o aktualności i istotności podjętej przez Doktorantkę tematyki badawczej.

W rozprawie w sposób bezpośredni nie sformułowano tezy pracy – zamiast tego w podrozdziale 1.5 wskazano cel główny pracy, który zdefiniowano jako konieczność wykazania, że: „wieloaspektowa analiza bezpieczeństwa systemów IoT, pozwala określić nowe zagrożenia dotyczące ataków typu DDoS". Jako główne narzędzie w osiągnięciu tego celu Autorka wykorzystała dedykowany język Quality of Protection Modeling Language (QoP-ML), który pozwala wykonywać tego typu analizy systemów teleinformatycznych. Ponadto, Doktorantka uzależniła osiągnięcie celu głównego rozprawy poprzez realizację czterech celów pośrednich. Pierwszy z nich polegał na sformułowaniu metodyki służącej do uzyskiwania niezawodnych metryk bezpieczeństwa pozwalających na scharakteryzowanie wpływu środków ochrony na jakość zabezpieczeń urządzeń w środowisku IoT. Drugi z nich

został określony jako stworzenie modelu systemu monitorowania linii wysokonapięciowych (system typu *smart grid*) wraz ze wskazaniem potencjalnych zagrożeń wpływających na dostępność takiego systemu, a które odnoszą się przede wszystkim do jego procesu przetwarzania. Trzecim celem pośrednim było przeprowadzenie wieloaspektowej analizy wolumetrycznych ataków DDoS na sieci WSN wraz z oceną ich wpływu na funkcjonowanie atakowanej sieci. Ostatnim celem była budowa systemu wspomagania decyzji pozwalającego na wykonanie kompleksowej analizy różnych atrybutów złożonych, heterogenicznych środowisk cechujących się dużą dynamiką (takich jak np. IoT).

2. Analiza treści rozprawy oraz uzyskanych wyników

Rozprawa została przygotowana częściowo w języku polskim (rozdziały 1 i 3) oraz w języku angielskim (rozdział 2) i składa się z łącznie z 3 rozdziałów oraz bibliografii. Całość pracy obejmuje 121 stron. Wyniki zasadniczych prac badawczych Doktorantki przedstawiono w rozdziale 2.

Pierwszy rozdział rozprawy stanowi wprowadzenie do poruszanej problematyki i obejmuje przedstawienie motywacji, celu głównego pracy oraz syntetycznego podsumowania oryginalnego wkładu Doktorantki w aktualny stan wiedzy w dziedzinie bezpieczeństwa sieciowego, a w szczególności w wieloaspektowej analizie ataków DDoS w sieciach IoT.

Stan dotychczasowych badań w głównym zakresie tematycznym rozprawy przedstawiono w rozdziale stanowiącym wprowadzenie do pracy (rozdział 1) oraz częściowo także w rozdziale 2 – w każdym z prezentowanych w ramach rozprawy artykułów naukowych. Na tej podstawie można stwierdzić, że Doktorantka wykazała się bardzo dobrą znajomością stanu wiedzy w dziedzinie będącej przedmiotem pracy oraz umiejętnością analizy literatury i poprawnego formułowania wniosków na jej podstawie.

W rozdziale 2 Autorka przedstawiła jako zasadniczą część swojej rozprawy cztery, tematycznie spójne artykuły w języku angielskim, w których we wszystkich jest pierwszym autorem, a które zostały opublikowane w czasopismach z tzw. listy filadelfijskiej. Wszystkie one związane są z główną tematyką rozprawy, czyli wieloaspektowym modelowaniem rozproszonych ataków odmowy usługi w sieciach IoT.

W pierwszym artykule pt. "The robust measurement method for security metrics generation" Doktorantka zaproponowała modyfikację normy ISO/IEC 27004 poprzez wzbogacenie modelu wykonywania pomiarów o metody kontrolowania ich jakości. Ulepszony przez Autorkę model pozwala uzyskiwać powtarzalne i rzetelne pomiary, co w rezultacie powoduje, że zebrane metryki charakteryzują się większą niezawodnością. Ponadto, zaprezentowany rozszerzony model zawiera także elementy odpowiedzialne za walidację metod wykonywania pomiarów, weryfikację bazowych wartości pomiarowych, a także sprawdzenie pomiarów pochodnych względem podstawowych. W celu sprawdzenia poprawności zmodyfikowanego przez Autorkę modelu w omawianym artykule przedstawiono jego przykładowe zastosowanie poprzez obliczenie współczynników wydajnościowych dla wybranych modułów kryptograficznych z wykorzystaniem zrealizowanego na potrzeby tej pracy automatycznego narzędzia o nazwie CMTool.

W kolejnym artykule prezentowanym jako osiągnięcie ocenianej rozprawy pt. „Secure and Time-Aware Communication of Wireless Sensors Monitoring Overhead Transmission Lines" opisano jakie parametry techniczne oraz wymagania są niezbędne do monitorowania i raportowania stanu sieci energetycznych (smart grids) z wykorzystaniem inteligentnych urządzeń. W pracy zaproponowano bezpieczny a zarazem efektywny sposób przesyłania danych zebranych z wykorzystaniem bezprzewodowej sieci sensorowej w środowisku sieci

energetycznej. Opracowana metoda koncentruje się przede wszystkim na przekazywaniu informacji pomiarowych tak, aby dotarły one do celu w odpowiednim czasie (mimo możliwości wystąpienia potencjalnych zagrożeń i zakłóceń z nimi związanych). Podstawowym założeniem zaproponowanego rozwiązania był podział WSN wykonującej pomiary energetycznej linii transmisyjnej na klastry logiczne. W ramach takiego klastra wyróżniono sensor główny, który jest odpowiedzialny za odebranie danych od pozostałych węzłów (tj. sensorów rozmieszonych na słupie elektrycznym) i przekazanie pakietów zawierających dane pomiarowe do sensora rezydującego na sąsiednim słupie lub bezpośrednio do stacji bazowej. Następnie korzystając z języka QoP-ML utworzono model takiego rozwiązania, a następnie przeprowadzono jego wieloaspektową analizę.

W artykule „Multilevel Modeling of Distributed Denial of Service Attacks in Wireless Sensor Networks" Doktorantka z zastosowaniem języka QoP-ML zamodelowała i zaimplementowała przykładową sieć WSN, której rolą było wykonywanie pomiarów wybranych charakterystyk historycznego budynku. Taka sieć sensorów została następnie poddana rozproszonemu atakowi odmowy usługi typu wolumetrycznego. Następnie dla tak przyjętego scenariusza przeprowadzono wielopoziomową analizę uwzględniającą między innymi takie elementy jak: wpływ ataku DDoS na wydajność sieci, zużycie jej zasobów energetycznych, czas życia urządzeń oraz zapewnianie odpowiednich usług bezpieczeństwa. W pracy tej, dzięki przeprowadzonej analizie, Autorka wskazała nowy rodzaj ataku DDoS, a mianowicie opóźniony rozproszony atak odmowy usługi (DDDoS), którego skutki działania są możliwe do wykrycia dopiero po pewnym czasie. Jest to szczególnie groźne dla sieci sensorowej, ponieważ posiada ona ograniczone zasoby energetyczne, które w wyniku takiego ataku mogą ulec wyczerpaniu, a w konsekwencji może dojść do całkowitego sparaliżowania jej funkcjonowania.

W czwartym, ostatnim artykule pt. „On Security Management: Improving Energy Efficiency, Decreasing Negative Environmental Impact and Reducing Financial Costs for Data Centers" zaprezentowano kompleksową analizę systemu realizującego zapytania do centrum danych na różnym poziomie bezpieczeństwa, a także wskazano zależności pomiędzy zastosowanym poziomem zabezpieczeń a obciążeniem znajdujących się tam systemów, co w sposób bezpośredni wpływa na dostępność realizowanych tam usług. Doktorantka zaproponowała, aby taki model centrum danych analizować biorąc pod uwagę następujące aspekty: czasowy, energetyczny, jakości zabezpieczeń, finansowy czy emisji dwutlenku węgla. W publikacji tej zaprezentowano także architekturę systemu wspomagania decyzji związanych z bezpieczeństwem dla heterogenicznych środowisk teleinformatycznych, w skład których wchodzą inteligentne urządzenia IoT. Zaprojektowany w ten sposób system podejmowania decyzji wspiera wybór najlepszych z dostępnych środków ochrony bezpieczeństwa.

Ostatni rozdział rozprawy, czyli rozdział 3, zawiera podstawowe informacje o Doktorantce dotyczące jej wykształcenia, dotychczasowego zatrudnienia w jednostkach naukowych, doświadczeniu dydaktycznym oraz dorobku naukowym.

3. Najistotniejsze osiągnięcia przedstawione w rozprawie

Oceniając dorobek rozprawy stwierdzam, że mgr Katarzyny Mazur wniosła oryginalny wkład w dziedzinę bezpieczeństwa sieciowego poprzez realizację wieloaspektowej analizy ataków rozproszonej odmowy usługi w środowisku IoT.

W ocenie recenzenta cel główny pracy sformułowany w jej wstępie (podrozdział 1.5) jak również cele pośrednie zostały osiągnięte. Autorka na podstawie aktualnego stanu wiedzy zawartego w literaturze oraz własnych doświadczeń i przemyśleń, w swojej rozprawie

doktorskiej dokonała kompleksowej i wieloaspektowej analizy oraz modelowania rozproszonych ataków odmowy usługi w środowisku Internetu Rzeczy.

Do najistotniejszych osiągnięć ocenianej rozprawy zaliczyć należy:

- Opracowanie efektywnej metodyki służącej do uzyskiwania metryk bezpieczeństwa pozwalających na scharakteryzowanie wpływu środków ochrony na jakość zabezpieczeń urządzeń w środowisku IoT.

- Stworzenie modelu systemu typu *smart grid* służącego do monitorowania linii wysokonapięciowych wraz z analizą możliwych ataków zagrażających dostępności takiego systemu i związanych przede wszystkim z jego procesem przetwarzania.

- Wykonanie wieloaspektowej ewaluacji wolumetrycznych ataków DDoS na bezprzewodowe sieci sensorowe wraz z analizą ich wpływu na funkcjonowanie atakowanej sieci.

- Propozycję systemu wspomagania decyzji umożliwiającego przeprowadzanie kompleksowych analiz w dynamicznych i heterogenicznych środowiskach sieciowych np. IoT.

Każde ze wspomnianych powyżej osiągnięć naukowych Doktorantki przekłada się na jeden z czterech artykułów umieszczonych w rozdziale 2 rozprawy. Ponadto, co warte podkreślenia, wszystkie te prace zostały opublikowane przez Autorkę w czasopismach z tzw. listy filadelfijskiej o wysokim współczynniku *Impact Factor* oraz punktacji przypisanej przez MNiSW (we wszystkich publikacjach Doktorantka występuje jako pierwszy autor, a każdy z artykułów jest napisany przez trzech współautorów):

1. K. Mazur, B. Księżopolski, Z. Kotulski, The robust measurement method for security metrics generation, *The Computer Journal*, Oxford, v. 58 (10), pp. 2280-2296, 2015 [IF = 1, PKT = 25]

2. K. Mazur, M. Wydra, B.Księżopolski, Secure and Time-Aware Communication of Wireless Sensors Monitoring Overhead Transmission Lines, *Sensors* 17, 1610, 2017 [IF = 2.475, PKT = 30]

3. K. Mazur, B. Księżopolski, R. Nielek, Multilevel Modeling of Distributed Denial of Service Attacks in Wireless Sensor Networks, *Journal of Sensors*, Volume 2016, Article ID 5017248, 2016 [IF = 1.704, PKT = 25]

4. K. Mazur, B. Księżopolski, A. Wierzbicki, On Security Management: Improving Energy Efficiency, Decreasing Negative Environmental Impact and Reducing Financial Costs for Data Centers, *Mathematical Problems in Engineering*, v.2015, 418535, pp. 1-19, 2015 [IF = 0.644, PKT = 20]

Zaletą niniejszej rozprawy jest także to, że niektóre z jej osiągnięć zostały wykorzystane przy opracowaniu kolejnych jej elementów. Przykładowo, metodyka generowania metryk (zaproponowana w pozycji 1), jak i proces wieloaspektowej analizy (pozycja 4), znalazły zastosowanie w badaniach nad atakami rozproszonej odmowy usługi w sieciach IoT opisanych w pozycji 3. Zatem zaprezentowane osiągnięcia mimo, że przedstawione w postaci czterech rozdzielnych artykułów naukowych są spójne tematycznie i koncepcyjnie.

4. Uwagi merytoryczne, kwestie dyskusyjne

Rozprawa jako całość nie ma istotnych wad. Niemniej jednak w trakcie jej czytania nasuwają się pewne uwagi o charakterze dyskusyjnym. Należą do nich:

- W rozprawie występuje pewna nieścisłość i brak spójności tłumaczenia terminu DDoS. W tytule i streszczeniu rozprawy tłumaczony jest on jako „rozproszony atak odmowy usługi", natomiast w rozdziale 1 jako „rozproszony atak odmowy dostępu do usługi".

- W podrozdziale 1.2 (str. 4) będącym wprowadzeniem do właściwej treści rozprawy Doktorantka pisze:

  „Celem ataków skierowanych w protokół jest wyczerpanie dostępnych zasobów atakowanego urządzenia i spowodowanie jego awarii poprzez wykorzystanie słabości protokołów warstwy sieciowej i transportowej modelu OSI (...). Najbardziej znanymi atakami skierowanymi na protokół są SYN flood, Ping of Death, Smurf oraz wszelkie ataki wykorzystujące fragmentację pakietów."

  W ocenie recenzenta tego typu sformułowanie nie oddaje w pełni istoty tego typu ataków, gdyż w tym przypadku atakujący wykorzystuje często raczej słabość implementacji/realizacji danego protokołu niż występującą w nim lukę. Przykładowo, w ataku SYN flood tworzonych jest wiele niedokończonych połączeń TCP, które w następstwie mają doprowadzić do wyczerpania pamięci dostępnej na przechowywanie informacji o nich na maszynie ofiary. Problemem w tym przypadku nie jest zatem sam protokół TCP jako taki a jedynie sposób obsługi pamięci przeznaczonej do przechowywania półotwartych połączeń (tzn. brak umiejętnego zwalniania tej pamięci w przypadku długo trwających niedokończonych połączeń).

- Na koniec rozdziału 1 będącego wprowadzeniem do właściwej treści rozprawy Autorka nie zawarła dalszych potencjalnych kierunków badawczych, które mogą być realizowane w przyszłości w oparciu o doświadczenia zebrane przy opracowywaniu niniejszej rozprawy (podrozdział „1.7 Wnioski i podsumowanie" zawiera jedynie syntezę poszczególnych prac i osiągnięć Doktorantki). Oczywiście w ostatnich rozdziałach (podsumowaniach) części z prezentowanych artykułów zawarto ogólne zarysy dalszych problemów i kierunków badawczych, jednak warto by było spojrzeć na to zagadnienie szerzej biorąc pod uwagę całość zagadnień przedstawionych w rozprawie. Brak takiego podsumowania jest o tyle dziwny, że w streszczeniu pracy zawarto zdanie: „Praca doktorska kończy się sformułowaniem konkluzji oraz określeniem dalszych kierunków rozwoju badań opisanych w powyższych publikacjach".

- W artykule „Multilevel Modeling of Distributed Denial of Service Attacks in Wireless Sensor Networks" Autorka wskazuje na zdefiniowanie nowego typu ataku DDoS na sieci WSN o akronimie DDDoS (Delayed DDoS). Warto jednak zauważyć, że taka nazwa nie oddaje w pełni istoty tego ataku. W tym przypadku chodzi przede wszystkim o to, że tego rodzaju działanie atakującego zostanie *wykryte z opóźnieniem*. W związku z tym trafniejszą nazwą w tym przypadku byłoby określenie Detection-delayed DDoS (lub podobne). Ponadto, warto było także jasno zaznaczyć, że taki atak należy do szerokiej rodziny ataków (D)DoS z rodziny „Battery/energy/power-exhaustion" określanym czasem także nazwą „Denial-of-Sleep".

- Dobrym dopełnieniem zaprezentowanych w rozprawie badań byłoby

przeprowadzenie eksperymentów w rzeczywistej sieci WSN i porównanie ich z symulacjami przeprowadzonymi z wykorzystaniem QoP-ML oraz wykonanie analizy porównawczej uzyskanych w ten sposób wyników. Pozwoliło by to na precyzyjne określenie skuteczności i precyzji takiego podejścia do modelowania cyberbezpieczeństwa i cyberzagrożeń.

5. Uwagi redakcyjne i edytorskie

Struktura pracy jest poprawna. Jak wspomniano rozprawa zawiera najpierw wprowadzenie do tematyki pracy oraz charakteryzuje wkład Doktorantki w dziedzinę bezpieczeństwa sieciowego w języku polskim, a następnie w kolejnym rozdziale zawiera tematycznie spójne cztery artykuły naukowe w języku angielskim.

Rozprawa jest dobrze zredagowana i napisana precyzyjnym językiem. Należy jednak zauważyć, że w szczególności w pierwszej części pracy brakuje materiałów ilustracyjnych, które pomogły by pełniej wyjaśnić przedstawiane zagadnienia. Ponadto, cała treść wprowadzenia napisana jest, w zasadzie, tekstem ciągłym to znaczy np. bez podziału na akapity, co nieco utrudnia analizę jego zawartości.

W rozprawie można odnaleźć także niedociągnięcia edytorskie bądź językowe. Przykładowo:

- Str. 1, przy wprowadzeniu terminu DDoS brakuje zarówno przedstawienia definicji tego typu ataków jaki i rozwinięcia użytego pierwszy raz skrótu.
- Str. 1, w zdaniu „(...) obiektów„ które mają możliwość gromadzenia (...)" brak jest znaku zamknięcia cytatu.
- Str. 5, ostatnie zdanie na zakończenie podrozdziału 1.2 tj. „Innym popularnym wykorzystaniem ataku DDoS" jest niepełne.
- Literówki: str. 6, w zdaniu „(...) które znjdowały się (...)" jest literówka; str. 9 w zdaniu „wsórd których badacze"; str. 12, „posłuzyć"; str. 13, „Standrad"; str. 14, „niezależność".
- Str. 17, „W przedstawionej pracy przedstawiono (...)".
- Str. 21, ostatnie zdanie na zakończenie podrozdziału 1.7 tj. „Poniżej zsummaryzowane" jest nieprawidłowe i niepełne.
- Cześć literatury wymienionej w bibliografii na stronach 22-25 jest zacytowana nieprecyzyjnie np. pozycja nr. 11, w pracy ma postać:

  Doddapaneni Chaitanya and Ghosh Arindam. Analysis of denial-of-service attacks on wireless sensor networks using simulation. 2011.

  a poprawna forma to:

  Doddapaneni Chaitanya and Ghosh Arindam, "Analysis of denial-of-service attacks on wireless sensor networks using simulation," in Proceedings of the IT Security for the Next Generation—European Cup, University of Applied Sciences, Erfurt, Germany, January 2011.

Podobne braki dotyczą innych pozycji literaturowych np. [15], [45], [57], [59], itp. Ponadto, pozycje [38] i [39] są dokładnie takie same.

6. Przydatność rozprawy dla nauk technicznych

Przedstawione powyżej uwagi merytoryczne oraz redakcyjne nie mają istotnego wpływu na jakość i wagę przedstawionych rozwiązań i w żadnym stopniu nie obniżają wartości rozprawy. Przedstawione przez Autorkę badane aspekty zostały ujęte wystarczająco szczegółowo i dokładnie.

Praktyczna przydatność rozprawy dla nauk technicznych jest duża. Należy zauważyć, że realizacja przez cyberprzestępców ataków DDoS z wykorzystaniem urządzeń IoT jest relatywnie nowym trendem, a w związku z tym niezbędne jest przeprowadzenie dogłębnej analizy tego rodzaju ataków w takich heterogenicznych i cechujących się dużą dynamiką środowiskach. Odpowiedzią na to zapotrzebowanie jest proponowana przez Doktorantkę wieloaspektowa analiza bezpieczeństwa systemów IoT, która umożliwia scharakteryzowanie nowych aspektów zagrożeń takich jak DDoS w systemach i sieciach z ograniczonymi zasobami (takimi jak np. WSN, IoT, itp.).

7. Podsumowanie.

Biorąc pod uwagę zaprezentowany dorobek naukowy Doktorantki, a w szczególności cztery publikacje o zasięgu międzynarodowym z tzw. listy filadelfijskiej składające się na ocenianą rozprawę uważam recenzowaną pracę za wybitnie dobrą i zasługującą na wyróżnienie.

dr hab. inż. Wojciech Mazurczyk